Segurança da Plataforma Apple

Primavera de 2020

Conteúdo

Introdução à segurança da plataforma Apple

A Apple coloca a segurança no centro de suas plataformas. Aproveitando a experiência obtida com a criação do sistema operacional mais avançado do mundo para dispositivos móveis, a Apple criou arquiteturas de segurança que atendem aos requisitos especiais de dispositivos móveis, relógios, computadores e casas.

Cada dispositivo Apple combina hardware, software e serviços projetados para trabalhar em conjunto e proporcionar o máximo de segurança e uma experiência transparente para o usuário a serviço do objetivo final de manter informações pessoais seguras. O hardware de segurança personalizado fornece recursos de segurança essenciais. As proteções de software trabalham para manter a segurança do sistema operacional e de apps de terceiros. Os serviços fornecem um mecanismo para atualizações de software seguras e oportunas, proporcionam um ecossistema de apps mais seguro, comunicações e pagamentos seguros, além de proporcionarem uma experiência mais segura na internet. Os dispositivos Apple protegem não apenas o dispositivo e seus dados, mas também todo o ecossistema, incluindo tudo o que os usuários fazem localmente, em redes e nos principais serviços da internet.

Assim como projetamos nossos produtos para serem simples, intuitivos e poderosos, os projetamos para serem seguros. Recursos importantes de segurança, como a criptografia do dispositivo com base no hardware, não podem ser desativados por engano. Outros recursos, como o Touch ID e o Face ID, melhoram a experiência do usuário tornando a segurança do dispositivo mais simples e intuitiva. E como muitos desses recursos são ativados por padrão, os usuários ou departamentos de TI não precisam realizar configurações extensas.

Esta documentação fornece detalhes de como a tecnologia e os recursos de segurança são implementados nas plataformas Apple. Ela também ajuda as organizações a combinar a tecnologia e os recursos de segurança da plataforma Apple com as suas próprias políticas e procedimentos para atender às suas necessidades de segurança específicas.

O conteúdo está organizado nos seguintes temas:

- **Segurança de Hardware e Biometria:** o hardware que forma a base da segurança nos dispositivos Apple, incluindo o Secure Enclave, um mecanismo de criptografia AES dedicado, o Touch ID e o Face ID.
- **Segurança do Sistema:** as funções integradas de hardware e software que proporcionam segurança na inicialização, atualização e operação dos sistemas operacionais da Apple.
- **Criptografia e Proteção de Dados:** a arquitetura e o design que protegem os dados do usuário caso o dispositivo seja perdido ou roubado ou se uma pessoa ou processo não autorizado tentar usá-lo ou modificá-lo.

- **Segurança de Apps:** o software e os serviços que fornecem um ecossistema seguro de apps e permitem que os apps sejam executados em segurança e sem comprometer a integridade da plataforma.
- **Segurança de Serviços:** os serviços da Apple para identificação, gerenciamento de senhas, pagamentos, comunicações e busca de dispositivos perdidos.
- **Segurança de Rede:** protocolos de rede padrão do setor que fornecem autenticação e criptografia segura de dados em transmissões.
- **Kits para Desenvolvedores:** frameworks para o gerenciamento seguro e privado da casa e saúde, além da extensão de recursos de serviços e dispositivos Apple para apps de terceiros.
- **Gerenciamento Seguro de Dispositivos:** métodos que permitem o gerenciamento de dispositivos Apple, impedem o uso não autorizado e ativam o apagamento remoto caso o dispositivo seja perdido ou furtado.
- **Certificações de Segurança e Privacidade:** informações sobre certificações ISO, validação criptográfica, certificação Common Criteria e o programa Commercial Solutions for Classified (CSfC).

Um compromisso com a segurança

A Apple está comprometida a ajudar na proteção de clientes usando tecnologias de privacidade e segurança de ponta — criadas para o resguardo de informações pessoais — e métodos abrangentes — para ajudar a proteger dados corporativos em ambientes empresariais. A Apple oferece o Apple Security Bounty, recompensando pesquisadores pelo trabalho realizado na descoberta de vulnerabilidades. Detalhes do programa e categorias de recompensas estão disponíveis em https://developer.apple.com/security-bounty/ (em inglês).

Nós mantemos uma equipe de segurança exclusiva para oferecer suporte a todos os produtos da Apple. A equipe realiza auditorias e testes de segurança dos produtos, tanto os que estão em desenvolvimento quanto os já lançados. A equipe da Apple também fornece ferramentas e treinamento de segurança e monitora ativamente em busca de ameaças e relatórios de novos problemas de segurança. A Apple é membro do Forum of Incident Response and Security Teams (FIRST).

A Apple continua a romper as barreiras do que é possível na segurança e privacidade. Por exemplo, o recurso Buscar usa primitivas criptográficas existentes para permitir a capacidade inovadora de busca distribuída de um Mac off-line — sem expor a ninguém, inclusive à Apple, a identidade ou os dados da localização de qualquer usuário envolvido. Para aprimorar a segurança do firmware do Mac, a Apple fez uso de uma analogia de tabelas de páginas para bloquear o acesso indevido a periféricos, mas em um ponto tão cedo no processo de inicialização que a RAM ainda sequer foi carregada. E conforme invasores continuam aumentando a sofisticação das técnicas de exploração, a Apple está controlando de forma dinâmica os privilégios de execução em memória no iPhone e iPad ao usar instruções personalizadas da CPU — não disponíveis em nenhum outro dispositivo móvel — para impedir o comprometimento. Tão importante quanto a inovação das novas capacidades de segurança, os novos recursos são projetados tendo a privacidade e a segurança como fatores centrais do design.

Para tirar o máximo de proveito dos apurados recursos de segurança integrados a nossas plataformas, as organizações são encorajadas a analisar suas políticas de TI e segurança, visando a fazer o melhor uso possível das camadas de tecnologia de segurança oferecidas por essas plataformas.

Para saber mais sobre como comunicar problemas à Apple e assinar notificações de segurança, consulte Relatar vulnerabilidades de segurança ou privacidade.

A Apple acredita que a privacidade é um direito humano fundamental e oferece diversos controles e opções integradas para permitir que os usuários decidam como e quando apps usam suas informações, além de quais informações são usadas. Para saber mais sobre a abordagem da Apple em relação à privacidade, controles de privacidade em dispositivos Apple e a política de privacidade da Apple, consulte https://www.apple.com/br/privacy**.**

Nota: salvo indicação em contrário, esta documentação cobre as seguintes versões destes sistemas operacionais: iOS 13.4, iPadOS 13.4, macOS 10.15.4, tvOS 13.4 e watchOS 6.2.

Segurança do Hardware e Biometria

Visão geral da segurança do hardware

Um software seguro requer uma base de segurança integrada ao hardware. É por isso que os dispositivos Apple — que executam iOS, iPadOS, macOS, watchOS ou tvOS — possuem recursos de segurança projetados em silício. Entre eles estão funcionalidades personalizadas da CPU que fornecem recursos de segurança do sistema e silício dedicado a funções de segurança. O componente mais importante é o coprocessador Secure Enclave, presente em todos os dispositivos iOS, iPadOS, watchOS e tvOS modernos e todos os computadores Mac que possuem o chip Apple T2 Security. O Secure Enclave fornece a base para a criptografia de dados em repouso, a inicialização segura no macOS e biometria.

Todo iPhone, iPad e computador Mac moderno com um chip T2 possui um mecanismo de hardware AES dedicado que oferece criptografia de alta velocidade à medida que os arquivos são lidos ou gravados. Isso garante que a Proteção de Dados e o FileVault protegem os arquivos dos usuários sem expor chaves de criptografia de longa duração à CPU ou ao sistema operacional. Para obter mais informações sobre qual hardware Apple contém o Secure Enclave, consulte a visão geral do Secure Enclave.

A inicialização segura dos dispositivos Apple garante a não adulteração dos níveis mais baixos do software e assegura que apenas o software confiável do sistema operacional da Apple seja carregado durante a inicialização. Em dispositivos iOS e iPadOS, a segurança começa no código imutável chamado de ROM de Inicialização, que é colocado durante a fabricação do chip e é conhecido como *raiz de confiança do hardware*. Em computadores Mac com um chip T2, a confiança da inicialização segura do macOS começa com o próprio chip T2 (o T2 e o Secure Enclave também executam seus próprios processos de inicialização segura).

O Secure Enclave permite que o Touch ID e o Face ID em dispositivos Apple forneçam autenticação segura e mantenham a privacidade e segurança dos dados biométricos dos usuários. Assim os usuários podem contar com a segurança de códigos e senhas mais longas e complexas e, em muitos casos, com a conveniência de uma autenticação ágil.

Os recursos de segurança dos dispositivos Apple são possibilitados pela combinação de projeto de silício, hardware, software e serviços disponibilizada apenas pela Apple.

Secure Enclave

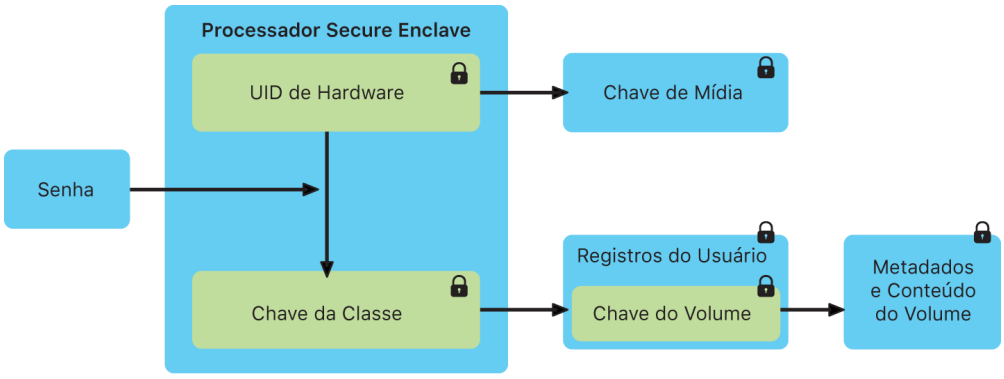
Visão geral do Secure Enclave

O Secure Enclave é um coprocessador seguro que inclui um gerenciador de chaves baseado em hardware, o qual é isolado do processador principal para fornecer uma camada extra de segurança. O Secure Enclave é um recurso de hardware em algumas versões do iPhone, iPad, Mac, Apple TV, Apple Watch e HomePod. São elas:

- iPhone 5s (ou posterior)
- iPad Air (ou posterior)
- Computadores Mac que contêm o chip T1 ou o chip Apple T2 Security
- Apple TV 4ª geração (ou posterior)
- Apple Watch Series 1 (ou posterior)
- HomePod

Os dados das chaves são criptografados no sistema no chip (SoC) do Secure Enclave, que possui um gerador de números aleatórios.

O Secure Enclave também mantém a integridade das operações criptográficas mesmo que o kernel do dispositivo tenha sido comprometido. A comunicação entre o Secure Enclave e o processador de aplicativo é estritamente controlada por meio do isolamento em uma caixa de correio com interrupções e buffers de dados de memória compartilhada.



O processador Secure Enclave.

ROM de Inicialização Dedicada e serviços de antirreprodução

ROM de Inicialização dedicada

O Secure Enclave inclui uma ROM de Inicialização de Secure Enclave dedicada. Similar à ROM de Inicialização do processador de aplicativo, a ROM de Inicialização do Secure Enclave é um código imutável que estabelece a raiz de confiabilidade do hardware para o Secure Enclave. Ela também executa um OS do Secure Enclave baseado em um microkernel personalizado da família L4. O SO de Secure Enclave é assinado pela Apple, verificado pela ROM de Inicialização do Secure Enclave e atualizado por meio de um processo de atualização de software personalizado.

Quando o dispositivo é inicializado, uma chave transitória de proteção de memória é criada pela ROM de Inicialização do Secure Enclave, trançada ao ID exclusivo (UID) do dispositivo e usada para criptografar o espaço de memória dedicado ao Secure Enclave no dispositivo. Exceto no A7 da Apple, a memória do Secure Enclave também é autenticada com a chave de proteção de memória. Nos SoCs A11 (e posteriores) e S4, uma árvore de integridade é usada para impedir a reprodução da memória de segurança crítica do Secure Enclave, autenticada pela chave de proteção de memória e nonces armazenados no chip SRAM integrado.

No iOS e iPadOS, os arquivos são criptografados com uma chave trançada ao UID do Secure Enclave e um nonce antirreprodução conforme são gravados no volume de dados. Nos SoCs A9 (e posteriores), o nonce antirreprodução usa entropia criada pelo gerador de números aleatórios de hardware. O suporte do nonce antirreprodução tem como base um circuito integrado (IC) dedicado de memória não volátil. De forma semelhante, em computadores Mac com o chip Apple T2 Security, a hierarquia de chaves do FileVault é vinculada ao UID do Secure Enclave.

Em dispositivos com SoCs A12 (e posteriores) e S4, o Secure Enclave é emparelhado com um IC de armazenamento seguro para armazenamento do nonce antirreprodução. O IC de armazenamento seguro é criado com um código de ROM imutável, um gerador de números aleatórios, mecanismos de criptografia e detecção de fraude física. Para ler e atualizar os nonces, o Secure Enclave e o IC de armazenamento empregam um protocolo seguro que garante acesso exclusivo a eles.

Serviços de antirreprodução

Os serviços de antirreprodução no Secure Enclave são usados para revogar os dados em eventos que definem limites antirreprodução, incluindo, dentre outros, os seguintes:

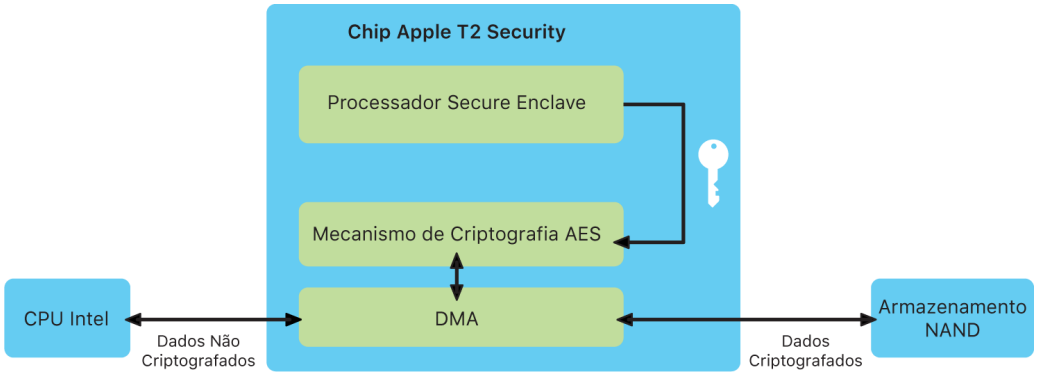
- Alteração do código
- Ativação ou desativação do Touch ID ou Face ID
- Adição ou remoção de uma impressão digital do Touch ID ou rosto do Face ID
- Redefinição do Touch ID ou Face ID
- Adição ou remoção de um cartão do Apple Pay
- Apagar Todo o Conteúdo e Ajustes

Mecanismo AES dedicado

Todos os dispositivos Apple com um Secure Enclave possuem um mecanismo de criptografia dedicado AES-256 integrado ao caminho DMA, entre o armazenamento flash e a memória principal do sistema, tornando a criptografia de arquivos um processo altamente eficiente. Em processadores A9 ou posteriores da série A, o subsistema de armazenamento flash encontra-se em um barramento isolado que só recebe acesso à memória que contém os dados do usuário pelo mecanismo de criptografia DMA.

O Secure Enclave gera de forma segura suas próprias chaves — IDs exclusivos (UIDs), IDs de grupos de dispositivos (GIDs) e outras — e apaga de forma segura as chaves salvas quando necessário. Essas são chaves AES de 256 bits fundidas (UID) ou compiladas (GID) no Secure Enclave durante a fabricação. Nenhum software ou firmware pode lê-las diretamente, somente visualizar os resultados das operações de criptografia ou descriptografia realizadas por mecanismos AES dedicados implementados em silício usando esses UIDs ou GIDs como chave.

O processador de aplicativos e o Secure Enclave possuem, cada um, seus próprios UID e GID, e os UID e GID do Secure Enclave podem ser usados apenas pelo mecanismo AES dedicado ao Secure Enclave. Os UIDs e GIDs não estão disponíveis através do Grupo de Ação de Teste Conjunto (JTAG) nem por outras interfaces de depuração.



O mecanismo de criptografia AES fornece criptografia de alta velocidade no caminho DMA em computadores Mac que possuem o chip Apple T2 Security.

Geração de chaves criptográficas

Cada Secure Enclave gera seu próprio UID (ID exclusivo) durante o processo de fabricação. Já que o UID é exclusivo a cada dispositivo e por ser gerado completamente dentro do Secure Enclave (em vez de em um sistema de fabricação fora do dispositivo), ele não está disponível para acesso ou armazenamento por parte da Apple ou de nenhum de seus fornecedores. Isso se aplica a todos os SoCs posteriores ao processador Apple A8.

O software em execução no Secure Enclave aproveita-se do UID para proteger segredos específicos do dispositivo. O UID permite que os dados sejam criptograficamente atrelados a um dispositivo específico. Por exemplo, a hierarquia de chaves que protege o sistema de arquivos inclui o UID; então, se o armazenamento SSD interno for movido fisicamente de um dispositivo para outro, os arquivos ficam inacessíveis. O UID não está relacionado a nenhum outro identificador do dispositivo. Entre outros segredos protegidos específicos do dispositivo estão os dados do Touch ID ou Face ID. O armazenamento em dispositivos não conectados ao chip Apple T2 Security não recebem esse nível de criptografia. Por exemplo, dispositivos de armazenamento externo conectados via USB ou armazenamentos baseados em PCIe adicionados ao Mac Pro de 2019 não são criptografados pelo chip T2.

No nível do dispositivo está o ID do grupo de dispositivos (GID), que é comum a todos os processadores em uma classe de dispositivos (como todos os dispositivos que usam o processador A8 da Apple, por exemplo).

Com exceção do UID e do GID, todas as outras chaves criptográficas em dispositivos iOS e iPadOS são criadas pelo gerador de números aleatórios (RNG) do sistema e usam um algoritmo baseado em CTR_DRBG. A entropia do sistema é gerada a partir de variações do temporizador durante a inicialização e, adicionalmente, ao interromper o temporizador após a inicialização do dispositivo ser concluída. As chaves geradas no Secure Enclave usam seu próprio gerador de números aleatórios de hardware com base em vários osciladores ring pós-processados com CTR_DRBG.

Apagamento seguro de dados

Apagar as chaves salvas em segurança é tão importante quanto gerá-las. É especialmente desafiador fazer isso em armazenamento flash, onde, por exemplo, o nivelamento por uso pode significar que várias cópias de dados precisam ser apagadas. Para abordar esse problema, os dispositivos com Secure Enclave possuem um recurso dedicado a garantir o apagamento seguro de dados, chamado de Armazenamento Apagável. Esse recurso acessa a tecnologia de armazenamento base (NAND, por exemplo) para endereçar e apagar diretamente um número pequeno de blocos em um nível bem baixo.

Touch ID e Face ID

Visão geral do Touch ID e Face ID

Códigos e senhas são cruciais à segurança de dispositivos Apple, e usuários precisam ser capazes de acessar seus dispositivos rapidamente — até centenas de vezes ao dia. A autenticação biométrica oferece a oportunidade de manter a segurança de um código forte — ou até de aumentar a robustez do código ou senha, já que o mesmo não precisa ser digitado manualmente — ao mesmo tempo em que oferece a conveniência de pressionar ou olhar para o dispositivo para desbloqueá-lo rapidamente. O Touch ID e o Face ID não substituem a senha ou o código, mas aceleram e simplificam o acesso na maioria das situações.

Segurança do Touch ID

O Touch ID é o sistema de detecção de impressão digital que acelera e facilita o acesso a dispositivos Apple compatíveis. Essa tecnologia lê dados de impressões digitais de qualquer ângulo e, com o passar do tempo, aprende mais informações sobre a impressão digital de um usuário, pois o sensor continua a expandir o mapa de impressão digital conforme nós de sobreposição adicionais são identificados a cada uso.

Os dispositivos Apple que possuem um sensor Touch ID podem ser desbloqueados usando uma impressão digital. O Touch ID não substitui a necessidade de um código do dispositivo ou uma senha de usuário, que ainda são necessários após a inicialização ou reinicialização do dispositivo, ou encerramento de sessão (no Mac). Em alguns apps, o Touch ID também pode ser usado no lugar do código do dispositivo ou da senha do usuário — por exemplo, para desbloquear notas protegidas por senha no app Notas, sites protegidos pelas chaves e senhas de apps compatíveis. No entanto, o código do dispositivo ou a senha de usuário são sempre exigidos em alguns cenários. Por exemplo, para alterar o código do dispositivo ou a senha de usuário existente ou para remover impressões digitais cadastradas ou criar novas.

Quando o sensor de impressão digital detecta o toque de um dedo, ele aciona a matriz avançada de leitura para escanear o dedo e envia a digitalização para o Secure Enclave. A comunicação entre o processador e o sensor do Touch ID ocorre através de um barramento de interface periférico serial. O processador encaminha os dados para o Secure Enclave, mas é incapaz de lê-los. Eles são criptografados e autenticados com uma chave de sessão negociada usando uma chave compartilhada fornecida para cada sensor do Touch ID e seu respectivo Secure Enclave na fábrica. A chave compartilhada é forte, aleatória e diferente para cada sensor do Touch ID. A troca de chaves da sessão usa a embalagem de chaves AES com ambos os lados fornecendo uma chave aleatória que estabelece a chave da sessão e usa a criptografia de transporte AES-CCM.

Enquanto é vetorizado para análise, o escaneamento de varredura é armazenado temporariamente em uma memória criptografada dentro do Secure Enclave, sendo descartado depois. A análise utiliza mapeamento de ângulo dos fluxos subdérmicos, um processo com perda que descarta dados de minúcias que seriam necessários para reconstruir a impressão digital real do usuário. O mapa de nós resultante é armazenado em formato criptografado e sem nenhuma informação de identificação, podendo ser lido apenas pelo Secure Enclave. Os dados nunca saem do dispositivo. Eles não são enviados à Apple nem incluídos nos backups do dispositivo.

Segurança do Face ID

Com um simples olhar, o Face ID desbloqueia dispositivos Apple compatíveis. Ele fornece uma autenticação intuitiva e segura através do sistema de câmera TrueDepth, que usa tecnologias avançadas para mapear com precisão a geometria do rosto do usuário. O Face ID usa redes neurais para determinar atenção, correspondência e anti-spoofing, de modo que o usuário possa desbloquear seu telefone com um olhar. O Face ID se adapta automaticamente às mudanças na aparência e resguarda cuidadosamente a privacidade e segurança dos dados biométricos do usuário.

O Face ID é projetado para confirmar a atenção do usuário, fornecer autenticação robusta com uma proporção baixa de identificação falsa e mitigar enganos digitais e físicos.

A câmera TrueDepth busca o rosto do usuário automaticamente quando ele desperta dispositivos Apple que têm Face ID (ao elevá-los ou tocar na tela), assim como quando tais dispositivos tentam autenticar o usuário a fim de mostrar uma notificação recebida ou quando um app compatível exige autenticação pelo Face ID. Quando um rosto é detectado, o Face ID detecta se os olhos do usuário estão abertos e sua atenção está direcionada para o dispositivo para confirmar a intenção de desbloqueio; na acessibilidade, isso é desativado quando o VoiceOver está ativado e, se necessário, pode ser desativado separadamente.

Depois de confirmar a presença de um rosto atento, a câmera TrueDepth projeta e lê mais de 30.000 pontos infravermelhos de um mapa de profundidade do rosto, além de uma imagem infravermelha em 2D. Esses dados são usados para criar uma sequência de imagens 2D e mapas de profundidade, que são assinados digitalmente e enviados para o Secure Enclave. Para combater enganos digitais e físicos, a câmera TrueDepth aleatoriza a sequência de capturas de imagens 2D e mapas de profundidade e projeta um padrão aleatório específico do dispositivo. Uma parte do mecanismo neural dos SoCs (protegida dentro do Secure Enclave) transforma esses dados em uma representação matemática e a compara com os dados faciais registrados. Esses dados faciais registrados são, na verdade, uma representação matemática do rosto capturado em diversas poses.

Touch ID, Face ID, códigos e senhas

Para usar o Touch ID ou o Face ID, os usuários devem configurar o dispositivo para que um código ou uma senha sejam exigidos para desbloqueá-lo. Quando o Touch ID ou o Face ID fazem uma identificação bem-sucedida, o dispositivo do usuário é desbloqueado sem solicitar o código ou a senha. Isso faz com que o uso de um código ou uma senha mais longa e complexa seja mais prático, já que os usuários não precisam digitá-los com tanta frequência. O Touch ID e o Face ID não substituem o código ou a senha do usuário, mas oferecem acesso fácil ao dispositivo dentro de limites e restrições de tempo cuidadosamente considerados. Isso é importante porque um código ou uma senha forte formam a base de como os dispositivos iOS, iPadOS, macOS ou watchOS protegem criptograficamente os dados do usuário.

Quando um código ou senha do dispositivo são exigidos

Usuários podem usar um código ou senha a qualquer momento em vez do Touch ID ou Face ID, mas há alguns casos onde a biometria não é permitida. As seguintes operações relacionadas à segurança sempre exigem a inserção de um código ou senha:

- Atualização do software
- Apagamento do dispositivo
- Visualização ou alteração dos ajustes de código
- Instalação de perfis de configuração
- Desbloqueio do painel das preferências Segurança e Privacidade nas Preferências do Sistema do Mac
- Desbloqueio do painel das preferências Usuários e Grupos nas Preferências do Sistema do Mac (se o FileVault estiver ativado)

Também é necessário um código ou senha se o dispositivo estiver nos estados seguintes:

- O dispositivo acabou de ser ligado ou reiniciado.
- O usuário encerrou a sessão no Mac (ou não iniciou uma sessão ainda).
- O usuário não desbloqueou o dispositivo nas últimas 48 horas.
- O usuário não usou o código ou senha para desbloquear o dispositivo nas últimas 156 horas (seis dias e meio) e o usuário não usou uma biometria para desbloquear o dispositivo nas últimas 4 horas.
- O dispositivo recebeu um comando de bloqueio remoto.
- Após manter pressionado qualquer botão de volume e o botão Repousar/Despertar simultaneamente por 2 segundos e pressionar Cancelar para sair do desligamento/SOS de Emergência.
- Após cinco tentativas malsucedidas de identificação biométrica (embora, por motivos de usabilidade, o dispositivo possa oferecer a possibilidade de digitação do código ou senha em vez do uso de biometria após um número menor de falhas).

Quando o Touch ID ou o Face ID estão ativados no iPhone ou iPad, o dispositivo é bloqueado imediatamente quando o botão Repousar/Despertar é pressionado e sempre que entra em repouso. O Touch ID e o Face ID exigem uma identificação bem-sucedida — ou, opcionalmente, o código — sempre que o dispositivo sai do repouso.

A probabilidade de que uma pessoa aleatória entre a população possa desbloquear o iPhone, iPad ou Mac de um usuário é de 1 em 50.000 com o Touch ID ou 1 em 1.000.000 com o Face ID. Essa probabilidade aumenta quando há várias impressões digitais registradas (até 1 em 10.000 com cinco impressões digitais) ou visuais (até 1 em 500.000 com dois registros visuais). Para ter mais proteção, o Touch ID e o Face ID permitem apenas cinco tentativas malsucedidas de identificação antes que um código ou senha sejam exigidos para obter acesso ao dispositivo ou conta do usuário. Com o Face ID, a probabilidade de uma identificação incorreta é diferente para gêmeos e irmãos que se pareçam com o usuário e para crianças menores de 13 anos, já que seus traços faciais pessoais podem não ter se desenvolvido completamente. Caso isso seja um motivo de preocupação, a Apple recomenda o uso de um código para autenticação.

Identificação facial

A identificação facial é realizada dentro do Secure Enclave e usa redes neurais treinadas especificamente para esse propósito. Ao desenvolver as redes neurais de identificação facial, a Apple usou mais de um bilhão de imagens, incluindo imagens infravermelhas e de profundidade coletadas em estudos realizados com o consentimento informado dos participantes. Em seguida a Apple trabalhou com participantes do mundo todo para incluir um grupo expressivo de pessoas levando-se em conta gênero, idade, etnia e outros fatores. Os estudos foram ampliados conforme o necessário para fornecer um alto grau de precisão para uma ampla gama de usuários. O Face ID foi projetado para funcionar com chapéus, cachecóis, óculos, lentes de contato e muitos óculos escuros. Além disso, ele foi projetado para funcionar em ambientes fechados, ambientes abertos e até na escuridão total. Uma rede neural adicional treinada para identificar e resistir a enganos defende o dispositivo de tentativas de desbloqueio com fotos ou máscaras. Os dados do Face ID, incluindo as representações matemáticas do rosto do usuário, são criptografados e disponibilizados somente para o Secure Enclave. Os dados nunca saem do dispositivo. Eles não são enviados à Apple nem incluídos nos backups do dispositivo. Os seguintes dados do Face ID são salvos, criptografados somente para uso pelo Secure Enclave, durante a operação normal:

- As representações matemáticas do rosto do usuário, calculadas durante o registro
- As representações matemáticas do rosto do usuário, calculadas durante algumas tentativas de desbloqueio caso o Face ID as julgue necessárias para melhorar a identificação futura

As imagens de rosto capturadas durante a operação normal não são salvas, e sim imediatamente descartadas depois da representação matemática ser calculada — tanto para o registro inicial quanto para a comparação com os dados do Face ID registrados.

Aprimoramento da identificação do Face ID

Para aprimorar o desempenho da identificação e acompanhar as mudanças naturais de um rosto e da aparência, o Face ID amplia sua representação matemática com o passar do tempo. A partir da identificação bem-sucedida, o Face ID pode usar a nova representação matemática calculada (se sua qualidade for suficiente) para um número finito de identificações adicionais antes de descartar esses dados. Reciprocamente, se o Face ID não conseguir reconhecer um rosto, mas a qualidade da identificação for superior a um certo limite e o usuário digitar o código imediatamente após o não reconhecimento, o Face ID faz uma outra captura e amplia os dados do Face ID registrados com a nova representação matemática calculada. Esses novos dados do Face ID são descartados se o usuário não for mais identificado por eles e após um número finito de identificações. Esse processo de ampliação permite que o Face ID acompanhe mudanças dramáticas em pelos faciais ou no uso de maquiagem por parte de um usuário, ao mesmo tempo em que minimiza a aceitação falsa.

Desbloqueio de um dispositivo ou conta de usuário

Com o Touch ID ou o Face ID desativados, ao bloquear um dispositivo ou conta, as chaves das classes mais altas da Proteção de Dados (mantidas no Secure Enclave) são descartadas. Os arquivos e os itens das Chaves dessa classe ficam inacessíveis até que o usuário digite o código ou a senha para desbloquear o dispositivo ou a conta.

Com o Touch ID ou o Face ID ativados, as chaves não são descartadas quando o dispositivo ou a conta são bloqueados. Ao invés disso, elas são embaladas com uma chave fornecida ao subsistema do Touch ID ou Face ID dentro do Secure Enclave. Quando um usuário tenta desbloquear o dispositivo ou a conta, caso o dispositivo detecte uma identificação bem-sucedida, ele fornece a chave para desembalar as chaves de Proteção de Dados, desbloqueando o dispositivo ou a conta. Esse processo fornece proteção adicional ao exigir a cooperação entre a Proteção de Dados e os subsistemas do Touch ID ou Face ID para desbloquear o dispositivo.

Quando o dispositivo é reinicializado, as chaves exigidas pelo Touch ID ou Face ID para desbloquear o dispositivo ou a conta são perdidas. Elas são descartadas pelo Secure Enclave caso qualquer condição que exija a digitação do código ou senha seja atendida.

Proteção de compras com o Apple Pay

O usuário também pode usar o Touch ID e o Face ID com o Apple Pay para fazer pagamentos em lojas, apps e na web de maneira fácil e segura.

Para autorizar um pagamento em uma loja com o Face ID, primeiro o usuário precisa pressionar o botão lateral duas vezes para confirmar a intenção de fazer o pagamento. Isso captura a intenção do usuário com um gesto físico diretamente relacionado ao Secure Enclave, o que é invulnerável à falsificação por parte de um processo malicioso. Depois, o usuário usa o Face ID para autenticar antes de aproximar o dispositivo do leitor de pagamento por proximidade. Um método de pagamento diferente do Apple Pay pode ser selecionado após a autenticação com o Face ID, o que requer uma nova autenticação, mas o usuário não precisará pressionar novamente o botão lateral duas vezes.

Para fazer um pagamento dentro de apps ou na web, o usuário precisa pressionar o botão lateral duas vezes para confirmar a intenção de pagar e autenticar com o Face ID para autorizar o pagamento. Se a transação do Apple Pay não for concluída em 60 segundos depois do botão lateral ter sido pressionado duas vezes, o usuário deve fazer isso novamente para reconfirmar a intenção de pagar.

No caso do Touch ID, a intenção de pagar é confirmada com o gesto de ativação do sensor do Touch ID combinado à identificação bem-sucedida da impressão digital do usuário.

Outros usos para o Touch ID e o Face ID

Apps de terceiros podem usar as APIs fornecidas pelo sistema para solicitar que o usuário use o Touch ID, o Face ID, um código ou uma senha para autenticar. Os apps que oferecem suporte ao Touch ID são automaticamente compatíveis com o Face ID sem que nenhuma alteração seja necessária. Ao usar o Touch ID ou o Face ID, o app recebe uma notificação apenas quanto ao êxito da autenticação; ele não pode acessar o Touch ID, o Face ID ou os dados associados ao usuário registrado.

Proteção de itens das Chaves

Os itens das Chaves também podem ser protegidos pelo Touch ID ou Face ID, sendo liberados pelo Secure Enclave apenas pela identificação bem-sucedida ou pelo código do dispositivo ou senha da conta. Os desenvolvedores de apps possuem APIs para verificar se um código ou uma senha foram definidos pelo usuário antes de exigir o Touch ID, o Face ID, um código ou uma senha para desbloquear itens das Chaves. Os desenvolvedores de apps podem fazer o seguinte:

- Exigir que as operações de autenticação da API não usem a senha de um app ou o código do dispositivo como alternativa. Eles podem consultar se um usuário está registrado, permitindo que o Touch ID ou o Face ID sejam usados como um segundo fator em apps que requerem segurança.
- Gerar e usar chaves ECC dentro do Secure Enclave que podem ser protegidas pelo Touch ID ou Face ID. As operações com essas chaves são realizadas sempre dentro do Secure Enclave depois que ele autoriza o uso.

Realização e aprovação de compras

Os usuários também podem configurar o Touch ID ou o Face ID para aprovar compras na iTunes Store, App Store, Apple Books e outros locais, para que não precisem digitar a senha do ID Apple. No iOS 11 ou posterior ou no macOS 10.12.5 ou posterior, as chaves ECC do Secure Enclave protegidas pelo Touch ID e Face ID são usadas para autorizar uma compra por meio da assinatura do pedido da loja.

Desconexão do microfone por hardware no Mac e iPad

Todos os notebooks Mac que possuem o chip Apple T2 Security possuem uma desconexão por hardware que assegura que o microfone seja desativado sempre que a tampa é fechada. No MacBook Pro de 13 polegadas, e computadores MacBook Air com o chip T2 e MacBook Pro de 15 polegadas de 2019 ou posterior, essa desconexão é implementada apenas no hardware. A desconexão impede que qualquer software — mesmo com privilégios de usuário root ou de kernel no macOS, e até mesmo o software no chip T2 — acione o microfone enquanto a tela estiver fechada (a câmera não é desconectada no hardware porque seu campo de visão fica totalmente obstruído com a tela fechada).

Os modelos de iPad a partir de 2020 também apresentam a desconexão do microfone por hardware. Quando uma capa em conformidade com MFi (incluindo aquelas vendidas pela Apple) é conectada ao iPad e fechada, o microfone é desconectado no hardware, impedindo que dados de áudio do microfone sejam disponibilizados para qualquer software — mesmo com privilégios root ou kernel no iPadOS, ou no caso do firmware estar comprometido.

Cartões Expressos com reserva de energia no iPhone

Se o iOS não estiver sendo executado porque o iPhone precisa ser carregado, talvez ainda haja energia suficiente na bateria para permitir transações de Cartões Expressos. Dispositivos iPhone compatíveis com este recurso aceitam:

- Um cartão de transporte público designado como o cartão Express Card;
- Cartões de ID de estudante com o modo Express Card ativado.

Ao pressionar o botão lateral, o ícone de bateria fraca aparece, bem como o texto indicando que há Cartões Expressos disponíveis para uso. O controlador NFC realiza transações com Express Cards sob as mesmas condições de quando o iOS é executado, exceto pelo fato de as transações serem indicadas somente por uma notificação tátil. Não aparece nenhuma notificação visível.

Esse recurso não fica disponível quando um desligamento é iniciado por um usuário padrão.

Segurança do Sistema

Visão geral da segurança do sistema

Aproveitando os recursos exclusivos do hardware da Apple, a segurança do sistema foi projetada para maximizar a segurança dos sistemas operacionais dos dispositivos Apple sem comprometer a usabilidade. A segurança do sistema abrange o processo de inicialização, as atualizações de software e a operação do SO.

A inicialização segura começa no hardware e constrói uma cadeia de confiança por meio do software, em que cada etapa garante que a seguinte está funcionando corretamente antes de ceder o controle. Este modelo de segurança funciona não apenas na inicialização padrão dos dispositivos Apple, mas também nos diversos modos de recuperação e atualização dos dispositivos iOS, iPadOS e macOS.

As versões mais recentes do iOS, iPadOS ou macOS são as mais seguras. O mecanismo de atualização de software não fornece apenas atualizações pontuais a dispositivos Apple, como também disponibiliza apenas softwares validados pela Apple. O sistema de atualização pode inclusive evitar ataques a versões antigas, de modo que os dispositivos não podem voltar a uma versão mais antiga do sistema operacional (que um invasor sabe atacar) como método de roubo dos dados do usuário.

Por último, os dispositivos Apple possuem proteções de inicialização e tempo de execução para que mantenham a integridade durante a operação. Essas proteções variam significativamente entre os dispositivos iOS, iPadOS e macOS de acordo com os diferentes conjuntos de recursos de cada um e os ataques que eles devem, portanto, impedir.

Geração de números aleatórios

Os geradores criptográficos de números pseudoaleatórios (CPRNGs) são um elemento básico importante de um software seguro. Para esse fim, a Apple fornece um software de CPRNG confiável em execução nos kernels do iOS, iPadOS, macOS, tvOS e watchOS. Ele é responsável por agregar a entropia bruta do sistema e fornecer números aleatórios seguros para clientes tanto no kernel quanto no espaço do usuário.

Fontes de entropia

O CPRNG do kernel é alimentado por várias fontes de entropia durante a inicialização e ao longo da vida do dispositivo. Algumas delas são (de acordo com a disponibilidade):

- O RNG de hardware do Secure Enclave
- Oscilações com base no tempo coletadas durante a inicialização

- Entropia coletada em interrupções de hardware
- Um arquivo inicial usado para persistência da entropia entre inicializações
- Instruções aleatórias da Intel, como RDSEED e RDRAND (apenas para macOS)

O CPRNG do Kernel

O CPRNG do kernel possui um projeto derivado do Fortuna e tem como objetivo um nível de segurança de 256 bits. Ele fornece números aleatórios de alta qualidade para clientes no espaço do usuário através das seguintes APIs:

- A chamada de sistema `getentropy`(2)
- O dispositivo aleatório, ou seja, /dev/random

O CPRNG do kernel aceita a entropia fornecida pelo usuário através de gravações no dispositivo aleatório.

Inicialização segura

A cadeia de inicialização segura do iOS e iPadOS

Cada etapa do processo de inicialização contém componentes assinados criptograficamente pela Apple para garantir a integridade e prosseguir somente após a verificação da cadeia de confiança. Isso inclui gerenciadores de inicialização, kernel, extensões do kernel e firmware de banda base. Essa cadeia de inicialização segura ajuda a garantir a não adulteração dos níveis mais baixos do software.

Quando um dispositivo iOS ou iPadOS é ligado, o processador de aplicativos executa imediatamente o código da memória somente leitura, chamada de ROM de Inicialização. Esse código imutável, conhecido como raiz de confiança do hardware, é colocado durante a fabricação do chip e é implicitamente confiável. O código da ROM de Inicialização contém a chave pública da AC de Raiz da Apple, usada para verificar se o gerenciador de inicialização iBoot está assinado pela Apple antes de permitir que ele seja carregado. Esse é o primeiro passo na cadeia de confiança, na qual cada passo garante que o próximo seja assinado pela Apple. Ao terminar suas tarefas, o iBoot verifica e executa o kernel do iOS ou iPadOS. Em dispositivos com processador A9 ou anterior da série A, um estágio adicional do Gerenciador de Inicialização de Baixo Nível (LLB) é carregado e verificado pela ROM de Inicialização, que por sua vez, carrega e verifica o iBoot.

Problemas de carregamento ou verificação dos estágios seguintes são tratados de modo diferente conforme o hardware:

- *O ROM de Inicialização não consegue carregar LLB (dispositivos mais antigos):* modo de Atualização do Firmware do Dispositivo (DFU)
- *LLB ou iBoot:* modo de Recuperação

Nos dois casos, o dispositivo deve estar conectado ao iTunes (no macOS 10.14 ou anterior) ou ao Finder (macOS 10.15 ou posterior) por meio de USB e ser restaurado para os ajustes padrão de fábrica.

O Registro de Progresso de Inicialização (BPR) é usado pelo Secure Enclave para limitar o acesso a dados de usuário em diversos modos e é atualizado antes de entrar nos modos a seguir:

- *Modo DFU:* definido pela ROM de Inicialização em dispositivos com o Apple A12 ou SoCs mais recentes
- *Modo de recuperação:* definido pelo iBoot em dispositivos com o Apple A10, S2 ou SoCs mais recentes

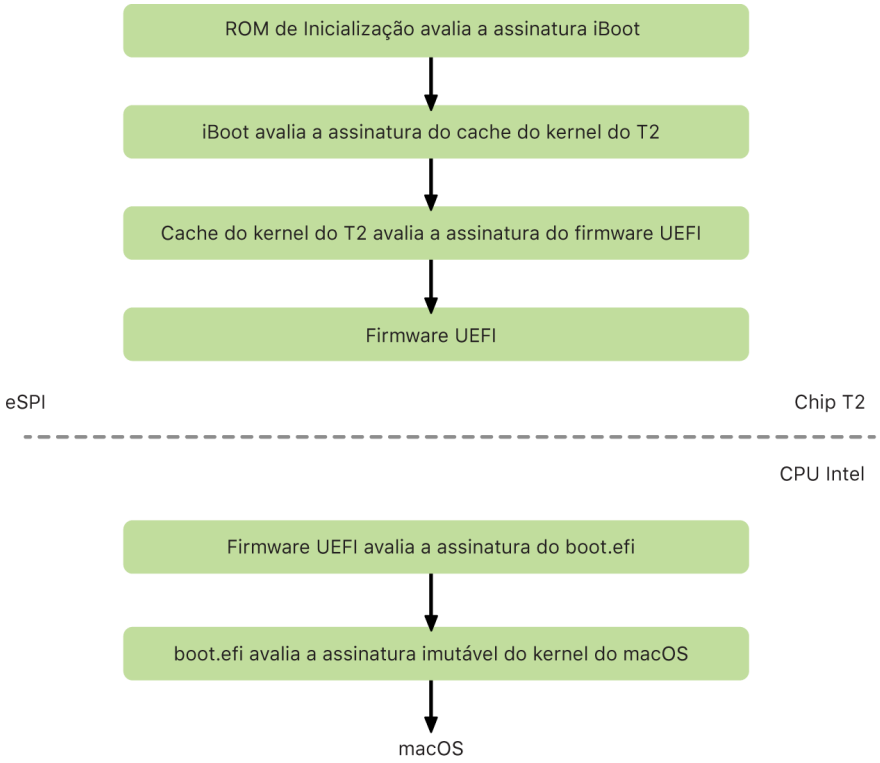
Em dispositivos com acesso "cellular", o subsistema de banda base também utiliza o seu próprio processo similar de inicialização segura com o software assinado e chaves verificadas pelo processador de banda base.

O coprocessador do Secure Enclave também utiliza um processo de inicialização segura que garante que o seu software separado esteja verificado e assinado pela Apple.

Modos de inicialização do macOS

Processo de inicialização dos computadores Mac

Quando um computador Mac com o chip Apple T2 Security é ligado, o chip executa o código da memória somente leitura, conhecida como ROM de Inicialização. Esse código imutável, chamado de *raiz de confiança do hardware*, é colocado durante a fabricação do chip, auditado em busca de vulnerabilidades e é implicitamente confiável. O código da ROM de Inicialização contém a chave pública da AC de Raiz da Apple, usada para verificar se o gerenciador de inicialização iBoot está assinado pela chave privada da Apple antes de permitir que ele seja carregado. Esse é o primeiro passo na cadeia de confiança. O iBoot verifica o kernel e o código de extensão do kernel do chip T2 que, em seguida, verifica o firmware da Intel UEFI. O firmware da UEFI e a assinatura associada ficam disponíveis de início apenas para o chip T2.



Cadeia de inicialização segura do macOS.

Após a verificação, a imagem do firmware da UEFI é mapeada em uma parte da memória do chip T2. Essa memória é disponibilizada para a CPU Intel através da Interface Periférica Serial aprimorada (eSPI). Na primeira inicialização da CPU Intel, ela obtém o firmware da UEFI através da eSPI na cópia mapeada em memória do firmware, localizada no chip T2, cuja integridade foi verificada.

A avaliação da cadeia de confiança continua na CPU Intel, com a avaliação da assinatura do boot.efi (o gerenciador de inicialização do macOS) por parte do firmware da UEFI. As assinaturas da inicialização segura do macOS, residentes no processador Intel, são armazenadas no mesmo formato Image4 usado na inicialização segura do iOS, iPadOS e chip T2. Além disso, o código que analisa os arquivos Image4 é o mesmo código reforçado da implementação atual da inicialização segura do iOS e iPadOS. Em seguida, o boot.efi verifica a assinatura de um novo arquivo, chamado immutablekernel. Quando a inicialização segura está ativada, o arquivo immutablekernel representa o conjunto completo das extensões do kernel da Apple necessárias para inicializar o macOS. A política de inicialização segura é encerrada na passagem para o immutablekernel. Depois disso, as políticas de segurança do macOS (como a Proteção da Integridade do Sistema e as extensões do kernel assinadas) entram em vigor.

Caso haja qualquer erro ou falha nesse processo, o Mac entre no modo Recuperação do macOS, modo Recuperação do chip Apple T2 Security ou modo DFU do chip Apple T2 Security.

Visão geral dos modos de inicialização dos computadores Mac

Os computadores Mac possuem uma variedade de modos de inicialização que o usuário pode ativar no momento da inicialização ao pressionar combinações de teclas, que são reconhecidas pelo firmware da UEFI ou inicializador. Alguns modos de inicialização, como o Modo de Usuário Único, não funcionarão exceto se a política de segurança for alterada para Sem Segurança no Utilitário de Segurança da Inicialização.

Modo	Combinação de teclas	Descrição
Inicialização do macOS	Nenhuma	O firmware da UEFI passa o controle para o inicializador do macOS (um aplicativo da UEFI), que o passa para o kernel do macOS. Na inicialização padrão do Mac com o FileVault ativado, o inicializador do macOS é o código que apresenta a interface da Janela de Início de Sessão a fim de obter a senha para descriptografar o armazenamento.
Gerenciador de Inicialização	Opção (⌥)	O firmware da UEFI inicia o aplicativo UEFI integrado que apresenta a interface de seleção do dispositivo de inicialização ao usuário.

Modo	Combinação de teclas	Descrição
Modo de Disco de Destino (TDM)	T	O firmware da UEFI inicia o aplicativo UEFI integrado que expõe o dispositivo de armazenamento interno como um dispositivo de armazenamento bruto baseado em blocos via FireWire, Thunderbolt, USB ou qualquer combinação dos três (de acordo com o modelo do Mac).
Modo de Usuário Único	Comando (⌘) + S	O kernel do macOS passa a opção `-s` no vetor de argumentos do launchd, que cria a interface de linha de comando de usuário único no tty do app Console. *Nota:* se o usuário sair da interface de linha de comando, o macOS continua a inicialização até a janela de início de sessão.
RecoveryOS	Comando (⌘) + R	O firmware da UEFI carrega um macOS mínimo a partir de uma imagem de disco (.dmg) assinada no dispositivo de armazenamento interno.
RecoveryOS via Internet	Opção (⌥) + Comando (⌘) + R	A imagem de disco assinada é baixada da internet via HTTP.
Diagnóstico	D	O firmware da UEFI carrega um ambiente de diagnóstico UEFI mínimo a partir de uma imagem de disco assinada no dispositivo de armazenamento interno.
Diagnóstico via Internet	Opção (⌥) + D	A imagem de disco assinada é baixada da internet via HTTP.
NetBoot (Para computadores Mac sem o chip Apple T2 Security)	N	O firmware da UEFI baixa o inicializador do macOS de um servidor TFTP local, o inicializador baixa o kernel do macOS do mesmo servidor TFTP e o kernel do macOS monta um sistema de arquivos a partir de um compartilhamento de rede por NFS ou HTTP.
Inicialização no Windows	Nenhuma	Se o Windows tiver sido instalado usando o BootCamp, o firmware da UEFI passa o controle para o inicializador do Windows, que o passa para o kernel do Windows.

recoveryOS e ambientes de diagnóstico nos computadores Mac

O recoveryOS é totalmente separado do macOS principal e todo o seu conteúdo é armazenado em um arquivo de imagem de disco chamado BaseSystem.dmg. Também há um BaseSystem.chunklist associado, que é usado para verificar a integridade do BaseSystem.dmg. O chunklist é uma série de hashes de pedaços de 10 MB do BaseSystem.dmg. O firmware da UEFI avalia a assinatura do arquivo chunklist e depois avalia o hash de um pedaço do BaseSystem.dmg de cada vez para garantir que ele corresponda ao conteúdo assinado presente no chunklist. Se algum desses hashes não corresponder, a inicialização do SO de recuperação local é abortada e o firmware da UEFI tenta inicializar a partir da Recuperação pela Internet.

Se a verificação for concluída com sucesso, o firmware da UEFI monta o BaseSystem.dmg como um ramdisk e inicia o boot.efi nele contido. Não há necessidade do firmware da UEFI realizar uma verificação específica do boot.efi, nem do boot.efi realizar uma verificação do kernel, pois o conteúdo completo do SO (do qual esses elementos são apenas um subconjunto) já teve sua integridade verificada.

O procedimento para inicializar o ambiente de diagnóstico local é basicamente o mesmo do que o para iniciar o recoveryOS. São usados arquivos AppleDiagnostics.dmg e AppleDiagnostics.chunklist separados, mas eles são verificados da mesma forma que os arquivos BaseSystem. Em vez de iniciar o boot.efi, o firmware da UEFI inicia um arquivo dentro do dmg chamado diags.efi, que por sua vez é responsável por chamar vários outros drivers UEFI que podem interagir e verificar erros no hardware.

recoveryOS via Internet e ambientes de diagnóstico nos computadores Mac

Se tiver ocorrido um erro ao iniciar a recuperação local ou os ambientes de diagnóstico, o firmware da UEFI tenta baixar as imagens da internet. Além disso, o usuário pode solicitar que as imagens sejam obtidas da internet ao manter sequências especiais de teclas pressionadas durante a inicialização. A validação da integridade das imagens de disco e chunklists baixados do Servidor de Recuperação do SO é realizada da mesma forma que com as imagens obtidas no dispositivo de armazenamento.

Embora a conexão ao Servidor de Recuperação do SO seja feita usando HTTP, o conteúdo completo baixado ainda tem sua integridade verificada da forma descrita anteriormente, não sendo, portanto, vulnerável à manipulação por um invasor que tenha controle da rede. Caso a verificação de integridade de um pedaço individual seja malsucedida, ele é solicitado novamente 11 vezes ao Servidor de Recuperação do SO antes que as tentativas sejam interrompidas e um erro seja exibido.

Inicialização no Microsoft Windows em computadores Mac

Por padrão,os computadores Mac que oferecem suporte à inicialização segura confiam apenas no conteúdo assinado pela Apple. Contudo, para melhorar a segurança das instalações do Boot Camp, a Apple também oferece suporte à inicialização segura do Windows. O firmware da UEFI possui uma cópia do certificado Microsoft Windows Production CA 2011 usado para autenticar os carregadores de inicialização da Microsoft.

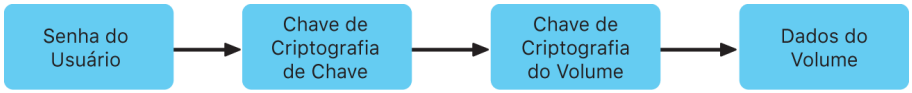
Nota: atualmente não é fornecida confiança para o Microsoft Corporation UEFI CA 2011, o que permitiria a verificação de código assinado pelos parceiros da Microsoft. Esta AC da UEFI é comumente usada para verificar a autenticidade dos carregadores de inicialização de outros sistemas operacionais, como variantes de Linux.

O suporte à inicialização segura do Windows não é ativado por padrão. Ele deve ser ativado com o Assistente do Boot Camp (BCA). Quando o usuário executa o BCA, o macOS é reconfigurado para confiar no código assinado pela Microsoft durante a inicialização. Após o término do BCA, se o macOS não tiver êxito na avaliação de confiança da Apple durante a inicialização segura, o firmware da UEFI tenta avaliar a confiança do objeto de acordo com a formatação da Inicialização Segura da UEFI. Se a avaliação de confiança for bem-sucedida, o Mac dá prosseguimento à inicialização do Windows. Caso contrário, o Mac entra na Recuperação do macOS e informa o usuário sobre a falha na avaliação de confiança.

Processo de inicialização de computadores Mac sem o chip Apple T2 Security

Os computadores Mac que não possuem o chip Apple T2 Security não oferecem inicialização segura. Dessa forma, o firmware da UEFI carrega o inicializador do macOS (boot.efi) do sistema de arquivos sem verificação e o inicializador carrega o kernel (prelinkedkernel) do sistema de arquivos sem verificação. Para proteger a integridade da cadeia de inicialização, os usuários devem ativar todos os mecanismos de segurança a seguir:

- *Proteção da Integridade do Sistema:* ativada por padrão, ela protege o inicializador e o kernel contra gravações maliciosas de dentro de um macOS em execução.
- *FileVault:* pode ser ativado de duas formas: pelo usuário ou por um administrador de gerenciamento de dispositivos móveis (MDM). Ele protege contra um invasor fisicamente presente, usando o Modo de Disco de Destino para sobrescrever o inicializador.
- *Senha de firmware:* pode ser ativada de duas formas: pelo usuário ou por um administrador de gerenciamento de dispositivos móveis (MDM). Ela impede que um invasor fisicamente presente ative modos alternativos de inicialização, como o recoveryOS, Modo de Usuário Único ou Modo Disco de Destino, nos quais o inicializador pode ser sobrescrito. Ela também impede a inicialização de outras mídias, método por meio do qual um invasor poderia executar código para sobrescrever o inicializador.



Processo de desbloqueio de computadores Mac sem o chip Apple T2 Security.

Utilitário de Segurança da Inicialização

Visão geral do Utilitário de Segurança da Inicialização

O Utilitário de Segurança da Inicialização substitui o antigo Utilitário de Senha de Firmware. Em computadores Mac com o chip Apple T2 Security, ele cuida de um conjunto maior de ajustes de políticas de segurança. Os computadores Mac sem o chip T2 continuam usando o Utilitário de Senha de Firmware. O utilitário pode ser acessado ao inicializar no recoveryOS e selecionar o Utilitário de Segurança da Inicialização no menu Utilitários. A vantagem de colocar controles importantes de políticas de segurança do sistema (como a inicialização segura ou SIP) no recoveryOS é que todo o SO tem sua integridade verificada. Isso garante que nenhum código invasor que tenha violado o Mac possa se fazer passar pelo usuário de forma trivial com o objetivo de continuar desativando políticas de segurança.

Utilitário de Segurança da Inicialização.

As alterações importantes nas políticas agora exigem autenticação, mesmo no modo de Recuperação. Esse recurso está disponível apenas nos computadores Mac que contêm o chip T2. Na primeira vez que o Utilitário de Segurança da Inicialização é aberto, ele pede ao usuário que digite uma senha de administrador da instalação primária do macOS associada à Recuperação do macOS atualmente inicializada. Caso não exista nenhum administrador, ele deve ser criado para que a política possa ser alterada. O chip T2 exige que o computador Mac esteja inicializado na Recuperação do macOS e que tenha ocorrido uma autenticação com uma credencial assegurada pelo Secure Enclave para que tal alteração na política possa ser realizada. As alterações nas políticas de segurança possuem dois requisitos implícitos. A Recuperação do macOS deve:

- Ser inicializada a partir de um dispositivo de armazenamento diretamente conectado ao chip T2, pois as partições de outros dispositivos não possuem credenciais asseguradas pelo Secure Enclave vinculadas ao dispositivo de armazenamento interno.

- Estar em um volume APFS, pois há suporte apenas armazenar as credenciais de Autenticação na Recuperação enviadas ao Secure Enclave no volume APFS "Preboot" de uma unidade. Os volumes formatados como HFS+ não podem usar a inicialização segura.

Esta política é mostrada apenas no Utilitário de Segurança da Inicialização em computadores Mac que possuem o chip Apple T2 Security. Embora a maioria dos casos não deva requerer alterações à política de inicialização segura, o controle final dos ajustes do dispositivo está nas mãos dos usuários, que podem escolher desativar ou reduzir a funcionalidade de inicialização segura no Mac de acordo com as suas necessidades.

As alterações na política de inicialização segura feitas dentro deste app aplicam-se apenas à avaliação da cadeia de confiança sendo verificada no processador Intel. A opção "Inicialização segura do chip T2" está sempre ativada.

A política de inicialização segura pode ser configurada como um de três ajustes: Segurança Total, Segurança Média e Sem Segurança. A opção Sem Segurança desativa completamente a avaliação da inicialização segura no processador Intel e permite que o usuário inicialize o que desejar.

Política de inicialização Segurança Total

A Segurança Total é o padrão e se comporta como o iOS e iPadOS. Quando o software é baixado e está pronto para ser instalado, em vez de usar a assinatura global fornecida com o software, o macOS se comunica com o mesmo servidor de assinatura da Apple usado para o iOS e iPadOS e solicita uma nova assinatura "personalizada". Uma assinatura é considerada personalizada quando inclui o ECID (um ID exclusivo específico do chip T2 neste caso) como parte da solicitação de assinatura. Assim a assinatura que é retornada pelo servidor de assinatura é exclusiva e pode ser usada apenas por aquele chip T2 específico. Quando a política Segurança Total está em vigor, o firmware da UEFI garante que uma determinada assinatura não esteja apenas assinada pela Apple, mas também assinada para este Mac específico, essencialmente vinculando essa versão do macOS a esse Mac.

O uso de um servidor de assinatura on-line também oferece uma proteção melhor contra ataques com versões anteriores em comparação a abordagens típicas de assinatura global. Em um sistema de assinatura global, o período de segurança pode ter sido ultrapassado diversas vezes, mas um sistema que nunca viu o firmware mais recente não sabe disso. Por exemplo, um computador que acredite estar no período de segurança 1 aceita software do período de segurança 2, mesmo que o período atual de segurança seja o 5. Com um tipo de sistema on-line de assinatura iOS e iPadOS, o servidor de assinatura pode recusar a criação de assinaturas para softwares que não estejam no período de segurança mais recente.

Além disso, se um invasor descobrir uma vulnerabilidade após uma alteração do período de segurança, ele não pode simplesmente pegar o software vulnerável de um período anterior no Sistema A e aplicá-lo ao Sistema B para atacá-lo. O fato de que o software vulnerável de um período anterior tenha sido personalizado para o Sistema A impede que ele seja transferido e seja usado para atacar um Sistema B. Todos esses mecanismos trabalham em conjunto para fornecer garantias muito maiores para que os invasores não possam colocar intencionalmente softwares vulneráveis em um computador para contornar as proteções oferecidas pelo software mais recente. Mas o usuário que possui um nome de usuário e senha de administrador do Mac sempre pode escolher a política de segurança que se encaixa melhor nos seus casos de uso.

Política de inicialização Segurança Média

A Segurança Média é semelhante à situação tradicional de inicialização segura com UEFI, na qual um fornecedor (neste caso, a Apple) gera uma assinatura digital para o código para garantir que ele tenha vindo do fornecedor. Dessa forma os invasores ficam impedidos de inserir um código sem assinatura. Essa assinatura é chamada de assinatura "global", pois pode ser usada em qualquer Mac, por qualquer período, para os computadores Mac que tenham atualmente um conjunto de políticas de Segurança Média. As assinaturas globais não são aceitas pelo iOS, iPadOS ou chip T2.

Uma limitação dos esquemas de assinatura global tem a ver com a prevenção de "ataques com versões anteriores". Em um ataque com versões anteriores, o invasor coloca um software antigo com vulnerabilidades conhecidas, mas legítimo e assinado corretamente, em um sistema e explora essas vulnerabilidades para assumir o controle do sistema. Muitos sistemas de assinatura global nem sequer tentam evitar ataques com versões anteriores. Aqueles que o fazem, geralmente fazem isso através do uso de uma "versão de segurança" ou "período de segurança". Esse é um número que geralmente é abrangido pela assinatura e avaliado após a verificação da assinatura. O computador precisa de armazenamento persistente seguro para registrar o maior valor de período que já tenha visto em códigos assinados e desaprovar qualquer código (mesmo que assinado corretamente) que possua um período menor.

Caso um fornecedor queira avançar o período, ele assina um software com um novo período que seja maior que os contidos em qualquer software disponibilizado anteriormente. O firmware que detectar um período com valor maior do que o observado por último em seu armazenamento seguro, atualiza o valor do período no armazenamento. Depois disso ele rejeita todos os códigos assinados anteriores com períodos menores que o valor armazenado mais recente. Se o sistema não possuir armazenamento seguro, um invasor pode simplesmente reduzir o próprio valor do período e, em seguida, restaurar um software mais antigo e atacá-lo. É por isso que muitos sistemas que implementam períodos armazenam o número do período em um vetor de fusíveis de programação única. Quando os fusíveis se queimam, os valores não podem ser alterados. Porém, isso também possui a limitação de que um invasor pode simplesmente queimar todos os fusíveis para tornar todas as assinaturas inválidas e, assim, impedir permanentemente a inicialização do sistema operacional.

O esquema de assinatura global da Apple não possui um período de segurança porque esses sistemas são inflexíveis e frequentemente causam problemas consideráveis de usabilidade. A proteção contra ataques com versões anteriores é melhor alcançada pelo modo Segurança Total, que é o padrão e possui um comportamento muito semelhante ao iOS e iPadOS. Os usuários que desejam aproveitar a proteção contra ataques com versões anteriores devem manter a política Segurança Total padrão. Contudo, o modo Segurança Média é disponibilizado aos usuários que talvez não possam aproveitar o modo Segurança Total.

Política de inicialização de mídia

A política de inicialização de mídia é mostrada apenas em computadores Mac com um chip Apple T2 Security e é totalmente independente da política de inicialização segura. Mesmo que um usuário desative a inicialização segura, o comportamento padrão de desaprovar a inicialização a partir de qualquer coisa que não seja o dispositivo de armazenamento diretamente conectado ao chip T2 permanece inalterado.

Historicamente, computadores Mac podiam inicializar a partir de um dispositivo externo por padrão. Essa abordagem poderia permitir que um invasor com a posse física do dispositivo executasse um código arbitrário a partir do volume inicializado. A combinação de proteções como o FileVault e o SecureBoot fazem com que não haja pontos fracos conhecidos na arquitetura por meio dos quais um invasor executando em um volume externo poderia acessar os dados do usuário sem saber a senha desse usuário. Porém, a possibilidade da execução de código arbitrário, mesmo que temporária, pode permitir que um invasor manipule o Mac de formas que podem preparar dados controlados por ele para explorar vulnerabilidades que a Apple desconhece. A criação de código arbitrário pode então, potencialmente, levar ao comprometimento da inicialização do usuário e, subsequentemente, ao comprometimento dos dados do usuário.

A Apple alterou a política de inicialização externa para "negar por padrão", com possibilidade de alteração em computadores Mac com o chip T2. Em computadores Mac sem o chip T2, os usuários sempre tiveram a opção de definir uma senha de firmware para aderir a esse comportamento de negar por padrão. Contudo, as senhas de firmware não eram bem conhecidas e tiveram uma adoção muito baixa. Com essa mudança de política, a Apple está alterando o comportamento do Mac para fornecer a melhor proteção possível por padrão, em vez de colocar o ônus da ativação sobre os usuários.

Proteção da Senha de Firmware

O macOS permite o uso de uma Senha de Firmware para evitar modificações indesejadas nos ajustes de firmware em um Mac específico. A Senha de Firmware é usada para impedir a seleção de modos de inicialização alternativos, como as inicializações no recoveryOS, modo de Usuário Único, Modo Disco de Destino ou a partir de um volume não autorizado.

O modo mais básico da Senha de Firmware pode ser alcançado a partir do Utilitário de Senha de Firmware do recoveryOS, em computadores Mac sem o chip Apple T2 Security, e a partir do Utilitário de Segurança da Inicialização, em computadores Mac com o chip T2. Opções avançadas (como a capacidade de solicitar a senha a cada inicialização) estão disponíveis na ferramenta de linha de comando `firmwarepasswd` no macOS.

Como descrito em Processo de inicialização de computadores Mac sem o chip Apple T2 Security, a definição de uma Senha de Firmware é importante especialmente para reduzir o risco de ataques a computadores Mac sem o chip T2 realizados por um invasor fisicamente presente (por exemplo, em um computador em um laboratório ou escritório). A senha de firmware pode impedir que um invasor inicialize no recoveryOS, de onde ele poderia desativar a Proteção da Integridade do Sistema. Além disso, a restrição da inicialização de mídias alternativas impede que um invasor execute código privilegiado de outro SO para atacar o firmware de periféricos.

Existe um mecanismo de redefinição da Senha de Firmware para ajudar usuários que esqueceram a senha. Os usuários pressionam uma combinação de teclas na inicialização e veem uma string específica do modelo para fornecer ao AppleCare. O AppleCare assina digitalmente um recurso cuja assinatura é verificada pelo Identificador Uniforme de Recursos (URI). Caso a assinatura seja validada e o conteúdo seja para o Mac específico, o firmware da UEFI remove a Senha de Firmware.

Para os usuários que não desejam que mais ninguém possa remover a Senha de Firmware através do software, exceto o próprio usuário, a opção `-disable-reset-capability` foi acrescentada à ferramenta de linha de comando `firmwarepasswd` no macOS 10.15. Antes de configurar essa opção, os usuários devem aceitar que, caso a senha seja esquecida e precise ser removida, o usuário deverá arcar com o custo da substituição da placa-mãe necessária para tal. Organizações que desejam proteger seus computadores Mac de invasores externos e funcionários devem definir uma Senha de Firmware em sistemas de propriedade da organização. Isso pode ser feito no dispositivo:

- Durante o processo de provisão, usando manualmente a ferramenta de linha de comando `firmwarepasswd`
- Com ferramentas de gerenciamento de terceiros que usam a ferramenta de linha de comando `firmwarepasswd`
- Com o gerenciamento de dispositivos móveis (MDM)

Atualizações seguras de software

Visão geral das atualizações seguras de software

A Apple lança atualizações de software regularmente para abordar questões de segurança emergentes e fornecer novos recursos. Essas atualizações geralmente são fornecidas simultaneamente para todos os dispositivos compatíveis. Os usuários de dispositivos iOS e iPadOS recebem notificações de atualização no dispositivo e no iTunes (no macOS 10.14 ou anterior) ou Finder (macOS 10.15 ou posterior). As atualizações do macOS estão disponíveis nas Preferências do Sistema. As atualizações são entregues via conexão sem fio para que as correções de segurança mais recentes sejam adotadas rapidamente.

O processo de inicialização ajuda a garantir que apenas o código assinado pela Apple seja instalado. Por exemplo, a Autorização do Software do Sistema assegura que apenas cópias legítimas das versões do sistemas operacionais que estão sendo ativamente assinadas pela Apple possam ser instaladas nos dispositivos iOS e iPadOS ou em computadores Mac nos quais o ajuste Segurança Total tenha sido configurado como a política de inicialização segura no Utilitário de Segurança da Inicialização. Esse sistema impede que versões anteriores que não possuem as atualizações de segurança mais recentes sejam instaladas nos dispositivos iOS e iPadOS e pode ser usado pela Apple para impedir reversões semelhantes no macOS. Sem essa proteção, um invasor que conseguisse se apossar de um dispositivo poderia instalar uma versão mais antiga do iOS ou iPadOS e explorar uma vulnerabilidade já corrigida em versões mais recentes.

Além disso, quando um dispositivo está fisicamente conectado ao Mac, uma cópia completa do iOS ou iPadOS é baixada e instalada. Mas para as atualizações de software via conexão sem fio (OTA), apenas os componentes necessários para completar uma atualização são baixados, melhorando a eficiência da rede por não baixar todo o sistema operacional. Além disso, as atualizações de software podem ser armazenadas em um Mac com o macOS 10.13 ou posterior que tenha o Conteúdo em Cache ativado, para que os dispositivos iOS e iPadOS não precisem baixar novamente a atualização necessária da internet. Eles ainda precisarão contatar os servidores da Apple para concluir o processo de atualização.

Processo da atualização segura de software

Durante as atualizações, uma conexão é feita ao servidor de autorização de instalações da Apple, que inclui uma lista de medições criptográficas de cada parte do pacote a ser instalado (iBoot, kernel e imagem do sistema operacional, por exemplo), um valor antirreprodução aleatório (nonce) e o Identificador Exclusivo do Dispositivo (ECID).

O servidor de autorização verifica a lista de medições apresentada e a compara com versões em que a instalação é permitida. Caso encontre uma correspondência, ele adiciona o ECID à medição e informa o resultado. O servidor passa ao dispositivo um conjunto completo de dados assinados como parte do processo de atualização. A adição do ECID "personaliza" a autorização para o dispositivo solicitante. Ao autorizar e assinar somente as medições conhecidas, o servidor garante que a atualização aconteça exatamente conforme fornecida pela Apple.

A avaliação da cadeia de confiança no momento da inicialização verifica se a assinatura vem da Apple e se a medição do item carregado do dispositivo de armazenamento, combinada com o ECID do dispositivo, corresponde ao que estava coberto pela assinatura. Tais passos garantem que a autorização é para um dispositivo específico e que uma versão mais antiga do firmware do iOS, iPadOS ou chip Apple T2 Security não pode ser copiada de um dispositivo para outro. O nonce impede que um invasor salve a resposta do servidor e a use para adulterar um dispositivo ou alterar o software do sistema de outra maneira.

Em dispositivos com o Secure Enclave, o coprocessador do Secure Enclave também usa a Autorização do Software do Sistema para garantir a integridade de seu software e impedir instalações de versões mais antigas.

Integridade do sistema operacional no iOS e iPadOS

Visão geral da segurança do sistema no iOS e iPadOS

A Apple criou a plataforma iOS tendo a segurança como fator fundamental. Quando decidimos criar a melhor plataforma móvel possível, utilizamos décadas de experiência como base para construir uma arquitetura totalmente nova. Levamos em consideração os riscos à segurança do ambiente de computadores e definimos uma nova abordagem para segurança na criação do iOS. Desenvolvemos e incorporamos recursos inovadores que reforçam a segurança móvel e protegem todo o sistema por padrão. Como resultado, o iOS e, subsequentemente, o iPadOS são um grande avanço em segurança para dispositivos móveis.

Proteção da Integridade do Kernel

Após o término da inicialização dos kernels do iOS e iPadOS, a Proteção da Integridade do Kernel (KIP) é ativada para evitar modificações do código do kernel e de drivers. O controlador de memória fornece uma região protegida de memória física que é usada pelo iBoot para carregar o kernel e as extensões do kernel. Após a conclusão da inicialização, o controlador de memória recusa gravações na região da memória física protegida. Além disso, a Unidade de Gerenciamento de Memória (MMU) do processador do aplicativo é configurada para impedir código privilegiado de mapeamento a partir da memória física fora da região de memória protegida e para impedir mapeamentos graváveis da memória física dentro da região de memória do kernel.

Para impedir a reconfiguração, o hardware usado para ativar a KIP é bloqueado após a conclusão do processo de inicialização. A KIP é compatível com SoCs a partir do Apple A10 e S4.

No SoC do Apple A11 Bionic, uma nova primitiva de hardware foi apresentada. Essa primitiva introduz um registrador de CPU para restringir permissões rapidamente por thread. Com essas restrições de permissões rápidas (ou APRR), o iOS e o iPadOS são capazes de remover permissões de execução da memória — sem o custo de uma chamada de sistema e uma consulta ou descarte da tabela de páginas.

Proteção da Integridade do Coprocessador do Sistema

O firmware do coprocessador lida com muitas tarefas críticas do sistema — por exemplo, com o Secure Enclave, o processador do sensor de imagens e o coprocessador de Movimento. Sendo assim, sua segurança é parte essencial da segurança do sistema como um todo. Para impedir a modificação do firmware do coprocessador, a Apple usa um mecanismo chamado Proteção da Integridade do Coprocessador do Sistema (SCIP), compatível com SoCs a partir do Apple A12 e S4.

A SCIP funciona de maneira bem semelhante à Proteção da Integridade do Kernel: no momento da inicialização, o iBoot carrega o firmware de cada coprocessador em uma região de memória protegida, reservada e separada da região da KIP. O iBoot configura a unidade de memória de cada coprocessador a fim de impedir:

- Mapeamentos executáveis fora da sua parte da região de memória protegida
- Mapeamentos graváveis dentro da sua parte da região de memória protegida

Também no momento da inicialização, o sistema operacional do Secure Enclave é usado para configurar a SCIP para o Secure Enclave. Depois que o processo de inicialização é concluído, o hardware usado para ativar a SCIP é bloqueado para impedir a reconfiguração.

Códigos de Autenticação de Ponteiros

Códigos de autenticação de ponteiros (PACs) são compatíveis com SoCs a partir do Apple A12 e S4 e usados para proteger contra a exploração de erros de corrupção de memória. O software do sistema e os apps integrados usam PACs para impedir a modificação dos ponteiros de função e endereços de retorno (ponteiros de código). O PAC usa cinco valores secretos de 128 bits para assinar instruções e dados do kernel, e cada processo do espaço do usuário possui suas próprias chaves B. Os itens usam sal e assinaturas conforme indicado a seguir:

Item	Chave	Sal
Endereço de retorno de função	IB	Endereço de armazenamento
Ponteiros de função	IA	0
Função de chamada de bloco	IA	Endereço de armazenamento
Cache de métodos de Objective-C	IB	Endereço de armazenamento + Classe + Seletor
Entradas em tabelas virtuais de C++	IA	Endereço de armazenamento + hash (nome do método truncado)
Etiqueta GoTo calculada	IA	Hash (nome da função)
Estado de threads do kernel	GA	•
Registradores de estado de threads do usuário	IA	Endereço de armazenamento
Ponteiros de tabelas virtuais de C++	DA	0

O valor da assinatura é armazenado nos bits de preenchimento não utilizados no início do ponteiro de 64 bits. A assinatura é verificada antes do uso e o preenchimento é restaurado para garantir que o endereço do ponteiro possa ser usado. A falha na verificação resulta na definição de um valor especial que invalida o endereço e, no iOS 13 e iPadOS 13.1, aborta. Essa verificação aumenta a dificuldade de vários ataques como o de Programação Orientada a Retorno (ROP), que procura enganar o dispositivo para que execute um código existente de maneira maliciosa ao manipular endereços de retorno de função armazenados na pilha. Os PACs são compatíveis com SoCs a partir do Apple A12 e S4.

Camada de Proteção de Página

A Camada de Proteção de Página (PPL) no iOS e iPadOS protege o código no espaço do usuário contra modificações após a verificação da assinatura do código. Ela aproveita a KIP e APRR para gerenciar cuidadosamente as substituições de permissões da tabela de páginas e assegurar que apenas a PPL possa alterar as páginas protegidas que contêm o código do usuário e as tabelas de páginas. O sistema fornece uma enorme redução da superfície de ataque ao oferecer suporte à exigência da integridade do código em todo o sistema, mesmo no caso de um kernel comprometido.

Integridade do SO no macOS

Visão geral da segurança do sistema no macOS

A Apple projetou a plataforma macOS com uma abordagem integrada de hardware, software e serviços que integra a segurança ao projeto e simplifica a configuração, a implantação e o gerenciamento. O macOS possui as principais tecnologias de segurança de que um profissional de TI precisa para ajudar a proteger dados corporativos e fazer a integração dentro de ambientes seguros de redes empresariais. A Apple também tem trabalhado com órgãos de definição de padrões para garantir a conformidade com as certificações de segurança mais recentes.

Segurança do firmware no Mac

Visão geral da segurança do firmware da UEFI

Desde 2006, computadores Mac com uma CPU baseada em Intel usam um firmware da Intel baseado na versão 1 ou 2 do kit de desenvolvimento (EDK) da Interface de Firmware Extensível (EFI). O código baseado no EDK2 está em conformidade com a especificação da Interface de Firmware Extensível Unificada (UEFI). Esta seção refere-se ao firmware da Intel como firmware da UEFI. O firmware da UEFI era o primeiro código a ser executado no chip Intel.

Para impedir ataques que vinculam-se fisicamente ao chip de armazenamento do firmware que armazena o firmware da UEFI, a arquitetura dos computadores Mac foi modificada desde 2017 para colocar a raiz de confiança no firmware da UEFI armazenado no chip Apple T2 Security. Nesses computadores Mac, a raiz de confiança do firmware da UEFI é especificamente o firmware do T2. Esse design conta com o T2 para proteger o firmware da UEFI (e a Inicialização Segura como um todo) contra uma infecção persistente, da mesma forma que a inicialização é protegida pelo SoC A Series no iOS e iPadOS.

Nos computadores Mac que não possuem o chip Apple T2 Security, a raiz de confiança do firmware da UEFI é o chip onde o firmware está armazenado. As atualizações do firmware da UEFI são assinadas digitalmente pela Apple e verificadas pelo firmware antes da atualização do armazenamento. Para impedir ataques com versões mais antigas, as atualizações sempre devem ter uma versão mais recente que a versão existente. Porém, um invasor que tiver acesso físico ao Mac poderia usar um hardware para se conectar ao chip de armazenamento do firmware e atualizá-lo para que contenha conteúdo malicioso. Da mesma forma, se forem encontradas vulnerabilidades no processo inicial de inicialização do firmware da UEFI (antes que ele restrinja as gravações no chip de armazenamento), isso também poderia levar à infecção persistente do firmware da UEFI. Essa limitação da arquitetura do hardware é comum na maioria dos PCs baseados em Intel e está presente em todos os computadores Mac que não possuem o chip T2.

Para resolver essa limitação, a arquitetura dos computadores Mac foi modificada para colocar a raiz de confiança no firmware da UEFI no chip Apple T2 Security. Nesses computadores Mac, a raiz de confiança do firmware da UEFI é especificamente o firmware do T2, como descrito na seção sobre a inicialização do macOS a seguir nesta seção. Para causar uma infecção persistente do firmware da UEFI, um invasor teria que conseguir uma infecção persistente do firmware do T2.

Mecanismo de Gerenciamento Intel (ME)

Um subcomponente que fica armazenado no firmware da UEFI é o firmware do Mecanismo de Gerenciamento Intel (ME). O ME — um processador e subsistema separado dentro dos chips Intel — pode ser usado para gerenciamento remoto, áudio e vídeo protegidos e aprimoramento da segurança. Para reduzir a superfície de ataque, os computadores Mac executam um firmware ME personalizado, do qual a maioria dos componentes foram removidos. Isso permite que o firmware ME do Mac seja menor que a versão mínima padrão disponibilizada pela Intel. Consequentemente, muitos componentes (como a Tecnologia de Gerenciamento Ativo) que foram alvo de ataques públicos realizados por pesquisadores de segurança no passado, não estão presentes no firmware ME do Mac. O uso principal do ME é a proteção de copyright de áudio e vídeo em computadores Mac que possuem apenas gráficos Intel.

Modo de Gerenciamento do Sistema (SMM)

Os processadores Intel possuem um modo especial de execução que é diferente da operação normal. Chamado de Modo de Gerenciamento do Sistema (SMM), ele foi introduzido originalmente para cuidar de operações sensíveis ao tempo, como o gerenciamento de energia. Contudo, para realizar tais ações, computadores Mac usavam historicamente um microcontrolador separado, chamado de Controlador do Gerenciamento do Sistema (SMC). O SMC não é mais um microcontrolador separado, ele foi integrado ao chip Apple T2 Security.

Em PCs que oferecem suporte à inicialização segura, o SMM possui a função adicional de ser um ambiente de execução protegido que pode receber acesso exclusivo a conteúdo sensível ao tempo que requeira segurança, como o acesso de gravação no código e a política de segurança armazenada no chip de armazenamento do firmware da UEFI. Dessa forma, muitas vezes é de interesse do invasor violar o ambiente de execução do SMM como forma de aumentar os privilégios para executar operações que o kernel não pode realizar e possivelmente comprometer a inicialização segura. Em computadores Mac, o ambiente de execução do SMM é usado o mínimo possível e não é tratado como limite de segurança para fins de inicialização segura. Assim, mesmo que o SMM seja comprometido, a Inicialização Segura permanece inalterada. No chip T2, o limite de privilégios é a ação que pode ser realizada exclusivamente pelo chip.

Proteções de DMA

Para atingir altas taxas de transferência em interfaces de alta velocidade como PCIe, FireWire, Thunderbolt e USB, os computadores devem oferecer suporte ao Acesso Direto à Memória (DMA) de periféricos. Ou seja, eles devem ser capazes de ler e gravar na RAM sem o envolvimento contínuo da CPU Intel. Desde 2012, computadores Mac implementaram várias tecnologias para se proteger o DMA, resultando no melhor e mais abrangente conjunto de proteções ao DMA em qualquer PC.

A Tecnologia de Virtualização para E/S Direcionada da Intel (VT-d) é uma tecnologia usada desde 2012 nos computadores Mac, sendo usada pela primeira vez no OS X 10.9 para impedir que o kernel fosse sobrescrito na memória por periféricos maliciosos. No entanto, periféricos maliciosos podem sobrescrever o código e os dados *enquanto* o firmware da UEFI estiver sendo executado, a fim de comprometer a segurança da inicialização. O macOS 10.12.3 atualizou o firmware da UEFI em todos os computadores Mac compatíveis com VT-d para que usem a VT-d para se proteger contra periféricos FireWire e Thunderbolt maliciosos. Ele também isola os periféricos para que eles possam ver apenas seus próprios intervalos de memória e não a memória de outros periféricos. Por exemplo, um periférico Ethernet em execução na UEFI não é capaz de ler a memória de um periférico de armazenamento.

As proteções de DMA no firmware da UEFI continuaram sendo melhoradas no macOS 10.13, com antecipação da inicialização na sequência de inicialização do firmware da UEFI para proteção contra:

- Processadores de periféricos internos maliciosos no barramento PCIe
- Uma classe de ataques de Interrupção com Sinalização de Mensagem (MSI) apresentada por pesquisadores de segurança

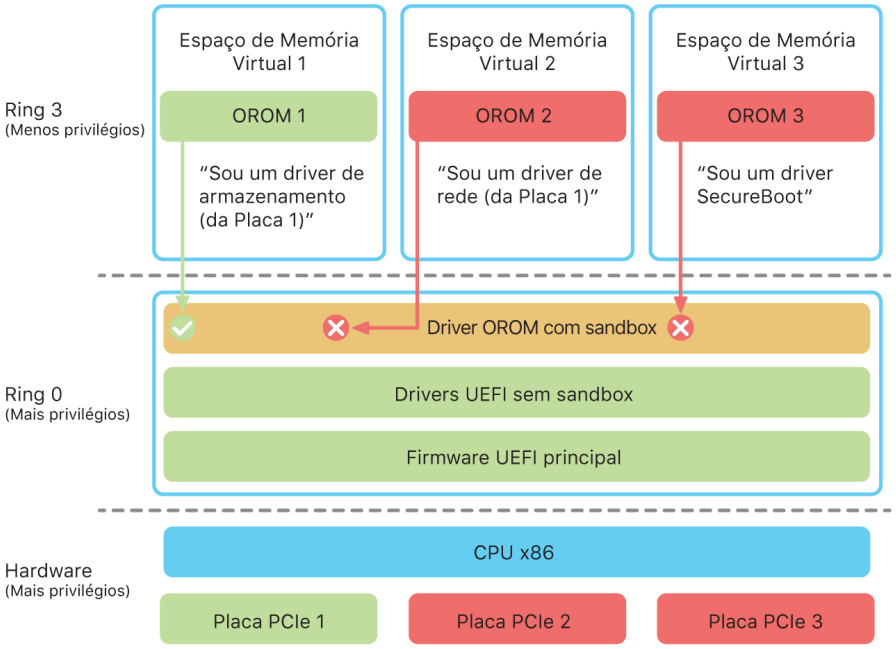
Todos os computadores Mac que possuem o chip Apple T2 Security vêm com proteções de DMA ainda mais aprimoradas, nas quais a inicialização é realizada o mais cedo possível. Especificamente, a proteção é ativada antes que qualquer RAM esteja disponível para o firmware da UEFI. Isso oferece proteção contra qualquer dispositivo violado de PCIe com barramento zero (como o Intel ME) que possam estar em execução e tenham capacidade de DMA no momento da disponibilização da RAM. Esta proteção também foi adicionada a computadores Mac sem o chip T2 no macOS 10.15.

ROMs de Opção

Tanto os dispositivos Thunderbolt quanto PCIe possuem uma "ROM de Opção" (OROM) fisicamente conectada ao dispositivo (geralmente ela não é uma ROM verdadeira, mas um chip regravável que armazena firmware). Em sistemas baseados em UEFI, esse firmware geralmente é um driver de UEFI, que é lido pelo firmware da UEFI e executado. O código executado deve inicializar e configurar o hardware do qual foi obtido, para que o hardware possa ser usado pelo restante do firmware. Essa habilidade é necessária para que hardwares especializados de terceiros possam carregar e operar durante as primeiras fases da inicialização — por exemplo, para inicializar a partir de matrizes RAID externas.

Contudo, como as OROMs geralmente são regraváveis, se um invasor sobrescrevesse a OROM de um periférico legítimo, o código do invasor seria executado no início do processo de inicialização, e poderia adulterar o ambiente de execução e violar a integridade dos softwares carregados posteriormente. Da mesma forma, se o invasor introduzir seu próprio dispositivo malicioso no sistema, ele também poderia executar um código malicioso.

No macOS 10.12.3, o comportamento dos computadores Mac vendidos após 2011 foi alterado, para que as OROMs não fossem executadas por padrão durante a inicialização do Mac, a menos que uma combinação especial de teclas fosse pressionada. Essa combinação de teclas ofereceu proteção contra a introdução não intencional de OROMs maliciosas na sequência de inicialização do macOS. O comportamento padrão do Utilitário de Senha de Firmware também foi alterado para que quando o usuário definisse uma senha de firmware, as OROMs não pudessem ser executadas *mesmo* que a combinação de teclas fosse pressionada. Isso protegia contra a introdução de uma OROM maliciosa por um invasor fisicamente presente. Para os usuários que ainda precisam executar OROMs enquanto a senha de firmware estiver definida, uma opção não padrão pode ser configurada com a ferramenta de linha de comando `firmwarepasswd` no macOS.



Sandbox da ROM de Opção (OROM).

Sandbox da OROM

No macOS 10.15, o firmware da UEFI foi atualizado para conter um mecanismo de sandbox e retirada de privilégios de OROMs. O firmware da UEFI geralmente executa todo o código, incluindo OROMs, no nível máximo de privilégio da CPU Intel, chamado de "ring 0", e com um espaço único e compartilhado de memória virtual para todo o código e os dados. Ring 0 é também o nível de privilégio no qual o kernel do macOS é executado, enquanto o nível mais baixo (ring 3), é onde os apps são executados. O sandbox da OROM utiliza a separação da memória virtual da mesma forma que o kernel e faz as OROMs serem executadas no ring 3, retirando os privilégios das OROMs.

Além disso, o sandbox restringe significativamente tanto as interfaces que podem ser chamadas pelas OROMs (o que é semelhante à filtragem de chamadas de sistema em kernels) quanto o tipo de dispositivo que uma OROM pode usar para se registrar (o que é semelhante a uma lista de aplicativos confiáveis). O benefício desse design é que as OROMs maliciosas não podem mais gravar diretamente em nenhum lugar dentro da memória do ring 0, ficando limitadas a uma interface de sandbox bastante estreita e bem definida. Essa interface limitada reduz significativamente a superfície de ataque e obriga os invasores a primeiro escapar do sandbox e aumentar o privilégio.

Segurança do firmware de periféricos

Os computadores Mac possuem vários processadores integrados de periféricos dedicados a tarefas como rede, processamento gráfico e gerenciamento de energia ou de barramentos de dados, como USB ou Thunderbolt. Geralmente, o firmware do periférico tem um objetivo único e é muito menos poderoso que a CPU Intel. Porém, os periféricos integrados que não implementam a segurança de forma suficiente se tornam um alvo para invasores que buscam alvos ainda mais fáceis de explorar para infectar permanentemente o sistema operacional. Com um firmware de processador de periférico infectado, um invasor poderia visar o software da CPU Intel ou capturar diretamente dados sigilosos (um dispositivo Ethernet poderia ver o conteúdo dos pacotes que não estão criptografados, por exemplo).

A Apple trabalha de forma estratégica com fornecedores externos para reduzir (sempre que possível) o número necessário de processadores de periféricos ou evitar designs que exijam firmware. Mas, quando o firmware é necessário, são tomadas medidas para garantir que um invasor não possa persistir nesse processador. Isso pode ser conseguido:

- Ao executar o processador em um modo onde ele baixa um firmware verificado da CPU Intel na inicialização
- Ao se garantir que o processador do periférico implemente sua própria cadeia de inicialização segura na qual ele verifica o próprio firmware a cada inicialização

A Apple trabalha com os fornecedores para auditar suas implementações e aprimorar seus projetos para incluir propriedades desejadas como:

- Garantia de um poder criptográfico mínimo
- Revogação forte de firmware reconhecidamente problemático
- Desativação de interfaces de depuração
- Assinatura do firmware com chaves criptográficas armazenadas nos Módulos de Segurança de Hardware (HSMs) controlados pela Apple

Nos últimos anos a Apple tem trabalhado com alguns fornecedores externos para adotar as mesmas estruturas de dados “Image4”, código de verificação e infraestrutura de assinatura usados pelo iOS, iPadOS e computadores Mac com o chip Apple T2 Security.

Quando nem a operação sem armazenamento nem o armazenamento com a inicialização segura são uma opção, o projeto exige que as atualizações de firmware sejam criptograficamente assinadas e verificadas antes da atualização do armazenamento persistente.

Controles de acesso obrigatórios

O macOS também usa controles de acesso obrigatórios — políticas que definem restrições de segurança criadas pelo desenvolvedor e que não podem ser substituídas. Esta abordagem é diferente dos controles de acesso discricionários, que permitem que os usuários substituam as políticas de segurança de acordo com suas preferências.

Os controles de acesso obrigatórios não são visíveis para os usuários, mas são a tecnologia subjacente que ajuda a fornecer vários recursos importantes, como sandbox, controles parentais, preferências gerenciadas, extensões e a Proteção da Integridade do Sistema.

Proteção da Integridade do Sistema

O OS X 10.11 ou posterior possui uma proteção no nível do sistema, chamada de *Proteção da Integridade do Sistema*, a qual restringe componentes a somente leitura em locais específicos e importantes do sistema de arquivos para impedir que códigos maliciosos o modifiquem. A Proteção da Integridade do Sistema é um ajuste específico do computador que é ativado por padrão quando um usuário atualiza para o OS X 10.11 ou posterior. Sua desativação remove a proteção para todas as partições do dispositivo de armazenamento físico. O macOS aplica essa política de segurança a todos os processos em execução no sistema, independentemente de estarem sendo executados em sandbox ou com privilégios administrativos.

Extensões do kernel

As extensões do kernel (KEXTs) não são mais recomendadas para o macOS. As KEXTs colocam em risco a integridade e a confiabilidade do sistema operacional e os usuários devem dar preferência a soluções que não exijam a extensão do kernel.

O macOS 10.15 permite que os desenvolvedores estendam as funcionalidades do macOS por meio da instalação e gerenciamento de extensões do sistema que são executadas no espaço do usuário e não no nível do kernel. Por serem executadas no espaço do usuário, as extensões do sistema aumentam a estabilidade e a segurança do macOS. Enquanto as KEXTs têm inerentemente acesso total a todo o sistema operacional, as extensões em execução no espaço do usuário recebem apenas os privilégios necessários para realizar suas funções especificadas.

Os desenvolvedores podem usar frameworks como DriverKit, EndpointSecurity e NetworkExtension para escrever drivers de USB e interface humana, ferramentas de segurança de pontos de extremidade (como prevenção de perda de dados ou outros agentes de pontos de extremidade) e ferramentas de VPN e rede — tudo isso sem precisar escrever KEXTs. Agentes de segurança de terceiros devem ser usados apenas se fizerem uso dessas APIs ou possuírem um planejamento robusto para fazer a transição para seu uso em vez de extensões do kernel.

O macOS ainda fornece um mecanismo de extensões do kernel para permitir o carregamento dinâmico de código dentro do kernel sem a necessidade de recompilar ou vincular novamente. Para melhorar a segurança, o consentimento do usuário é necessário para o carregamento de extensões do kernel instaladas com o macOS 10.13 ou após sua instalação. Isso é chamado de Carregamento de Extensões do Kernel Aprovado pelo Usuário. A autorização do administrador é necessária para aprovar uma extensão do kernel.

As extensões do kernel não exigem autorização caso elas:

- Tenham sido instaladas no Mac antes da atualização para o macOS 10.13
- Estejam substituindo extensões aprovadas anteriormente
- Tenham permissão para serem carregadas sem o consentimento do usuário por meio do uso da ferramenta de linha de comando `spctl`, disponível após a inicialização na Recuperação do macOS
- Tenham permissão para serem carregadas usando a configuração do gerenciamento de dispositivos móveis (MDM)

  A partir do macOS 10.13.2, os usuários podem usar o MDM para especificar uma lista de extensões do kernel que podem ser carregadas sem o consentimento do usuário. Essa opção requer um Mac com macOS 10.13.2 que esteja registrado no MDM — através do Apple School Manager, Apple Business Manager ou registro no MDM aprovado pelo usuário.

Segurança do sistema no watchOS

Visão geral da segurança do sistema no watchOS

O Apple Watch usa os recursos e a tecnologia de segurança feitos para o iOS e iPadOS para ajudar a proteger os dados do dispositivo, e para proteger as comunicações com o iPhone com o qual está emparelhado e com a internet. Isso inclui tecnologias como a Proteção de Dados e o controle de acesso às Chaves. O código do usuário também é trançado ao UID do dispositivo para criar chaves de criptografia.

A segurança do emparelhamento do Apple Watch com o iPhone é feita usando um processo fora de banda (OOB) para trocar chaves públicas, seguido pelo segredo compartilhado do link Bluetooth Low Energy (BLE). O Apple Watch exibe um padrão animado, capturado pela câmera do iPhone. Este padrão contém um segredo codificado usado pelo emparelhamento fora de banda BLE 4.1. O padrão de emparelhamento BLE Passkey Entry é usado como método alternativo, se necessário.

Depois que a sessão do BLE é estabelecida e criptografada usando o mais alto protocolo de segurança disponível na Especificação Bluetooth Core, o Apple Watch e o iPhone trocam chaves usando um processo adaptado do Serviço de Identidade da Apple (IDS), conforme descrito em visão geral do iMessage. Após as chaves serem trocadas, a chave da sessão Bluetooth é descartada e todas as comunicações entre o Apple Watch e o iPhone são criptografadas usando IDS — com os links Bluetooth, Wi-Fi e Celular criptografados fornecendo uma camada de criptografia secundária. O endereço Bluetooth Low Energy é trocado em intervalos de 15 minutos para reduzir o risco de rastreamento local do dispositivo por meio da transmissão de um identificador persistente.

Para oferecer suporte aos apps que necessitam de dados de transmissão, a criptografia é fornecida com os métodos descritos em FaceTime, usando o serviço IDS oferecido pelo iPhone emparelhado ou uma conexão direta à internet.

O Apple Watch implementa o armazenamento criptografado por hardware e a proteção de arquivos e itens de Chaves com base em classes, como descrito na seção “Criptografia e Proteção de Dados” deste documento. Keybags de acesso controlado também são usadas em itens das Chaves. As chaves usadas para as comunicações entre o relógio e o iPhone também são mantidas em segurança através do uso de proteção com base em classes.

Quando o Apple Watch não está dentro do alcance do Bluetooth, é possível usar Wi-Fi ou dados celulares. O Apple Watch conecta-se automaticamente a redes Wi-Fi que já foram conectadas pelo iPhone emparelhado e cujas credenciais foram sincronizadas com o Apple Watch enquanto os dispositivos estavam no raio de alcance. Esse comportamento de conexão automática pode então ser configurado por rede, na seção Wi-Fi do app Ajustes do Apple Watch. As redes Wi-Fi que nunca foram conectadas anteriormente em nenhum dos dispositivos podem ser conectadas manualmente na seção Wi-Fi do app Ajustes do Apple Watch.

Quando o Apple Watch e o iPhone estão fora do raio de alcance, o Apple Watch conecta-se diretamente aos servidores do iCloud e Gmail para obter os dados do Mail, em vez de sincronizar os dados do Mail com o iPhone emparelhado pela internet. Para contas do Gmail, o usuário precisa autenticar no Google na seção Mail do app Watch no iPhone. O token do OAuth recebido do Google será enviado ao Apple Watch em formato criptografado por meio do Serviço de Identidade da Apple (IDS), para que possa ser usado para obtenção dos dados do Mail. Esse token do OAuth jamais é usado para conectividade com o servidor do Gmail a partir do iPhone emparelhado.

Se a detecção de braço estiver ativada, o dispositivo é bloqueado automaticamente logo após ser removido do braço do usuário. Se a detecção de braço estiver desativada, a Central de Controle oferece uma opção para bloquear o Apple Watch. Quando o Apple Watch está bloqueado, o Apple Pay só pode ser usado se o código do relógio for digitado. A detecção de braço pode ser desativada no app Apple Watch do iPhone. Esse ajuste também pode ser aplicado por meio de uma solução de gerenciamento de dispositivos móveis (MDM).

O iPhone emparelhado também pode desbloquear o relógio, desde que o relógio esteja sendo usado. Isso é realizado ao estabelecer uma conexão autenticada pelas chaves reconhecidas durante o emparelhamento. O iPhone envia a chave, a qual é usada pelo relógio para desbloquear suas chaves de Proteção de Dados. O código do relógio não é de conhecimento do iPhone nem é transmitido. Esse recurso pode ser desativado no app Apple Watch do iPhone.

O Apple Watch pode ser emparelhado apenas com um iPhone por vez. O iPhone comunica instruções para apagar todo o conteúdo e dados do Apple Watch quando desemparelhado.

O Apple Watch pode ser configurado para uma atualização de software do sistema na mesma noite. Para obter mais informações sobre como o código do Apple Watch é armazenado e usado durante a atualização, consulte Keybags.

A ativação do Buscar no iPhone emparelhado também ativa o Bloqueio de Ativação no Apple Watch. O Bloqueio de Ativação dificulta o uso ou venda de um Apple Watch perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário para desemparelhar, apagar ou reativar o Apple Watch.

Uso do Apple Watch com o macOS

Desbloqueio Automático com o Apple Watch no macOS

Os usuários com o Apple Watch podem usá-lo para desbloquear automaticamente o Mac. O Bluetooth Low Energy (BLE) e o Wi-Fi peer-to-peer permitem que o Apple Watch desbloqueie o Mac de forma segura depois de garantir a proximidade entre os dispositivos. Isso exige uma conta do iCloud com a autenticação de dois fatores (TFA) configurada.

Ao permitir que um Apple Watch desbloqueie um Mac, um link seguro, que usa Identidades de Desbloqueio Automático, é estabelecido. O Mac cria um segredo de desbloqueio aleatório de uso único e o transmite para o Apple Watch através do link. O segredo é armazenado no Apple Watch e pode ser acessado apenas quando o Apple Watch está desbloqueado. O token de desbloqueio não é a senha do usuário.

Durante uma operação de desbloqueio, o Mac usa BLE para criar uma conexão com o Apple Watch. As chaves compartilhadas (usadas ao ativar o link pela primeira vez) são então usadas para estabelecer um link seguro entre os dois dispositivos. Depois, o Mac e o Apple Watch usam Wi-Fi peer-to-peer e uma chave segura derivada do link seguro para determinar a distância entre os dois dispositivos. Se os dispositivos estiverem dentro do alcance, o link seguro é usado para transferir o segredo pré-compartilhado para desbloquear o Mac. Depois do desbloqueio bem-sucedido, o Mac substitui o segredo de desbloqueio atual por um novo segredo de desbloqueio de uso único e o transmite para o Apple Watch por meio do link.

Aprovação com Apple Watch

Quando o Desbloqueio Automático com o Apple Watch está ativado, o Apple Watch pode ser usado no lugar do Touch ID ou em conjunto com ele para aprovar solicitações de autorização e autenticação de:

- macOS e apps Apple que solicitam autorização
- Apps de terceiros que solicitam autenticação
- Senhas salvas do Safari
- Notas Seguras

Criptografia e Proteção de Dados

Visão geral da Criptografia e Proteção de Dados

Os recursos da cadeia de inicialização segura, de segurança do sistema e de apps ajudam a garantir que apenas códigos confiáveis sejam executados em um dispositivo. Os dispositivos Apple possuem recursos de criptografia adicionais para resguardar os dados do usuário, mesmo que outras partes da infraestrutura de segurança tenham sido comprometidas (por exemplo se um dispositivo for perdido ou estiver executando código não confiável). Todos esses recursos beneficiam tanto usuários quanto administradores de TI, protegendo informações pessoais e corporativas a todos os momentos e fornecendo métodos para o apagamento remoto completo e imediato no caso de roubo ou perda do dispositivo.

Os dispositivos iOS e iPadOS usam uma metodologia de criptografia de arquivos chamada Proteção de Dados, enquanto os dados em computadores Mac são protegidos com uma tecnologia de criptografia de volumes chamada FileVault. De forma semelhante, a raiz das hierarquias de gerenciamento de chaves dos dois modelos fica no silício dedicado do Secure Enclave (nos dispositivos que possuem um SEP). Além disso, ambos fazem uso de um mecanismo AES dedicado para fornecer criptografia de alta velocidade e garantir que chaves de criptografia de longa duração nunca precisem ser fornecidas ao kernel do SO ou à CPU (onde podem ser comprometidas).

Além disso, os kernels do sistema operacional aplicam controles para impedir o acesso não autorizado a dados. Esses controles, na maioria das vezes, assumem a forma de apps com sandbox (o que restringe quais dados um app pode acessar), além de aplicar Cofres de Dados. Cofres de dados podem ser considerados como sandboxes invertidos. Em vez de restringir as chamadas que um app pode fazer, os Cofres de Dados restringem o acesso aos dados protegidos (novamente, aplicados pelo kernel, independente da criptografia do arquivo), independentemente de o processo originário ter sandbox ou não.

Como a Apple protege as informações pessoais dos usuários

Além de criptografar os dados em repouso, os dispositivos Apple usam várias técnicas, incluindo Cofre de Dados, para ajudar a impedir que apps acessem as informações pessoais de um usuário sem permissão. Nos Ajustes do iOS ou iPadOS ou nas Preferências do Sistema no macOS, os usuários podem ver quais a quais apps eles permitiram acessar certas informações, assim como conceder ou revogar qualquer acesso futuro. O acesso é controlado nos seguintes itens:

- *iOS, iPadOS e macOS:* Calendários, Câmera, Contatos, Microfone, Fotos, Lembretes, Reconhecimento de Fala
- *iOS e iPadOS:* Bluetooth, Casa, Mídia, apps de Mídia e Apple Music, Movimento e Preparo Físico
- *iOS e watchOS:* Saúde
- *macOS:* monitoramento de entrada (por exemplo, teclas pressionadas), solicitações, gravações da tela (por exemplo, capturas de tela estáticas e vídeos), Preferências do Sistema

Desde o iOS 13.4 e iPadOS 13.4, todos os apps de terceiros têm seus dados protegidos automaticamente em um Cofre de Dados. Isso ajuda a proteger contra o acesso não autorizado aos dados, mesmo a partir de processos que não usam sandbox.

Se o usuário iniciar a sessão no iCloud, os apps no iOS e iPadOS recebem acesso ao iCloud Drive por padrão. Os usuários podem controlar o acesso de cada app na seção iCloud dos Ajustes. Além disso, o iOS e iPadOS fornecem restrições que impedem o movimento de dados entre apps e contas instaladas através de uma solução de gerenciamento de dispositivos móveis (MDM) e aqueles instalados pelo usuário.

Função do Apple File System

O Apple File System (APFS) é um sistema de arquivos proprietário que foi projetado levando em consideração a criptografia. O APFS funciona em todas as plataformas Apple: iOS, iPadOS, macOS, tvOS e watchOS. Otimizado para armazenamento Flash/SSD, ele possui criptografia forte, metadados copiados na gravação, compartilhamento de espaço, clonagem de arquivos e diretórios, capturas, dimensionamento rápido de diretórios, primitivas atômicas de salvamento seguro e elementos básicos aprimorados de sistemas de arquivos, além de um projeto exclusivo de “copiar ao gravar” que usa aglutinação de E/S para proporcionar desempenho máximo sem deixar de garantir a confiabilidade dos dados.

O APFS aloca o espaço de armazenamento sob demanda. Quando um único contêiner APFS possui vários volumes, o espaço livre do contêiner é compartilhado e pode ser alocado a qualquer volume conforme necessário. Cada volume usa apenas parte do contêiner total, portanto o espaço disponível é o tamanho total do contêiner menos o espaço usado em todos os volumes nele contidos.

No macOS 10.15, um contêiner APFS usado para inicializar o Mac deve conter pelo menos cinco volumes, sendo os três primeiros ocultados do usuário:

- *Volume de Pré-inicialização:* contém os dados necessários para inicializar cada volume do sistema no contêiner
- *Volume de VM:* usado pelo macOS para armazenar arquivos de troca
- *Volume de Recuperação:* contém o recoveryOS
- *Volume do Sistema:* contém o seguinte:
  - Todos os arquivos necessários para inicializar o Mac
  - Todos os apps instalados nativamente pelo macOS (apps que costumavam ficar na pasta /Aplicativos agora ficam na pasta Sistema/Aplicativos)
- *Volume de Dados:* contém os dados sujeitos a mudança, como:

- Qualquer dado dentro da pasta do usuário, incluindo fotos, músicas, vídeos e documentos
- Apps instalados pelo usuário, incluindo aplicativos AppleScript e do Automator
- Frameworks e daemons personalizados instalados pelo usuário, organização ou apps de terceiros
- Outros locais de propriedade do usuário e nos quais ele pode gravar, como /Aplicativos, /Biblioteca, /Usuários, /Volumes, /usr/local, /private, /var e /tmp

Um volume de Dados é criado para cada volume de Sistema adicional. Os volumes de Pré-inicialização, VM e Recuperação são compartilhados, e não duplicados.

Nota: por padrão, nenhum processo pode gravar no volume de Sistema, até mesmo processos do sistema da Apple.

Proteção de Dados no iOS e iPadOS

Visão geral da Proteção de Dados

No iOS e iPadOS, a Apple usa uma tecnologia chamada Proteção de Dados para proteger os dados guardados no armazenamento flash do dispositivo. A Proteção de Dados permite que o dispositivo responda a eventos comuns, como ligações telefônicas, mas também possibilita um alto nível de criptografia nos dados de usuário. Os apps principais do sistema, como Mensagens, Mail, Calendário, Contatos, Fotos e os valores de dados do app Saúde usam a Proteção de Dados por padrão, e os apps de terceiros instalados no iOS 7 ou posterior e iPadOS 13.1 recebem essa proteção automaticamente.

Implementação

A Proteção de Dados é implementada pela construção e gerenciamento de uma hierarquia de chaves, aproveitando as tecnologias de criptografia de hardware integradas a dispositivos iOS e iPadOS. A Proteção de Dados é controlada por arquivo, atribuindo uma classe a cada um deles; a acessibilidade é determinada de acordo com a constatação do desbloqueio das chaves de classe. Com o advento do Apple File System (APFS), o sistema de arquivos agora pode subdividir ainda mais as chaves de acordo com um padrão por perímetro (onde partes de um arquivo podem ter chaves diferentes).

Arquitetura

No iOS e iPadOS, o armazenamento é dividido em dois volumes APFS:

- *Volume do Sistema:* o conteúdo do sistema é armazenado no volume do Sistema e os dados do usuário são armazenados no volume de Dados.
- *Volume de Dados:* sempre que um arquivo é criado no volume de dados, a Proteção de Dados cria uma nova chave de 256 bits (a chave única por arquivo) e a fornece ao mecanismo AES de hardware, que usa a chave para criptografar o arquivo conforme ele é gravado no armazenamento flash. A criptografia usa AES128 no modo XTS, onde a chave única por arquivo de 256 bits é dividida para fornecer chaves de ajuste e cifra de 128 bits cada.

Como os arquivos de dados são criados e protegidos

Em dispositivos com SoC A7, S2 ou S3, é utilizado o modo AES-CBC. O vetor de inicialização é calculado com o offset do bloco dentro do arquivo, criptografado com o hash SHA-1 da chave única por arquivo.

A chave única por arquivo (ou por extensão) é embalada por uma das várias chaves de classe, dependendo das circunstâncias em que se poderá acessar o arquivo. Como todos os outros embalamentos que usam o RFC 3394, este é executado usando o embalamento de chaves AES NIST. A chave única por arquivo embalada é armazenada nos metadados do arquivo.

Dispositivos com o formato APFS podem oferecer suporte à clonagem de arquivos (cópias de custo zero que usam a tecnologia "copiar ao gravar"). Se um arquivo for clonado, cada metade do clone recebe uma nova chave para aceitar gravações e permitir que novos dados sejam gravados na mídia com uma nova chave. Com o passar do tempo, o arquivo pode ser composto de várias extensões (ou fragmentos), cada um sendo mapeado a chaves diferentes. Entretanto, todas as extensões que compõem um arquivo são protegidas pela mesma chave de classe.

Quando um arquivo é aberto, seus metadados são descriptografados com a chave do sistema de arquivos, revelando a chave única por arquivo embalada e uma notação de qual classe o protege. A chave única por arquivo (ou por perímetro) é desembalada pela chave de classe e fornecida ao mecanismo AES de hardware, que descriptografa o arquivo conforme ele é lido do armazenamento flash. Todo o tratamento da chave do arquivo embalada ocorre no Secure Enclave; a chave do arquivo nunca é exposta diretamente à CPU Intel. No momento da inicialização, o Secure Enclave negocia uma chave transitória com o mecanismo AES. Quando o Secure Enclave desembala as chaves de um arquivo, elas são reembaladas pela chave transitória e enviadas de volta para o processador do aplicativo.

Os metadados de todos os arquivos no sistema de arquivos do volume de dados são criptografados com uma chave de volume aleatória, criada na primeira instalação do iOS ou iPadOS ou quando o dispositivo é apagado pelo usuário. Essa chave é criptografada e embalada por uma chave de embalamento de chaves conhecida apenas pelo Secure Enclave para armazenamento de longo prazo. A chave de embalamento de chaves é alterada sempre que o usuário apaga o dispositivo. Nos SoCs A9 (e posteriores), o Secure Enclave faz uso de entropia, assistida por um nonce antirreprodução, para possibilitar o apagamento e proteger sua chave de embalamento de chaves, além de outros materiais.

Assim como chaves únicas por arquivo ou por extensão, a chave de metadados do volume de dados nunca é exposta diretamente ao processador de aplicativos; o Secure Enclave fornece uma versão transitória única por inicialização. Quando armazenada, a chave criptografada do sistema de arquivos é embalada ainda por uma "chave apagável", armazenada no Armazenamento Apagável. Essa chave não oferece confidencialidade de dados adicional. Em vez disso, ela é projetada para ser apagada rapidamente sob demanda (por um usuário, por meio da opção "Apagar Todo o Conteúdo e Ajustes", ou por um usuário ou administrador ao emitir um comando de apagamento remoto a partir de uma solução de gerenciamento de dispositivos móveis (MDM), Microsoft Exchange ActiveSync ou iCloud). O apagamento de uma chave dessa maneira deixa todos os arquivos criptograficamente inacessíveis.

O conteúdo de um arquivo pode ser criptografado com uma ou mais chaves únicas por arquivo (ou por extensão) que são embaladas com uma chave de classe e armazenadas nos metadados de um arquivo que, por sua vez, é criptografado com a chave do sistema de arquivos. A chave de classe é protegida pelo UID do hardware e, em algumas classes, pelo código do usuário. Essa hierarquia fornece flexibilidade e bom desempenho. Por exemplo, a alteração da classe de um arquivo requer apenas que a chave única por arquivo seja reembalada e a alteração do código reembala somente a chave de classe.

Classes de Proteção de Dados

Quando um novo arquivo é criado em um dispositivo iOS ou iPadOS, o app que o criou atribui a ele uma classe. Cada classe usa políticas diferentes para determinar quando os dados podem ser acessados. As classes e políticas básicas são descritas nas seções a seguir.

Proteção Completa

(NSFileProtectionComplete): a chave de classe é protegida por uma chave derivada do código do usuário e do UID do dispositivo. Logo depois do usuário bloquear um dispositivo (10 segundos, se o ajuste em Exigir Senha for Imediatamente), a chave de classe descriptografada é descartada, deixando todos os dados nesta classe inacessíveis até que o usuário digite o código novamente ou use o Touch ID ou Face ID para desbloquear o dispositivo.

Protegido Exceto se Aberto

(NSFileProtectionCompleteUnlessOpen): talvez seja necessário gravar alguns arquivos enquanto o dispositivo estiver bloqueado. Um bom exemplo disso é o download em segundo plano de um anexo de e-mail. Esse comportamento é executado através do uso da criptografia assimétrica de curva elíptica (ECDH sobre Curve25519). A chave única por arquivo habitual é protegida por uma chave derivada que usa o Acordo de Chaves Diffie-Hellman de Um Passo, como descrito no NIST SP 800-56A.

A chave pública transitória do Acordo é armazenada em conjunto com a chave única por arquivo embalada. A KDF é a Função de Derivação da Chave de Concatenação (Alternativa Aprovada 1), como descrita em 5.8.1 do NIST SP 800-56A. O AlgorithmID é omitido. PartyUInfo é uma chave pública transitória e PartyVInfo é uma chave pública estática. SHA-256 é usado como a função hash. Assim que o arquivo é fechado, a chave única por arquivo é apagada da memória. Para abri-lo novamente, o segredo compartilhado é recriado usando a chave privada da classe Protegido Exceto se Aberto e a chave pública transitória do arquivo, que são usadas para desembalar a chave única por arquivo, que por sua vez, é usada para descriptografar o arquivo.

Protegido Até a Primeira Autenticação do Usuário

(NSFileProtectionCompleteUntilFirstUserAuthentication): essa classe se comporta da mesma maneira que a Proteção Completa, exceto pelo fato de que a chave de classe descriptografada não é removida da memória quando o dispositivo é bloqueado. A proteção desta classe tem propriedades semelhantes à criptografia de volume completo em computadores de mesa e protege os dados de ataques que envolvem reinicialização. Essa é a classe padrão de todos os dados de apps de terceiros que não tiverem sido atribuídos a uma classe de Proteção de Dados.

Sem Proteção

(NSFileProtectionNone): essa chave de classe é protegida apenas pelo UID e é mantida no Armazenamento Apagável. Como todas as chaves necessárias para descriptografar os arquivos desta classe são armazenadas no dispositivo, a criptografia oferece apenas o benefício do apagamento remoto rápido. Se um arquivo não for atribuído a uma classe de Proteção de Dados, ele ainda é armazenado criptografado (como todos os dados em um dispositivo iOS e iPadOS).

Tabela das classes de Proteção de Dados

Classe	Tipo de proteção
Classe A: Proteção Completa	(NSFileProtectionComplete)
Classe B: Protegido Exceto se Aberto	(NSFileProtectionCompleteUnlessOpen)
Classe C: Protegido Até a Primeira Autenticação do Usuário	(NSFileProtectionComplete UntilFirstUserAuthentication)
Classe D: Sem Proteção	(NSFileProtectionNone)

Acesso a chaves protegidas em modos de recuperação

Em dispositivos com SoCs Apple A10, A11 e S3, as chaves de classe protegidas pelo código do usuário não podem ser acessadas a partir do modo de Recuperação. Os SoCs A12 e S4 estendem essa proteção ao modo de Atualização do Firmware do Dispositivo (DFU).

O mecanismo AES do Secure Enclave é equipado com bits de núcleo de software bloqueáveis. Quando chaves são criadas a partir do UID, esses bits de núcleo são incluídos na função de derivação da chave para criar hierarquias de chave adicionais.

Desde os SoCs Apple A10 e S3, um bit de núcleo é dedicado a distinguir chaves protegidas pelo código do usuário. O bit de núcleo é definido para chaves que requerem o código de usuário (incluindo Proteção de Dados para chaves de Classe A, Classe B e Classe C) e removido para chaves que não requerem o código do usuário (incluindo a chave de metadados do sistema de arquivos e chaves da Classe D).

Em um SoC A12, a ROM de Inicialização do Secure Enclave bloqueia o bit de núcleo do código se o processador do aplicativo tiver entrado no modo DFU ou modo de Recuperação. Quando o bit de núcleo está bloqueado, nenhuma operação de alteração é permitida, o que impede o acesso a dados protegidos pelo código do usuário.

Nos SoCs Apple A10, A11, S3 e S4, o bit de núcleo do código é bloqueado pelo Sistema Operacional do Secure Enclave se o dispositivo tiver entrado no modo de Recuperação. Tanto a ROM de Inicialização do Secure Enclave quanto o sistema operacional verificam o Registro de Progresso de Inicialização (BPR) para determinar com segurança o modo atual.

Além disso, no iOS 13 e iPadOS 13.1 ou posterior em dispositivos com o A10 ou posterior, todos os dados do usuário ficam criptograficamente inacessíveis quando os dispositivos são inicializados no modo de Recuperação. Isso é feito por meio da introdução de um bit de núcleo adicional cuja definição governa a capacidade de acesso à chave de mídia, que por sua vez é necessária para acessar os metadados e, portanto, o conteúdo de todos os arquivos no volume de dados criptografados com a Proteção de Dados. Esta proteção engloba os arquivos protegidos em todas as classes (A, B, C e D), não apenas aqueles que exigem o código do usuário.

A restauração de um dispositivo depois que ele entra no modo DFU o leva novamente a um estado conhecidamente bom, com a certeza de que apenas código não modificado e assinado pela Apple está presente. O modo DFU pode ser acessado manualmente.

Consulte o artigo de Suporte da Apple a seguir para saber como colocar um dispositivo no modo DFU:

Dispositivo	Artigo
iPhone, iPad, iPod touch	Se você esqueceu o código de acesso do iPhone, iPad ou iPod touch ou o dispositivo está desativado
Apple TV	Restaurar a Apple TV

Proteção e classes de dados das Chaves

Visão geral da proteção de dados das Chaves

Muitos apps precisam gerenciar senhas e outros dados simples, porém sensíveis, como chaves e tokens de acesso. As Chaves do iOS e iPadOS oferecem uma maneira segura de armazenar esses itens.

Os itens das Chaves são criptografados usando duas chaves AES-256-GCM diferentes: uma chave de tabela (metadados) e uma chave por linha (chave secreta). Os metadados das Chaves (todos os atributos que não sejam kSecValue) são criptografados com a chave dos metadados para acelerar buscas, enquanto o valor secreto (kSecValueData) é criptografado com a chave secreta. A chave dos metadados é protegida pelo Secure Enclave, mas é armazenada em cache no processador de aplicativos para permitir consultas rápidas às chaves. A chave secreta sempre requer uma passagem completa pelo Secure Enclave.

As Chaves são implementadas na forma de um banco de dados SQLite, armazenado no sistema de arquivos. Existe apenas um banco de dados e o daemon `securityd` determina quais itens das Chaves cada processo ou app pode acessar. As APIs de acesso às chaves resultam em chamadas ao daemon, que consulta os direitos “grupos-acesso-Chaves”, “identificador-aplicativo” e “grupo-aplicativo” do app. Ao invés de limitar o acesso a um único processo, os grupos de acesso permitem que os itens das Chaves sejam compartilhados entre apps.

Os itens das Chaves podem ser compartilhados apenas entre apps do mesmo desenvolvedor. O gerenciamento disso é feito ao solicitar que apps de terceiros usem grupos de acesso com um prefixo a eles alocado através do Programa de Desenvolvedor da Apple, por meio de grupos de aplicativos. A exigência do prefixo e a exclusividade do grupo do aplicativo são aplicadas através da assinatura de código, perfis de provisão e o Programa de Desenvolvedor da Apple (em inglês).

Os dados das Chaves são protegidos usando uma estrutura de classes semelhante à usada na Proteção de Dados de arquivos. Essas classes apresentam comportamentos equivalentes às classes de Proteção de Dados de arquivos, mas usam chaves distintas e são parte das APIs que são denominadas de forma diferente.

Disponibilidade	Proteção de Dados de Arquivos	Proteção de Dados das Chaves
Quando desbloqueado	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
Enquanto bloqueado	NSFileProtectionCompleteUnlessOpen	NA
Depois do primeiro desbloqueio	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Sempre	NSFileProtectionNone	kSecAttrAccessibleAlways
Código ativado	NA	kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly

Os apps que utilizam serviços de atualização em segundo plano podem usar *kSecAttrAccessibleAfterFirstUnlock* para itens das Chaves que precisam ser acessados durante atualizações em segundo plano.

A classe *kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly* se comporta da mesma maneira que *kSecAttrAccessibleWhenUnlocked*, mas fica disponível apenas quando o dispositivo está configurado com um código. Essa classe existe somente na Keybag do sistema e:

- Não é sincronizada nas Chaves do iCloud;
- Não recebe backup;
- Não é incluída em keybags de guarda segura.

Se o código for removido ou redefinido, os itens serão inutilizados por meio do descarte das chaves de classe.

Outras classes das Chaves têm uma contraparte “Somente este dispositivo”, a qual está sempre protegida pelo UID ao ser copiada do dispositivo durante um backup, inutilizando-a caso ela seja restaurada em um dispositivo diferente. A Apple equilibrou segurança e usabilidade cuidadosamente, escolhendo classes de Chaves que dependem do tipo de informação sendo protegida e de quando o iOS e iPadOS precisam dela. Por exemplo, um certificado VPN deve estar sempre disponível para que o dispositivo mantenha uma conexão contínua, mas é classificado como “não migratório” para que não possa ser movido para outro dispositivo.

Proteções de classes de dados das Chaves

Para os itens das Chaves criados pelo iOS e iPadOS, as seguintes proteções de classe são exigidas:

Item	Acessível
Senhas de Wi-Fi	Depois do primeiro desbloqueio
Contas do Mail	Depois do primeiro desbloqueio
Contas do Microsoft Exchange ActiveSync	Depois do primeiro desbloqueio
Senhas de VPN	Depois do primeiro desbloqueio
LDAP, CalDAV, CardDAV	Depois do primeiro desbloqueio
Tokens de contas de redes sociais	Depois do primeiro desbloqueio
Chaves de criptografia de anúncio de Handoff	Depois do primeiro desbloqueio
Token do iCloud	Depois do primeiro desbloqueio
Senha do compartilhamento pessoal	Quando desbloqueado
Senhas do Safari	Quando desbloqueado
Favoritos do Safari	Quando desbloqueado
Backup do iTunes	Quando desbloqueado, não migratório
Certificados de VPN	Sempre, não migratório
Chaves do Bluetooth®	Sempre, não migratório
Token do Serviço de Notificações Push da Apple (APNs)	Sempre, não migratório
Certificados e chaves privadas do iCloud	Sempre, não migratório
Chaves do iMessage	Sempre, não migratório
Certificados e chaves privadas instalados por um perfil de configuração	Sempre, não migratório
PIN do SIM	Sempre, não migratório
Token do Buscar	Sempre
Voicemail	Sempre

Controle de acesso às Chaves

As Chaves podem usar listas de controle de acesso (ACLs) para definir políticas de acessibilidade e requisitos de autenticação. Os itens podem estabelecer condições que exijam a presença do usuário, especificando que os mesmos não poderão ser acessados a menos que o usuário tenha autenticado através do Touch ID, Face ID ou pela digitação do código do dispositivo. O acesso a itens também pode ser limitado ao especificar que os registros do Touch ID ou Face ID não tenham sido alterados desde que o item foi adicionado. Essa limitação ajuda a impedir que um invasor adicione sua própria impressão digital para acessar um item das Chaves. As ACLs são avaliadas no Secure Enclave e liberadas ao kernel somente se as restrições especificadas forem atendidas.

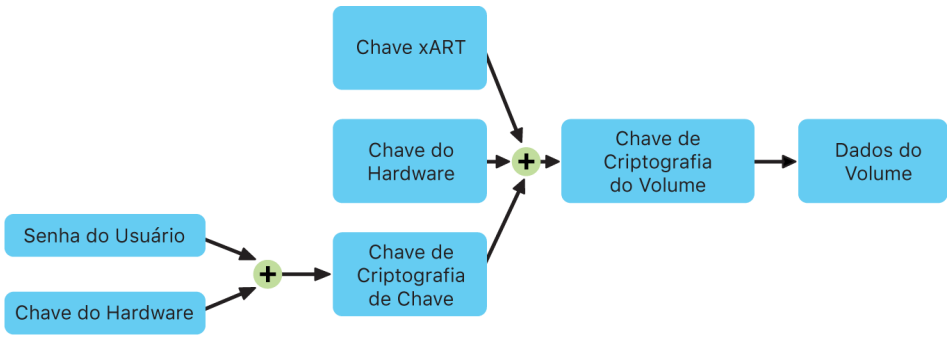
Criptografia no macOS

Criptografia do volume interno quando o FileVault está ativado

No Mac OS X 10.3 ou posterior, os computadores Mac oferecem o FileVault, um recurso integrado de criptografia para proteger todos os dados em repouso. O FileVault usa o algoritmo de criptografia de dados AES-XTS para proteger volumes inteiros em dispositivos de armazenamento internos e removíveis. Nos computadores Mac que possuem o chip Apple T2 Security, os dispositivos de armazenamento interno criptografados conectados diretamente ao chip T2 fazem uso dos recursos de segurança de hardware do chip. Depois que um usuário ativa o FileVault no Mac, suas credenciais são exigidas durante o processo de inicialização.

Sem credenciais de início de sessão válidas ou uma chave de recuperação criptográfica, o volume APFS interno (no macOS 10.15, isso inclui os volumes de Sistema e Dados) permanece criptografado e protegido contra acesso não autorizado, mesmo que o dispositivo de armazenamento físico seja removido e conectado a outro computador. A criptografia de volumes internos em um Mac com o chip T2 é implementada pela construção e gerenciamento de uma hierarquia de chaves, aproveitando as tecnologias de criptografia de hardware integradas ao chip. Esta hierarquia de chaves é projetada para cumprir simultaneamente quatro objetivos:

- Exigir a senha do usuário para descriptografia
- Proteger o sistema contra um ataque de força bruta diretamente contra mídias de armazenamento removidas do Mac
- Fornecer um método ágil e seguro para apagar conteúdos por meio do apagamento de materiais criptográficos necessários
- Permitir que os usuários alterem suas senhas (e, com isso, as chaves criptográficas usadas para proteger seus arquivos) sem a necessidade de criptografar novamente todo o volume



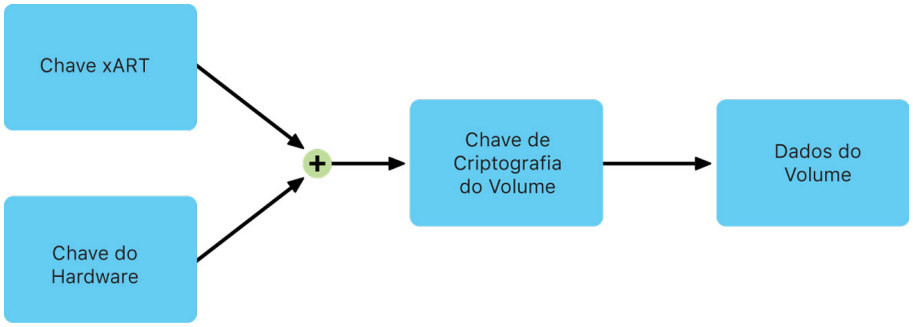
Criptografia do volume interno quando o FileVault está ativado no macOS.

Em computadores Mac com o chip T2, todo o tratamento de chaves do FileVault ocorre no Secure Enclave; as chaves de criptografia nunca são expostas diretamente à CPU Intel. Todos os volumes APFS são criados com uma chave de volume por padrão. O conteúdo do volume e os metadados são criptografados com essa chave do volume, que é embalada com a chave de classe. A chave de classe é protegida por uma combinação da senha do usuário e do UID do hardware quando o FileVault está ativado. Esta proteção é padrão nos computadores Mac que contêm o chip T2.

Nota: a criptografia de dispositivos de armazenamento externos não utiliza os recursos de segurança do chip Apple T2 Security, sendo realizada da mesma maneira que nos computadores Mac sem o chip T2.

Criptografia do volume interno quando o FileVault está desativado

Se o FileVault não estiver ativado em um Mac com o chip Apple T2 Security durante o processo inicial do Assistente de Configuração, o volume ainda é criptografado, mas a chave do volume é protegida apenas pelo UID do hardware no Secure Enclave.



Criptografia do volume interno quando o FileVault está desativado no macOS.

Se o FileVault for ativado posteriormente — um processo que é imediato, já que os dados já estavam criptografados — um mecanismo antirreprodução impede que a chave antiga (baseada apenas no UID do hardware) seja usada para descriptografar o volume. Assim, o volume é protegido por uma combinação da senha do usuário e do UID do hardware, como descrito anteriormente.

Apagamento de volumes com FileVault

Ao apagar um volume, a chave de volume é apagada com segurança pelo Secure Enclave. Isso impede o acesso futuro com essa chave, mesmo pelo Secure Enclave. Além disso, todas as chaves de volume são embaladas com uma chave de mídia. A chave de mídia não fornece nenhuma confidencialidade adicional dos dados, mas é feita para proporcionar o apagamento ágil e seguro dos dados porque, sem ela, é impossível descriptografá-los.

A chave de mídia está localizada no Armazenamento Apagável e foi projetada para ser apagada rapidamente sob demanda — por exemplo, ao usar o Buscar ou uma solução de gerenciamento de dispositivos móveis (MDM) para fazer o apagamento remoto. O Armazenamento Apagável acessa a tecnologia de armazenamento base (NAND, por exemplo) para endereçar e apagar diretamente um número pequeno de blocos em um nível bem baixo. O apagamento da chave de mídia dessa maneira deixa o volume criptograficamente inacessível.

Proteção contra ataques de força bruta e malware

Para impedir ataques de força bruta, quando o Mac é inicializado, não são permitidas mais de 30 tentativas de senha na Janela de Início de Sessão ou no uso do Modo de Disco de Destino, com intervalos de tempo cada vez maiores sendo impostos após tentativas incorretas. Os intervalos são aplicados pelo coprocessador Secure Enclave no chip T2. Se o Mac for reiniciado durante um intervalo programado, o intervalo ainda é imposto e o timer é reiniciado para o período atual.

Para impedir que malwares causem perda permanente de dados ao tentar atacar a senha do usuário, esses limites não são aplicados depois que o usuário iniciou uma sessão no Mac, mas são impostos novamente após a reinicialização. Se as 30 tentativas forem esgotadas, mais 10 tentativas estão disponíveis após a inicialização na Recuperação do macOS. Se elas também forem esgotadas, outras 60 tentativas estão disponíveis para cada mecanismo de recuperação do FileVault ativado (recuperação do iCloud, chave de recuperação do FileVault e chave institucional), totalizando um máximo de 180 tentativas adicionais. Depois que essas tentativas adicionais também são esgotadas, o Secure Enclave não processa mais nenhuma solicitação de descriptografar o volume ou verificar a senha e os dados da unidade tornam-se irrecuperáveis.

Para proteger dados em um ambiente empresarial, a TI deve definir e aplicar políticas de configuração do FileVault usando o gerenciamento de dispositivos móveis (MDM). As organizações têm várias opções de gerenciamento de volumes criptografados, como chaves de recuperação institucionais, pessoais (que podem ser opcionalmente armazenadas com o MDM por garantia) ou uma combinação de ambas. A alternância de chaves também pode ser definida como política no MDM.

Intervalos entre as tentativas de digitação da senha

Tentativas	Intervalo aplicado
1–14	Nenhuma
15–17	1 minuto
18–20	5 minutos
21–26	15 minutos
27–30	1 hora

Gerenciamento do FileVault

Uso do SecureToken

O Apple File System (APFS) no macOS 10.13 ou posterior altera a forma como as chaves de criptografia do FileVault são geradas. Nas versões anteriores do macOS em volumes CoreStorage, as chaves usadas no processo de criptografia do FileVault eram criadas quando um usuário ou organização ativava o FileVault em um Mac. No macOS em volumes APFS, as chaves são geradas ou durante a criação do usuário ou durante o primeiro início de sessão realizado por um usuário do Mac. Essa implementação das chaves de criptografia, o momento em que são geradas e a forma como são armazenadas fazem parte do SecureToken. Especificamente, um SecureToken é uma versão embalada de uma Chave de Criptografia de Chaves (KEK) protegida pela senha do usuário.

Ao implantar o FileVault no APFS, o usuário pode continuar a:

- Usar as ferramentas e processos existentes, como a guarda da Chave de Recuperação Pessoal (PRK) em uma solução de gerenciamento de dispositivos móveis (MDM)
- Criar e usar uma Chave de Recuperação Institucional (IRK)
- Adiar a ativação do FileVault até que um usuário inicie ou encerre uma sessão no Mac

Uso do Bootstrap Token

O macOS 10.15 apresenta um novo recurso, o Bootstrap Token, para ajudar na concessão de um SecureToken tanto para contas móveis quanto para a conta opcional de administrador criada no registro do dispositivo (“administrador gerenciado”). O administrador gerenciado pode ser criado ao configurar uma solução MDM para criá-lo durante o processo de registro que acontece com o Apple School Manager ou o Apple Business Manager. O uso do novo recurso Bootstrap Token do macOS 10.15 requer:

- Registro do Mac no MDM usando Apple School Manager ou Apple Business Manager
- Suporte do fornecedor do MDM

Nota: um Bootstrap Token não pode ser gerado automaticamente pelo macOS durante a configuração se a criação de uma conta de usuário local for completamente ignorada. No macOS 10.15.4 ou posterior, um Bootstrap Token é gerado para ser guardado no MDM quando qualquer usuário que tenha um SecureToken inicia a sessão pela primeira vez, caso a solução MDM seja compatível com o recurso. Um Bootstrap Token também pode ser gerado e guardado no MDM ao usar a ferramenta de linha de comando `profiles`, se necessário.

Quando o usuário configura o Mac por conta própria

Quando o usuário configura o Mac por conta própria, os departamentos de TI não aprovisionam o dispositivo. Todas as políticas e configurações são fornecidas por meio de uma solução de gerenciamento de dispositivos móveis (MDM) ou por ferramentas de gerenciamento de configuração. O Assistente de Configuração é usado para criar a conta de administrador local inicial e o usuário recebe um SecureToken. Se a solução MDM for compatível com o recurso Bootstrap Token e informar o Mac durante o registro no MDM, um Bootstrap Token é gerado pelo Mac e guardado pela solução MDM.

Se um Mac estiver registrado em uma solução MDM, dependendo dos recursos disponíveis no MDM, a conta inicial pode ser uma conta de administrador ou uma conta local. Se o usuário for rebaixado a um usuário padrão usando o MDM, ele recebe automaticamente um SecureToken. Se o usuário for rebaixado, a partir do macOS 10.15.4, nenhum Bootstrap Token é gerado.

Nota: se a criação da conta de usuário local for ignorada por completo usando o MDM e, em vez disso, um serviço de diretório com contas móveis for usado, o usuário do diretório não receberá um SecureToken durante o início de sessão e nenhum Bootstrap Token é gerado. Se não houver nenhum usuário com SecureToken no Mac, a conta móvel ainda pode ter o FileVault ativado através da ativação adiada e um SecureToken é concedido ao usuário no momento da ativação do FileVault. A partir do momento em o usuário tiver um SecureToken, no macOS 10.15.4 e posterior, um Bootstrap Token é gerado automaticamente e guardado na solução MDM ao iniciar a seção, caso o MDM seja compatível com o recurso.

Em qualquer um dos cenários acima, como o primeiro e principal usuário recebe um SecureToken, ele pode ter o FileVault ativado por meio da ativação adiada. A ativação adiada permite que a organização ative o FileVault, mas adie sua ativação até que um usuário inicie ou finalize uma sessão no Mac. Também é possível personalizar se o usuário pode ignorar a ativação do FileVault (opcionalmente, um número de vezes definido). O resultado é que o usuário principal do Mac (seja um usuário local de qualquer tipo ou uma conta móvel) pode desbloquear o dispositivo de armazenamento quando estiver criptografado com o FileVault.

Em computadores Mac nos quais um Bootstrap Token tenha sido gerado e guardado em uma solução MDM, se a conta do administrador gerenciado iniciar uma sessão no Mac em um momento futuro, o Bootstrap Token é usado para conceder automaticamente um SecureToken, o que significa que a conta também está ativada para o FileVault e pode desbloquear o volume FileVault. Para modificar a capacidade da conta do administrador gerenciado de desbloquear o volume, o usuário pode usar: `fdesetup remove -user`.

Quando o Mac é aprovisionado por uma organização

Quando o Mac é aprovisionado por uma organização antes de ser entregue a um usuário, o departamento de TI configura o dispositivo. A conta administrativa local criada no Assistente de Configuração do macOS usado para aprovisionar ou configurar o Mac recebe um SecureToken. No macOS 10.15, se a solução MDM for compatível com o recurso Bootstrap Token, um Bootstrap Token também é gerado durante o processo de configuração do macOS e guardado na solução MDM. Se a conta do administrador gerenciado iniciar uma sessão no Mac em um momento futuro, o Bootstrap Token é usado para conceder automaticamente um SecureToken.

Se o Mac for colocado em um serviço de diretório e configurado para criar contas móveis e se não houver um Bootstrap Token, os usuários do serviço de diretório são solicitados a informar, na primeira vez que iniciam uma sessão, o nome de usuário e senha de um administrador existente com SecureToken para fornecer um SecureToken às suas contas. As credenciais de administrador local usadas para configurar o Mac devem ser informadas. Se o SecureToken não for necessário, o usuário deve clicar em Ignorar. No macOS 10.13.5 ou posterior, é possível omitir por completo o diálogo do SecureToken se o FileVault não for usado com as contas móveis. Para omitir o diálogo do SecureToken, aplique um perfil de configuração com ajustes personalizados no MDM com as chaves e valores a seguir:

Ajuste	Valor
Domínio	com.apple.MCX
Chave	cachedaccounts.askForSecureTokenAuthBypass
Valor	True

Se a solução MDM for compatível com o recurso Bootstrap Token e um Bootstrap Token tiver sido gerado pelo Mac e estiver guardado na solução MDM, os usuários de contas móveis não verão esse aviso. Em vez disso, eles recebem automaticamente um SecureToken durante o início de sessão.

Se usuários locais adicionais forem necessários no Mac em vez de contas de um serviço de diretório, esses usuários locais recebem automaticamente um SecureToken quando são criados nas Preferências do Sistema > Usuários e Grupos por um administrador atual com SecureToken. Se for necessário usar a linha de comando para criar usuários locais, a ferramenta de linha de comando `sysadminctl` pode ser usada para criar usuários e capacitá-los para o SecureToken.

Nesses cenários, os usuários a seguir podem desbloquear o volume criptografado com FileVault:

- O administrador local original usado para o aprovisionamento
- Qualquer usuário adicional do serviço de diretório que tenha recebido o SecureToken durante o processo de início de sessão, seja de forma interativa usando o diálogo ou automática com o Bootstrap Token
- Qualquer usuário local novo criado nas Preferências do Sistema

Para modificar se contas específicas podem desbloquear o dispositivo de armazenamento, o usuário pode usar `fdesetup remove -user`.

Ao usar um dos fluxos de trabalho descritos acima, o SecureToken é gerenciado pelo macOS sem a necessidade de nenhuma configuração ou script adicional. Ele se torna um detalhe de implementação e não algo que precise ser gerenciado ou manipulado de forma ativa.

Uso de ferramentas de linha de comando

Há ferramentas de linha de comando disponíveis para o gerenciamento do Bootstrap Token, FileVault e SecureToken. O Bootstrap Token normalmente é gerado no Mac e guardado pela solução de gerenciamento de dispositivos móveis (MDM) durante o processo de configuração do macOS depois que a solução MDM informa ao Mac que ela é compatível com o recurso. Porém, um Bootstrap Token também pode ser gerado em um Mac que já tenha sido implantado. Por exemplo, se a solução MDM adicionar a compatibilidade com este recurso depois da implantação inicial do macOS 10.15. No macOS 10.15.4 ou posterior, um Bootstrap Token é gerado e guardado no MDM quando qualquer usuário que tenha um SecureToken ativado inicia a sessão pela primeira vez, caso a solução MDM seja compatível com o recurso. Isso reduz a necessidade de uso da ferramenta de linha de comando `profiles` depois de configurar o dispositivo para gerar e guardar um Bootstrap Token na solução MDM.

A ferramenta de linha de comando `profiles` tem algumas opções para interagir com o Bootstrap Token.

- `sudo profiles install -type bootstraptoken`: este comando gera um novo Bootstrap Token e o guarda na solução MDM. Este comando requer informações do administrador com SecureToken existente para gerar inicialmente o Bootstrap Token. Além disso, a solução MDM deve ser compatível com o recurso e o número de série do computador Mac deve aparecer no Apple School Manager ou Apple Business Manager e estar registrado nessa solução MDM específica.
- `sudo profiles remove -type bootstraptoken`: remove o Bootstrap Token existente no Mac e solução MDM.
- `sudo profiles status -type bootstraptoken`: informa se a solução MDM é compatível com o recurso Bootstrap Token e o estado atual do Bootstrap Token no Mac.

Ferramenta de linha de comando fdesetup

Configurações de MDM ou a ferramenta de linha de comando `fdesetup` podem ser usados para configurar o FileVault. No macOS 10.15 ou posterior, o uso de `fdesetup` para ativar o FileVault ao fornecer o nome de usuário e a senha não é mais usado e não será reconhecido em uma versão futura. Em vez disso, considere o uso da ativação adiada com o MDM. Para saber mais sobre a ferramenta de linha de comando `fdesetup`, abra o app Terminal e digite `man fdesetup` ou `fdesetup help` para obter mais informações.

Ferramenta de linha de comando sysadminctl

A ferramenta de linha de comando `sysadminctl` pode ser usada especificamente para modificar o estado do SecureToken de contas de usuário no Mac. Isso deve ser feito com cuidado e apenas quando necessário. A alteração do estado do SecureToken de um usuário por meio de `sysadminctl` sempre requer o nome de usuário e a senha de um administrador existente com SecureToken, seja de forma interativa ou por meio das opções correspondentes no comando. Tanto o comando `sysadminctl` quanto as Preferências do Sistema impedem o apagamento do último administrador ou usuário com SecureToken no Mac. Se a criação de usuários locais adicionais for realizada por meio de um script que use `sysadminctl`, para que esses usuários usem o SecureToken, credenciais atuais do administrador com SecureToken devem ser fornecidas, seja por meio da opção interativa ou diretamente com as opções `-adminUser` e `-adminPassword` de `sysadminctl`. Use `sysadminctl -h` para ver outras instruções de uso.

Códigos e senhas

Códigos

Ao configurar um código no dispositivo, o usuário ativa automaticamente a Proteção de Dados. O iOS e iPadOS oferecem suporte a códigos de seis e quatro dígitos, além de códigos alfanuméricos de tamanho arbitrário. Além de desbloquear o dispositivo, um código fornece entropia para certas chaves de criptografia. Isso significa que se um invasor se apossar de um dispositivo, ele não conseguirá acessar os dados em classes de proteção específicas sem o código.

O código é trançado ao UID do dispositivo, portanto, ataques de força bruta precisam ser realizados no dispositivo sendo atacado. Um grande número de iterações é usado para fazer com que as tentativas sejam cada vez mais lentas. O número de iterações é calibrado de forma que uma tentativa dure aproximadamente 80 milissegundos. Isso significa que levaria mais de cinco anos e meio para tentar todas as combinações de um código alfanumérico de seis caracteres com letras minúsculas e números.

Quanto mais forte for o código do usuário, mais forte se torna a chave de criptografia. O Touch ID e o Face ID podem ser usados para melhorar essa equação, permitindo que o usuário defina um código muito mais forte do que seria, de outra maneira, prático. Isso aumenta a quantidade efetiva de entropia que protege as chaves de criptografia usadas pela Proteção de Dados, sem prejudicar a experiência do usuário ao desbloquear um dispositivo iOS ou iPadOS várias vezes ao dia.

Para desencorajar ainda mais os ataques de força bruta ao código, há um incremento no tempo de atraso entre as tentativas depois que um código inválido é digitado na tela Bloqueada. Se Ajustes > Touch ID e Código > Apagar Dados estiver ativado, o dispositivo apaga os dados automaticamente após 10 tentativas incorretas consecutivas de digitação do código. Tentativas consecutivas do mesmo código incorreto não são contabilizadas no limite. Esse ajuste também está disponível como política administrativa através de uma solução de gerenciamento de dispositivos móveis (MDM) compatível com esse recurso e do Microsoft Exchange ActiveSync, podendo ser definido em um valor mais baixo.

Em dispositivos com Secure Enclave, os atrasos são exigidos pelo coprocessador do Secure Enclave. Se o dispositivo for reiniciado durante um atraso programado, o atraso ainda é imposto e o timer é reiniciado para o período atual.

Especificação de códigos mais longos

Se uma senha longa contendo apenas números for digitada, um teclado numérico é exibido na tela Bloqueada em vez do teclado completo. Pode ser mais fácil digitar um código numérico longo do que um código alfanumérico curto (a segurança fornecida por ambos é similar).

Os usuários podem selecionar “Código Alfanumérico Personalizado” nas “Opções de Código” em Ajustes > Código para especificar um código alfanumérico maior.

Intervalos entre as tentativas de digitação do código

Tentativas	Intervalo aplicado
1–4	Nenhuma
5	1 minuto
6	5 minutos
7–8	15 minutos
9	1 hora

Ativação segura de conexões de dados

Para melhorar a segurança e manter a usabilidade, é necessário Touch ID, Face ID ou digitação de código para ativar conexões de dados por meio de interface Lightning, USB ou Smart Connector, se nenhuma conexão de dados tiver sido estabelecida recentemente. Isso limita a superfície de ataque contra dispositivos conectados fisicamente, como carregadores maliciosos, ao mesmo tempo que permite o uso de outros acessórios dentro de limites de tempo razoáveis. Caso tenha se passado mais de uma hora desde que o dispositivo iOS ou iPadOS foi bloqueado ou desde que uma conexão de dados de um acessório foi terminada, o dispositivo não permitirá quaisquer conexões de dados novas até que o dispositivo seja desbloqueado. Durante esse período de uma hora, serão permitidas somente conexões de dados de acessórios que já tenham sido conectados anteriormente em estado desbloqueado. Esses acessórios são memorizados por 30 dias depois da última vez em que foram conectados. Tentativas de um acessório desconhecido para abrir uma conexão de dados durante esse período desativarão todas as conexões de dados por meio de Lightning, USB ou Smart Connector até que o dispositivo seja desbloqueado novamente. Esse período de uma hora:

- Garante que usuários frequentes de conexões a um Mac ou PC, a acessórios ou que usem conexão por fio ao CarPlay não precisarão digitar o código sempre que conectarem seu dispositivo.
- É necessário porque o ecossistema de acessórios não oferece uma maneira criptograficamente confiável de identificar acessórios antes de estabelecer uma conexão de dados.

Além disso, se tiverem se passado mais de três dias desde o estabelecimento de uma conexão de dados a um acessório, o dispositivo desautorizará novas conexões de dados imediatamente após o bloqueio. Isso aumenta a proteção de usuários que não costumam usar tais acessórios com frequência. As conexões de dados via Lightning, USB e Smart Connector também são desativadas sempre que o dispositivo está em um estado em que requer um código para reativar a autenticação biométrica.

O usuário tem a opção de reativar conexões de dados sempre ativas nos Ajustes (a configuração de alguns dispositivos assistivos faz isso automaticamente).

Função das senhas

Nos computadores Mac com o chip Apple T2 Security, a senha cumpre uma função semelhante à dos códigos discutidos acima, com a exceção de que a chave gerada é usada para criptografia do FileVault em vez de proteção de dados. o macOS também oferece opções adicionais de recuperação da senha:

- Recuperação do iCloud
- Recuperação do FileVault
- Chave institucional do FileVault

Autenticação e assinatura digital

Assinatura digital e criptografia

Listas de Controle de Acesso

Os dados das Chaves são particionados e protegidos com Listas de Controle de Acesso (ACLs). Assim, as credenciais armazenadas por apps de terceiros não podem ser acessadas por apps com identidades diferentes a menos que o usuário as aprove explicitamente. Essa proteção fornece o mecanismo para a proteção de credenciais de autenticação em dispositivos Apple para uma série de apps e serviços dentro da organização.

Mail

No app Mail, os usuários podem enviar mensagens assinadas e criptografadas digitalmente. O Mail descobre automaticamente, com distinção entre maiúsculas e minúsculas e conformidade com o RFC 5322, o endereço de e-mail, assunto ou nomes alternativos em certificados de assinatura digital e criptografia em tokens PIV conectados em smart cards compatíveis. Se uma conta de e-mail configurada corresponder a um endereço de e-mail em um certificado de assinatura digital ou criptografia em um token PIV conectado, o Mail mostra automaticamente o botão de assinatura na barra de ferramentas da janela de nova mensagem. Se o Mail tiver o certificado de criptografia de e-mail do destinatário ou puder descobri-lo na Lista de Endereços Global (GAL) do Microsoft Exchange, um ícone de cadeado desbloqueado aparece na barra de ferramentas da nova mensagem. Um ícone de cadeado bloqueado indica que a mensagem será enviada criptografada com a chave pública do destinatário.

S/MIME por mensagem

O iOS, iPadOS e macOS são compatíveis com S/MIME por mensagem. Isso significa que os usuários de S/MIME têm a opção de sempre assinar e criptografar mensagens por padrão ou selecionar mensagens individuais que desejam assinar e criptografar.

As identidades usadas com S/MIME podem ser disponibilizadas a dispositivos Apple por meio de um perfil de configuração, uma solução de gerenciamento de dispositivos móveis (MDM), o Simple Certificate Enrollment Protocol (SCEP) ou Autoridade de Certificação do Microsoft Active Directory.

Smart cards

O macOS 10.12 ou posterior possui compatibilidade nativa com cartões de verificação de identidade pessoal (PIV). Esses cartões são amplamente usados em organizações comerciais ou públicas para autenticação com dois fatores, assinatura digital e criptografia.

Os smart cards possuem uma ou mais identidades digitais que têm um par de chaves públicas e privadas e um certificado associado. O desbloqueio de um smart card com o número de identificação pessoal (PIN) fornece acesso às chaves privadas usadas nas operações de autenticação, criptografia e assinatura. O certificado determina o que uma chave pode fazer, quais atributos são associados a ela e se ela foi validada (assinada) por uma AC.

Os smart cards podem ser usados na autenticação com dois fatores. Os dois fatores necessários para desbloquear um cartão são "algo que o usuário possui" (o cartão) e "algo que o usuário sabe" (o PIN). O macOS 10.12 ou posterior também possui compatibilidade nativa com autenticação em janelas de início de sessão com smart card e autenticação por certificado de cliente a sites no Safari. Ele também é compatível com a autenticação do Kerberos por meio de pares de chaves (PKINIT), para início de sessão único em dispositivos compatíveis com Kerberos. Para saber mais sobre Smart cards e macOS, consulte Introdução à integração de smart card (em inglês) na *Referência de Implantação para Mac*.

Imagens de disco criptografadas

No macOS, as imagens de disco criptografadas atuam como contêineres seguros nos quais os usuários podem armazenar ou transferir documentos e outros arquivos sigilosos. As imagens de disco criptografadas são criadas com o Utilitário de Disco, localizado em /Aplicativos/Utilitários/. As imagens de disco podem ser criptografadas usando criptografia AES de 128 bits ou 256 bits. Como uma imagem de disco montada é tratada como um volume local conectado ao Mac, os usuários podem copiar, mover e abrir arquivos e pastas armazenados nela. Assim como com o FileVault, o conteúdo de uma imagem de disco é criptografado e descriptografado em tempo real. Para trocar documentos, arquivos e pastas de forma segura com imagens de disco criptografadas, os usuários podem salvar uma imagem de disco criptografada em uma mídia removível, enviá-la como anexo de e-mail ou armazená-la em um servidor remoto. Para obter mais informações sobre imagens de disco criptografadas, consulte o Manual do Usuário do Utilitário de Disco.

Arquitetura das Chaves no macOS

O macOS oferece um repositório, chamado Chaves, que armazena de forma conveniente e segura nomes de usuário e senhas, incluindo identidades digitais, chaves de criptografia e notas seguras. Ele pode ser acessado por meio do app Acesso às Chaves em /Aplicativos/Utilitários/. O uso das Chaves elimina a necessidade de digitar (ou mesmo de lembrar) as credenciais de cada recurso. Um conjunto inicial e padrão de chaves é criado para cada usuário do Mac, embora os usuários possam criar outros conjuntos com objetivos específicos.

Além das chaves do usuário, o macOS usa uma série de chaves do sistema que mantêm ativos de autenticação que não são específicos do usuário, como credenciais de rede e identidades de infraestrutura de chave pública (PKI). Um desses conjuntos de chaves, o Raízes do Sistema, é imutável e armazena certificados de autoridades de certificação (AC) raiz de PKI da internet para a realização de tarefas comuns como transações bancárias on-line e e-commerce. De forma semelhante, o usuário pode implantar certificados de AC fornecidos internamente em computadores Mac gerenciados para ajudar a validar sites e serviços internos.

Keybags

Visão geral das keybags no iOS e iPadOS

As chaves das classes de arquivo e da Proteção de Dados das Chaves são coletadas e gerenciadas em keybags. O iOS e iPadOS usam as seguintes keybags: usuário, dispositivo, backup, guarda e Backup do iCloud.

Keybag do usuário

A keybag do usuário é onde as chaves de classe embaladas, usadas em operações normais, são armazenadas. Por exemplo, quando um código é digitado, a *NSFileProtectionComplete* é carregada a partir da keybag do usuário e desembalada. Ela é um arquivo binário de lista de propriedades (.plist) armazenado na classe Sem Proteção.

No caso de dispositivos com SoCs anteriores ao A9, o conteúdo do arquivo .plist é criptografado com uma chave guardada no Armazenamento Apagável. Para oferecer mais segurança às keybags, essa chave é apagada e gerada novamente sempre que um usuário altera seu código.

No caso de dispositivos com o SoC A9 ou posterior, o arquivo .plist contém uma chave que indica que a keybag está armazenada em um cofre protegido por um nonce antirreprodução controlado pelo Secure Enclave.

O Secure Enclave gerencia a keybag do usuário e pode ser consultado sobre o estado de bloqueio de um dispositivo. Ele informa que o dispositivo está desbloqueado somente se todas as chaves de classe da keybag do usuário estiverem acessíveis e desembaladas corretamente.

Keybag do dispositivo

A keybag do dispositivo é usada para armazenar as chaves de classe embaladas usadas em operações que envolvem dados específicos do dispositivo. Os dispositivos iOS e iPadOS configurados para uso compartilhado às vezes precisam de acesso a credenciais antes que um usuário tenha iniciado uma sessão. Portanto é necessária uma keybag que não esteja protegida pelo código do usuário.

O iOS e iPadOS não são compatíveis com a separação criptográfica do conteúdo do sistema de arquivos por cada usuário, o que significa que o sistema usa chaves de classe da keybag do dispositivo para embalar chaves únicas por arquivo. Porém, as Chaves usam chaves de classe da keybag do usuário para proteger itens nas Chaves do usuário. Em dispositivos iOS e iPadOS configurados para uso de um único usuário (configuração padrão), a keybag do dispositivo e a keybag do usuário são uma só e a mesma, protegidas pelo código do usuário.

Keybag de backup

A keybag de backup é criada quando o iTunes (no macOS 10.14 ou anterior) ou o Finder (macOS 10.15 ou posterior) fazem um backup criptografado que é armazenado no computador onde o backup do dispositivo foi feito. Uma nova keybag é criada com um novo conjunto de chaves e os dados do backup são criptografados novamente com essas novas chaves. Como explicado anteriormente, os itens não migratórios das Chaves permanecem embalados pela chave derivada do UID, permitindo que eles sejam restaurados para o dispositivo do qual o backup foi feito originalmente, mas deixando-os inacessíveis em um dispositivo diferente.

A keybag — protegida com a senha definida no iTunes (no macOS 10.14 ou anterior) ou Finder (macOS 10.15 ou posterior) — é processada por 10 milhões de iterações do PBKDF2. Apesar dessa contagem de iteração extensa, não há vínculos com um dispositivo específico e, portanto, teoricamente, seria possível tentar um ataque de força bruta à keybag do backup usando vários computadores em paralelo. Essa ameaça pode ser atenuada com uma senha suficientemente forte.

Se um usuário decidir não criptografar o backup, os arquivos não são criptografados, independentemente de suas classes de Proteção de Dados, mas as Chaves permanecem protegidas por uma chave derivada do UID. É por isso que os itens das Chaves são migrados para um novo dispositivo apenas se uma senha de backup for definida.

Keybag de guarda

A keybag de guarda é usada para a sincronização com o iTunes e o gerenciamento de dispositivos móveis (MDM). Essa keybag permite o backup e a sincronização do iTunes sem exigir que o usuário digite uma senha e permite também que uma solução MDM limpe o código de um usuário remotamente. Ela é armazenada no computador usado para sincronizar com o iTunes ou na solução MDM que gerencia o dispositivo remotamente.

A keybag de guarda melhora a experiência do usuário durante a sincronização do dispositivo, o que potencialmente requer acesso a todas as classes de dados. Quando um dispositivo bloqueado por código é conectado pela primeira vez ao iTunes, o usuário é solicitado a digitar um código. Em seguida, o dispositivo cria uma keybag de guarda que contém as mesmas chaves de classe usadas no dispositivo, protegida por uma nova chave recém-gerada. A keybag de guarda e a chave que a protege são divididas entre o dispositivo e o host ou servidor, com os dados armazenados no dispositivo na classe Protegido Até a Primeira Autenticação do Usuário. É por isso que o código do dispositivo deve ser digitado antes que o usuário faça um backup no iTunes da primeira vez após uma reinicialização.

No caso de uma atualização de software sem fio (OTA), é solicitado que o usuário digite o código ao iniciar a atualização. Isso é feito para criar, de forma segura, um Token de Desbloqueio único, o qual desbloqueia a keybag do usuário depois da atualização. Esse token não pode ser gerado sem que o código do usuário seja digitado e todos os tokens gerados anteriormente são invalidados se o código do usuário for alterado.

Os Tokens de Desbloqueio Único servem para atualizações de software feitas com ou sem supervisão. Eles são criptografados com uma chave derivada do valor atual de um contador monotônico no Secure Enclave, o UUID da keybag e o UID do Secure Enclave.

No caso de dispositivos com SoCs anteriores ao A9, o aumento do contador do Token de Desbloqueio de uso único no Secure Enclave invalida todos os tokens existentes. O contador aumenta quando um token é usado, depois do primeiro desbloqueio de um dispositivo reiniciado, quando uma atualização de software é cancelada (pelo usuário ou pelo sistema) ou quando o timer da política de um token tiver expirado.

Nos SoCs A9 (e posteriores), o Token de Desbloqueio não reutilizável não usa mais contadores ou o Armazenamento Apagável. Em vez disso, ele é protegido por um nonce antirreprodução controlado pelo Secure Enclave.

O Token de Desbloqueio de uso único de atualizações de software supervisionadas expira depois de 20 minutos. Em versões anteriores ao iOS 13, esse token é exportado do Secure Enclave e gravado no Armazenamento Apagável. Um timer da política aumenta o contador se o dispositivo não tiver sido reinicializado nos últimos 20 minutos. No iOS 13 e iPadOS 13.1, o token é armazenado em um cofre protegido pelo Secure Enclave.

Atualizações de software automáticas ocorrem quando o sistema detecta que há uma atualização disponível e:

- As atualizações automáticas estão configuradas no iOS 12 (ou posterior)

ou

- O usuário escolhe “Instalar Mais Tarde” ao receber a notificação sobre a atualização

Após o usuário digitar seu código, um Token de Desbloqueio não reutilizável é gerado e pode permanecer válido no Secure Enclave por até oito horas. Se a atualização ainda não tiver ocorrido, o Token de Desbloqueio não reutilizável será destruído a cada bloqueio e recriado a cada desbloqueio subsequente. Cada desbloqueio reinicia a contagem de oito horas. Após oito horas, um timer de política invalida o Token de Desbloqueio não reutilizável.

Keybag do Backup do iCloud

A keybag do Backup do iCloud assemelha-se à keybag de backup. Todas as chaves de classe nessa keybag são assimétricas (usando Curve25519, como a classe de Proteção de Dados “Protegido Exceto se Aberto”). Uma keybag assimétrica também é usada para o backup no aspecto de recuperação de Chaves das Chaves do iCloud.

Segurança de Apps

Visão geral da segurança de apps

Os apps estão entre os elementos mais importantes de uma arquitetura de segurança moderna. Eles oferecem aos usuários benefícios incríveis na produtividade, mas também têm o potencial de impactar negativamente a segurança e estabilidade do sistema, assim como os dados do usuário, se não forem gerenciados corretamente.

Por isso, a Apple fornece camadas de proteção para assegurar que os apps estejam livres de malwares conhecidos e que não tenham sido adulterados. Proteções adicionais garantem que o acesso dos apps aos dados dos usuários seja cuidadosamente mediado. Esses controles de segurança proporcionam uma plataforma segura e estável para os apps, permitindo que milhares de desenvolvedores ofereçam centenas de milhares de apps para iOS, iPadOS e macOS — tudo isso sem afetar a integridade do sistema. Os usuários podem acessar esses apps em seus dispositivos Apple sem terem medo de vírus, malware ou ataques não autorizados.

No iPhone, iPad e iPod touch, todos apps são obtidos na App Store (e todos são sandboxed), proporcionando os controles mais restritivos.

No Mac, muitos apps são obtidos na App Store, mas os usuários de Mac também baixam e usam apps da internet. Para proporcionar segurança nos downloads da internet, o macOS tem camadas adicionais de controles. Primeiramente, por padrão no macOS 10.15 ou posterior, todos os apps para Mac precisam ser autenticados pela Apple para iniciar. Esse requisito garante que esses apps estejam livres de malwares conhecidos sem exigir que os apps sejam fornecidos pela App Store. Além disso, o macOS possui uma proteção antivírus de ponta para bloquear (e, se necessário, remover) malware.

Como um controle adicional nas diferentes plataformas, o sandbox ajuda a proteger os dados dos usuários contra acesso não autorizado de apps. No macOS, os dados em áreas importantes ficam eles próprios em sandbox, garantindo que os usuários mantenham o controle do acesso de todos os apps aos arquivos na Mesa, Documentos, Downloads e outras áreas, estejam esses apps em sandbox ou não.

Capacidade nativa	**Equivalente de terceiros**
Lista de plug-ins não aprovados, lista de extensões do Safari não aprovadas	Definições de Vírus/Malware
Quarentena de arquivo	Definições de Vírus/Malware
Assinaturas do XProtect/Yara	Definições de Vírus/Malware

Capacidade nativa	Equivalente de terceiros
MRT (Ferramenta de Remoção de Malware)	Proteção no ponto final
Gatekeeper	Proteção no ponto final. Exige a assinatura de apps para garantir a execução apenas de softwares confiáveis.
eficheck (Necessário para computadores Mac sem o chip Apple T2 Security)	Proteção no ponto final — detecção de rootkit
Firewall de aplicativo	Proteção no ponto final — uso de firewall
Filtro de Pacotes (pf)	Soluções de firewall
Proteção da Integridade do Sistema	Apenas a Apple pode fornecer isso
Controles de Acesso Obrigatórios	Apenas a Apple pode fornecer isso
Lista de exclusão de KEXT	Apenas a Apple pode fornecer isso
Assinatura obrigatória do código de apps	Apenas a Apple pode fornecer isso
Autenticação de apps	Apenas a Apple pode fornecer isso

Segurança de apps no iOS e iPadOS

Visão geral da segurança de apps no iOS e iPadOS

Ao contrário de outras plataformas de dispositivos móveis, o iOS e iPadOS não permitem que os usuários instalem apps não assinados e potencialmente maliciosos de sites ou executem apps não confiáveis. Durante a execução, verificações de assinatura de código de todas as páginas de memória executáveis são feitas conforme elas são carregadas para garantir que o app não tenha sido modificado desde que foi instalado ou atualizado pela última vez.

Após a confirmação de que o app provém de uma fonte confiável, o iOS e iPadOS aplicam medidas de segurança criadas para impedir que ele comprometa outros apps ou o restante do sistema.

Processo de assinatura de código de apps

Assinatura obrigatória de código

Depois de ser iniciado, o kernel do iOS e iPadOS controla quais processadores e apps podem ser executados. Para garantir que todos os apps provenham de uma fonte conhecida e aprovada e que não tenham sido adulterados, o iOS e iPadOS exigem que todos os códigos executáveis sejam assinados por um certificado emitido pela Apple. Os apps fornecidos com o dispositivo, como o Mail e o Safari, são assinados pela Apple. Os apps de terceiros também precisam ser validados e assinados por um certificado emitido pela Apple. A assinatura de código obrigatória estende o conceito de cadeia de confiança do sistema operacional aos apps e impede que apps de terceiros carreguem recursos de código não assinado ou usem código que se modifique sozinho.

Como os desenvolvedores assinam os apps

Validação de certificado

Para desenvolver e instalar apps em dispositivos iOS e iPadOS, os desenvolvedores devem se registrar na Apple e se associar ao Programa de Desenvolvedor da Apple. A identidade real de cada desenvolvedor, seja ele um indivíduo ou uma empresa, é verificada pela Apple antes da emissão de seu certificado. Esse certificado permite que os desenvolvedores assinem e enviem apps à App Store para distribuição. Como resultado, todos os apps que estão na App Store foram enviados por uma pessoa ou organização identificável, o que mitiga a criação de apps maliciosos. Os apps também foram revisados pela Apple para garantir que funcionem de forma geral como descrito e não contenham erros óbvios ou outros problemas marcantes. Além da tecnologia já discutida, esse processo de curadoria permite que os usuários possam confiar na qualidade dos apps que adquirem.

Validação de bibliotecas dinâmicas

O iOS e iPadOS permitem que os desenvolvedores integrem frameworks aos seus apps, que podem ser usados pelo próprio app ou por extensões integradas a ele. Para proteger o sistema e outros apps do carregamento de códigos de terceiros em seu espaço de endereço, o sistema executa uma validação da assinatura de código de todas as bibliotecas dinâmicas das quais um processo depende ao ser aberto. Essa verificação é realizada através do identificador da equipe (ID da Equipe), extraído do certificado emitido pela Apple. O identificador da equipe é uma string alfanumérica de 10 caracteres, como 1A2B3C4D5F, por exemplo. Um programa pode depender de qualquer biblioteca de plataforma fornecida com o sistema ou qualquer biblioteca com o mesmo identificador de equipe na assinatura de código do executável principal. Como os executáveis fornecidos como parte do sistema não possuem um identificador de equipe, eles só podem depender de bibliotecas fornecidas com o próprio sistema.

Verificação de apps empresariais

As empresas também podem desenvolver apps próprios para uso interno e distribuí-los aos seus funcionários. As empresas e organizações podem se candidatar ao Programa Empresarial de Desenvolvedor da Apple (ADEP) com um número D-U-N-S. A Apple aprova os candidatos depois de verificar suas identidades e elegibilidades. Após se tornar membro do ADEP, uma organização pode se registrar para obter um perfil de provisão que permite que os apps desenvolvidos internamente sejam executados nos dispositivos que ela autoriza.

Os usuários precisam ter o perfil de provisão instalado para executar esses apps. Isso garante que apenas usuários autorizados possam carregar os apps em seus dispositivos iOS e iPadOS. Os apps instalados por meio do gerenciamento de dispositivos móveis (MDM) são implicitamente confiáveis porque o relacionamento entre a organização e o dispositivo já está estabelecido. Caso contrário, os usuários precisam aprovar o perfil de provisão do app nos Ajustes. As organizações podem restringir a aprovação de apps de desenvolvedores desconhecidos por seus usuários. Ao abrir um app empresarial pela primeira vez, o dispositivo precisa receber uma confirmação positiva da Apple, indicando que o app tem permissão para ser executado.

Segurança do processo em tempo de execução

Sandbox

Todos os apps de terceiros são “sandboxed” e, portanto, não podem acessar os arquivos armazenados por outros apps ou fazer alterações no dispositivo. O sandbox impede que um app colete ou modifique informações armazenadas por outros apps. Cada app possui um diretório inicial exclusivo para seus arquivos, atribuído aleatoriamente quando o app é instalado. Se um app de terceiros precisar acessar informações que não as suas próprias, ele usará os serviços fornecidos explicitamente pelo iOS e iPadOS.

Os arquivos e recursos do sistema também são protegidos dos apps do usuário. A maior parte do iOS e iPadOS é executado como o usuário não privilegiado “mobile”, assim como todos os apps de terceiros. Toda a partição do sistema operacional é montada como somente leitura. Ferramentas desnecessárias, como serviços de início de sessão remoto, não estão incluídas no software do sistema e as APIs não permitem que apps ampliem seus próprios privilégios para modificar outros apps ou o iOS e iPadOS.

Uso de direitos

O acesso de apps de terceiros a informações do usuário e recursos, como o iCloud e a extensibilidade, é controlado através de direitos declarados. Os direitos são pares chave-valor assinados em um app e permitem a autenticação além dos fatores de tempo de execução, como o ID de usuário UNIX. Os direitos não podem ser alterados, já que são assinados digitalmente. Os direitos são usados extensivamente pelos daemons e apps do sistema para realizar operações privilegiadas específicas que, de outra forma, necessitariam que o processo fosse executado como root. Isso reduz de maneira significativa a possibilidade do aumento de privilégio de um daemon ou app do sistema comprometido.

Além disso, os apps só podem executar processamento em segundo plano através das APIs fornecidas pelo sistema. Isso permite que os apps continuem a funcionar sem prejudicar o desempenho ou impactar dramaticamente a vida útil da bateria.

Proteções adicionais

Aleatorização do Espaço de Endereço

A Aleatorização de Espaço de Endereço (ASLR) protege contra a exploração de erros de corrupção da memória. Os apps integrados usam a ASLR para garantir que todas as regiões da memória sejam aleatorizadas na inicialização. A organização aleatória dos endereços de memória do código executável, das bibliotecas do sistema e dos construtos de programação relacionados reduz a possibilidade de diversos aproveitamentos sofisticados. Por exemplo, um ataque return-to-libc tenta enganar um dispositivo para que ele execute um código malicioso através da manipulação dos endereços das bibliotecas de contêineres e do sistema. A aleatorização do posicionamento desses itens dificulta o ataque, especialmente em larga escala. O Xcode, o ambiente de desenvolvimento para iOS ou iPadOS, compila automaticamente os programas de terceiros com o suporte à ASLR ativo.

Nunca Executar

O iOS e iPadOS fornecem uma proteção ainda maior através do recurso Nunca Executar (XN) do ARM, que marca páginas de memória como não executáveis. As páginas de memória marcadas como graváveis e executáveis podem ser usadas por apps apenas sob condições rigorosamente controladas: o kernel verifica a presença de direitos dinâmicos de assinatura de código somente da Apple. Mesmo assim, apenas uma única chamada mmap pode ser feita para solicitar uma página executável e gravável, que recebe um endereço aleatorizado. O Safari usa essa funcionalidade em seu compilador JavaScript JIT.

Compatibilidade com extensões

O iOS e iPadOS permitem que os apps forneçam funcionalidade a outros apps através de extensões. As extensões são binários executáveis assinados de finalidade específica, empacotados em um app. Durante a instalação, o sistema detecta automaticamente as extensões e usa um sistema de correspondência para disponibilizá-las a outros apps.

Pontos de extensão

Uma área de sistema que oferece suporte a extensões é chamada de ponto de extensão. Cada ponto de extensão fornece APIs e aplica regras para tal área. O sistema determina quais extensões estão disponíveis com base em regras de correspondência de ponto de extensão específicas. O sistema abre os processos de extensão automaticamente conforme a necessidade e gerencia a sua vida útil. Direitos podem ser usados para restringir a disponibilidade das extensões a certos apps do sistema. Por exemplo, um widget da visualização “Hoje” é exibido apenas na Central de Notificações e uma extensão de compartilhamento só está disponível no painel Compartilhamento. Exemplos de pontos de extensão são: widgets Hoje, Compartilhar, Ações, Edição de Fotos, Provedor de Arquivos e Teclado Personalizado.

Como as extensões se comunicam

As extensões são executadas em seus próprios espaços de endereço. A comunicação entre a extensão e o app a partir do qual ela foi ativada usa comunicações interprocessuais mediadas pelo framework do sistema. Elas não têm acesso aos arquivos ou espaços de memória umas das outras. As extensões são criadas para serem isoladas umas das outras, dos apps que as contêm e dos apps que as usam. Elas são sandboxed como qualquer outro app de terceiro e possuem um contêiner separado do contêiner do app que as contém. Entretanto, elas compartilham o mesmo acesso aos controles de privacidade do app em que estão contidas. Portanto, se um usuário conceder a um app acesso aos Contatos, esse acesso também é concedido às extensões integradas ao app, mas não às extensões ativadas por ele.

Como os teclados personalizados são usados

Os teclados personalizados são um tipo especial de extensão, já que são ativadas pelo usuário para todo o sistema. Quando ativada, uma extensão de teclado é usada em qualquer campo de texto, exceto para a digitação do código e em visualizações de texto seguro. Para restringir a transferência de dados do usuário, os teclados personalizados são executados por padrão em um sandbox bastante restritivo que bloqueia o acesso à rede, a serviços que executam operações de rede em nome de um processo e a APIs que poderiam permitir que a extensão extraísse dados digitados. Os desenvolvedores de teclados personalizados podem solicitar Acesso Aberto às suas extensões, o que permite que o sistema execute a extensão no sandbox padrão após obter o consentimento do usuário.

MDM e extensões

No caso de dispositivos inscritos em uma solução de gerenciamento de dispositivos móveis (MDM), as extensões de documento e de teclado seguem as regras "Abrir com Gerenciado". Por exemplo, a solução MDM pode impedir que um usuário exporte um documento de um app gerenciado para um Provedor de Documentos não gerenciado ou use um teclado não gerenciado com um app gerenciado. Além disso, os desenvolvedores de apps podem impedir o uso de extensões de teclado de terceiros em seus apps.

Adoção da Proteção de Dados em apps

O Kit de Desenvolvimento de Software (SDK) do iOS e iPadOS oferece um conjunto completo de APIs que facilitam a adoção da Proteção de Dados por terceiros e desenvolvedores empresariais e ajudam a garantir o nível mais alto de proteção para seus apps. A Proteção de Dados está disponível para APIs de banco de dados e de arquivos, incluindo NSFileManager, CoreData, NSData e SQLite.

O banco de dados do app Mail (incluindo anexos), livros gerenciados, favoritos do Safari, imagens de abertura do app e dados de localização também são armazenados por meio de criptografia, com chaves protegidas pelo código do usuário no dispositivo. Os apps Calendário (excluindo anexos), Contatos, Lembretes, Notas, Mensagens e Fotos implementam o privilégio de Proteção de Dados "Protegido Até a Primeira Autenticação do Usuário".

Os apps instalados pelo usuário que não optam por uma classe específica de Proteção de Dados recebem "Protegido Até a Primeira Autenticação do Usuário" por padrão.

Participação de um Grupo de Apps

Apps e extensões de propriedade de uma certa conta de desenvolvedor podem compartilhar conteúdo quando configurados como parte de um Grupo de Apps. Cabe ao desenvolvedor criar os grupos apropriados no Portal Apple Developer e incluir o conjunto de apps e extensões desejados. Quando configurados para ser parte de um Grupo de Apps, os apps têm acesso ao seguinte:

- Um contêiner compartilhado no volume para armazenamento, que permanece no dispositivo enquanto houver ao menos um app do grupo instalado;
- Preferências compartilhadas;
- Itens compartilhados das Chaves.

O Portal Apple Developer assegura a exclusividade dos IDs de Grupo (GID) de Apps por todo o ecossistema de apps.

Verificação de acessórios

O programa de licenciamento Made for iPhone, iPad e iPod touch (MFi) fornece a fabricantes de acessórios verificados o acesso ao Protocolo de Acessórios para iPod (iAP) e aos componentes de hardware de suporte necessários.

Quando um acessório MFi se comunica com um dispositivo iOS ou iPadOS usando um conector Lightning ou por meio de Bluetooth, o dispositivo solicita que o acessório comprove ter sido autorizado pela Apple, respondendo com um certificado fornecido pela Apple, verificado pelo dispositivo. Então, o dispositivo envia um desafio e o acessório precisa respondê-lo com uma resposta assinada. Esse processo é gerenciado completamente por um circuito integrado (CI) personalizado que a Apple fornece a fabricantes de acessórios aprovados, sendo transparente ao acessório em si.

Os acessórios podem solicitar acesso a diferentes funcionalidades e métodos de transporte, como por exemplo, o acesso a transmissões de áudio digital através do cabo Lightning ou às informações de localização fornecidas por Bluetooth. Um CI de autenticação garante que apenas os acessórios aprovados possuam acesso total ao dispositivo. Se um acessório não oferecer suporte à autenticação, seu acesso é limitado ao áudio analógico e a um pequeno subconjunto de controles de reprodução de áudio serial (UART).

O AirPlay também usa o CI de autenticação para verificar se os receptores foram aprovados pela Apple. As transmissões de áudio AirPlay e vídeo CarPlay usam o MFi-SAP (Protocolo de Associação Segura), o qual usa AES-128 no modo CTR para criptografar a comunicação entre o acessório e o dispositivo. As chaves transitórias são trocadas usando a troca de chaves ECDH (Curve25519) e assinadas usando a chave RSA de 1024 bits do CI de autenticação como parte do protocolo Station-to-Station (STS).

Segurança de apps no macOS

Visão geral da segurança de apps no macOS

A segurança de apps no macOS consiste em uma série de camadas sobrepostas, das quais a primeira é a opção de executar apenas apps assinados e confiáveis da App Store. Além disso, o macOS dispõe proteções em camadas para garantir que apps baixados da internet não tenham malwares conhecidos. Ele oferece tecnologias para detectar e remover malware, além de proteções adicionais projetadas para impedir que apps não confiáveis acessem dados do usuário. Em última análise, os usuários do macOS estão livres para operar dentro do modelo de segurança que faz sentido para eles, mesmo que isso signifique executar códigos totalmente não assinados e não confiáveis.

Processo de assinatura do código de apps no macOS

Todos os apps da App Store são assinados pela Apple para assegurar que não tenham sido adulterados ou alterados. A Apple assina todos os apps fornecidos com os dispositivos Apple.

No macOS 10.15, todos os apps distribuídos fora da App Store devem ser assinados pelo desenvolvedor com um certificado Developer ID emitido pela Apple (combinado com uma chave privada) e autenticados pela Apple para serem executados com os ajustes padrão do Gatekeeper. Os apps desenvolvidos internamente também devem ser assinados com um Developer ID emitido pela Apple para que os usuários possam validar sua integridade.

No macOS, a assinatura de código e a autenticação funcionam de forma independente com fins diferentes (e podem ser realizados por atores diferentes). A assinatura de código é realizada pelo desenvolvedor usando o certificado Developer ID (emitido pela Apple) e a verificação dessa assinatura comprova para o usuário que o software do desenvolvedor não foi adulterado desde que o desenvolvedor o compilou e assinou. A autenticação pode ser realizada por qualquer pessoa na cadeia de distribuição de software e comprova que a Apple recebeu uma cópia do código para verificar a existência de malwares e que nenhum malware conhecido foi encontrado. A saída da autenticação é um tíquete, que é armazenado nos servidores da Apple e pode ser opcionalmente grampeado no app (por qualquer pessoa) sem invalidar a assinatura do desenvolvedor.

Os Controles de Acesso Obrigatórios (MACs) requerem a assinatura de código para usar direitos protegidos pelo sistema. Por exemplo, os apps que exigem acesso através do firewall devem ter seu código assinado com o direito MAC correspondente.

Gatekeeper e proteção em tempo de execução

Gatekeeper

O macOS traz uma tecnologia chamada de Gatekeeper que garante que, por padrão, apenas softwares confiáveis sejam executados no Mac do usuário. Quando um usuário baixa e abre um app, um plug-in ou um pacote de instalação de fora da App Store, o Gatekeeper verifica se o software provém de um desenvolvedor identificado, é autenticado pela Apple para garantir a ausência de conteúdo malicioso e não foi alterado. O Gatekeeper também solicita a aprovação do usuário antes de abrir softwares baixados pela primeira vez para garantir que o usuário não tenha sido enganado com o objetivo de abrir um código executável que acreditava ser apenas um arquivo de dados.

Por padrão, o Gatekeeper garante que todo software baixado tenha sido assinado pela App Store ou por um desenvolvedor registrado e tenha sido autenticado pela Apple. Tanto o processo de revisão da App Store quanto o canal de autenticação garantem que os apps não contenham malwares conhecidos. Portanto, *todo software no macOS é verificado em busca de conteúdo malicioso conhecido na primeira vez que é aberto, independentemente da forma como tenha chegado ao Mac*.

Os usuários e as organizações têm a opção de permitir apenas softwares instalados a partir da App Store. Além disso, os usuários podem substituir as políticas do Gatekeeper e abrir qualquer software, a menos que isso seja restringido pela solução de gerenciamento de dispositivos móveis (MDM). As organizações podem usar o MDM para configurar os ajustes do Gatekeeper, incluindo a permissão de softwares assinados com identidades alternativas. Caso necessário, o Gatekeeper também pode ser desativado por completo.

O Gatekeeper protege contra a distribuição de plug-ins maliciosos com apps benignos, em que o uso do app aciona o carregamento de um plug-in malicioso sem o conhecimento do usuário. Quando necessário, o Gatekeeper abre apps a partir de locais aleatórios somente leitura, impedindo o carregamento automático de plug-ins distribuídos com o app.

Proteção em tempo de execução

Os arquivos de sistema, recursos e o kernel são protegidos do espaço de apps do usuário. Todos os apps da App Store são sandboxed para restringir o acesso a dados armazenados por outros apps. Se um app da App Store precisar acessar dados de outro app, ele só pode fazer isso por meio do uso de APIs e serviços fornecidos pelo macOS.

Proteção contra malware

XProtect

O macOS inclui uma tecnologia antivírus de ponta, chamada Xprotect, para a detecção de malware com base em assinatura, e seu uso oferece suporte às práticas recomendadas de proteção contra vírus e malware. O sistema usa assinaturas YARA, as quais são atualizadas regularmente pela Apple. A Apple monitora novas infecções e variantes de malware, e atualiza automaticamente as assinaturas (independentemente das atualizações do sistema) para ajudar a proteger computadores Mac de infecções por malware. O XProtect detecta e bloqueia automaticamente a execução de malwares conhecidos. No macOS 10.15 ou posterior, o XProtect busca conteúdo malicioso conhecido sempre que um app:

- É aberto pela primeira vez
- Tenha sido alterado

Quando o XProtect detecta um malware conhecido, o software é bloqueado e o usuário é notificado, recebendo a opção de movê-lo para o Lixo.

Ferramenta de Remoção de Malware

Se um malware conseguir chegar ao Mac, o macOS também possui uma tecnologia para solucionar as infecções. A Ferramenta de Remoção de Malware (MRT) é um mecanismo do macOS que remedia infecções com base em atualizações fornecidas automaticamente pela Apple (como parte das atualizações automáticas dos arquivos de dados do sistema e das atualizações de segurança). Além de monitorar a atividade de malwares no ecossistema para poder revogar Developer IDs (se aplicável) e lançar atualizações do XProtect, a Apple também lança atualizações da MRT para remover malware de qualquer sistema afetado que esteja configurado para receber atualizações automáticas de segurança. A MRT remove malware ao receber informações atualizadas e continua verificando infeções ao reiniciar e iniciar a sessão. A MRT não reinicializa o Mac automaticamente.

Atualizações automáticas de segurança

A Apple lança as atualizações do XProtect e da ferramenta de remoção de malware automaticamente, com base nas informações mais recentes disponíveis sobre ameaças. Por padrão, o macOS busca essas atualizações diariamente. Para obter mais informações sobre as atualizações automáticas de segurança, consulte o artigo de Suporte da Apple: Atualizações automáticas de segurança.

Controle do acesso de apps a arquivos

A Apple acredita que os usuários devem ter total transparência, consentimento e controle do que os apps fazem com os seus dados. No macOS 10.15, este modelo é aplicado pelo sistema para garantir que todos os apps devam obter o consentimento do usuário antes de acessar arquivos em Documentos, Downloads, Mesa, iCloud Drive ou volumes na rede. No macOS 10.13 ou posterior, os apps que exigem acesso a todo o dispositivo de armazenamento devem ser adicionados explicitamente nas Preferências do Sistema. Além disso, as funcionalidades de acessibilidade e automação requerem a permissão do usuário para assegurar que não contornem outras proteções. Dependendo da política de acesso, os usuários podem receber uma solicitação ou devem alterar o ajuste nas Preferências do Sistema > Segurança e Privacidade > Privacidade:

Item	App faz solicitação ao usuário	Usuário deve editar os ajustes de privacidade do sistema
Acessibilidade		✓
Acesso total ao armazenamento interno		✓
Arquivos e pastas *Nota:* inclui: Mesa, Documentos, Downloads, volumes de rede e volumes removíveis	✓	
Automação (eventos da Apple)	✓	

Os itens que estão no Lixo do usuário são protegidos de qualquer app que use o Acesso Total ao Disco; o usuário não é solicitado para o acesso do app. Se o usuário desejar que os apps acessem os arquivos, eles devem ser movidos do Lixo para um outro local.

Os usuários que ativarem o FileVault no Mac são solicitados a fornecer credenciais válidas antes de continuar o processo de inicialização e obter acesso a modos de inicialização especializados. Sem credenciais de início de sessão válidas ou uma chave de recuperação, todo o volume permanece criptografado e protegido contra acesso não autorizado, mesmo que o dispositivo de armazenamento físico seja removido e conectado a outro computador.

Para proteger dados em um ambiente empresarial, a TI deve definir e aplicar políticas de configuração do FileVault usando o gerenciamento de dispositivos móveis (MDM). As organizações têm várias opções de gerenciamento de volumes criptografados, como chaves de recuperação institucionais, pessoais (que podem ser opcionalmente armazenadas com o MDM por garantia) ou uma combinação de ambas. A alternância de chaves também pode ser definida como política no MDM.

Recursos de segurança no app Notas

Notas Seguras

O app Notas inclui um recurso de Notas Seguras, que permite aos usuários protegerem os conteúdos de notas específicas. As notas seguras são criptografadas de ponta a ponta por meio de uma senha fornecida pelo usuário que é exigida para a visualização das notas no iOS, iPadOS, macOS e no site do iCloud. Cada conta do iCloud (incluindo contas de dispositivos "Em Meu") pode ter uma senha separada.

Quando um usuário utiliza uma nota segura, uma chave de 16 bytes é derivada da senha do usuário por meio de PBKDF2 e SHA256. A nota e todos os seus anexos são criptografados usando AES-GCM. Novos registros são criados no Core Data e CloudKit para armazenar a nota criptografada, os anexos, a etiqueta e o vetor de inicialização. Depois da criação dos novos registros, os dados originais não criptografados são apagados. Entre os anexos compatíveis com criptografia estão: imagens, desenhos, tabelas, mapas e sites. Notas que contêm outros tipos de anexos não podem ser criptografadas e anexos incompatíveis não podem ser adicionados a notas seguras.

Para visualizar uma nota segura, o usuário deve inserir a senha ou se autenticar usando o Touch ID ou Face ID. Depois que o usuário é autenticado com sucesso, tanto para visualizar ou criar uma nota segura, o app Notas abre uma sessão segura. Enquanto a sessão segura estiver aberta, o usuário pode visualizar ou proteger outras notas sem autenticação adicional. Contudo, a sessão segura aplica-se somente às notas protegidas com a senha fornecida. O usuário ainda precisa se autenticar no caso de notas protegidas por uma senha diferente. A sessão segura é fechada quando:

- O usuário toca no botão Bloquear Agora no app Notas
- O Notas é enviado para segundo plano por mais de 3 minutos (8 minutos no macOS)
- O dispositivo iOS ou iPadOS é bloqueado

Para alterar a senha de uma nota segura, o usuário deve inserir a senha atual, pois o Touch ID e Face ID não estão disponíveis durante a alteração da senha. Depois de escolher uma nova senha, o app Notas reembala as chaves de todas as notas existentes na mesma conta que estejam criptografadas pela senha anterior.

Se o usuário digitar a senha incorretamente três vezes seguidas, o app Notas mostra uma dica fornecida pelo usuário, caso ela tenha sido fornecida pelo usuário na configuração. Se ainda assim não se lembrar da senha, o usuário pode redefini-la nos ajustes do app Notas. Esse recurso permite que os usuários criem novas notas seguras com uma nova senha, mas não permitirá que eles vejam notas seguras anteriores. As notas asseguradas anteriormente ainda poderão ser visualizadas se a senha antiga for lembrada. A redefinição da senha requer a frase-senha da conta do iCloud do usuário.

Notas Compartilhadas

As notas que não estão criptografadas de ponta a ponta com uma senha podem ser compartilhadas com outras pessoas. As notas compartilhadas ainda usam o tipo de dado criptografado CloudKit para qualquer tipo de texto ou anexo colocado em uma nota pelo usuário. Os materiais sempre são criptografados com uma chave que é criptografada no CKRecord. Metadados, como as datas de criação e modificação, não são criptografados. O CloudKit gerencia o processo pelo qual os participantes podem criptografar e descriptografar os dados uns dos outros.

Recursos de segurança no app Atalhos

No app Atalhos, os atalhos são sincronizados opcionalmente com todos os dispositivos Apple que usam o iCloud. Atalhos também podem ser compartilhados com outros usuários por meio do iCloud. Os atalhos são armazenados localmente em um formato criptografado.

Os atalhos personalizados são versáteis – são similares a scripts ou programas. Ao baixar atalhos da internet, o usuário é avisado de que o atalho não foi revisado pela Apple e recebe a oportunidade de inspecioná-lo. Para proteger contra atalhos maliciosos, definições atualizadas de malware são baixadas para identificar atalhos maliciosos no tempo de execução.

Os atalhos personalizados também podem executar JavaScript especificado pelo usuário em sites no Safari quando chamados a partir da folha de compartilhamento. Para proteger contra códigos JavaScript maliciosos que, por exemplo, enganem o usuário para executar um script em um site de rede social que colete seus dados, o JavaScript é validado em relação às definições de malware mencionadas anteriormente. Na primeira vez que um usuário executa JavaScript em um domínio, o usuário é solicitado a permitir que atalhos contendo JavaScript sejam executados na página atual desse domínio.

Segurança de Serviços

Visão geral da segurança dos serviços

A Apple criou um conjunto robusto de serviços para que os seus dispositivos sejam muito mais úteis para os usuários e os ajudem a ser mais produtivos. Esses serviços incluem ID Apple, iCloud, Iniciar sessão com a Apple, Apple Pay, iMessage, FaceTime e Buscar.

Esses serviços oferecem capacidades poderosas para armazenamento e sincronização na nuvem, autenticação, pagamento, mensagem, comunicações e muito mais, tudo isso enquanto protege a privacidade do usuário e a segurança de seus dados.

Nota: nem todos os serviços e conteúdos da Apple estão disponíveis em todos os países ou regiões.

ID Apple e ID Apple gerenciado

Visão geral do ID Apple e ID Apple gerenciado

O ID Apple é a conta usada para iniciar a sessão em serviços da Apple como o iCloud, iMessage, FaceTime, iTunes Store, App Store, app Apple TV e Loja de Livros, dentre outros. É importante que os usuários mantenham seus IDs Apple em segurança para impedir o acesso não autorizado às suas contas. Para ajudar com isso, os IDs Apple requerem senhas fortes que:

- Devem ter pelo menos oito caracteres
- Devem conter tanto letras quanto números
- Não devem conter mais do que três caracteres idênticos consecutivos
- Não podem ser senhas usadas com frequência

Os usuários são encorajados a exceder essas diretrizes através da adição de caracteres extras e sinais de pontuação para tornar suas senhas ainda mais fortes.

A Apple também notifica os usuários por e-mail ou notificações push quando alterações importantes são feitas às suas contas; por exemplo, se uma senha ou informação de cobrança for alterada ou se o ID Apple for usado para iniciar a sessão em um novo dispositivo. Se algo estiver fora do esperado, os usuários são instruídos a alterar a senha do ID Apple imediatamente.

Além disso, a Apple emprega diversas políticas e procedimentos feitos para proteger as contas dos usuários. Isso inclui limitar o número de tentativas de início de sessão e redefinição de senha, o monitoramento ativo contra fraude para ajudar na identificação de ataques à medida que ocorrem e revisões regulares das políticas, o que permite à Apple adaptar-se a quaisquer informações novas que possam afetar a segurança do usuário.

Nota: a política de senha do ID Apple Gerenciado é definida por um administrador do Apple School Manager ou Apple Business Manager.

Autenticação de dois fatores com ID Apple

Para ajudar usuários a dar ainda mais segurança às suas contas, a Apple oferece a autenticação de dois fatores, uma camada extra de segurança para IDs Apple. Ela foi desenvolvida para garantir que somente o proprietário da conta possa acessar a conta, mesmo que mais alguém saiba a senha. Com a autenticação de dois fatores, a conta do usuário pode ser acessada apenas em dispositivos autorizados, como o iPhone, iPad, iPod touch ou Mac do usuário, ou em outros dispositivos após uma verificação feita a partir de um desses dispositivos autorizados ou de um número de telefone autorizado. Para iniciar a sessão pela primeira vez em qualquer dispositivo novo, são necessárias duas informações: a senha do ID Apple e um código de verificação de seis dígitos que é exibido nos dispositivos autorizados do usuário ou enviado para um número de telefone autorizado. Ao digitar o código, o usuário confirma que autoriza o dispositivo novo e que é seguro iniciar a sessão. Como apenas uma senha não é mais suficiente para acessar a conta de um usuário, a autenticação de dois fatores melhora a segurança do ID Apple do usuário e de todas as informações pessoais que ele armazena junto à Apple. Ela é integrada diretamente ao iOS, iPadOS, macOS, tvOS, watchOS e aos sistemas de autenticação usados pelos sites da Apple.

Quando o usuário inicia uma sessão em um site da Apple com um navegador, uma solicitação de segundo fator é enviada a todos os dispositivos autorizados associados à conta do iCloud do usuário, solicitando a aprovação da sessão web. Nos casos em que o usuário inicia a sessão no site da Apple com um navegador em um dispositivo autorizado, ele vê o código exibido localmente no dispositivo que está usando. Ao digitá-lo, a sessão web com o dispositivo autorizado do usuário é aprovada.

Recuperação de conta

Ao usar um dispositivo de confiança para redefinir a senha do ID Apple, uma conta do ID Apple pode ser restaurada se a senha for esquecida. Se um dispositivo de confiança não estiver disponível, mas a senha for conhecida, um número de telefone pode ser usado para autenticar através da verificação por SMS. Além disso, um código usado anteriormente pode ser usado para redefinir um ID Apple em conjunto com a verificação por SMS para fornecer a recuperação imediata de um ID Apple. Se essas opções não forem possíveis, o processo de recuperação da conta deve ser seguido. Consulte o artigo de Suporte da Apple Recuperar o ID Apple caso não seja possível redefinir a senha.

Verificação de duas etapas com ID Apple

Desde 2013, a Apple também oferece um método de segurança semelhante, chamado de verificação de duas etapas. Quando a verificação de duas etapas está ativada, a identidade do usuário deve ser verificada com um código temporário enviado para um dos dispositivos de confiança do usuário. A verificação de duas etapas é exigida antes que alterações sejam permitidas nas informações da conta do ID Apple; antes de iniciar a sessão no iCloud, iMessage, FaceTime ou Game Center; e antes que uma compra seja feita com um novo dispositivo na iTunes Store, App Store, app Apple TV ou Apple Books. Uma Chave Reserva de 14 caracteres também é fornecida aos usuários para que ela seja armazenada em um local seguro, caso esqueçam as senhas ou percam o acesso aos dispositivos autorizados. Embora recomende-se que a maioria dos usuários use a autenticação de dois fatores, ainda há algumas situações onde é preferível usar a verificação de duas etapas.

IDs Apple Gerenciados

Os IDs Apple Gerenciados funcionam de maneira bem semelhante a um ID Apple, mas são de propriedade e controle de empresas ou organizações de ensino. Essas organizações podem redefinir senhas, limitar compras e comunicações como FaceTime e Mensagens, além de configurar permissões por cargo para funcionários, professores e alunos.

Em IDs Apple Gerenciados, alguns serviços da Apple são desativados (por exemplo, Apple Pay, Chaves do iCloud, HomeKit e Buscar).

Inspeção de IDs Apple Gerenciados

Os IDs Apple Gerenciados também oferecem suporte à inspeção, o que permite que as organizações atendam a regulamentações legais e de privacidade. Um administrador, gerente ou professor do Apple School Manager pode inspecionar contas específicas de ID Apple Gerenciado.

Os inspetores podem monitorar apenas as contas que estão abaixo deles na hierarquia da organização. Por exemplo, professores podem monitorar alunos, gerentes podem inspecionar professores e alunos, e administradores podem inspecionar gerentes, professores e alunos.

Quando credenciais de inspeção são solicitadas através do Apple School Manager, é gerada uma conta especial que dá acesso somente ao ID Apple Gerenciado para o qual a inspeção foi solicitada. Assim o inspetor pode ler e modificar o conteúdo do usuário armazenado no iCloud ou em apps compatíveis com o CloudKit. Todas as solicitações de acesso de auditoria são registradas no Apple School Manager. Os registros mostram quem foi o inspetor, o ID Apple Gerenciado para o qual ele solicitou acesso, a hora da solicitação e se a inspeção foi realizada.

IDs Apple Gerenciados e dispositivos pessoais

Os IDs Apple Gerenciados também podem ser usados em dispositivos iOS e iPadOS e computadores Mac de propriedade individual. Para iniciar a sessão no iCloud, os alunos usam o ID Apple Gerenciado emitido pela instituição e uma senha adicional para uso doméstico, que serve como o segundo fator do processo de autenticação de dois fatores do ID Apple. Durante o uso de um ID Apple Gerenciado em um dispositivo pessoal, as Chaves do iCloud não ficam disponíveis e a instituição pode restringir outros recursos, como FaceTime ou Mensagens. Qualquer documento do iCloud criado por alunos enquanto tiverem uma sessão iniciada está sujeito à auditoria, conforme descrito anteriormente nesta seção.

iCloud

Visão geral do iCloud

O iCloud armazena contatos, calendários, fotos, documentos e outros itens de um usuário, mantendo as informações atualizadas em todos os dispositivos do usuário automaticamente. O iCloud também pode ser usado por apps de terceiros para armazenar e sincronizar documentos, assim como valores essenciais de dados de apps, conforme definido pelo desenvolvedor. Para configurar o iCloud, o usuário inicia a sessão com um ID Apple e escolhe quais serviços deseja usar. Certos recursos do iCloud, iCloud Drive, e Backup do iCloud podem ser desativados por administradores de TI com perfis de configuração de gerenciamento de dispositivos móveis (MDM). O serviço não leva em consideração aquilo que é armazenado e lida com o conteúdo de arquivos da mesma maneira, como uma coleção de bytes.

Cada arquivo é dividido em pedaços e criptografado pelo iCloud com AES-128 e uma chave derivada do conteúdo de cada pedaço. Essas chaves usam SHA-256. As chaves e os metadados do arquivo são armazenados pela Apple na conta do iCloud do usuário. Os pedaços criptografados do arquivo são armazenados sem qualquer informação que identifique o usuário nem as chaves, usando serviços de armazenamento da Apple e de terceiros (como Amazon Web Services ou Google Cloud Platform), mas esses parceiros não têm as chaves para descriptografar os dados do usuário armazenados nos servidores deles.

iCloud Drive

O iCloud Drive adiciona chaves baseadas em conta para proteger documentos armazenados no iCloud. O iCloud Drive divide e criptografa o conteúdo dos arquivos e armazena as partes criptografadas em serviços de terceiros. No entanto, as chaves de conteúdo do arquivo são embaladas por chaves de registro armazenadas com os metadados do iCloud Drive. Por sua vez, essas chaves de registro são protegidas pela Chave de Serviço do iCloud Drive do usuário, que é então armazenada na conta do iCloud do usuário. Os usuários obtêm acesso aos metadados de seus documentos do iCloud através da autenticação no iCloud, mas eles também precisam ter a Chave de Serviço do iCloud Drive para expor partes protegidas do armazenamento do iCloud Drive.

Backup do iCloud Drive

O iCloud também faz o backup de informações — incluindo os ajustes do dispositivo, dados de apps, fotos e vídeos do Rolo da Câmera e conversas do app Mensagens — diariamente via Wi-Fi. O iCloud criptografa o conteúdo para dar segurança ao transmiti-lo pela internet, armazenando-o em formato criptografado e usando tokens de segurança para a autenticação. O Backup do iCloud ocorre somente quando o dispositivo está bloqueado, conectado a uma fonte de alimentação e possui acesso via Wi-Fi à internet. Por conta da criptografia usada no iOS e iPadOS, o Backup do iCloud é feito para manter os dados seguros e, ao mesmo tempo, permitir que ocorram backups incrementais não supervisionados e restaurações.

Quando arquivos são criados em classes de Proteção de Dados que não estão acessíveis quando o dispositivo está bloqueado, suas chaves únicas por arquivo são criptografadas pelas chaves de classe da keybag do Backup do iCloud, com um backup feito no iCloud em seus estados originais criptografados. Todos os arquivos são criptografados durante o trânsito e, quando armazenados, criptografados com chaves baseadas em conta, conforme descrito em CloudKit.

A keybag do Backup do iCloud contém chaves assimétricas (Curve25519) para as classes de Proteção de Dados que não estão acessíveis quando o dispositivo está bloqueado. O conjunto do backup é armazenado na conta do iCloud do usuário e consiste em uma cópia dos arquivos do usuário e a keybag do Backup do iCloud. A keybag do Backup do iCloud é protegida por uma chave aleatória, também armazenada no conjunto do backup (a senha do iCloud do usuário não é usada para a criptografia, portanto a alteração da senha do iCloud não invalida os backups existentes).

Enquanto o banco de dados das Chaves do usuário tiver um backup no iCloud, ele continuará protegido por uma chave trançada ao UID. Isso permite que as Chaves sejam restauradas apenas no mesmo dispositivo onde foram originadas e significa que ninguém, nem mesmo a Apple, pode ler os itens das Chaves do usuário.

Ao restaurar, os arquivos que tenham backup, a keybag do Backup do iCloud e a chave da keybag são obtidos da conta do iCloud do usuário. A keybag do Backup do iCloud é descriptografada com sua própria chave. Em seguida, as chaves únicas por arquivo na keybag são usadas para descriptografar os arquivos no conjunto do backup, os quais são gravados no sistema de arquivos como novos arquivos, sendo criptografados novamente de acordo com suas classes de Proteção de Dados.

Conteúdo do Backup do iCloud

O Backup do iCloud faz o backup do conteúdo a seguir:

- Registros de músicas, filmes, programas de TV, apps e livros comprados. O Backup do iCloud de um usuário inclui informações sobre o conteúdo comprado presente no dispositivo, mas não o conteúdo comprado em si. Ao restaurar um Backup do iCloud, o conteúdo comprado de um usuário é baixado automaticamente da iTunes Store, App Store, app Apple TV ou Apple Books. Alguns tipos de conteúdo não são transferidos automaticamente em todos os países ou regiões. Além disso, compras anteriores podem estar indisponíveis caso tenham sido ressarcidas ou não estejam mais disponíveis na loja. O histórico de compras completo é associado ao ID Apple de um usuário.

- Fotos e vídeos nos dispositivos do usuário. Observe que, se o usuário ativar as Fotos do iCloud no iOS 8.1, iPadOS 13.1 ou OS X 10.10.3 (ou posterior), suas fotos e vídeos já estão armazenados no iCloud, não sendo incluídos no Backup do iCloud do usuário.
  - iOS 8.1 ou posterior
  - iPadOS 13.1
  - OS X 10.10.3 ou posterior
- Contatos, eventos do calendário, lembretes e notas
- Ajustes do dispositivo
- Dados de apps
- Tela de Início e organização dos apps
- Configuração do HomeKit
- Dados da Ficha Médica
- Senha do Visual Voicemail (requer o cartão SIM usado durante o backup)
- Mensagens do iMessage, Bate-papo de Negócios, de texto (SMS) e MMS (requer o cartão SIM usado durante o backup)

Quando Mensagens no iCloud está ativado, as mensagens do iMessage, Chat de Negócios, texto (SMS) e MMS são removidas do Backup do iCloud existente do usuário e armazenadas em um contêiner criptografado de ponta a ponta do CloudKit para o app Mensagens. O Backup do iCloud do usuário retém uma chave para esse contêiner. Se o usuário desativar posteriormente o Backup do iCloud, a chave desse contêiner é revertida, a nova chave é armazenada somente nas Chaves do iCloud (inacessível à Apple e a terceiros) e os novos dados gravados no contêiner não podem ser descriptografados com a chave antiga do contêiner.

A chave usada para restaurar as mensagens no Backup do iCloud é colocada em dois locais: nas Chaves do iCloud e em um backup no CloudKit. O backup no CloudKit é feito se o Backup do iCloud estiver ativado e incondicionalmente restaurado, independentemente de o usuário restaurar ou não um backup do iCloud.

Criptografia de ponta a ponta do CloudKit

Vários serviços da Apple, listados no artigo de Suporte da Apple Visão geral da segurança do iCloud, usam criptografia de ponta a ponta com uma Chave de Serviço do CloudKit protegida pela sincronização das Chaves do iCloud. Nesses contêineres do CloudKit, a hierarquia de chaves tem como base as Chaves do iCloud e, portanto, compartilha as características de segurança das Chaves do iCloud — particularmente, as chaves estão disponíveis apenas nos dispositivos autorizados do usuário, e não para a Apple nem nenhum terceiro. Se o acesso aos dados das Chaves do iCloud for perdido, os dados no CloudKit são redefinidos e, caso haja dados disponíveis no dispositivo autorizado local, eles são enviados novamente para o CloudKit. Para obter mais informações, consulte Segurança de guarda das Chaves do iCloud.

As Mensagens no iCloud também usam a criptografia de ponta a ponta do CloudKit com uma Chave do Serviço CloudKit protegida pela sincronização das Chaves do iCloud. Se o usuário tiver ativado o Backup do iCloud, a Chave do Serviço CloudKit usada no contêiner das Mensagens do iCloud tem um backup feito no iCloud para permitir que o usuário recupere suas mensagens mesmo se tiver perdido o acesso às Chaves do iCloud e seus dispositivos autorizados. Essa Chave de Serviço do iCloud é revertida sempre que o usuário desativa o Backup do iCloud.

Situação	**Opções de recuperação de usuário para criptografia de ponta a ponta do CloudKit**
Acesso a dispositivo autorizado	Recuperação de dados possível por meio de dispositivo autorizado ou recuperação pelas Chaves do iCloud.
Nenhum dispositivo autorizado	Recuperação de dados somente possível por meio da recuperação pelas Chaves do iCloud.
Backup do iCloud ativado e acesso a dispositivo autorizado	Recuperação de dados possível por meio de Backup do iCloud, acesso a dispositivo autorizado ou recuperação pelas Chaves do iCloud.
Backup do iCloud ativado e sem acesso a dispositivo autorizado	Recuperação de dados possível por Backup do iCloud ou recuperação pelas Chaves do iCloud.
Backup do iCloud desativado e acesso a dispositivo autorizado	Recuperação de dados possível por meio de dispositivo autorizado ou recuperação pelas Chaves do iCloud.
Backup desativado e nenhum dispositivo autorizado	Recuperação de dados somente possível por meio da recuperação pelas Chaves do iCloud.

Gerenciamento de código e senha

Visão geral do gerenciamento de código e senha

O iOS, iPadOS e macOS oferecem diversos recursos para facilitar aos usuários a autenticação segura e conveniente em apps de terceiros e sites que usam senhas para autenticação. A melhor maneira de gerenciar senhas é não ter que usar uma senha. O recurso Iniciar sessão com a Apple permite que os usuários iniciem uma sessão em apps e sites de terceiros sem precisar criar e gerenciar outra conta ou senha ao mesmo tempo que protege o início de sessão com a autenticação de dois fatores do ID Apple do usuário. No caso de sites que não são compatíveis com Iniciar sessão com a Apple, as Senhas Automáticas Fortes permitem que os dispositivos do usuário criem, sincronizem e insiram, de forma automática, senhas fortes exclusivas em sites e apps. As senhas são salvas em Chaves especiais do Preenchimento Automático de Senhas que o usuário pode controlar e gerenciar no iOS e iPadOS em Ajustes > Senhas e Contas > Senhas de Sites e Apps.

No macOS, as senhas salvas podem ser gerenciadas nas preferências de Senhas do Safari. Esse sistema de sincronização também pode ser usado para sincronizar senhas criadas manualmente pelo usuário.

Iniciar sessão com a Apple

O recurso Iniciar sessão com a Apple é uma alternativa que oferece privacidade fácil quando comparado a outros sistemas de início de sessão único. Ele fornece a conveniência e eficiência do início de sessão com um toque ao mesmo tempo que oferece ao usuário mais transparência e controle sobre suas informações pessoais.

O recurso Iniciar sessão com a Apple permite que os usuários configurem uma conta e iniciem a sessão em apps e sites com o ID Apple que já possuem, oferecendo aos usuários mais controle sobre suas informações pessoais. Apps podem solicitar apenas o nome e endereço de e-mail do usuário ao configurar uma conta, e o usuário sempre pode escolher: ele pode compartilhar seu endereço de e-mail pessoal com um app ou manter seu e-mail pessoal privado e usar o novo serviço de retransmissão de e-mail privado da Apple. Esse serviço de retransmissão de e-mail compartilha um endereço de e-mail anônimo e exclusivo com encaminhamento para o endereço pessoal do usuário, de forma que ele ainda possa receber comunicações úteis do desenvolvedor sem deixar de manter um grau de privacidade e controle das suas informações pessoais.

O recurso Iniciar sessão com a Apple é projetado para ser seguro. Cada usuário do serviço Iniciar sessão com a Apple é obrigado a ter a autenticação de dois fatores ativada. A autenticação de dois fatores ajuda a proteger não apenas o ID Apple do usuário, mas também as contas estabelecidas com os apps. Além disso, a Apple desenvolveu e integrou ao recurso Iniciar sessão com a Apple um sinal antifraude, com privacidade fácil, que proporciona aos desenvolvedores a confiança de que os novos usuários adquiridos sejam pessoas reais, e não bots ou contas geradas por scripts.

Senhas Automáticas Fortes

Quando as Chaves do iCloud estão ativadas, o iOS, iPadOS e macOS criam senhas fortes, aleatórias e exclusivas quando o usuário se inscreve ou altera a senha em um site no Safari. No iOS e iPadOS, as Senhas Automáticas Fortes também estão disponíveis em apps. Para não usar senhas fortes, os usuários devem desativá-las. As senhas geradas são salvas nas chaves e sincronizadas com todos os dispositivos com as Chaves do iCloud, quando essas estão ativadas.

Por padrão, as senhas geradas pelo iOS e iPadOS têm 20 caracteres. Elas contêm um dígito, um caractere maiúsculo, dois hifens e 16 caracteres minúsculos. Tais senhas geradas são fortes, com 71 bits de entropia.

As senhas são geradas com base em uma heurística que determina se uma experiência no campo de senha destina-se à criação de senhas. Se a heurística não conseguir reconhecer um contexto de senha como destinado à criação de senhas, os desenvolvedores de apps podem definir UITextContentType.newPassword no campo de texto e os desenvolvedores da web podem definir autocomplete="new-password" nos elementos <input>.

Para garantir que as senhas geradas sejam compatíveis com o serviço relevante, apps e sites podem fornecer regras. Os desenvolvedores fornecem essas regras usando UITextInputPasswordRules ou o atributo passwordrules em seus elementos <input>. Depois, os dispositivos geram a senha mais forte possível que satisfaça essas regras.

Preenchimento Automático de Senha

O Preenchimento Automático de Senha preenche automaticamente credenciais armazenadas nas chaves. O gerenciador de senhas das Chaves do iCloud e Preenchimento Automático de Senhas oferecem os recursos seguintes:

- Preenchimento de credenciais em apps e sites;
- Geração de senhas fortes;
- Salvamento de senhas tanto em apps quanto em sites no Safari;
- Compartilhamento seguro de senhas para os contatos de um usuário;
- Fornecimento de senhas a uma Apple TV próxima que solicite credenciais.

As ações de gerar e salvar senhas em apps, além de fornecer senhas à Apple TV, estão disponíveis apenas no iOS e iPadOS.

Preenchimento Automático de Senha em apps

O iOS e iPadOS permitem que os usuários insiram nomes de usuário e senhas salvas em campos relacionados a credenciais em apps, de forma semelhante ao Preenchimento Automático de Senha do Safari. Para fazer isso, no iOS e iPadOS, os usuários devem tocar em um elemento de chave na barra QuickType do teclado de software. No macOS, os apps compilados com Mac Catalyst exibem um menu expansível de Senhas abaixo de campos relacionados a credenciais.

Quando há uma forte associação entre um app e um site que usam o mesmo mecanismo de associação de apps e sites, analisada pelo arquivo apple-app-site-association, a barra QuickType do iOS e iPadOS, e o menu expansível do macOS sugerem credenciais diretamente ao app, caso haja uma salva nas Chaves de Preenchimento Automático de Senha. Isso permite que os usuários optem por revelar credenciais salvas pelo Safari a apps com a mesmas propriedades de segurança, mas sem que os apps tenham que adotar uma API.

O Preenchimento Automático de Senha não expõe nenhuma informação de credenciais a um app até que o usuário consinta em liberar uma credencial para o app. As listas de credenciais são desenhadas ou apresentadas fora do processo do app.

Quando um app e um site têm um relacionamento de confiança e um usuário envia credenciais dentro de um app, talvez o iOS e iPadOS perguntem ao usuário se deseja salvar tais credenciais nas Chaves de Preenchimento Automático de Senha para uso futuro.

Acesso de apps a códigos salvos

Os apps do iOS e iPadOS podem interagir com as Chaves de Preenchimento Automático de Senha usando as duas APIs a seguir:

- SecRequestSharedWebCredential
- SecAddSharedWebCredential

Os apps do iOS, iPadOS e macOS podem pedir ajuda às Chaves de Preenchimento Automático de Senha para iniciar a sessão de um usuário por meio de ASAuthorizationPasswordProvider. O fornecedor da Senha e sua solicitação podem ser usados em conjunto com o recurso Iniciar sessão com a Apple, de forma que a mesma chamada de API ajude usuários a iniciar a sessão em um app, independentemente de a conta do usuário usar uma senha ou ter sido criada com o recurso Iniciar sessão com a Apple.

Apps podem acessar as senhas salvas somente se o desenvolvedor do app e o administrador do site concederem aprovação e o usuário autorizar. Para expressar a intenção de acessar as senhas salvas do Safari, os desenvolvedores de apps incluem um direito no app. A lista de direitos contém os nomes de domínio de sites associados, e os sites devem colocar um arquivo em seu servidor listando os identificadores exclusivos de app referentes aos apps aprovados pela Apple.

Quando um app com o direito com.apple.developer.associated-domains está instalado, o iOS e iPadOS fazem uma solicitação TLS para cada site listado, pedindo um destes arquivos:

- apple-app-site-association
- .well-known/apple-app-site-association

Caso o arquivo liste o identificador do app sendo instalado, o iOS e iPadOS assinalam que o site e o app têm uma relação confiável. Somente com uma relação de confiança as chamadas a essas duas APIs resultam em uma solicitação ao usuário, o qual deve concordar antes que qualquer senha seja liberada ao app, atualizada ou apagada.

Auditoria de reutilização e nível de segurança de senhas

A lista de senhas das Chaves de Preenchimento Automático de Senha no iOS, iPadOS e macOS indicam quais senhas salvas pelo usuário serão reutilizadas em outros sites, assim como as senhas consideradas fracas.

O uso da mesma senha em mais de um serviço pode tornar essas contas vulneráveis a um ataque de inserção em massa de credenciais. Se um serviço for violado e senhas vazarem, os invasores podem tentar usar as mesmas credenciais em outros serviços para atacar outras contas.

A senhas são marcadas como fracas se puderem ser adivinhadas com facilidade por um invasor. O iOS, iPadOS e macOS detectam padrões comuns usados na criação de senhas fáceis de lembrar, como o uso de palavras encontradas em um dicionário, substituições comuns de caracteres (como usar “s3nh4” em vez de “senha”), padrões encontrados em um teclado (como “q12we34r” em um teclado QWERTY) ou sequências repetidas (como “123123”). Esses padrões são usados com frequência para criar senhas que satisfaçam requisitos mínimos de serviços, mas também são comumente usados por invasores ao tentar adivinhar uma senha por meio da força bruta.

Como muitos serviços exigem especificamente um código PIN de quatro ou seis dígitos, essas senhas curtas são avaliadas com regras diferentes. Os códigos PIN são considerados fracos se estiverem entre os códigos PIN mais comuns, se forem uma sequência crescente ou decrescente como “1234” ou “8765” ou se seguirem um padrão repetitivo, como “123123” ou “123321”.

As senhas fracas e reutilizadas são indicadas na lista de senhas. Se o usuário iniciar a sessão em um site no Safari usando uma senha salva anteriormente que é muito fraca, tal como uma das senhas mais comuns, ele recebe um alerta recomendando que faça a atualização para uma Senha Automática Forte.

Envio de senhas para outros usuários ou dispositivos

AirDrop

Quando o iCloud está ativado, os usuários podem enviar uma credencial salva — incluindo os sites para os quais está salva, seu nome de usuário e senha — via AirDrop para outro dispositivo. O envio de credenciais via AirDrop sempre opera no modo Somente Contatos, independentemente de quais sejam os ajustes do usuário. No dispositivo receptor, após o consentimento do usuário, a credencial é armazenada nas Chaves de Preenchimento Automático de Senhas do usuário.

Apple TV

O Preenchimento Automático de Senhas está disponível para preencher senhas em apps na Apple TV. Quando o usuário põe o foco em um nome de usuário ou campo de senha no tvOS, a Apple TV começa a anunciar uma solicitação de Preenchimento Automático de Senha por meio de Bluetooth Low Energy (BLE).

Qualquer iPhone, iPad ou iPod touch por perto mostra um aviso convidando o usuário a compartilhar uma credencial com a Apple TV. O método de criptografia é estabelecido desta maneira:

- Se o dispositivo e a Apple TV usarem e mesma conta do iCloud, a criptografia entre os dispositivos acontece automaticamente.
- Se o dispositivo tiver uma sessão iniciada em uma conta do iCloud diferente daquela usada na Apple TV, o usuário é solicitado a estabelecer uma conexão criptografada através do uso de um código PIN. Para receber essa solicitação, o iPhone deve estar desbloqueado e perto do Siri Remote emparelhado com a Apple TV.

Após o estabelecimento da conexão criptografada usando a criptografia do link BLE, a credencial é enviada à Apple TV e automaticamente preenchida nos campos de texto correspondentes no app.

Extensões de provedor de credenciais

No iOS iPadOS, os usuários podem designar um app de terceiros com conformidade como fornecedor de credenciais nos ajustes de preenchimento automático em Contas e Senhas. Esse mecanismo funciona por meio de extensões. A extensão do provedor de credenciais deve fornecer uma visualização para escolha de credenciais e pode fornecer opcionalmente metadados do iOS e iPadOS sobre as credenciais salvas, de modo que possam ser oferecidas diretamente na barra QuickType. Os metadados incluem o site da credencial e o nome de usuário associado, mas não a senha. O iOS e iPadOS se comunicam com a extensão para obter a senha quando o usuário opta por preenchê-la em um app ou site no Safari. Os metadados de credenciais são armazenados no sandbox do provedor da credencial e são removidos quando um app é desinstalado.

Chaves do iCloud

Visão geral das Chaves do iCloud

As Chaves do iCloud permitem que usuários sincronizem suas senhas com segurança entre dispositivos iOS e iPadOS e computadores Mac sem expor essas informações à Apple. Os objetivos que influenciaram fortemente o design e a arquitetura das Chaves do iCloud (além do enfoque forte em privacidade e segurança) foram a facilidade de uso e a possibilidade de recuperação das Chaves. As Chaves do iCloud são compostas de dois serviços: sincronização das Chaves e recuperação das Chaves.

A Apple projetou as Chaves do iCloud e a recuperação das Chaves para que as senhas de um usuário estejam protegidas mesmo em circunstâncias em que:

- A conta do iCloud de um usuário seja comprometida.
- O iCloud seja comprometido por um ataque externo ou de um funcionário.
- Terceiros acessem contas de usuários.

Sincronização das chaves

Quando um usuário ativa as Chaves do iCloud pela primeira vez, o dispositivo estabelece um círculo de confiança e cria uma identidade de sincronização para si. A identidade de sincronização consiste em uma chave privada e uma chave pública. A chave pública da identidade de sincronização é colocada no círculo e o círculo é assinado duas vezes: primeiro pela chave privada da identidade de sincronização e depois por uma chave elíptica assimétrica (usando P-256) derivada da senha da conta do iCloud do usuário. Também armazenados no círculo estão os parâmetros (sal e iterações aleatórios) usados para criar a chave baseada na senha do iCloud do usuário.

O círculo de sincronização assinado é colocado na área de armazenamento de valores de chaves do iCloud do usuário. Ele não pode ser lido sem o conhecimento da senha do iCloud do usuário e não pode ser modificado legalmente sem a chave privada da identidade de sincronização do seu integrante.

Quando o usuário ativa as Chaves do iCloud em um outro dispositivo, as Chaves do iCloud percebem que o usuário possui um círculo de sincronização estabelecido anteriormente no iCloud do qual o dispositivo não é um integrante. O dispositivo cria o seu par de chaves de identidade de sincronização e um tíquete de candidatura para solicitar o ingresso no círculo. O tíquete consiste na chave pública da identidade de sincronização do dispositivo e o usuário é solicitado a autenticar com a sua senha do iCloud. Os parâmetros de geração da chave elíptica são obtidos do iCloud e geram uma chave que é usada para assinar o tíquete de candidatura. Finalmente, o tíquete de candidatura é colocado no iCloud.

Quando o primeiro dispositivo percebe o recebimento de um tíquete de candidatura, ele pede ao usuário que reconheça a solicitação do novo dispositivo para entrar no círculo de sincronização. O usuário digita a sua senha do iCloud e o tíquete de candidatura é verificado como assinado através da correspondência de uma chave privada. Agora, os usuários que geraram a solicitação para entrar no círculo podem entrar.

Depois que o usuário aprova a adição do novo dispositivo ao círculo, o primeiro dispositivo adiciona a chave pública do novo integrante ao círculo de sincronização e a assina novamente com a identidade de sincronização e a chave derivada da senha do iCloud do usuário. O novo círculo de sincronização é colocado no iCloud, onde é assinado pelo novo integrante do círculo de maneira semelhante.

Agora há dois integrantes no círculo de sincronização e cada integrante possui a chave pública do outro dispositivo. Eles começam a trocar itens individuais das Chaves através do armazenamento de valores de chaves do iCloud ou os armazenam no CloudKit, seja qual for o mais apropriado à situação. Se os dois integrantes do círculo tiverem o mesmo item, aquele com a data de modificação mais recente é sincronizado. Se o outro integrante possuir o item e as datas de modificação forem idênticas, o item é ignorado. Cada item sincronizado é criptografado, de modo que possa ser descriptografado somente por um dispositivo dentro do círculo de confiança do usuário; ele não pode ser descriptografado por nenhum outro dispositivo ou pela Apple.

Esse processo repete-se conforme novos dispositivos entram no círculo de sincronização. Por exemplo, quando da entrada de um terceiro dispositivo, a confirmação é exibida nos outros dois dispositivos do usuário. O usuário pode aprovar o novo integrante de qualquer um desses dispositivos. Conforme novos dispositivos são adicionados, cada um é sincronizado ao novo para garantir que todos os integrantes tenham os mesmos itens das Chaves.

No entanto, as Chaves completas não são sincronizadas. Alguns itens são específicos a cada dispositivo (como identidades VPN) e não devem sair do dispositivo. Apenas os itens com o atributo kSecAttrSynchronizable são sincronizados. A Apple definiu esse atributo para os dados de usuário do Safari (incluindo nomes de usuários, senhas e números de cartão de crédito), além de senhas de Wi-Fi e chaves de criptografia do HomeKit.

Além disso, os itens das Chaves adicionados por apps de terceiros não são sincronizados por padrão. Os desenvolvedores devem definir o atributo kSecAttrSynchronizable ao adicionar itens às Chaves.

Recuperação das Chaves do iCloud

A recuperação das Chaves proporciona aos usuários uma maneira de guardar suas Chaves com a Apple, sem permitir que a Apple leia suas senhas ou outros dados contidos. Mesmo que o usuário tenha um único dispositivo, a recuperação das Chaves proporciona uma camada de segurança contra a perda de dados. Isso é particularmente importante quando o Safari é usado para gerar senhas fortes e aleatórias para contas da web, pois o único registro dessas senhas encontra-se nas Chaves.

Um dos pilares da recuperação das Chaves é a autenticação secundária e um serviço de guarda segura, criado pela Apple para oferecer suporte a esse recurso especificamente. As Chaves do usuário são criptografadas usando um código forte e o serviço de guarda fornece uma cópia das Chaves somente se um conjunto de condições específicas for atendido.

Há diversas maneiras de estabelecer um código forte:

- Se a autenticação de dois fatores estiver ativada na conta do usuário, o código do dispositivo é usado para recuperar Chaves guardadas.
- Se a autenticação de dois fatores não estiver configurada, o usuário é solicitado a fornecer um código de seis dígitos para criar um Código de Segurança do iCloud. Opcionalmente, sem a autenticação de dois fatores, os usuários podem especificar seus próprios (e maiores) códigos ou permitir que seus dispositivos criem um código criptograficamente aleatório que possa ser registrado e mantido em separado.

Depois disso, muitos usuários desejam guardar suas chaves junto à Apple. O processo se dá desta forma: o dispositivo iOS, iPadOS ou macOS exporta uma cópia das Chaves do usuário, criptografa-as embaladas em chaves dentro de uma keybag assimétrica e as coloca na área de armazenamento de valores de chaves do iCloud do usuário. A keybag é embalada pelo Código de Segurança do iCloud do usuário e com a chave pública do cluster do módulo de segurança de hardware (HSM) que armazena o registro de guarda. Isso se torna o Registro de Guarda do iCloud do usuário.

Se o usuário decide aceitar um código de segurança criptograficamente aleatório em vez de especificar o seu próprio código ou usar um valor de quatro dígitos, o registro de guarda não é necessário. No lugar disso, a chave aleatória é embalada diretamente pelo Código de Segurança do iCloud.

Além de estabelecer um código de segurança, os usuários devem registrar um número de telefone. Isso proporciona um nível secundário de autenticação durante a recuperação das Chaves. O usuário recebe um SMS que deve ser respondido para que a recuperação continue.

Segurança de guarda das Chaves do iCloud

O iCloud proporciona uma infraestrutura segura para a guarda de Chaves para garantir que apenas os usuários e dispositivos autorizados possam fazer uma recuperação. Os clusters HSM que armazenam os registros de guarda encontram-se posicionados topograficamente atrás do iCloud. Como descrito anteriormente, cada um possui uma chave que é usada para criptografar os registros de guarda pelos quais são responsáveis.

Para recuperar suas Chaves, o usuário deve usar sua conta e senha do iCloud para autenticar e responder a um SMS enviado para o número de telefone registrado. Depois disso feito, o usuário deve digitar o seu Código de Segurança do iCloud. O cluster HSM usa o protocolo SRP (Secure Remote Password) para verificar se o usuário sabe o seu Código de Segurança do iCloud; o código em si não é enviado à Apple. Cada integrante do cluster verifica independentemente se o usuário não excedeu o número máximo de tentativas permitidas para recuperar seu registro, conforme descrito abaixo. Havendo consenso da maioria, o cluster abre o registro de guarda e o envia para o dispositivo do usuário.

A seguir, o dispositivo usa o Código de Segurança do iCloud para desembalar a chave aleatória usada para criptografar as Chaves do usuário. Com essa chave, as Chaves — obtidas do armazenamento de valores de chaves do iCloud — são descriptografadas e restauradas no dispositivo. O iOS, iPadOS e macOS permitem apenas 10 tentativas para autenticar e recuperar um registro de guarda. Depois de várias tentativas malsucedidas, o registro é bloqueado e o usuário precisará ligar para o Suporte da Apple para obter mais tentativas. Depois da décima tentativa malsucedida, o cluster HSM destrói o registro de guarda e as Chaves se perdem para sempre. Isso fornece proteção contra tentativas de aquisição do registro com força bruta, às custas da eliminação dos dados das Chaves como consequência.

Essas políticas estão codificadas no firmware HSM. Os cartões de acesso administrativo que permitem a alteração do firmware foram destruídos. Qualquer tentativa de alterar o firmware ou acessar a chave privada faz com que o cluster HSM a destrua. Caso isso ocorra, o proprietário de cada uma das Chaves protegidas pelo cluster recebe uma mensagem que o informa sobre a perda do seu registro de guarda. Depois disso, ele pode optar por se inscrever novamente.

Integração do Safari com as Chaves do iCloud

O Safari pode gerar automaticamente strings aleatórias criptograficamente fortes para criar senhas de sites, que são armazenadas nas Chaves e sincronizadas com os outros dispositivos. Os itens das Chaves são transferidos de dispositivo para dispositivo através de servidores da Apple, mas são criptografados de tal maneira que nem a Apple e nem outros dispositivos possam ler seu conteúdo.

Apple Pay

Visão geral do Apple Pay

Com o Apple Pay, os usuários podem usar dispositivos iOS, iPad, Mac e Apple Watch compatíveis para fazer pagamentos de maneira fácil, segura e privada em lojas, apps e na web, com o Safari. Os usuários também podem adicionar cartões de transporte público compatíveis com o Apple Pay ao app Wallet. É uma solução simples para os usuários e construída com segurança integrada, tanto no hardware como no software.

O Apple Pay também foi projetado para proteger as informações pessoais do usuário. O Apple Pay não coleta nenhuma informação de transação que possa ser atrelada ao usuário. As transações de pagamentos ocorrem entre o usuário, o comerciante e a administradora do cartão.

Componentes do Apple Pay

Elemento Seguro

O Elemento Seguro é um chip certificado padrão que usa a plataforma Java Card, a qual encontra-se em conformidade com os requisitos da indústria financeira para pagamentos eletrônicos. O CI do Elemento Seguro e a plataforma Java Card são certificados de acordo com o processo de Avaliação de Segurança da EMVCo. Depois da conclusão bem-sucedida da Avaliação de Segurança, a EMVCo emite um certificado exclusivo para o CI e a plataforma.

O CI do Elemento Seguro foi certificado com base no padrão Common Criteria.

Controlador NFC

O controlador NFC gerencia os protocolos do tipo “Near Field Communication” e encaminha a comunicação entre o processador de aplicativos e o Elemento Seguro, e entre o Elemento Seguro e o terminal de vendas.

Apple Wallet

A Apple Wallet é usada para adicionar e gerenciar cartões de crédito, débito e cartões de lojas, além de fazer pagamentos com o Apple Pay. Na Apple Wallet, os usuários podem visualizar seus cartões e talvez possam ver informações adicionais fornecidas pela administradora do cartão, como a política de privacidade da administradora, transações recentes etc. Os usuários também podem adicionar cartões ao Apple Pay no:

- Assistente de Configuração e Ajustes do iOS e iPadOS
- App Watch para o Apple Watch

- Wallet e Apple Pay nas Preferências do Sistema de computadores Mac que possuem Touch ID

Além disso, a Apple Wallet permite que os usuários adicionem e gerenciem cartões de transporte público, cartões de fidelidade, cartões de embarque, ingressos, cartões-presente, cartões de ID de estudante e outros.

Secure Enclave

No iPhone, iPad, Apple Watch e computadores Mac com Touch ID, o Secure Enclave gerencia o processo de autenticação e permite o prosseguimento de transações de pagamento.

No Apple Watch, o dispositivo deve estar desbloqueado e o usuário precisa clicar duas vezes no botão lateral. Os dois cliques são detectados e encaminhados ao Elemento Seguro (ou Secure Enclave, quando disponível) sem passar pelo processador de aplicativos.

Servidores do Apple Pay

Os servidores do Apple Pay gerenciam a configuração e a provisão de cartões de crédito, débito, transporte público e Carteiras de Estudante no app Wallet. Os servidores também gerenciam os Números de Conta do Dispositivo armazenados no Elemento Seguro. Eles se comunicam com o dispositivo e com os servidores da rede de pagamento ou da administradora do cartão. Os servidores do Apple Pay também são responsáveis por criptografar novamente as credenciais de pagamento em pagamentos dentro de apps.

Como o Apple Pay usa o Elemento Seguro e o controlador NFC

Elemento Seguro

O Elemento Seguro hospeda um applet feito especificamente para gerenciar o Apple Pay. Também inclui applets certificados pelas redes de pagamento ou operadoras de cartões. Os dados de cartões de crédito, débito e pré-pagos são criptografados e enviados pela rede de pagamento ou administradora do cartão aos applets usando chaves que são de conhecimento apenas da rede de pagamento ou administradora do cartão e do domínio de segurança dos applets. Esses dados são armazenados nos applets e protegidos com os recursos de segurança do Elemento Seguro. Durante uma transação, o terminal se comunica diretamente com o Elemento Seguro através do controlador Near Field Communication (NFC) em um barramento dedicado.

Controlador NFC

Como gateway do Elemento Seguro, o controlador NFC garante que todos os pagamentos por proximidade sejam realizados em um terminal de vendas próximo ao dispositivo. Apenas solicitações de pagamento provenientes de um terminal dentro do alcance são marcadas pelo controlador NFC como transações por proximidade.

Após um pagamento com cartão de crédito, débito ou pré-pago (incluindo cartões de lojas) ser autorizado pelo titular do cartão com o Touch ID, Face ID ou código ou através de dois cliques no botão lateral de um Apple Watch desbloqueado, as respostas de proximidade preparadas pelos applets de pagamento dentro do Elemento Seguro são encaminhadas exclusivamente pelo controlador para o campo NFC. Consequentemente, os detalhes de autorizações de pagamento de transações de pagamento por proximidade ficam contidos no campo NFC local e nunca são expostos ao processador do aplicativo. Por outro lado, os detalhes de autorizações de pagamento dentro de apps e na web são encaminhados ao processador de aplicativos, mas apenas depois de criptografados pelo Elemento Seguro no servidor do Apple Pay.

Cartões de crédito, débito e pré-pagos

Visão geral da provisão de cartões de crédito, débito e pré-pagos com Apple Pay

Quando um usuário adiciona um cartão de crédito, débito ou pré-pago (incluindo cartões de lojas) à Apple Wallet, a Apple envia as informações do cartão com segurança, assim como outras informações sobre a conta e o dispositivo do usuário, à administradora do cartão ou ao provedor de serviços autorizado da administradora do cartão. Por meio do uso dessas informações, a administradora do cartão determina se o cartão será aprovado para uso na Apple Wallet.

Como parte do processo de provisão do cartão, o Apple Pay usa três chamadas do lado do servidor para enviar e receber comunicações com a administradora ou rede do cartão: Campos Obrigatórios, Verificação do Cartão, e Vínculo e Provisão. A administradora do cartão ou a rede usa essas chamadas para verificar, aprovar e adicionar cartões à Apple Wallet. Essas sessões cliente-servidor são criptografadas usando TLS v1.2.

Os números completos do cartão não são armazenados no dispositivo ou nos servidores do Apple Pay. Ao invés disso, um Número de Conta do Dispositivo é criado, criptografado e armazenado no Elemento Seguro. Esse Número de Conta do Dispositivo é criptografado de tal maneira que a Apple não consegue acessá-lo. O Número de Conta do Dispositivo é exclusivo e diferente da maioria dos números de cartões de crédito ou débito; a administradora do cartão ou rede de pagamento pode impedir seu uso em um cartão de tarja magnética, por telefone ou em sites. O Número de Conta do Dispositivo no Elemento Seguro nunca é armazenado nos servidores do Apple Pay ou incluído no backup do iCloud, e é isolado do iOS, iPadOS, watchOS e computadores Mac com Touch ID.

Os cartões para uso com o Apple Watch são fornecidos ao Apple Pay através do uso do app Apple Watch no iPhone ou dentro de um app da administradora do cartão no iPhone. A adição de um cartão ao Apple Watch exige que o relógio esteja dentro da área de comunicação do Bluetooth. Os cartões são registrados especificamente para uso com o Apple Watch e possuem um Número de Conta do Dispositivo próprio, armazenado no Elemento Seguro do Apple Watch.

Quando cartões de crédito, débito ou pré-pagos (incluindo cartões de lojas) são adicionados, eles aparecem em uma lista de cartões durante o Assistente de Configuração em dispositivos que tenham uma sessão iniciada na mesma conta do iCloud. Tais cartões permanecem nessa lista pelo tempo em que estiverem ativos em ao menos um dispositivo. Os cartões são removidos dessa lista após terem sido removidos de todos os dispositivos por sete dias. Esse recurso requer que a autenticação de dois fatores esteja ativada na respectiva conta do iCloud.

Adição manual de cartões de crédito ou débito ao Apple Pay

Para adicionar um cartão manualmente, o nome, número, data de validade e CVC do cartão são usados para facilitar o processo de provisão. Essas informações podem ser digitadas pelos usuários ou capturadas pela câmera do dispositivo nos apps Ajustes, Wallet ou Apple Watch. Quando a câmera captura as informações do cartão, a Apple tenta preencher o nome, número e data de validade do cartão. A foto nunca é salva no dispositivo ou armazenada na fototeca. Após todos os campos serem preenchidos, o processo de Verificação do Cartão confirmará todos os campos, exceto o CVC. Depois, as informações são criptografadas e enviadas ao servidor do Apple Pay.

Se um ID de termos e condições for retornado junto ao processo de Verificação do Cartão, a Apple transfere e exibe os termos e condições da administradora do cartão para o usuário. Caso o usuário aceite os termos e condições, a Apple envia o ID dos termos aceitos, assim como o CVC, para o processo de Vínculo e Provisão. Além disso, como parte do processo de Vínculo e Provisão, a Apple compartilha informações do dispositivo com a administradora ou rede do cartão, como informações sobre a atividade da conta da iTunes Store e da App Store do usuário (se ele tem um histórico longo de transações no iTunes, por exemplo), informações sobre o dispositivo do usuário (número de telefone, nome e modelo do dispositivo, além de qualquer dispositivo Apple complementar necessário para usar o Apple Pay) e a localização aproximada do usuário no momento em que o cartão é adicionado (se os Serviços de Localização estiverem ativados). Por meio do uso dessas informações, a administradora do cartão determina se o cartão será aprovado para uso no Apple Pay.

Dois fatores decorrem do processo de Vínculo e Provisão:

- O dispositivo inicia o download do tíquete da Wallet que representa o cartão de crédito ou débito.
- O dispositivo inicia o vínculo do cartão ao Elemento Seguro.

O tíquete contém URLs para baixar a imagem ilustrativa do cartão e metadados sobre o cartão (como informações de contato, app relacionado da administradora e recursos compatíveis). Ele também contém o estado do tíquete, que inclui informações sobre a conclusão da personalização do Elemento Seguro, a suspensão vigente do cartão pela administradora ou exigências de verificações adicionais para que o cartão possa fazer pagamentos com o Apple Pay.

Adição de cartões de crédito ou débito de uma conta da iTunes Store ao Apple Pay

No caso de cartões de crédito e débito já registrados no iTunes, o usuário pode ser solicitado a digitar a senha do seu ID Apple novamente. O número do cartão é obtido do iTunes e o processo de Verificação do Cartão é iniciado. Se o cartão for elegível para o Apple Pay, o dispositivo transfere e exibe os termos e condições para depois enviar o ID dos termos e o código de segurança do cartão para o processo de Vínculo e Provisão. Cartões já registrados em contas do iTunes poderão estar sujeitos a verificações adicionais.

Adição de cartões de crédito ou débito em um app de administradora de cartões

Quando o app está registrado para uso com o Apple Pay, chaves são estabelecidas para o app e para o servidor da administradora do cartão. Essas chaves são usadas para criptografar as informações do cartão enviadas à administradora do cartão, impedindo sua leitura pelo dispositivo Apple. O fluxo de provisão assemelha-se ao usado para cartões adicionados manualmente (descrito anteriormente), exceto pelo fato de que são usadas senhas de uso único em vez do CVC.

Verificação adicional com o Apple Pay

A administradora do cartão pode decidir se um cartão de crédito ou débito requer verificação adicional. Dependendo do que for oferecido pela administradora, talvez o usuário possa escolher entre diversas opções de verificação adicional, como mensagem de texto, e-mail, ligação do atendimento ao cliente ou um método em um app de terceiros aprovado para concluir a verificação. No caso de mensagens de texto ou e-mail, o usuário seleciona dentre as informações de contato registradas na administradora. É enviado um código, que deverá ser digitado no app Wallet, nos Ajustes ou no app do Apple Watch. No caso de atendimento ao cliente ou verificação ao usar um app, a administradora realiza o seu próprio processo de comunicação.

Autorização de pagamento com o Apple Pay

Em dispositivos com Secure Enclave, o Elemento Seguro permite que um pagamento seja feito apenas depois de receber autorização do Secure Enclave. No iPhone ou iPad, isso envolve a confirmação de que o usuário se autenticou com o Touch ID, o Face IDou o código do dispositivo. Caso disponíveis, o Touch ID ou o Face ID são os métodos padrão, mas o código pode ser usado a qualquer momento. Um código é oferecido automaticamente após três tentativas malsucedidas de identificação de uma impressão digital ou duas tentativas malsucedidas de identificação de um rosto e exigido após cinco tentativas malsucedidas. Um código também é exigido quando o Touch ID ou o Face ID não estão configurados ou ativados para o Apple Pay. Para que um pagamento seja feito no Apple Watch, o dispositivo deve ser desbloqueado com o código e o botão lateral deve ser clicado duas vezes.

A comunicação entre o Enclave Seguro e o Elemento Seguro ocorre através de uma interface serial, com o Elemento Seguro conectado ao controlador NFC, que por sua vez encontra-se conectado ao processador do aplicativo. Embora não estejam conectados diretamente, o Enclave Seguro e o Elemento Seguro podem comunicar-se em segurança usando uma chave de emparelhamento compartilhada, fornecida durante o processo de fabricação. A criptografia e a autenticação da comunicação são baseadas em AES, com nonces criptográficos usados em ambos os lados para proteção contra ataques de reprodução. A chave de emparelhamento é gerada dentro do Enclave Seguro a partir de sua chave UID e do identificador exclusivo do Elemento Seguro. A chave de emparelhamento é então transferida seguramente do Enclave Seguro para um módulo de segurança de hardware (HSM) na fábrica, que possui o material da chave necessário para injetar a chave de emparelhamento no Elemento Seguro.

Autorização de transações

Quando o usuário autoriza uma transação, a qual inclui um gesto físico comunicado diretamente ao Secure Enclave, o Secure Enclave envia os dados assinados sobre o tipo de autenticação e os detalhes do tipo de transação (proximidade ou dentro de apps) para o Secure Enclave, atrelados a um valor de Autorização Aleatório (AR). O AR é gerado no Secure Enclave na primeira vez que o usuário fornece um cartão de crédito e persiste enquanto o Apple Pay estiver ativado, protegido pela criptografia do Secure Enclave e pelo mecanismo antirreversão. Ele é entregue com segurança ao Elemento Seguro pela chave de emparelhamento. Ao receber um novo valor AR, o Elemento Seguro marca qualquer cartão adicionado anteriormente como apagado.

Código de segurança dinâmico específico à transação no Apple Pay

As transações de pagamento originadas de applets de pagamento incluem um criptograma de pagamento e um Número de Conta do Dispositivo. Esse criptograma, um código de uso único, é calculado por um contador de transações e uma chave. O contador de transações aumenta a cada nova transação. A chave é fornecida no applet de pagamento durante a personalização, sendo conhecida pela rede de pagamentos e/ou administradora do cartão. Dependendo do esquema de pagamento, outros dados também podem ser usados no cálculo, incluindo:

- Um Número Imprevisível de Terminal (em transações NFC)
- Um nonce do servidor do Apple Pay (em transações dentro de apps)

Esses códigos de segurança são fornecidos à rede de pagamentos e à administradora do cartão, o que permite ao emissor verificar cada transação. O tamanho desses códigos de segurança pode variar conforme o tipo de transação.

Pagamento com cartões de crédito e débito em lojas com o Apple Pay

Se o iPhone ou Apple Watch estiver ligado e detectar um campo NFC, ele apresenta ao usuário o cartão solicitado (se a seleção automática estiver ativada para esse cartão) ou o cartão padrão, que é gerenciado nos Ajustes. O usuário também pode acessar o app Wallet e escolher um cartão ou, quando o dispositivo estiver bloqueado:

- Clicar duas vezes no botão Início em dispositivos com Touch ID
- Clicar duas vezes no botão lateral em dispositivos com Face ID

A seguir, antes que as informações sejam transmitidas, o usuário precisa autenticar com o Touch ID, o Face ID ou o código. Quando o Apple Watch está desbloqueado, o cartão de pagamento padrão é ativado ao clicar duas vezes no botão lateral. Nenhuma informação de pagamento é enviada sem a autenticação do usuário.

Depois que o usuário autentica, o Número de Conta do Dispositivo e um código de segurança dinâmico específico à transação são usados ao processar o pagamento. A Apple e o dispositivo do usuário não enviam os números completos do cartão de crédito ou débito para os comerciantes. A Apple pode receber informações anônimas da transação, como a hora e o local aproximado da transação, o que ajuda a melhorar o Apple Pay e outros produtos e serviços da Apple.

Pagamento com cartões de crédito e débito em apps com o Apple Pay

O Apple Pay também pode ser usado para fazer pagamentos dentro de apps para iOS, iPadOS e Apple Watch. Quando os usuários pagam com o Apple Pay dentro de apps, a Apple recebe as informações criptografadas. Antes que essas informações sejam enviadas ao desenvolvedor ou comerciante, a Apple as criptografa novamente com uma chave específica do desenvolvedor. O Apple Pay retém informações anônimas sobre a transação, como o valor aproximado da compra. Essas informações não podem ser atreladas ao usuário e nunca incluem o que o usuário compra.

Quando um app inicia uma transação de pagamento do Apple Pay, os servidores do Apple Pay recebem a transação criptografada do dispositivo antes que o comerciante a receba. Depois, os servidores do Apple Pay criptografam novamente a transação com uma chave específica do comerciante antes de repassá-la ao comerciante.

Quando um app solicita um pagamento, ele recorre a uma API para determinar se o dispositivo é compatível com o Apple Pay e se o usuário tem cartões de crédito ou débito que podem fazer pagamentos em uma rede de pagamentos aceita pelo comerciante. O app solicita qualquer informação necessária para processar e executar a transação, como o endereço de cobrança e entrega e informações de contato. Em seguida, o app pede para que o iOS, iPadOS ou watchOS apresentem a folha do Apple Pay, que solicita informações para o app, assim como outras informações necessárias, como qual cartão usar.

Nesse momento, informações sobre a cidade, estado e CEP são apresentadas ao app para o cálculo do custo de entrega final. O conjunto completo de informações solicitadas não é fornecido ao app até que o usuário autorize o pagamento com o Touch ID, o Face ID ou o código do dispositivo. Depois que o pagamento é autorizado, as informações apresentadas na folha do Apple Pay são transferidas ao comerciante.

Autorização de pagamento em apps

Quando o usuário autoriza o pagamento, uma ligação é feita aos servidores do Apple Pay para obtenção de um nonce criptográfico (que se assemelha ao valor retornado por terminais NFC usados em transações em lojas). O nonce, assim como outros dados da transação, é passado ao Elemento Seguro para gerar uma credencial de pagamento que é criptografada com uma chave da Apple. Quando a credencial de pagamento criptografada sai do Elemento Seguro, ela é passada para os servidores do Apple Pay, que a descriptografam, comparam o nonce da credencial com aquele originalmente enviado pelos servidores do Apple Pay e criptografam a credencial de pagamento novamente com a chave do comerciante associada ao ID do Comerciante. Depois, o pagamento é reenviado ao dispositivo, que o redireciona ao app através da API. O app então a envia ao sistema do comerciante para processamento. O comerciante pode então descriptografar a credencial de pagamento usando sua chave privada para processamento. Isso, juntamente à assinatura dos servidores da Apple, permite que o comerciante verifique que a transação se destina especificamente a esse comerciante.

As APIs requerem um direito que especifique os IDs de Comerciante compatíveis. Um app também pode incluir dados adicionais (como um número de pedido ou identidade do cliente) para enviar ao Elemento Seguro para assinatura, o que impede que a transação seja desviada para outro cliente. Isso é realizado pelo desenvolvedor do app, que pode especificar applicationData em PKPaymentRequest. Um hash desses dados é incluído nos dados de pagamento criptografados. O comerciante fica então responsável por verificar se o hash do applicationData corresponde àquele incluído nos dados de pagamento.

Pagamento com cartões de crédito e débito na web com o Apple Pay

O Apple Pay pode ser usado para fazer pagamentos em sites com o iPhone, iPad e Apple Watch. As transações do Apple Pay também podem ser iniciadas no Mac e concluídas em um iPhone ou Apple Watch compatível com o Apple Pay que esteja usando a mesma conta do iCloud.

O uso do Apple Pay na web requer o registro dos sites participantes com a Apple. Os servidores da Apple realizam a validação do nome de domínio e emitem um certificado de cliente TLS. Os sites que oferecem suporte ao Apple Pay são obrigados a fornecer seu conteúdo por HTTPS. Em cada transação de pagamento, os sites precisam usar o certificado de cliente TLS emitido pela Apple para obter uma sessão de comerciante segura e exclusiva. Os dados da sessão do comerciante são assinados pela Apple. Depois da verificação da assinatura da sessão do comerciante, um site pode consultar se o usuário possui um dispositivo compatível com o Apple Pay e se ele tem um cartão de crédito, débito ou pré-pago ativado no dispositivo. Nenhum outro detalhe é compartilhado. Se o usuário não desejar compartilhar essas informações, ele pode desativar as consultas do Apple Pay nos ajustes de privacidade do Safari no iOS, iPadOS e macOS.

Depois da validação da sessão do comerciante, todas as medidas de segurança e privacidade são idênticas àquelas tomadas ao fazer pagamentos dentro de um app.

Se o usuário estiver transmitindo informações relacionadas a pagamento de um Mac para um iPhone ou Apple Watch, o Handoff do Apple Pay usa o protocolo de Serviço de Identidade da Apple (IDS) com criptografia de ponta a ponta para transmitir as informações relacionadas a pagamento entre o Mac do usuário e o dispositivo autorizador. O IDS usa as chaves do dispositivo do usuário para realizar a criptografia, de modo que nenhum outro dispositivo possa descriptografar essas informações. Além disso, as chaves não são disponibilizadas à Apple. A descoberta de dispositivos para o Handoff do Apple Pay contém o tipo e o identificador exclusivo dos cartões de crédito do usuário, além de alguns metadados. O número de conta específico do dispositivo do cartão do usuário não é compartilhado e continua armazenado com segurança no iPhone ou Apple Watch do usuário. A Apple também transmite com segurança os endereços de contato, entrega e cobrança usados recentemente pelo usuário através das Chaves do iCloud.

Depois que o usuário autoriza o pagamento com o Touch ID, Face ID, código ou clica duas vezes no botão lateral do Apple Watch, um token de pagamento criptografado exclusivamente para o certificado de comerciante de cada site é transmitido com segurança do iPhone ou Apple Watch para o Mac, sendo então entregue ao site do comerciante.

Apenas dispositivos próximos uns dos outros podem solicitar e concluir pagamentos. A proximidade é determinada através de anúncios de Bluetooth Low Energy (BLE).

Tíquetes por proximidade no Apple Pay

Para transmitir dados de tíquetes compatíveis a terminais NFC compatíveis, a Apple usa o protocolo de Serviços de Valor Agregado (Apple VAS) do app Wallet. O protocolo VAS pode ser implementado em terminais por proximidade e usa NFC para se comunicar com dispositivos Apple compatíveis. O protocolo VAS funciona a distâncias curtas e pode ser usado para apresentação de tíquetes por proximidade, independentemente ou como parte de uma transação do Apple Pay.

Quando o dispositivo é segurado próximo ao terminal NFC, o terminal inicia a recepção das informações do tíquete, solicitando um tíquete. Se o usuário tiver um tíquete com a identidade do emissor do tíquete, ele é solicitado a autorizar seu uso por meio do Touch ID, Face ID ou código. As informações do tíquete, uma marca temporal e uma chave ECDH P-256 aleatória de uso único são usadas com a chave pública do emissor do tíquete para derivar uma chave de criptografia para os dados do tíquete, a qual é enviada para o terminal.

Do iOS 12 ao iOS 13, os usuários podem selecionar um tíquete manualmente antes de apresentá-lo ao terminal NFC do comerciante. No iOS 13.1 ou posterior, os emissores de tíquetes podem configurar se os tíquetes selecionados manualmente precisam da autenticação do usuário ou podem ser usados sem autenticação.

Inutilização de cartões com o Apple Pay

Os cartões de crédito, débito e pré-pagos adicionados ao Elemento Seguro podem ser usados somente se uma autorização que use a mesma chave de emparelhamento e valor AR de quando o cartão foi adicionado for apresentada ao Elemento Seguro. Ao receber um novo valor AR, o Elemento Seguro marca qualquer cartão adicionado anteriormente como apagado. Isso permite que o sistema operacional instrua o Enclave Seguro a inutilizar os cartões, marcando suas cópias do AR como inválidas nos seguintes casos:

Método	Dispositivo
Quando o código é desativado	iPhone, iPad, Apple Watch
Quando a senha é desativada	Mac
O usuário encerra a sessão no iCloud	iPhone, iPad, Mac, Apple Watch
O usuário seleciona “Apagar Todo o Conteúdo e Ajustes”	iPhone, iPad, Apple Watch
O dispositivo é restaurado a partir do modo de Recuperação	iPhone, iPad, Mac, Apple Watch
Desemparelhamento	Apple Watch

Suspensão, remoção e apagamento de cartões

Os usuários podem usar o Buscar para colocar seus dispositivos no Modo Perdido e suspender o Apple Pay no iPhone, iPad e Apple Watch. Os usuários também podem usar o Buscar, iCloud.com ou o app Wallet (diretamente no dispositivo), para remover e apagar seus cartões do Apple Pay. No Apple Watch, os cartões podem ser removidos através dos ajustes do iCloud, do app Apple Watch no iPhone ou diretamente no relógio. A capacidade de fazer pagamentos usando cartões no dispositivo é suspensa ou removida do Apple Pay pela administradora do cartão ou rede de pagamentos correspondente, mesmo que o dispositivo esteja off-line e desconectado de uma rede celular ou Wi-Fi. Os usuários também podem ligar para a administradora do cartão para suspender ou remover cartões do Apple Pay.

Além disso, quando um usuário apaga todo o dispositivo com a opção "Apagar Todo o Conteúdo e Ajustes", Buscar ou ao restaurar o dispositivo no modo de Recuperação, os dispositivos iOS, iPadOS e macOS instruem o Elemento Seguro para marcar todos os cartões como apagados. Isso faz com que os cartões sejam alterados imediatamente para um estado não utilizável até que os servidores do Apple Pay possam ser contatados para apagar completamente os cartões do Elemento Seguro. De forma independente, o Enclave Seguro marca o AR como inválido, para que autorizações de pagamento posteriores com cartões previamente registrados não sejam possíveis. Quando o dispositivo estiver on-line, ele tentará contatar os servidores do Apple Pay para garantir que todos os cartões no Elemento Seguro sejam apagados.

Apple Cash

No iOS 11.2 ou posterior e watchOS 4.2 ou posterior, o Apple Pay pode ser usado em um iPhone, iPad ou Apple Watch para enviar, receber e pedir dinheiro para outros usuários. Quando um usuário recebe dinheiro, o dinheiro é adicionado a uma conta do Apple Cash (que pode ser acessada no app Wallet ou em Ajustes > Wallet e Apple Pay) em dispositivos qualificados nos quais o usuário tenha uma sessão iniciada com seu ID Apple.

Para usar pagamentos de pessoa a pessoa e o Apple Cash, o usuário deve ter uma sessão iniciada em sua conta do iCloud em um dispositivo compatível com o Apple Cash e a autenticação de dois fatores configurada na conta do iCloud.

Ao configurar o Apple Cash, as mesmas informações fornecidas ao adicionar um cartão de crédito ou débito podem ser compartilhadas com o Green Dot Bank (associado da Apple) ou com a Apple Payments Inc. (uma subsidiária integral criada para proteger a privacidade dos usuários), a qual armazena e processa informações separadamente do restante da Apple, de maneira que o restante da Apple não tenha conhecimento. Essas informações são usadas somente para a resolução de problemas, prevenção de fraudes e fins regulatórios.

Os pedidos de dinheiro e as transferências entre usuários são iniciadas a partir do app Mensagens ou ao pedir à Siri. Quando um usuário tenta enviar dinheiro, o iMessage exibe a folha do Apple Pay. O saldo do Apple Cash sempre é usado primeiro. Se necessário, fundos adicionais são sacados de um segundo cartão de crédito ou débito adicionado pelo usuário ao app Wallet.

O cartão do Apple Cash no app Wallet pode ser usado com o Apple Pay para fazer pagamentos em lojas, apps e na web. O dinheiro na conta do Apple Cash também pode ser transferido para uma conta bancária. Além de dinheiro recebido de outro usuário, quantias podem ser adicionadas à conta do Apple Cash a partir de um cartão de débito ou pré-pago no app Wallet.

A Apple Payments Inc. armazena e pode usar os dados de transação para a resolução de problemas, prevenção de fraudes e fins regulatórios quando uma transação é concluída. O restante da Apple não sabe para quem o dinheiro foi enviado, de quem o dinheiro foi recebido ou onde uma compra foi feita com o cartão do Apple Cash.

Quando o usuário envia dinheiro com o Apple Pay, adiciona dinheiro a uma conta do Apple Cash ou transfere dinheiro para uma conta bancária, uma ligação é feita para os servidores do Apple Pay para obtenção de um nonce criptográfico, o qual é similar ao valor retornado para o Apple Pay dentro de apps. O nonce, assim como outros dados da transação, é passado ao Elemento Seguro para gerar uma assinatura de pagamento. Quando a assinatura de pagamento sai do Elemento Seguro, ela é passada aos servidores do Apple Pay. A autenticação, integridade e exatidão da transação são verificadas pelos servidores do Apple Pay por meio da assinatura de pagamento e do nonce. Em seguida, a transferência do dinheiro é iniciada e o usuário é notificado sobre uma transação concluída.

Se a transação envolver um cartão de crédito ou débito para adicionar dinheiro ao Apple Cash, enviar dinheiro a outro usuário ou fornecer dinheiro complementar se o saldo do Apple Cash for insuficiente, uma credencial de pagamento criptografada também será produzida e enviada aos servidores do Apple Pay, de forma semelhante à usada para o Apple Pay dentro de apps e sites.

Depois que o saldo da conta do Apple Cash excede uma certa quantia ou uma atividade incomum é detectada, o usuário é solicitado a verificar sua identidade. As informações fornecidas para verificar a identidade do usuário — como o número de previdência social ou respostas a perguntas (por exemplo, para confirmar o nome de uma rua na qual o usuário morou anteriormente) — são transmitidas com segurança para o associado da Apple e criptografadas com a chave desse associado. A Apple não pode descriptografar esses dados.

Apple Card

Aplicativo Apple Card no app Wallet

No iOS 12.4 ou posterior, macOS 10.14.6 ou posterior, watchOS 5.3 ou posterior, o Apple Card pode ser usado com o Apple Pay para fazer pagamentos em lojas, apps e na web.

Para inscrever-se para um Apple Card, o usuário deve ter uma sessão iniciada em sua conta do iCloud em um dispositivo iOS ou iPadOS compatível com o Apple Pay e a autenticação de dois fatores configurada na conta do iCloud. Quando a solicitação é aprovada, o Apple Card fica disponível no app Wallet ou em Ajustes > Wallet e Apple Pay) em dispositivos qualificados nos quais o usuário tenha uma sessão iniciada com seu ID Apple.

Ao solicitar um Apple Card, as informações de identificação do usuário são verificadas com segurança pelos parceiros provedores de identidade da Apple e compartilhadas com o Goldman Sachs Bank USA para fins de identificação e avaliação de crédito.

As informações fornecidas na solicitação, como o número de previdência social ou a imagem de um documento de identidade, são transmitidas com segurança aos parceiros provedores de identidade da Apple e/ou ao Goldman Sachs Bank USA criptografadas com as suas respectivas chaves. A Apple não pode descriptografar esses dados.

As informações de renda durante a aplicação e as informações de conta bancária usadas para o pagamento de contas são transmitidas com segurança ao Goldman Sachs Bank USA, criptografadas com a chave do banco. As informações sobre a conta bancária são salvas nas Chaves. A Apple não pode descriptografar esses dados.

Ao adicionar um Apple Card ao app Wallet, as mesmas informações fornecidas ao adicionar um cartão de crédito ou débito podem ser compartilhadas com o banco parceiro da Apple, o Goldman Sachs Bank USA, e com a Apple Payments Inc. Essas informações são usadas somente para a resolução de problemas, prevenção de fraudes e fins regulatórios.

Um cartão físico pode ser solicitado no Apple Card no app Wallet. Depois que o cartão físico é recebido pelo usuário, o cartão é ativado usando a etiqueta NFC presente no envelope do cartão físico. A etiqueta é exclusiva por cartão e não pode ser usada para ativar o cartão de outro usuário. Como opção, o cartão pode ser ativado manualmente nos ajustes da Wallet. Além disso, o usuário também tem a opção de bloquear ou desbloquear o cartão físico a qualquer momento com o app Wallet.

Detalhes de pagamentos com Apple Card e tíquetes da Apple Wallet

Os pagamentos devidos na conta do Apple Card podem ser feitos no app Wallet no iOS com Apple Cash e uma conta bancária. Os pagamentos de contas podem ser agendados como recorrente ou como um pagamento único em uma data específica com o Apple Cash e uma conta bancária. Quando um usuário faz um pagamento, uma ligação é feita para os servidores do Apple Pay para obtenção de um nonce criptográfico, semelhante ao Apple Cash. O nonce, assim como os detalhes da configuração do pagamento, é passado ao Elemento Seguro para gerar uma assinatura. Quando a assinatura de pagamento sai do Elemento Seguro, ela é passada aos servidores do Apple Pay. A autenticação, integridade e exatidão do pagamento são verificadas pelos servidores do Apple Pay através da assinatura e do nonce, e a ordem é passada ao Goldman Sachs Bank USA para processamento.

Para que os detalhes do número do Apple Card sejam mostrados no tíquete com o app Wallet, o usuário deve se autenticar com o Face ID, Touch ID ou um código. Ele pode ser substituído pelo usuário na seção de informações do cartão, desativando o anterior.

Cartões de transporte público no app Wallet

Em vários mercados do mundo, os usuários podem adicionar cartões de transporte público compatíveis ao app Wallet em modelos de iPhone e Apple Watch compatíveis. Dependendo da operadora do transporte, o usuário pode transferir o valor e o bilhete único de transporte público de um cartão físico para representações digitais na Apple Wallet ou fornecer um novo cartão de transporte público ao app Wallet a partir do app Wallet ou do app da administradora do cartão. Após a adição dos cartões de transporte público ao app Wallet, basta que os usuários segurem o iPhone ou Apple Watch próximo ao leitor para utilizarem o transporte público. Alguns cartões também podem ser usados para fazer pagamentos.

Os cartões de transporte público adicionados são associados à conta do iCloud do usuário. Se o usuário adicionar mais de um cartão ao app Wallet, a Apple ou a administradora do cartão de transporte público pode ser capaz de associar as informações pessoais do usuário às informações de conta dos cartões. Os cartões de transporte público e as transações são protegidas por um conjunto de chaves criptográficas hierárquicas.

Durante o processo de transferência do saldo do cartão físico para o app Wallet, o usuário é solicitado a digitar informações específicas do cartão. Também pode ser necessário que os usuários forneçam informações pessoais como comprovante da propriedade do cartão. Ao transferir tíquetes do iPhone para o Apple Watch, ambos os dispositivos devem estar online durante a transferência.

O saldo pode ser recarregado com fundos de cartões de crédito, débito e pré-pagos por meio da Wallet ou a partir do app da administradora do cartão de transporte público. A segurança da recarga de saldo ao usar o Apple Pay é descrita em Pagamento com cartões de crédito e débito em apps com o Apple Pay. O processo de provisão do cartão de transporte público a partir do app da administradora do cartão de transporte público é descrito em Adição de cartões de crédito ou débito em um app de administradora de cartões.

Se for possível fazer o provisionamento a partir de um cartão físico, a administradora do cartão de transporte público possui as chaves criptográficas necessárias para autenticar o cartão físico e verificar os dados digitados pelo usuário. Depois de verificar os dados, o sistema cria um Número de Conta do Dispositivo para o Elemento Seguro e ativa o tíquete recém-adicionado no app Wallet com o saldo transferido. Em algumas cidades, após a conclusão do provisionamento com o cartão físico, ele é desativado.

No final de qualquer um dos tipos de provisionamento, se o saldo do cartão de transporte público estiver armazenado no dispositivo, ele é criptografado e armazenado em um applet designado no Elemento Seguro. A operadora de transporte público possui as chaves para realizar operações criptográficas nos dados do cartão para transações de saldo.

Por padrão, os usuários se beneficiam da experiência integrada do Transporte Público Expresso, o que permite que paguem e usem transportes públicos sem exigir Touch ID, Face ID ou um código. Informações como estações visitadas recentemente, histórico de transações e tíquetes adicionais podem ser acessadas por qualquer leitor de cartão por proximidade por perto com o Modo Expresso ativo. Os usuários podem desativar o Transporte Público Expresso para ativar o requisito autorização com de Touch ID, Face ID ou código nos ajustes da Wallet e Apple Pay.

Assim como com outros cartões do Apple Pay, os usuários podem suspender ou remover cartões de transporte público, bastando:

- Apagar o dispositivo remotamente com o Buscar
- Ativar o Modo Perdido com o Buscar
- Usar o comando de apagamento remoto do gerenciamento de dispositivos móveis (MDM)
- Remover todos os cartões da página da conta do ID Apple
- Remover todos os cartões em iCloud.com
- Remover todos os cartões do app Wallet
- Remover o cartão no app da administradora do cartão

Os servidores do Apple Pay notificam a operadora de transporte público para suspender ou desativar esses cartões. Se o usuário remover um cartão de transporte público de um dispositivo on-line, ele pode adicioná-lo novamente a um dispositivo com sessão iniciada com o mesmo ID Apple para recuperar o saldo. Se o dispositivo estiver off-line, desligado ou inutilizável, a recuperação pode não ser possível.

Cartões de crédito e débito para transporte público no app Wallet

Em algumas cidades, os leitores de transporte público aceitam o pagamento de viagens com cartões EMV. Quando os usuários apresentam um cartão de crédito ou débito a esses leitores, a autenticação do usuário é necessária assim como descrito em "Pagamento com cartões de crédito e débito em lojas".

No iOS 12.3 ou posterior, alguns cartões EMV de crédito/débito existentes no app Wallet podem ser ativados para o Transporte Público Expresso, que permite que o usuário pague uma viagem em operadoras de transporte público compatíveis sem exigir Touch ID, Face ID ou um código. Quando o usuário aprovisiona um cartão EMV de crédito ou débito, o primeiro cartão aprovisionado no app Wallet é ativado para o Transporte Público Expresso. Para desativar o Transporte Público Expresso em um cartão, o usuário pode tocar no botão Mais na parte frontal do cartão no app Wallet e definir Transporte Público Expresso > Nenhum. O usuário também pode selecionar um cartão de crédito ou débito diferente como seu cartão de Transporte Público Expresso no app Wallet. O Touch ID, Face ID ou um código são exigidos para reativar ou selecionar um cartão diferente para o Transporte Público Expresso.

O Apple Card e o Apple Cash são qualificados para o Transporte Público Expresso.

Cartões de ID de estudante no app Wallet

No iOS 12 ou posterior, alunos, docentes e funcionários de instituições participantes podem adicionar seus cartões de ID de estudante ao app Wallet em modelos de iPhone e Apple Watch compatíveis para acessar locais e fazer pagamentos em todos os lugares onde o cartão for aceito.

Um usuário adiciona seu cartão de ID de estudante ao app Wallet por meio de um app fornecido pelo emissor do cartão ou escola participante. O processo técnico pelo qual isso ocorre é o mesmo que o descrito na seção Adição de cartões de crédito ou débito em um app de administradora de cartões. Além disso, os apps das administradoras devem ser compatíveis com a autenticação de dois fatores nas contas que guardam o acesso aos cartões de ID de estudante. Um cartão pode estar configurado simultaneamente em até dois dispositivos Apple compatíveis, com sessão iniciada no mesmo ID Apple.

Quando um cartão de ID de estudante é adicionado ao app Wallet, o Modo Expresso é ativado por padrão. Os cartões de ID de estudante no Modo Expresso interagem com terminais compatíveis sem Touch ID, Face ID, autenticação por código ou clique duplo no botão lateral do Apple Watch. Para desativar esse recurso, o usuário pode tocar no botão Mais, na parte frontal do cartão no app Wallet e desativar o Modo Expresso. O Touch ID, Face ID ou um código são exigidos para reativar o Modo Expresso.

Os métodos para desativar ou remover cartões de ID de estudante são:

- Apagar o dispositivo remotamente com o Buscar

- Ativar o Modo Perdido com o Buscar
- Usar o comando de apagamento remoto do gerenciamento de dispositivos móveis (MDM)
- Remover todos os cartões da página da conta do ID Apple
- Remover todos os cartões em iCloud.com
- Remover todos os cartões do app Wallet
- Remover o cartão no app da administradora do cartão

iMessage

Visão geral do iMessage

O iMessage da Apple é um serviço de mensagens para dispositivos iOS e iPadOS, Apple Watch e computadores Mac. O iMessage oferece suporte a texto e anexos, como fotos, contatos, localizações, links e anexos diretamente em uma mensagem, como um ícone de sinal de positivo. As mensagens aparecem em todos os dispositivos registrados de um usuário para que a conversa possa ser continuada em qualquer um deles. O iMessage faz amplo uso do serviço de Notificações Push da Apple (APNs). A Apple não registra o conteúdo de mensagens ou anexos, que são protegidos por criptografia de ponta a ponta, para que ninguém, exceto o remetente e o destinatário, possa acessá-los. A Apple não pode descriptografar os dados.

Quando um usuário ativa o iMessage em um dispositivo, o dispositivo gera pares de chaves de criptografia e assinatura para uso com o dispositivo. Para criptografia, há uma chave de criptografia RSA de 1280 bits assim como uma chave de criptografia EC de 256 bits na curva NIST P-256. Para assinaturas, são usadas chaves de assinatura ECDSA de 256 bits. As chaves privadas são salvas nas Chaves do dispositivo e ficam disponíveis apenas após o primeiro desbloqueio. As chaves públicas são enviadas para o Serviço de Identidade da Apple (IDS), onde são associadas ao número de telefone ou endereço de e-mail do usuário, juntamente ao endereço APNs do dispositivo.

Conforme os usuários adicionam dispositivos para uso no iMessage, suas chaves de criptografia e assinatura pública, endereços APNs e números de telefone associados são adicionados ao serviço de diretório. Os usuários também podem adicionar outros endereços de e-mail, que são verificados através do envio de um link de confirmação. Os números de telefone são verificados pela rede e SIM da operadora. Em algumas redes, isso requer o uso de SMS (um diálogo de confirmação é apresentado ao usuário se o SMS tiver custo). A verificação do número de telefone pode ser exigida para vários serviços do sistema além do iMessage, como FaceTime e iCloud. Todos os dispositivos registrados do usuário exibem uma mensagem de alerta quando um novo dispositivo, número de telefone ou endereço de e-mail é adicionado.

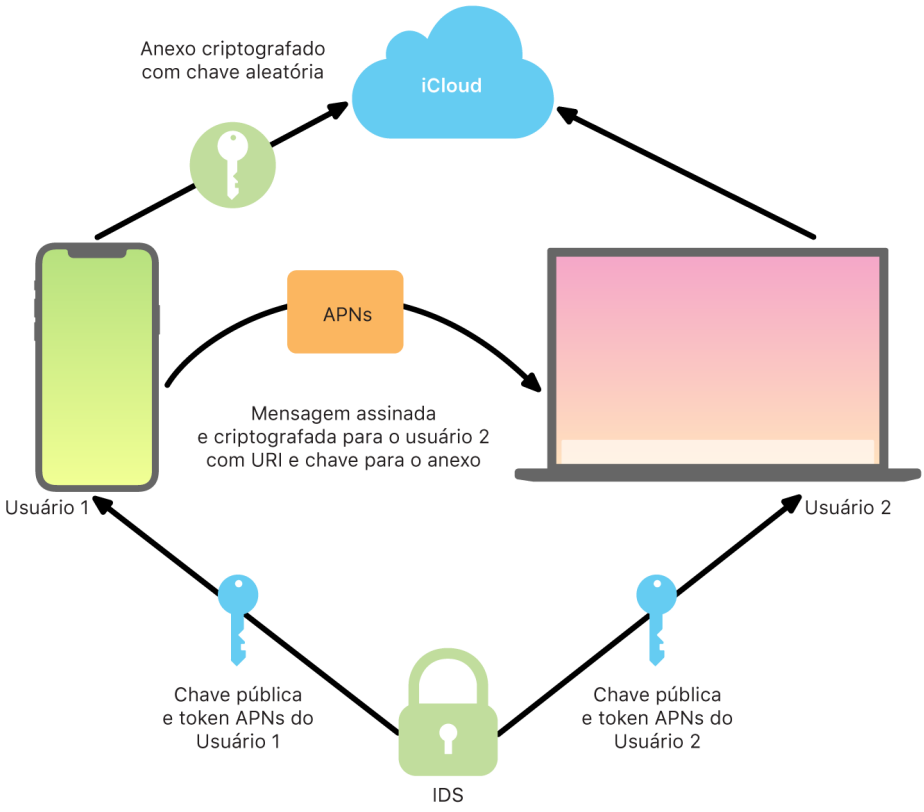
Como o iMessage envia e recebe mensagens

Para iniciar uma nova conversa do iMessage, os usuários digitam um endereço ou nome. Se um número de telefone ou endereço de e-mail for digitado, o dispositivo contata o Serviço de Identidade da Apple (IDS) para obter as chaves públicas e endereços do APNs de todos os dispositivos associados ao destinatário. Se o usuário digitar um nome, primeiro o dispositivo usa o app Contatos do usuário para coletar números de telefone e endereços de e-mail associados ao nome para depois obter as chaves públicas e endereços APNs do IDS.

A mensagem sendo enviada é criptografada individualmente para cada um dos dispositivos do destinatário. As chaves públicas de criptografia e assinatura dos dispositivos de destino são obtidas do IDS. Para cada dispositivo de destino, o dispositivo remetente gera um valor de 88 bits aleatório e o usa como uma chave HMACSHA256 para construir um valor de 40 bits derivado das chaves públicas do remetente e do destinatário e do texto simples. A concatenação dos valores de 88 bits e 40 bits cria uma chave de 128 bits, a qual usa AES para criptografar a mensagem no modo CTR. O valor de 40 bits é usado pelo lado do destinatário para verificar a integridade do texto simples descriptografado. Essa chave AES única por mensagem é criptografada à chave pública do dispositivo de destino usando RSA-OAEP. Depois, o hash SHA-1 é aplicado à combinação do texto e da chave da mensagem criptografada, e o hash é assinado com ECDSA usando a chave de assinatura privada do dispositivo de envio. A partir do iOS 13 e iPadOS 13.1, os dispositivos podem usar criptografia ECIES em vez de RSA.

As mensagens resultantes, uma para cada dispositivo de destino, consistem do texto da mensagem criptografada, chave da mensagem criptografada e assinatura digital do remetente. Elas então são despachadas para o APNs para entrega. Metadados, como a marca temporal e informações de roteamento do APNs, não são criptografados. A comunicação com o APNs é criptografada usando um canal TLS de encaminhamento secreto.

O APNs só pode transmitir mensagens de até 4 KB ou 16 KB, dependendo da versão do iOS ou iPadOS. Se a mensagem de texto for muito longa ou se um anexo (como uma foto) estiver incluído, o anexo é criptografado com AES no modo CTR com uma chave de 256 bits gerada aleatoriamente e enviado para o iCloud. A chave AES do anexo, seu Identificador Uniforme de Recursos (URI) e um hash SHA-1 de sua forma criptografada são enviados para o destinatário na forma de conteúdo de uma iMessage, com suas confidencialidade e integridade protegidas através da criptografia normal do iMessage, como mostrado no diagrama a seguir.



Como o iMessage envia e recebe mensagens.

Nas conversas em grupo, este processo é repetido para cada destinatário e seus dispositivos.

No lado recipiente, cada dispositivo recebe sua cópia da mensagem do APNs e, se necessário, obtém o anexo do iCloud. O número de telefone ou endereço de e-mail do remetente é correspondido ao contato do destinatário para que um nome seja exibido, quando possível.

Assim como em todas as notificações push, a mensagem é apagada do APNs quando entregue. No entanto, ao contrário de outras notificações push, as mensagens do iMessage são colocadas em fila para entrega a dispositivos off-line. As mensagens são armazenadas por 30 dias.

Compartilhamento de nomes e fotos no iMessage

O compartilhamento de nomes e fotos no iMessage permite que os usuários compartilhem nomes e fotos no iMessage. O usuário pode selecionar informações do seu Cartão Pessoal ou personalizar o nome e incluir qualquer imagem que desejar. O compartilhamento de nomes e fotos no iMessage usa um sistema de dois estágios para distribuir o nome e a foto.

Os dados são subdivididos em campos, cada um criptografado e autenticado separadamente e também autenticados em conjunto com o processo a seguir. Há três campos:

- Nome
- Foto
- Nome do arquivo da foto

A primeira etapa da criação de dados é a geração aleatória de uma chave de registro de 128 bits no dispositivo. Em seguida, essa chave de registro é derivada com HKDF-HMAC-SHA256 para criar três subchaves: Chave 1:Chave 2:Chave 3 = HKDF(chave de registro, “apelidos”). Para cada campo, um IV aleatório de 96 bits é gerado e os dados são criptografados com AES-CTR e a Chave 1. Em seguida, um código de autenticação de mensagem (MAC) é calculado com HMAC-SHA256 usando a Chave 2 e abrangendo o nome, o campo IV e o texto cifrado do campo. Por último, o conjunto de valores MAC dos campos individuais é concatenado e seu MAC é calculado com HMAC-SHA256 usando a Chave 3. O MAC de 256 bits é armazenado juntamente com os dados criptografados. Os primeiros 128 bits desse MAC são usados como o ID de Registro.

O registro criptografado é armazenado no banco de dados público do CloudKit com esse ID de Registro. Esse registro nunca é alterado. Todas as vezes que o usuário resolve mudar seu nome e foto, um novo registro criptografado é gerado. Quando o usuário 1 resolve compartilhar seu nome e foto com o usuário 2, ele envia a chave de registro juntamente com o ID de Registro dentro do payload do iMessage, que é criptografado.

Quando o dispositivo do usuário 2 recebe esse payload do iMessage, ele observa que o payload contém um ID de Registro e chave de apelido e foto. O dispositivo do usuário 2 acessa o banco de dados público do CloudKit para recuperar o nome e a foto criptografados no ID de Registro e os envia na iMessage.

Depois que a recuperação é realizada, o dispositivo do usuário 2 descriptografa o payload e verifica a assinatura usando o próprio ID de Registro. Caso a verificação seja concluída com sucesso, o Nome e a Foto são apresentados ao usuário 2, que pode optar por adicioná-los aos seus contatos ou usá-los no app Mensagens.

Bate-papo de Negócios

O Bate-papo de Negócios é um serviço de mensagens que permite que os usuários se comuniquem com uma empresa usando o app Mensagens. Somente usuários podem iniciar a conversa e a empresa recebe um identificador simples sobre o usuário. A empresa não recebe o número de telefone, endereço de e-mail ou informações da conta do iCloud do usuário. Quando o usuário conversa com a Apple, a Apple recebe um ID de Bate-papo de Negócios associado ao ID Apple dele. Os usuários permanecem no controle sobre querer ou não estabelecer a comunicação. O apagamento de uma conversa do Bate-papo de Negócios remove-a do app Mensagens do usuário e bloqueia o envio de mensagens pela empresa ao usuário.

As mensagens enviadas à empresa são criptografadas individualmente entre o dispositivo do usuário e os servidores de mensagens da Apple. Os servidores de mensagens da Apple descriptografam essas mensagens e as retransmitem à empresa via TLS. As respostas das empresas são enviadas, de maneira similar, via TLS aos servidores de mensagens da Apple, que, por sua vez, criptografam novamente a mensagem para o dispositivo do usuário. Da mesma forma como no iMessage, as mensagens são colocadas em fila para entrega a dispositivos off-line por até 30 dias.

FaceTime

O FaceTime é o serviço de ligações de vídeo e áudio da Apple. De maneira similar ao iMessage, o FaceTime também usa o serviço de Notificações Push da Apple (APNs) para estabelecer uma conexão inicial aos dispositivos registrados do usuário. O conteúdo de áudio/vídeo de ligações do FaceTime é protegido por criptografia de ponta a ponta, para que ninguém, exceto o remetente e o destinatário, possa acessá-lo. A Apple não pode descriptografar os dados.

A conexão inicial do FaceTime é feita através de uma infraestrutura de servidores da Apple, que retransmite pacotes de dados entre os dispositivos registrados do usuário. Através do uso de notificações APNs e mensagens STUN (Session Traversal Utilities for NAT) pela conexão de retransmissão, os dispositivos verificam seus certificados de identidade e estabelecem um segredo compartilhado para cada sessão. O segredo compartilhado é usado para derivar chaves de sessão para os canais de mídia transmitidos através do SRTP (Secure Real-time Transport Protocol). Os pacotes SRTP são criptografados com AES-256 em Counter Mode e HMAC-SHA1. Depois da conexão inicial e da configuração de segurança, o FaceTime usa STUN e ICE (Internet Connectivity Establishment) para estabelecer uma conexão peer-to-peer entre os dispositivos, se possível.

O FaceTime em Grupo estende o FaceTime para oferecer suporte a até 33 participantes simultâneos. Assim como no FaceTime clássico entre dois usuários, as ligações são criptografadas entre os dispositivos dos participantes convidados. Embora o FaceTime em Grupo reutilize a maior parte da infraestrutura e design do FaceTime entre dois usuários, as ligações do FaceTime em Grupo contam com um novo mecanismo de estabelecimento de chaves construído sobre a autenticidade oferecida pelo Serviço de Identidade da Apple (IDS). Esse protocolo proporciona sigilo avançado, o que significa que o comprometimento do dispositivo de um usuário não permitirá o vazamento do conteúdo de ligações anteriores. As chaves da sessão são embaladas por meio de AES-SIV e distribuídas entre os participantes usando uma construção ECIES com chaves transitórias P-256 ECDH.

Quando um novo número de telefone ou endereço de e-mail é adicionado a uma ligação em andamento do FaceTime em Grupo, os dispositivos ativos estabelecem novas chaves de mídia e nunca compartilham chaves usadas anteriormente com os dispositivos recém-convidados.

Buscar

Visão geral do Buscar

O app Buscar combina o Buscar iPhone e o Buscar Amigos em um único app no iOS, iPadOS e macOS. O Buscar pode ajudar usuários a localizar um dispositivo perdido — e até um Mac que esteja off-line. Um dispositivo on-line pode simplesmente comunicar sua localização ao usuário via iCloud. Para funcionar off-line, o Buscar envia sinais Bluetooth de curto alcance do dispositivo perdido, os quais podem ser detectados por outros dispositivos Apple sendo usados por perto. Esses dispositivos por perto retransmitem a localização detectada do dispositivo perdido para o iCloud, de forma que usuários possam localizá-lo no app Buscar — ao mesmo tempo em que protege a privacidade e segurança de todos os usuários envolvidos. O Buscar funciona até mesmo com um Mac que esteja off-line e em repouso.

Ao utilizar Bluetooth e as centenas de milhões de dispositivos iOS, iPadOS e macOS sendo usados em todo o mundo, o usuário pode localizar um dispositivo perdido, mesmo que o dispositivo não consiga se conectar a uma rede celular ou Wi-Fi. Qualquer dispositivo iOS, iPadOS ou macOS que possui a "busca off-line" ativada nos ajustes do Buscar pode funcionar como um "dispositivo localizador". Isso significa que o dispositivo pode usar Bluetooth para detectar a presença de outro dispositivo off-line perdido e usar sua conexão de rede para informar ao proprietário uma localização aproximada. Quando um dispositivo tem a busca off-line ativada, ele também pode ser localizado por outros participantes da mesma maneira. Toda essa interação é anônima, criptografada de ponta a ponta e foi projetada para eficiência no uso da bateria e dos dados, de forma que haja um impacto mínimo na duração da bateria, no uso do plano de dados celulares e que a privacidade do usuário seja protegida.

Nota: o Buscar pode não estar disponível em todos os países ou regiões.

Criptografia de ponta a ponta no Buscar

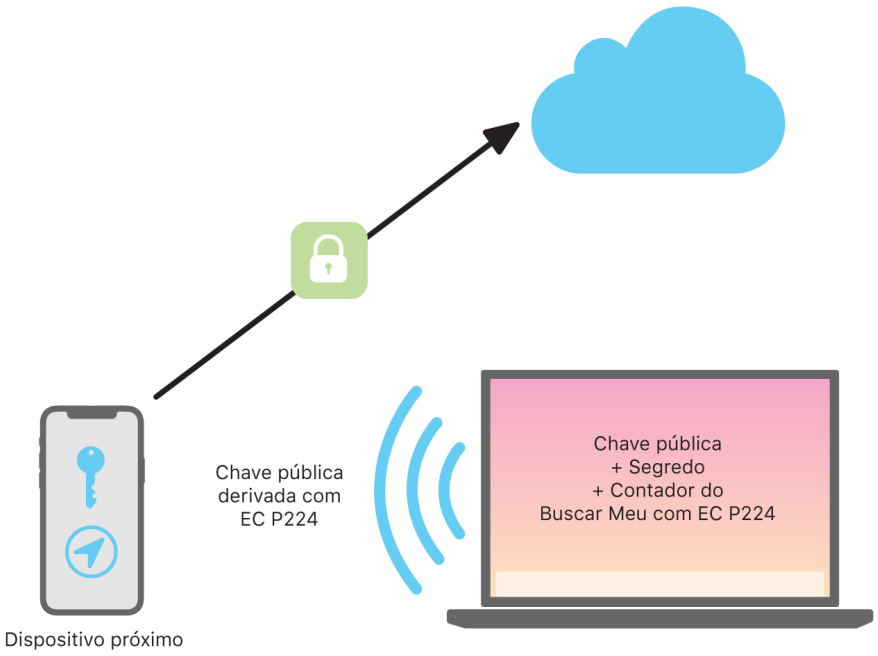
O Buscar possui uma base de criptografia avançada de chave pública. Quando a busca off-line está ativada nos ajustes do Buscar, um par de chaves de criptografia EC P-224 indicado por {d,P} é gerado diretamente no dispositivo, sendo que *d* é a chave privada e *P* a chave pública. Além disso, um SK_0 secreto de 256 bits e um contador $_i$ são inicializados como zero. O par privado de chaves e o segredo nunca são enviados à Apple, sendo sincronizados apenas entre os outros dispositivos do usuário com criptografia de ponta a ponta, usando as Chaves do iCloud. O segredo e o contador são usados para derivar a chave simétrica atual SK_i com esta construção recursiva: $SK_i = KDF(SK_{i-1}, \text{"update"})$.

Com base na chave SK_i, dois inteiros grandes u_i e v_i são calculados com (u_i,v_i) = KDF(SK_i, “diversify”). Tanto a chave privada P-224 indicada por *d* quanto a chave pública correspondente indicada por *P* são derivadas usando uma relação afim que envolve os dois inteiros para calcular um par de chaves de curta duração: a chave privada derivada é d_i em que $d_i = u_i * d + v_i$ (módulo da ordem da curva P-224) e a parte pública correspondente é P_i e segue $P_i = u_i*P + v_i*G$.

Quando um dispositivo é perdido e não consegue se conectar a uma rede celular ou Wi-Fi (um MacBook deixado sobre o banco de uma praça, por exemplo), ele começa a transmitir periodicamente a chave pública derivada P_i por um período limitado em um payload Bluetooth. Graças ao uso de P-224, a representação da chave pública cabe em um único payload Bluetooth. Para ajudar a localizar o dispositivo off-line, os dispositivos próximos podem criptografar a localização dele com a chave pública. A cada 15 minutos, aproximadamente, a chave pública é substituída por uma nova, usando um valor incrementado do contador e o processo acima, de forma que o usuário não possa ser rastreado por um identificador persistente. O mecanismo de derivação impede que as várias chaves públicas P_i sejam ligadas ao mesmo dispositivo.

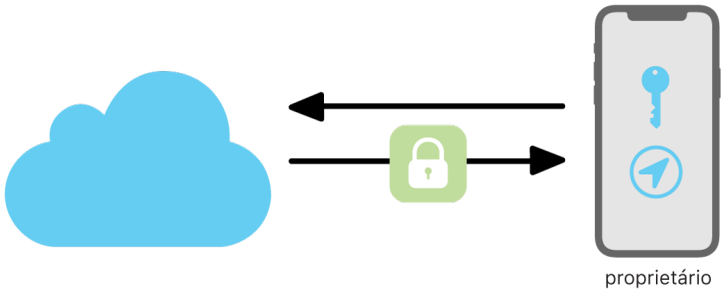
Localização de dispositivos perdidos no Buscar

Qualquer dispositivo Apple que esteja ao alcance do Bluetooth e possua a busca off-line ativada pode detectar este sinal e ler a chave transmitida atual P_i. Os dispositivos localizadores usam a construção ECIES e a chave pública P_i da transmissão para criptografar sua localização atual e encaminhá-la à Apple. A localização criptografada é associada a um índice de servidor, que é calculado como o hash SHA-256 da chave pública P-224 P_i obtida no payload Bluetooth. A Apple nunca possui a chave de descriptografia, portanto não consegue ler a localização criptografada pelo localizador. O proprietário do dispositivo perdido pode reconstruir o índice e descriptografar a localização criptografada.



Como o Buscar localiza dispositivos.

Ao tentar localizar o dispositivo perdido, um intervalo esperado de valores do contador é estimado para o período de busca. Com o conhecimento da chave privada P-224 original *d* e dos valores secretos SK_i no intervalo de valores do contador do período de busca, o proprietário pode reconstruir o conjunto de valores $\{d_i, \text{SHA-256}(P_i)\}$ de todo o período de busca. O dispositivo do proprietário usado para localizar o dispositivo perdido pode consultar o servidor usando o conjunto de valores de índice $\text{SHA-256}(P_i)$ e transferir as localizações criptografadas do servidor. Em seguida, o app Buscar descriptografa localmente as localizações criptografadas com as chaves privadas correspondentes d_i e mostra o local aproximado do dispositivo perdido no app. Relatórios de localização de vários dispositivos localizadores são combinados pelo app do proprietário para gerar uma localização mais precisa.



Como o proprietário obtém a localização do dispositivo no Buscar.

Se um usuário tiver o Buscar iPhone ativado em seu dispositivo, a busca off-line é ativada por padrão ao atualizar o dispositivo para iOS 13, iPadOS 13.1 e macOS 10.15. Isso garante que todo usuário tenha a melhor chance possível de localizar seu dispositivo caso ele seja perdido. Porém, se em algum momento o usuário preferir não participar, pode desativar a busca off-line nos ajustes do Buscar no dispositivo. Quando a busca off-line está desativada, o dispositivo não atua mais como localizador nem pode ser detectado por outros dispositivos localizadores. Contudo, o usuário ainda pode localizar o dispositivo, desde que ele possa se conectar a uma rede Wi-Fi ou celular.

Manutenção da anonimidade de usuários e dispositivos no Buscar

Além de garantir que as informações sobre a localização e outros dados sejam totalmente criptografados, as identidades dos participantes permanecem privadas entre si e com a Apple. O tráfego enviado pelos dispositivos localizadores à Apple não contém nenhuma informação de autenticação no conteúdo ou nos cabeçalhos. Como resultado, a Apple não sabe quem são o localizador ou o proprietário do dispositivo encontrado. Além disso, a Apple não registra informações que revelariam a identidade do localizador nem retém informações que permitiriam a correlação do localizador com o proprietário. O proprietário do dispositivo recebe apenas a informação criptografada sobre a localização, que é descriptografada e mostrada no app Buscar sem indicação de quem encontrou o dispositivo.

Visualização de dispositivos off-line no Buscar

Quando um dispositivo off-line perdido é localizado, o usuário recebe uma notificação e uma mensagem de e-mail informando que o dispositivo foi encontrado. Para visualizar a localização do dispositivo perdido, o usuário abre o app Buscar e seleciona a aba Dispositivos. Em vez de mostrar o dispositivo em um mapa em branco, como aconteceria antes do dispositivo ser encontrado, o Buscar mostra uma localização no mapa com um endereço aproximado e a informação de há quanto tempo o dispositivo foi detectado. Se houver mais relatórios de localização, a localização e a marca temporal são atualizadas automaticamente. Embora os usuários não possam reproduzir um som em um dispositivo off-line ou apagá-lo remotamente, eles podem usar as informações sobre a localização para refazer seus passos ou tomar outras medidas que ajudem a recuperá-lo.

Continuidade

Visão geral da Continuidade

A Continuidade aproveita-se de tecnologias como iCloud, Bluetooth e Wi-Fi para permitir que usuários continuem a atividade de um dispositivo em outro, façam e recebam ligações telefônicas, enviem e recebam mensagens de texto, e compartilhem uma conexão celular à internet.

Handoff

Com o Handoff, quando os dispositivos iOS, iPadOS e macOS de um usuário estão próximos, o usuário pode passar aquilo em que estiver trabalhando de um dispositivo para outro. O Handoff permite que o usuário alterne entre dispositivos e continue trabalhando imediatamente.

Quando um usuário inicia a sessão no iCloud em um segundo dispositivo compatível com o Handoff, os dois dispositivos estabelecem um emparelhamento Bluetooth Low Energy (BLE) 4.2 fora de banda usando o APNs. As mensagens individuais são criptografadas de maneira bem semelhante às mensagens do iMessage. Depois de emparelhados, cada dispositivo gera uma chave AES simétrica de 256 bits que é armazenada nas Chaves do dispositivo. A chave pode criptografar e autenticar os anúncios de BLE que comunicam a atividade atual do dispositivo para outros dispositivos emparelhados que usam o iCloud – usando AES-256 no modo GCM, com medidas de proteção contra reprodução.

Na primeira vez que um dispositivo recebe um anúncio de uma nova chave, ele estabelece uma conexão BLE ao dispositivo originário e realiza uma troca de chaves de criptografia de anúncios. O uso de criptografia padrão BLE 4.2 mantém essa conexão em segurança, assim como a criptografia de mensagens individuais, que assemelha-se à criptografia do iMessage. Em algumas situações, essas mensagens são enviadas usando APNs em vez de BLE. O payload da atividade é protegido e transferido da mesma maneira que uma iMessage.

Handoff entre apps nativos e sites

O Handoff permite que um app nativo do iOS, iPadOS e macOS retome a atividade do usuário em uma página web em domínios controlados legitimamente pelo desenvolvedor do app. Ele também permite que a atividade do usuário do app nativo seja retomada em um navegador.

Para impedir que apps nativos reivindiquem a retomada de sites que não sejam controlados pelo desenvolvedor, o app precisa demonstrar controle legítimo sobre os domínios web que deseja retomar. O controle sobre um domínio de site é estabelecido através do mecanismo de credenciais web compartilhadas. Para obter detalhes, consulte Acesso de apps a códigos salvos. O sistema deve validar o controle do nome de domínio de um app antes que o app tenha permissão para aceitar o Handoff da atividade do usuário.

A fonte do Handoff de uma página web pode ser qualquer navegador que tenha adotado as APIs do Handoff. Quando o usuário visualiza uma página web, o sistema anuncia o nome do domínio da página web em bytes de anúncio de Handoff criptografados. Somente os outros dispositivos do usuário são capazes de descriptografar os bytes de anúncio.

No dispositivo de destino, o sistema detecta que um app nativo instalado aceita o Handoff do nome de domínio anunciado e exibe o ícone do app nativo como opção de Handoff. Quando aberto, o app nativo recebe o URL completo e o título da página web. Nenhuma outra informação é passada do navegador para o app nativo.

Em contrapartida, um app nativo pode especificar um URL alternativo quando o dispositivo que estiver recebendo o Handoff não tiver o mesmo app nativo instalado. Nesse caso, o sistema exibe o navegador padrão do usuário como opção de app Handoff (caso o navegador tenha adotado as APIs do Handoff). Quando o Handoff é solicitado, o navegador é aberto e recebe o URL alternativo fornecido pelo app de origem. Não há requisitos para que a URL alternativa seja limitada a nomes de domínios controlados pelo desenvolvedor do app nativo.

Handoff de dados maiores

Além do uso de recursos básicos do Handoff, alguns apps podem optar por usar APIs que oferecem suporte ao envio de uma quantidade maior de dados através da tecnologia Wi-Fi peer-to-peer criada pela Apple (de forma similar ao AirDrop). O app Mail, por exemplo, usa essas APIs para que o rascunho de um e-mail (que talvez tenha anexos grandes) possa usar o Handoff.

Quando um app usa essa capacidade, a troca entre dois dispositivos é iniciada da mesma forma que no Handoff. No entanto, depois de receber o payload inicial usando Bluetooth Low Energy (BLE), o dispositivo receptor inicia uma nova conexão via Wi-Fi. Nessa conexão criptografada (com TLS), os dispositivos trocam seus certificados de identidade do iCloud. A identidade nos certificados é comparada com a identidade do usuário para verificá-la. Dados adicionais de payload são enviados por essa conexão criptografada até que a transferência seja concluída.

Área de Transferência Universal

A Área de Transferência Universal baseia-se no Handoff para passar o conteúdo da área de transferência de um usuário entre dispositivos com segurança, o que possibilita que o usuário copie em um dispositivo e cole em outro. O conteúdo é protegido da mesma maneira que outros dados de Handoff e compartilhado por padrão com a Área de Transferência Universal, a não ser que o desenvolvedor do app opte por não permitir o compartilhamento.

Os apps têm acesso aos dados da área de transferência independentemente de o usuário ter colado a área de transferência no app. Com a Área de Transferência Universal, esse acesso aos dados é ampliado a apps nos outros dispositivos do usuário (conforme estabelecido pelo início de sessão no iCloud).

Retransmissão de ligações celulares do iPhone

Quando o Mac, iPad, iPod touch ou HomePod de um usuário está na mesma rede Wi-Fi de seu iPhone, ele pode usar a conexão celular do iPhone para fazer e receber ligações telefônicas. A configuração requer que os dispositivos tenham uma sessão iniciada no iCloud e no FaceTime usando o mesmo ID Apple.

Quando uma ligação é recebida, todos os dispositivos configurados são notificados por meio do serviço de Notificações Push da Apple (APNs) e cada notificação usa a mesma criptografia de ponta a ponta do iMessage. Os dispositivos que estão na mesma rede mostram a notificação da ligação. Depois de atender à ligação, o áudio é transmitido continuamente do iPhone do usuário usando uma conexão peer-to-peer segura entre os dois dispositivos.

Quando uma ligação é atendida em um dispositivo, o toque de dispositivos próximos emparelhados com o iCloud é interrompido com um breve anúncio por meio de Bluetooth Low Energy (BLE). Os bytes do anúncio são criptografados pelo mesmo método dos anúncios do Handoff.

As ligações feitas também são retransmitidas para o iPhone através do APNs. De forma semelhante, o áudio é transmitido pela conexão peer-to-peer segura entre os dispositivos. Os usuários podem desativar a retransmissão de ligações telefônicas em um dispositivo, bastando desativar “Ligações via iPhone” nos ajustes do FaceTime.

Encaminhamento de Mensagens do iPhone

O Encaminhamento de Mensagens envia automaticamente as mensagens de texto SMS recebidas em um iPhone para um iPad, iPod touch ou Mac registrado do usuário. Cada dispositivo deve ter uma sessão iniciada no iMessage usando o mesmo ID Apple. Quando o Encaminhamento de Mensagens está ativado, o registro se dá automaticamente nos dispositivos dentro do círculo de confiança de um usuário se a autenticação de dois fatores estiver ativada. Caso contrário, o registro é verificado em cada dispositivo através da digitação de um código numérico aleatório de seis dígitos gerado pelo iPhone.

Após os dispositivos estarem conectados, o iPhone criptografa e encaminha as mensagens de texto SMS recebidas para cada dispositivo, usando os métodos descritos em iMessage. As respostas são enviadas de volta para o iPhone com o mesmo método, e o iPhone envia a resposta como uma mensagem de texto com o mecanismo de transmissão de SMS da operadora. O Encaminhamento de Mensagens pode ser ativado ou desativado nos ajustes do Mensagens.

Instant Hotspot

Os dispositivos iOS e iPadOS que oferecem suporte ao Instant Hotspot usam Bluetooth Low Energy (BLE) para descoberta e comunicação com dispositivos que tenham uma sessão iniciada na mesma conta individual do iCloud ou contas usadas com o Compartilhamento Familiar (no iOS 13 e iPadOS). Os computadores Mac compatíveis (com OS X 10.10 ou posterior) usam a mesma tecnologia para descoberta e comunicação com dispositivos iOS e iPadOS que usam Instant Hotspot.

Inicialmente, quando um usuário acessa os ajustes de Wi-Fi em um dispositivo, ele emite um anúncio BLE contendo um identificador com o qual todos os dispositivos que tenham uma sessão iniciada na mesma conta do iCloud concordam. O identificador é gerado a partir de um DSID (Identificador de Sinalização de Destino) que é atrelado à conta do iCloud e alternado periodicamente. Quando outros dispositivos que têm uma sessão iniciada na mesma conta do iCloud estão próximos e oferecem suporte ao Acesso Pessoal, eles detectam o sinal e respondem, comunicando a disponibilidade para usar o Instant Hotspot.

Quando um usuário que não faz parte do Compartilhamento Familiar escolhe um iPhone ou iPad para Acesso Pessoal, uma solicitação para ativar o Acesso Pessoal é enviada ao dispositivo. A solicitação é enviada através de um link que usa criptografia BLE, e criptografada de forma semelhante ao iMessage. Em seguida, o dispositivo responde através do mesmo link BLE usando a mesma criptografia por mensagem com informações de conexão para o Acesso Pessoal.

Para usuários que fazem parte do Compartilhamento Familiar, as informações de conexão ao Acesso Pessoal são compartilhadas com segurança ao usar um mecanismo similar ao usado por dispositivos HomeKit para sincronizar informações. Especificamente, a segurança da conexão que compartilha as informações do acesso entre os usuários é feita com uma chave efêmera ECDH (Curve25519) que é autenticada com as respectivas chaves públicas Ed25519 específicas do dispositivo do usuário. As chaves públicas usadas são aquelas que foram previamente sincronizadas entre os membros do Compartilhamento Familiar com IDS quando o Compartilhamento Familiar foi estabelecido.

Segurança de Rede

Visão geral da segurança de rede

Além das medidas de segurança integradas que a Apple usa para proteger os dados armazenados em dispositivos Apple, há várias medidas que podem ser tomadas por organizações para manter a segurança das informações enquanto em trânsito. Todas essas medidas de segurança tratam da segurança de redes.

Usuários devem poder acessar redes corporativas de qualquer lugar do mundo, o que faz com que seja importante garantir que eles estejam autorizados e seus dados protegidos durante a transmissão. Para que esses objetivos de segurança sejam alcançados, o iOS, iPadOS e macOS integram tecnologias comprovadas e os padrões mais recentes de conexões de rede Wi-Fi e dados celulares. É por isso que os nossos sistemas operacionais usam — e fornecem a desenvolvedores o acesso a — protocolos de rede padrão para comunicações autenticadas, autorizadas e criptografadas.

Segurança de redes com TLS

O iOS, iPadOS e macOS oferecem suporte ao Transport Layer Security (TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3) e ao Datagram Transport Layer Security (DTLS). O protocolo TLS oferece suporte a AES-128 e AES-256, e prefere conjuntos de cifras com encaminhamento secreto. Apps que usam a internet, como Safari, Calendário e Mail, usam esse protocolo automaticamente para ativar um canal de comunicação criptografado entre o dispositivo e os serviços de rede. As APIs de alto nível (como CFNetwork) facilitam a adoção do TLS por desenvolvedores em apps, enquanto as APIs de baixo nível (Network.framework) fornecem um controle mais detalhado. O CFNetwork não permite SSLv3 e os apps que usam WebKit (como o Safari) são proibidos de fazer uma conexão SSLv3.

No iOS 11 ou posterior e no macOS 10.13 ou posterior, os certificados SHA-1 não podem mais fazer conexões TLS sem ter a confiança do usuário. Certificados com chaves RSA com menos de 2048 bits também não são permitidos. O conjunto de cifras simétricas RC4 não é mais usado no iOS 10 e no macOS 10.12. Por padrão, clientes ou servidores TLS implementados com APIs de Transporte Seguro não têm os conjuntos de cifras RC4 ativados e não podem se conectar quando RC4 for o único conjunto de cifras disponível. Para ter mais segurança, serviços ou apps que requeiram RC4 devem ser atualizados para usar conjuntos de cifras modernos e seguros. No iOS 12.1, os certificados emitidos após 15 de outubro de 2018 a partir de um certificado-raiz autorizado pelo sistema devem ter uma sessão iniciada em um registro de Transparência de Certificado autorizado para terem acesso a conexões TLS. No iOS 12.2, o TLS 1.3 está ativado por padrão para APIs Network. framework e NSURLSession. Clientes TLS que usam APIs SecureTransport não podem usar TLS 1.3.

Segurança de Transporte em Apps

A Segurança de Transporte em Apps fornece requisitos de conexão padrão para que os apps possam seguir as melhores práticas de conexão segura ao usar as APIs NSURLConnection, CFURL ou NSURLSession. Por padrão, a Segurança de Transporte em Apps limita a seleção de cifras para incluir apenas os conjuntos que fornecem encaminhamento secreto, especificamente ECDHE_ECDSA_AES e ECDHE_RSA_AES nos modos GCM ou CBC. Apps podem desativar o requisito de encaminhamento secreto por domínio, adicionando, nesse caso, RSA_AES ao conjunto de cifras disponíveis.

Os servidores precisam oferecer suporte ao TLS v1.2 e encaminhamento secreto, e os certificados precisam ser válidos e assinados com SHA-256 ou mais forte com, no mínimo, uma chave RSA de 2048 bits ou chave de curva elíptica de 256 bits.

As conexões de rede que não atenderem a esses requisitos falharão, a não ser que o app substitua a Segurança de Transporte em Apps. Certificados inválidos sempre resultarão em falha e falta de conexão. A Segurança de Transporte em Apps é aplicada automaticamente a apps compilados para iOS 9 ou posterior e macOS 10.11 ou posterior.

Verificação da validade de certificados

A avaliação do estado de confiança de um certificado TLS é realizada de acordo com padrões de mercado consolidados, conforme definido no RFC 5280 e incorpora padrões novos como o RFC 6962 (Transparência de Certificado). No iOS 11 ou posterior e macOS 10.13 ou posterior, os dispositivos Apple são atualizados periodicamente com uma lista atual de certificados revogados e restringidos. A lista é agregada a partir de listas de revogação de certificados (CRLs) que são publicadas por todas as autoridades de certificação raiz integradas nas quais a Apple confia, assim como as ACs emissoras subordinadas. A lista também pode incluir outras restrições a critério da Apple. Essas informações são consultadas sempre que uma função de API de rede é usada para fazer uma conexão segura. Se houver um número grande demais de certificados revogados de uma AC para serem listados individualmente, uma avaliação de confiança pode exigir uma resposta de estado de certificado on-line (OCSP), e ser malsucedida caso a resposta não esteja disponível.

Redes Privadas Virtuais (VPNs)

Serviços seguros de rede, como as redes privadas virtuais, geralmente precisam de pouca configuração para funcionar com dispositivos iOS, iPadOS e macOS. Esses dispositivos funcionam com servidores de VPN compatíveis com os seguintes protocolos e métodos de autenticação:

- IKEv2/IPSec com autenticação por segredo compartilhado, Certificados RSA, Certificados ECDSA, EAP-MSCHAPv2 ou EAP-TLS
- VPN-SSL usando o devido app cliente da App Store
- L2TP/IPSec com autenticação do usuário por senha MS-CHAPV2 e autenticação por máquina por segredo compartilhado (iOS, iPadOS e macOS) e RSA SecurID ou CRYPTOCard (apenas macOS)
- Cisco IPSec com autenticação do usuário por senha, RSA SecurID ou CRYPTOCard e autenticação por máquina por segredo compartilhado e certificados (apenas macOS)

O iOS, iPadOS e macOS são compatíveis com os itens a seguir:

- *VPN por Demanda:* em redes que usam autenticação baseada em certificado. As políticas de TI especificam, por meio de um perfil de configuração VPN, quais domínios requerem conexão VPN.
- *VPN por App:* para realização de conexões VPN de forma muito mais granular. As soluções de gerenciamento de dispositivos móveis (MDM) podem especificar uma conexão para cada app gerenciado e domínios específicos do Safari. Isso ajuda a garantir que os dados seguros sempre transitem pela rede corporativa, mas não os dados pessoais de usuários.
- *VPN Sempre Ativa:* pode ser configurada em dispositivos gerenciados por uma solução MDM e supervisionada com o Apple Configurator 2, o Apple School Manager ou o Apple Business Manager. Isso elimina a necessidade de ativação da VPN pelos usuários para ativar a proteção ao se conectarem a redes Wi-Fi ou celulares. A VPN Sempre Ativa proporciona a organizações o controle total do tráfego do dispositivo, encapsulando todo o tráfego IP de volta à organização. O protocolo de encapsulamento padrão, IKEv2, protege o tráfego através da criptografia dos dados. As organizações podem monitorar e filtrar o tráfego de seus dispositivos, proteger os dados de suas redes e restringir o acesso de dispositivos à internet.

Segurança de Wi-Fi

Segurança de protocolos

Todas as plataformas Apple oferecem suporte aos protocolos padrão da indústria de autenticação e criptografia de Wi-Fi para fornecer acesso autenticado e confidencialidade na conexão às seguintes redes sem fio seguras:

- WPA2 Pessoal
- WPA2 Empresarial
- WPA2/WPA3 Transitório
- WPA3 Pessoal
- WPA3 Empresarial

- WPA3 Empresarial com segurança de 192 bits

O WPA2 e WPA3 autenticam cada conexão e fornecem criptografia AES de 128 bits para garantir a confidencialidade dos dados transferidos sem fio. Isso proporciona aos usuários o maior nível de segurança de dados, que permanecem protegidos durante o envio e recebimento de comunicações em conexões de rede Wi-Fi. O WPA3 é compatível com:

- iPhone 7 ou posterior
- iPad 5ª geração ou posterior
- Apple TV 4K ou posterior
- Apple Watch Series 3 ou posterior
- Computadores Mac (final de 2013 e posteriores) com 802.11ac ou posterior

Os dispositivos mais novos oferecem suporte à autenticação com WPA3 Empresarial com segurança de 192 bits, incluindo o suporte à criptografia AES de 256 bits em conexões com pontos de acesso (PAs) compatíveis. Isso oferece proteções de confidencialidade ainda maiores para o tráfego transferido sem fio. O WPA3 Empresarial com segurança de 192 bits é compatível com iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max e dispositivos iOS e iPadOS mais novos.

Além de proteger dados transferidos sem fio, as plataformas Apple estendem as proteções do nível de WPA2 e WPA3 a quadros de gerenciamento unicast e multicast por meio do serviço Quadro de Gerenciamento Protegido (PMF) definido no 802.11w. A compatibilidade com PMF está disponível para:

- iPhone 6 ou posterior
- iPad Air 2 ou posterior
- Apple TV 4ª geração ou posterior
- Apple Watch Series 3 ou posterior
- Computadores Mac (final de 2013 e posteriores) com 802.11ac ou posterior

Com suporte a 802.1X, os dispositivos Apple podem ser integrados a uma grande variedade de ambientes de autenticação RADIUS. Os métodos de autenticação sem fio 802.1X compatíveis incluem EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 e PEAPv1.

Protocolos descontinuados

Os produtos Apple aceitam os seguintes protocolos descontinuados de autenticação e criptografia via Wi-Fi:

- WEP Aberto, tanto com chaves de 40 bits quanto de 104 bits
- WEP Compartilhado, tanto com chaves de 40 bits quanto de 104 bits
- WEP Dinâmico
- Temporal Key Integrity Protocol (TKIP)
- WPA
- WPA/WPA2 Transitório

Esses protocolos não são mais considerados seguros e seu uso é vivamente desaconselhado por motivos de compatibilidade, confiabilidade, desempenho e segurança. Seu suporte é oferecido apenas para fins de compatibilidade com versões anteriores e podem ser removidos em versões futuras do software.

Todas as implementações de Wi-Fi são **fortemente** incentivadas a migrar para WPA3 Pessoal ou WPA3 Empresarial para fornecer as conexões Wi-Fi mais robustas, seguras e compatíveis possíveis.

Privacidade de Wi-Fi

Aleatorização do endereço MAC

As plataformas Apple usam um endereço MAC (Media Access Control) aleatório ao realizar varreduras de Wi-Fi quando não estão associadas a uma rede Wi-Fi. Essas varreduras podem ser realizadas para encontrar e conectar a uma rede Wi-Fi conhecida ou para auxiliar os Serviços de Localização em apps que usam cercas virtuais, como lembretes baseados em localização, ou para fixar uma localização no app Mapas da Apple. Observe que as varreduras de Wi-Fi que acontecem durante a tentativa de conexão a uma rede Wi-Fi preferida não são aleatorizadas.

As plataformas Apple também usam um endereço MAC aleatório ao realizar varreduras ePNO (Preferred Network Offload) aprimoradas quando um dispositivo não está associado a uma rede Wi-Fi ou seu processador está em repouso. As varreduras ePNO são executadas quando um dispositivo usa os Serviços de Localização em apps que usam cercas virtuais, como lembretes baseados em localização, que determinam se o dispositivo está próximo a uma localização específica.

Como o endereço MAC de um dispositivo é alterado ao desconectar-se de uma rede Wi-Fi, os observadores passivos de tráfego Wi-Fi não podem usá-lo para rastrear o dispositivo continuamente, mesmo quando ele está conectado a uma rede de dados celulares. A Apple informou aos fabricantes de Wi-Fi que as varreduras de Wi-Fi do iOS e iPadOS usam endereços MAC aleatórios e que nem os fabricantes nem a Apple podem prevê-los.

O suporte à aleatorização do endereço MAC do Wi-Fi está disponível no iPhone 5 ou posteriores.

Aleatorização de números de sequência de quadros de Wi-Fi

Os quadros de Wi-Fi possuem um número de sequência, que é usado pelo protocolo de baixo nível 802.11 para proporcionar comunicações eficientes e confiáveis via Wi-Fi. Como esses números de sequência são incrementados a cada quadro transmitido, eles poderiam ser usados para correlacionar informações transmitidas durante varreduras de Wi-Fi com outros quadros transmitidos pelo mesmo dispositivo.

Para se proteger contra isso, os dispositivos Apple usam números de sequência aleatórios sempre que um endereço MAC é alterado para um novo endereço aleatório. Isso inclui a aleatorização dos números de sequência a cada nova solicitação de varredura iniciada enquanto o dispositivo não está associado. Há suporte para essa aleatorização nos seguintes dispositivos:

- iPhone 7 ou posterior
- iPad 5ª geração ou posterior

- Apple TV 4K ou posterior
- Apple Watch Series 3 ou posterior
- iMac Pro (Retina 5K, 27 polegadas, 2017) ou posterior
- MacBook Pro (13 polegadas, 2018) ou posterior
- MacBook Pro (15 polegadas, 2018) ou posterior
- MacBook Air (Retina, 13 polegadas, 2018) ou posterior
- Mac mini (2018) ou posterior
- iMac (Retina 4K, 21,5 polegadas, 2019) ou posterior
- iMac (Retina 5K, 27 polegadas, 2019) ou posterior
- Mac Pro (2019) ou posterior

Conexões Wi-Fi e redes ocultas

Conexões

A Apple gera endereços MAC aleatórios nas conexões Wi-Fi peer-to-peer usadas para AirDrop e AirPlay. Os endereços aleatórios também são usados no Acesso Pessoal no iOS e iPadOS (com um cartão SIM) e no Compartilhamento de Internet no macOS.

Endereços novos e aleatórios são gerados sempre que essas interfaces de rede são iniciadas. Além disso, endereços exclusivos são gerados de forma independente para cada interface conforme necessário.

Redes ocultas

As redes Wi-Fi são identificadas pelo nome da rede, conhecido como Identificador de Conjunto de Serviço (SSID). Algumas redes Wi-Fi são configuradas para ocultar o SSID, fazendo com que o ponto de acesso sem fio não transmita o nome da rede. Essas redes são conhecidas como redes ocultas. O iPhone 6s ou posterior detecta automaticamente quando uma rede está oculta. Se uma rede estiver oculta, o dispositivo iOS ou iPadOS envia uma sondagem com o SSID incluído na solicitação, mas não de outra forma. Isso impede que o dispositivo transmita o nome de redes ocultas às quais o usuário se conectou anteriormente, garantindo assim mais privacidade.

Para eliminar os problemas de privacidade colocados pelas redes ocultas, o iPhone 6s ou posterior detecta automaticamente quando uma rede é oculta. Se a rede não é oculta, o dispositivo iOS ou iPadOS não envia uma sondagem com o SSID incluído na solicitação. Isso impede que o dispositivo transmita o nome de redes conhecidas não ocultas, garantindo assim que ele não revele estar procurando essas redes.

Proteções da plataforma

Os sistemas operacionais da Apple protegem o dispositivo de vulnerabilidades no firmware do processador de rede; controladores de rede, incluindo Wi-Fi, têm acesso limitado à memória do processador de aplicativos.

- Quando USB ou SDIO são usados para criar uma interface com o processador de rede, o processador de rede não pode iniciar transações de Acesso Direto à Memória (DMA) com o processador de aplicativos.

- Quando PCIe é usado, cada processador de rede encontra-se isolado em seu próprio barramento PCIe. Um IOMMU em cada barramento PCIe limita ainda mais o acesso DMA do processador de rede apenas à memória e aos recursos que contêm seus pacotes de rede e estruturas de controle.

Segurança de Bluetooth

Existem dois tipos de Bluetooth nos dispositivos Apple, o Bluetooth Classic e o Bluetooth Low Energy (BLE). O modelo de segurança das duas versões de Bluetooth inclui os seguintes recursos de segurança distintos:

- *Emparelhamento:* o processo de criação de uma ou mais chaves de segredo compartilhado
- *Vinculação:* o ato de armazenar as chaves criadas durante o emparelhamento para uso em conexões subsequentes para formar um par de dispositivos confiáveis
- *Autenticação:* verificação de que os dois dispositivos possuem as mesmas chaves
- *Criptografia:* confidencialidade das mensagens
- *Integridade da mensagem:* proteção contra falsificação de mensagens
- *Emparelhamento Simples Seguro:* proteção contra espionagem passiva e ataques man-in-the-middle (MITM)

O Bluetooth versão 4.1 acrescentou o recurso Conexões Seguras ao transporte físico BR/EDR.

Os recursos de segurança de cada tipo de Bluetooth estão na lista abaixo:

Compatibilidade	**Bluetooth Classic**	**Bluetooth Low Energy**
Emparelhamento	Curva elíptica P-256	Algoritmos aprovados pelo FIPS (AES-CMAC e curva elíptica P-256)
Vinculação	As informações de emparelhamento são armazenadas em um local seguro nos dispositivos iOS, iPadOS, macOS, tvOS e watchOS	As informações de emparelhamento são armazenadas em um local seguro nos dispositivos iOS, iPadOS, macOS, tvOS e watchOS
Autenticação	Algoritmos aprovados pelo FIPS (HMAC-SHA-256 e AES-CTR)	Algoritmos aprovados pelo FIPS
Criptografia	Criptografia AES-CCM realizada no Controlador	Criptografia AES-CCM realizada no Controlador
Integridade da mensagem	AES-CCM é usado para integridade da mensagem	AES-CCM é usado para integridade da mensagem
Emparelhamento Simples Seguro: proteção contra espionagem passiva	Elliptic Curve Diffie-Hellman Exchange (ECDHE)	Elliptic Curve Diffie-Hellman Exchange (ECDHE)
Emparelhamento Simples Seguro: proteção contra ataques man-in-the-middle (MITM)	Dois métodos numéricos assistidos pelo usuário: comparação numérica ou digitação de código	Dois métodos numéricos assistidos pelo usuário: comparação numérica ou digitação de código Os emparelhamentos requerem uma resposta do usuário, incluindo todos os modos de emparelhamento não-MITM

Compatibilidade	Bluetooth Classic	Bluetooth Low Energy
Bluetooth 4.1 ou posterior	iMac (final de 2015 ou posterior) MacBook Pro (início de 2015 ou posterior)	iOS 9 ou posterior iPadOS 13.1 ou posterior macOS 10.12 ou posterior tvOS 9 ou posterior watchOS 2.0 ou posterior
Bluetooth 4.2 ou posterior	iPhone 6 ou posterior	iOS 9 ou posterior iPadOS 13.1 ou posterior macOS 10.12 ou posterior tvOS 9 ou posterior watchOS 2.0 ou posterior

Privacidade do Bluetooth Low Energy

Para ajudar a proteger a privacidade do usuário, o BLE possui estes dois recursos: aleatorização de endereço e derivação de chave entre transportes.

A aleatorização de endereço é um recurso que altera o endereço do dispositivo Bluetooth, reduzindo a capacidade de se rastrear um dispositivo BLE. Para que um dispositivo que usa o recurso de privacidade se reconecte a dispositivos conhecidos, o endereço do dispositivo, chamado de endereço privado, deve poder ser resolvido pelo outro dispositivo. O endereço privado é gerado usando a chave de identidade de resolução (IRK) trocada durante o procedimento de emparelhamento.

O iOS 13 e o iPadOS 13.1 possuem a capacidade de derivar chaves de links entre os transportes. Por exemplo, uma chave de link gerada com BLE pode ser usada para derivar uma chave de link de Bluetooth Classic. Além disso, a Apple adicionou suporte de Bluetooth Classic para BLE em dispositivos compatíveis com o recurso Conexões Seguras introduzido na Bluetooth Core Specification versão 4.1 (consulte a Bluetooth Core Specification 5.1).

Tecnologia de banda ultralarga

O novo chip U1 criado pela Apple usa tecnologia de banda ultralarga para detecção espacial, permitindo que o iPhone 11, iPhone 11 Pro e iPhone 11 Pro Max localizem com precisão outros dispositivos Apple que também possuam o chip U1. A tecnologia de banda ultralarga usa a mesma tecnologia para aleatorizar dados encontrados em outros dispositivos Apple compatíveis:

- Aleatorização do endereço MAC, como em outros dispositivos Apple compatíveis
- Aleatorização de números de sequência de quadros de Wi-Fi

Início de sessão único

Início de sessão único

O iOS e iPadOS oferecem suporte à autenticação em redes empresariais através do Início de Sessão Único (SSO). O SSO trabalha com redes baseadas em Kerberos para autenticar usuários nos serviços em que são autorizados a acessar. O SSO pode ser usado em uma série de atividades de rede, de sessões seguras do Safari até apps de terceiros. Também há suporte à autenticação baseada em certificados (como PKINIT).

O macOS oferece suporte à autenticação em redes empresariais por meio do Kerberos. Os apps podem usar o Kerberos para autenticar usuários nos serviços que são autorizados a acessar. O Kerberos também pode ser usado em uma série de atividades de rede, de sessões seguras do Safari e autenticação em sistemas de arquivos em rede até apps de terceiros. Também há suporte à autenticação baseada em certificados (PKINIT), embora o app seja obrigado a adotar uma API de desenvolvedor.

O SSO do iOS, iPadOS e macOS usa tokens SPNEGO e o protocolo HTTP Negotiate para funcionar com gateways de autenticação baseados em Kerberos e sistemas de Autenticação Integrada do Windows que oferecem suporte a tíquetes do Kerberos. O suporte ao SSO é baseado no projeto Heimdal de código aberto.

Os seguintes tipos de criptografia são aceitos no iOS, iPadOS e macOS:

- AES-128-CTS-HMAC-SHA1-96;
- AES-256-CTS-HMAC-SHA1-96;
- DES3-CBC-SHA1;
- ARCFOUR-HMAC-MD5.

O Safari oferece suporte ao SSO e os apps de terceiros que usam APIs de rede padrão do iOS e iPadOS também podem ser configurados para usá-lo. Para configurar o SSO, o iOS e iPadOS oferecem suporte ao payload de um perfil de configuração que permite que soluções de gerenciamento de dispositivos móveis (MDM) acionem os ajustes necessários. Isso inclui a definição do nome principal do usuário (ou seja, a conta do usuário no Active Directory) e os ajustes do domínio Kerberos, assim como a definição de quais apps e URLs do Safari devem ter permissão para usar o SSO.

Para configurar o Kerberos no macOS, obtenha tíquetes com o Ticket Viewer, inicie uma sessão em um domínio do Active Directory do Windows ou use a ferramenta de linha de comando `kinit`.

Início de sessão único extensível

Os desenvolvedores de apps podem fornecer suas próprias implementações do início de sessão único por meio de extensões do SSO. As extensões SSO são chamadas quando um app nativo ou web precisa usar algum provedor de identidade para autenticação do usuário. Os desenvolvedores podem fornecer dois tipos de extensões: as que redirecionam para HTTPS e as que usam um mecanismo de desafio/resposta, como Kerberos. Isso permite que os esquemas de autenticação do OpenID, OAuth, SAML2 e Kerberos sejam usados com o início de sessão único extensível.

Para usar uma extensão de início de sessão único, um app pode usar a API AuthenticationServices ou o mecanismo de interceptação de URL oferecido pelo sistema operacional. O WebKit e CFNetwork fornecem uma camada de interceptação que permite suporte integrado ao Início de sessão único em qualquer app nativo ou WebKit. Para que uma extensão de início de sessão único seja chamada, uma configuração fornecida por um administrador deve ser instalada por meio de um perfil de gerenciamento de dispositivos móveis (MDM). Além disso, as extensões do tipo redirecionamento devem usar o payload de Domínios Associados para provar que o servidor de identidade ao qual oferecem suporte está ciente da sua existência.

A única extensão fornecida com o sistema operacional é a extensão de SSO do Kerberos.

Segurança do AirDrop

Os dispositivos Apple que oferecem suporte ao AirDrop usam tecnologia Bluetooth Low Energy (BLE) e tecnologia Wi-Fi peer-to-peer criada pela Apple para enviar arquivos e informações para dispositivos próximos, incluindo dispositivos iOS compatíveis com AirDrop com iOS 7 ou posterior e computadores Mac com OS X 10.11 ou posterior. O sinal de rádio Wi-Fi é usado para comunicação direta entre dispositivos, sem usar nenhuma conexão à internet ou ponto de acesso sem fio (PA). No macOS, essa conexão é criptografada com TLS.

O AirDrop é configurado com a opção de compartilhamento Apenas Contatos por padrão. Os usuários também podem optar por usar o AirDrop para compartilhar com todos ou desativar o recurso completamente. As organizações podem restringir o uso do AirDrop para dispositivos ou apps sendo gerenciados por uma solução de gerenciamento de dispositivos móveis (MDM).

Operação do AirDrop

O AirDrop usa serviços do iCloud para ajudar na autenticação de usuários. Quando um usuário inicia uma sessão no iCloud, uma identidade RSA de 2048 bits é armazenada no dispositivo. Quando o usuário ativa o AirDrop, um hash de identificação breve do AirDrop é criado com base nos endereços de e-mail e números de telefone associados ao ID Apple do usuário.

Quando um usuário escolhe o AirDrop como método de compartilhamento de um item, o dispositivo de envio emite um sinal AirDrop através de BLE que inclui o hash de identificação breve do AirDrop do usuário. Outros dispositivos Apple que estejam despertos, nas proximidades e que estejam com o AirDrop ativado detectam o sinal e respondem usando Wi-Fi peer-to-peer, de modo que o dispositivo de envio possa descobrir a identidade de quaisquer dispositivos que respondam.

No modo Apenas Contatos, o hash de identificação breve do AirDrop recebido é comparado aos hashes das pessoas incluídas no app Contatos do dispositivo receptor. Se uma correspondência for encontrada, o dispositivo receptor responde por Wi-Fi peer-to-peer com as informações de sua identidade. Se não houver correspondência, o dispositivo não responde.

No modo Todos, o mesmo processo geral é usado. Porém, o dispositivo receptor responde mesmo que não haja nenhuma correspondência no app Contatos do dispositivo.

O dispositivo emissor então inicia uma conexão via AirDrop usando Wi-Fi peer-to-peer, usando essa conexão para enviar um hash de identificação longo para o dispositivo receptor. Se o hash de identificação longo corresponder ao hash de uma pessoa conhecida nos Contatos do receptor, então o receptor responderá com seus hashes de identificação longos.

Se os hashes forem verificados, o nome e a foto do receptor (se existentes no app Contatos) são exibidos na folha de compartilhamento do AirDrop do remetente. No iOS e iPadOS, eles são mostrados na seção "Pessoas" ou "Dispositivos". Os dispositivos que não foram verificados ou autenticados são mostrados na folha de compartilhamento do AirDrop do remetente com um ícone de silhueta e o nome do dispositivo, como definido em Ajustes > Geral > Sobre > Nome. No iOS e iPadOS, eles aparecem na seção "Outras Pessoas" da folha de compartilhamento do AirDrop.

O usuário remetente pode selecionar com quem deseja compartilhar. Após a seleção do usuário, o dispositivo remetente inicia uma conexão criptografada (TLS) com o dispositivo receptor, que troca seus certificados de identidade do iCloud. A identidade nos certificados é comparada com o app Contatos de cada usuário para verificá-la.

Se os certificados forem verificados, o usuário receptor é solicitado a aceitar a transferência do usuário ou dispositivo identificado. Se vários destinatários forem selecionados, este processo é repetido para cada um deles.

Compartilhamento de senhas de Wi-Fi

Os dispositivos iOS e iPadOS que oferecem suporte ao compartilhamento de senhas de Wi-Fi usam um mecanismo similar ao AirDrop para enviar uma senha de Wi-Fi de um dispositivo para outro.

Quando um usuário seleciona uma rede Wi-Fi (solicitante) e a senha do Wi-Fi é solicitada ao usuário, o dispositivo Apple inicia um anúncio de Bluetooth Low Energy (BLE), indicando que ele deseja a senha do Wi-Fi. Outros dispositivos Apple que não estão em repouso, encontram-se por perto e têm a senha da rede Wi-Fi selecionada, usam BLE para se conectar ao dispositivo solicitante.

O dispositivo que tem a senha do Wi-Fi (concessor) exige as informações de contato do solicitante, que deve usar um mecanismo similar ao AirDrop para comprovar sua identidade. Depois de comprovar a identidade, o concessor envia o código ao solicitante, o qual pode ser usado para conexão à rede.

Organizações podem restringir o uso do compartilhamento de senhas de Wi-Fi em dispositivos ou apps sendo gerenciados por uma solução de gerenciamento de dispositivos móveis (MDM).

Firewall no macOS

O macOS possui um firewall integrado para proteger o Mac de acesso à rede e ataques de negação de serviço. Ele pode ser configurado no painel das preferências Segurança e Privacidade nas Preferências do Sistema e aceita as configurações a seguir:

- Bloquear todas as conexões recebidas, independentemente do app
- Permitir automaticamente que softwares integrados recebam conexões

- Permitir automaticamente que softwares transferidos e assinados recebam conexões
- Adicionar ou negar o acesso com base em apps especificados pelo usuário
- Evitar que o Mac responda a sondagens ICMP e solicitações de varredura de portas

Kits para Desenvolvedores

Visão geral dos kits para desenvolvedores

A Apple fornece diversos frameworks para permitir que desenvolvedores externos ampliem os serviços da Apple. Estes frameworks tratam a segurança e a privacidade do usuário como fatores fundamentais:

- HomeKit
- HealthKit
- CloudKit
- SiriKit
- DriverKit
- ReplayKit
- Câmera e ARKit

HomeKit

Identidade HomeKit

O HomeKit oferece uma infraestrutura de automação doméstica que usa a segurança do iCloud e do iOS, iPadOS e macOS para proteger e sincronizar dados privados sem expô-los à Apple.

A segurança e identidade do HomeKit são baseadas em pares de chaves públicas-privadas Ed25519. Um par de chaves Ed25519 é gerado no dispositivo iOS, iPadOS e macOS para cada usuário do HomeKit, definindo sua respectiva identidade HomeKit. Ela é usada para autenticar a comunicação entre dispositivos iOS, iPadOS e macOS e entre dispositivos iOS, iPadOS e macOS e acessórios.

As chaves — armazenadas nas Chaves e incluídas apenas em backups criptografados das Chaves — são sincronizadas entre dispositivos através das Chaves do iCloud, onde disponíveis. O HomePod e a Apple TV recebem chaves por meio de toque para configurar ou do modo de configuração descrito abaixo. As Chaves são compartilhadas a partir de um iPhone para um Apple Watch emparelhado por meio do Serviço de Identidade da Apple (IDS).

Comunicação com acessórios HomeKit

Os acessórios HomeKit geram seus próprios pares de chaves Ed25519 para uso nas comunicações com dispositivos iOS, iPadOS e macOS. Se o acessório for restaurado aos ajustes de fábrica, um novo par de chaves é gerado.

Para estabelecer um relacionamento entre um dispositivo iOS, iPadOS e macOS e um acessório HomeKit, as chaves são trocadas usando o protocolo Secure Remote Password (3072 bits), utilizando um código de oito dígitos fornecido pelo fabricante do acessório, digitado no dispositivo iOS ou iPadOS pelo usuário e criptografado usando CHACHA20-POLY1305 AEAD com chaves derivadas HKDF-SHA-512. A certificação MFi do acessório também é verificada durante a configuração. Acessórios sem um chip MFi podem adquirir a compatibilidade para autenticação de software no iOS 11.3 ou posterior.

Quando o dispositivo iOS, iPadOS e macOS e um acessório HomeKit se comunicam durante o uso, um autentica o outro pelas chaves trocadas no processo acima. Cada sessão é estabelecida usando o protocolo Station-to-Station e criptografada com chaves derivadas HKDF-SHA-512, baseadas em chaves Curve25519 únicas por sessão. Isso se aplica tanto a acessórios com base em IP como a acessórios Bluetooth Low Energy (BLE).

Para dispositivos BLE compatíveis com notificações transmitidas, o acessório recebe uma chave de criptografia de transmissão de um dispositivo iOS, iPadOS e macOS emparelhado por meio de uma sessão segura. Essa chave é usada para criptografar os dados sobre mudanças de estado do acessório, que são notificadas por meio de anúncios do BLE. A chave de criptografia de transmissão é uma chave derivada HKDF-SHA-512, e os dados são criptografados usando o algoritmo Criptografia Autenticada com Dados Associados (AEAD) CHACHA20-POLY1305. A chave de criptografia de transmissão é alterada periodicamente pelo dispositivo iOS, iPadOS e macOS e sincronizada a outros dispositivos usando o iCloud, conforme descrito em Sincronização de dados entre dispositivos e usuários.

Armazenamento de dados locais do HomeKit

O HomeKit armazena os dados de casas, acessórios, cenas e usuários em um dispositivo iOS, iPadOS e macOS do usuário. Os dados armazenados são criptografados usando chaves derivadas das chaves de identidade HomeKit do usuário em conjunto com um nonce aleatório. Além disso, os dados do HomeKit são armazenados usando a classe de Proteção de Dados "Protegido Até a Primeira Autenticação do Usuário". O backup dos dados do HomeKit é sempre criptografado, portanto, backups não criptografados do iTunes, por exemplo, não contêm dados do HomeKit.

Sincronização de dados entre dispositivos e usuários

Os dados do HomeKit podem ser sincronizados entre os dispositivos iOS, iPadOS e macOS de um usuário através do iCloud e das Chaves do iCloud. Eles são criptografados durante a sincronização usando as chaves derivadas da identidade HomeKit do usuário e um nonce aleatório. Durante a sincronização, esses dados são tratados como uma bolha opaca. A bolha mais recente é armazenada no iCloud para permitir a sincronização, mas ela não é usada para nenhum outro propósito. Como os dados são criptografados usando chaves disponíveis apenas nos dispositivos iOS, iPadOS e macOS do usuário, seu conteúdo se torna inacessível durante a transmissão e o armazenamento no iCloud.

Os dados do HomeKit também são sincronizados entre os vários usuários da mesma casa. Esse processo usa a mesma autenticação e criptografia usadas entre um dispositivo iOS, iPadOS e macOS e um acessório HomeKit. A autenticação é baseada em chaves públicas Ed25519, que são trocadas entre os dispositivos quando um usuário é adicionado a uma casa. Depois que um novo usuário é adicionado a uma casa, todas as comunicações posteriores são autenticadas e criptografadas usando o protocolo Station-to-Station e chaves únicas por sessão.

O usuário que criou a casa no HomeKit inicialmente ou outro usuário com permissões de edição pode adicionar novos usuários. O dispositivo do proprietário configura os acessórios com a chave pública do novo usuário para que os acessórios possam autenticar e aceitar comandos do novo usuário. Quando um usuário com permissões de edição adiciona um novo usuário, o processo é delegado a uma central da casa para concluir a operação.

O processo de autorização da Apple TV para uso com o HomeKit é realizado automaticamente quando o usuário inicia a sessão no iCloud. A autenticação de dois fatores deve estar ativada na conta do iCloud. A Apple TV e o dispositivo do proprietário trocam chaves públicas Ed25519 temporárias através do iCloud. Quando o dispositivo do usuário e a Apple TV estão na mesma rede local, as chaves temporárias são usadas para garantir uma conexão através da rede local usando o protocolo Station-to-Station e chaves únicas por sessão. Esse processo usa a mesma autenticação e criptografia usadas entre um dispositivo iOS, iPadOS e macOS e um acessório HomeKit. Por meio dessa conexão local segura, o dispositivo do proprietário transfere os pares de chaves públicas-privadas Ed25519 do usuário para a Apple TV. Essas chaves são então usadas para dar segurança à comunicação entre a Apple TV e os acessórios HomeKit e também entre a Apple TV e outros dispositivos iOS, iPadOS e macOS que façam parte da casa com HomeKit.

Se um usuário não tiver vários dispositivos e não conceder acesso a usuários adicionais em sua casa, nenhum dado do HomeKit é sincronizado com o iCloud.

App e dados da casa

O acesso aos dados da casa por apps é controlado pelos ajustes de Privacidade do usuário. Os usuários são solicitados a conceder acesso quando os apps solicitam dados da casa, de maneira semelhante aos apps Contatos, Fotos e outras fontes de dados do iOS, iPadOS e macOS. Se o usuário aprovar, os apps terão acesso aos nomes dos cômodos e acessórios, em qual quarto cada acessório se encontra e outras informações, conforme detalhado na documentação do desenvolvedor do HomeKit em: https://developer.apple.com/homekit/ (em inglês).

HomeKit e Siri

A Siri pode ser usada para consultar e controlar acessórios e para ativar cenas. Informações mínimas sobre a configuração da casa são fornecidas anonimamente à Siri para fornecer o nome de quartos, acessórios e cenas necessários para o reconhecimento de comandos. O áudio enviado para a Siri pode indicar acessórios ou comandos específicos, mas tais dados da Siri não são associados a outros recursos da Apple, como o HomeKit.

Câmeras IP do HomeKit

As câmeras IP no HomeKit enviam transmissões de vídeo e áudio diretamente para o dispositivo iOS, iPadOS e macOS que acessam a transmissão na rede local. As transmissões são criptografadas com chaves geradas aleatoriamente no dispositivo iOS, iPadOS e macOS e na câmera IP, as quais são trocadas através da sessão segura do HomeKit para a câmera. Quando um dispositivo iOS, iPadOS ou macOS não está na rede local, as transmissões são retransmitidas através da central da casa para o dispositivo. A central da casa não descriptografa as transmissões e funciona apenas como um retransmissor entre o dispositivo iOS, iPadOS e macOS e a câmera IP. Quando um app exibe o vídeo da câmera IP do HomeKit para o usuário, o HomeKit está renderizando os fotogramas de vídeo com segurança a partir de um processo do sistema à parte, para que o app não possa acessar ou armazenar a transmissão de vídeo. Além disso, os apps não têm permissão para fazer capturas de tela dessa transmissão.

Vídeo seguro do HomeKit

O HomeKit oferece um mecanismo seguro e privado de ponta a ponta para gravar, analisar e visualizar clipes de câmeras IP do HomeKit sem expor esse conteúdo de vídeo à Apple ou nenhum terceiro. Quando um movimento é detectado pela câmera IP, os clipes de vídeo são enviados diretamente ao dispositivo Apple que age como central da casa por uma conexão de rede local dedicada entre a central da casa e a câmera IP. A conexão de rede local é criptografada com um par de chaves por sessão derivado de HKDF-SHA-512, negociado por uma sessão do HomeKit entre a central da casa e a câmera IP. O HomeKit descriptografa as transmissões de áudio e vídeo na central da casa e analisa os fotogramas de vídeo localmente em busca de eventos significativos. Se um evento significativo for detectado, o HomeKit usa AES-256-GCM com uma chave AES-256 gerada aleatoriamente para criptografar o clipe de vídeo. O HomeKit também gera fotogramas-pôster para cada clipe e esses fotogramas-pôster são criptografados com a mesma chave AES-256. Os dados de fotogramas-pôster, áudio e vídeo são enviados para os servidores do iCloud. Os respectivos metadados de cada clipe, incluindo a chave de criptografia, usam a criptografia de ponta a ponta do iCloud quando são enviados.

Quando o app Casa é usado para visualizar os clipes de uma câmera, os dados são baixados do iCloud e as chaves para descriptografar as transmissões usam a descriptografia de ponta a ponta do iCloud para serem desembaladas localmente. O conteúdo de vídeo criptografado é transmitido dos servidores e descriptografado localmente no dispositivo iOS antes de aparecer no visualizador. Cada sessão de clipe de vídeo pode ser dividida em subseções, onde cada subseção criptografa a transmissão de conteúdo com sua própria chave única.

Roteadores HomeKit

Roteadores compatíveis com o HomeKit permitem ao usuário melhorar a segurança da rede doméstica ao gerenciar o acesso Wi-Fi que os acessórios do HomeKit têm à rede local e à internet. Eles também são compatíveis com a autenticação PPSK, para que os acessórios possam ser adicionados à rede Wi-Fi com uma chave específica do acessório, a qual pode ser revogada quando necessário. Isso melhora a segurança ao não expor a senha principal do Wi-Fi aos acessórios, além de permitir que o roteador identifique um acessório com segurança, mesmo que seu endereço MAC mude eventualmente.

Com o app Casa, um usuário pode configurar restrições de acesso em grupos de acessórios da seguinte maneira:

- *Sem Restrições:* permite acesso irrestrito à internet e à rede local.
- *Automático:* esse é o ajuste padrão. Permite acesso irrestrito à internet e à rede local com base em uma lista de sites da internet e portas locais fornecidas à Apple pelo fabricante do acessório. Essa lista inclui todos os sites e portas necessários ao acessório para que ele funcione corretamente (Sem Restrições é usado até que tal lista esteja disponível).
- *Restringir à Casa:* nenhum acesso à internet ou à rede local, exceto por conexões exigidas pelo HomeKit para descobrir e controlar o acessório a partir da rede local (incluindo conexões da central da Casa para oferecer suporte ao controle remoto).

A PPSK é uma senha WPA2 Pessoal forte, específica do acessório, que é gerada automaticamente pelo HomeKit e revogada se ou quando o acessório for posteriormente removido da Casa. Uma PPSK é usada quando um acessório é adicionado à rede Wi-Fi pelo HomeKit em uma casa configurada com um roteador HomeKit (os acessórios adicionados ao Wi-Fi antes da adição do roteador retêm suas credenciais existentes).

Como uma medida de segurança adicional, o usuário deve usar o app do fabricante do roteador HomeKit para configurá-lo, de forma que o app possa validar se o usuário possui acesso ao roteador e tem permissão para adicioná-lo ao app Casa.

Acesso remoto do iCloud para acessórios HomeKit

Alguns acessórios HomeKit legados ainda exigem a capacidade de se conectar diretamente ao iCloud para permitir que dispositivos iOS, iPadOS e macOS os controlem quando a comunicação via Bluetooth ou Wi-Fi não está disponível. O acesso remoto através de uma central da casa (como um HomePod, Apple TV ou iPad) é preferencialmente usada sempre que possível.

O acesso remoto do iCloud em dispositivos legados ainda é compatível e foi projetado cuidadosamente para que os acessórios sejam controlados e enviem notificações sem revelar suas identidades à Apple ou quais comandos e notificações estão sendo enviados. O HomeKit não envia informações sobre a casa através do acesso remoto do iCloud.

Quando um usuário envia um comando usando o acesso remoto do iCloud, o acessório e o dispositivo iOS, iPadOS e macOS são autenticados mutuamente e os dados são criptografados usando o mesmo procedimento descrito para conexões locais. O conteúdo das comunicações é criptografado e não pode ser visualizado pela Apple. O endereçamento através do iCloud é baseado nos identificadores do iCloud registrados durante o processo de configuração.

Os acessórios que oferecem suporte ao acesso remoto do iCloud são disponibilizados durante o processo de configuração do acessório. O processo de disponibilização começa com o início de sessão do usuário no iCloud. A seguir, o dispositivo iOS e iPadOS solicita que o acessório assine um desafio usando o Coprocessador de Autenticação da Apple, integrado a todos os acessórios "Built for HomeKit". O acessório também gera chaves de curva elíptica prime256v1 e a chave pública é enviada ao dispositivo iOS e iPadOS juntamente com o desafio assinado e o certificado X.509 do coprocessador de autenticação. Esses dados são usados para solicitar um certificado do servidor de provisão do iCloud para o acessório. O certificado é armazenado pelo acessório, mas não contém nenhuma informação de identificação sobre o acessório, além de ter recebido acesso remoto ao iCloud do HomeKit. O dispositivo iOS e iPadOS que está realizando a provisão também envia um pacote ao acessório, o qual contém os URLs e outras informações necessárias para conexão ao servidor de acesso remoto do iCloud. Essas informações não são específicas a nenhum usuário ou acessório.

Cada acessório registra uma lista de usuários permitidos no servidor de acesso remoto do iCloud. A capacidade de controlar o acessório foi concedida a esses usuários pelo usuário que adicionou o acessório à casa. Os usuários recebem um identificador pelo servidor do iCloud e podem ser mapeados a uma conta do iCloud com o intuito de receberem mensagens de notificações e respostas dos acessórios. De maneira semelhante, os acessórios possuem identificadores emitidos pelo iCloud, mas eles são opacos e não revelam nenhuma informação sobre o acessório em si.

Quando um acessório se conecta ao servidor de acesso remoto do iCloud do HomeKit, ele apresenta seu certificado e um tíquete. O tíquete é obtido de um servidor do iCloud diferente e não é exclusivo para cada acessório. Quando um acessório solicita um tíquete, ele inclui seu fabricante, modelo e versão do firmware na solicitação. Nenhuma informação que identifique o usuário ou a casa é enviada nessa solicitação. Para ajudar a proteger a privacidade, a conexão ao servidor de tíquetes não é autenticada.

Os acessórios se conectam ao servidor de acesso remoto do iCloud através de HTTP/2 e são protegidos por TLS v1.2 com AES-128-GCM e SHA-256. O acessório mantém a conexão ao servidor de acesso remoto do iCloud aberta para receber mensagens e enviar respostas e notificações para dispositivos iOS, iPadOS e macOS.

Acessórios do HomeKit TV Remote

Os acessórios de terceiros para o HomeKit TV Remote fornecem eventos de Design de Interface de Usuário (HID) e áudio da Siri a uma Apple TV associada, adicionada através do app Casa. Os eventos HID são enviados por meio da sessão segura entre a Apple TV e o Remote. Um TV Remote compatível com Siri envia os dados de áudio à Apple TV quando o usuário ativa explicitamente o microfone no Remote usando um botão Siri dedicado. Os quadros do áudio são enviados diretamente à Apple TV usando uma conexão de rede local dedicada entre a Apple TV e o Remote. A conexão de rede local é criptografada com um par de chaves por sessão derivado de HKDF-SHA-512, negociado por uma sessão do HomeKit entre a Apple TV e o TV Remote. O HomeKit descriptografa os quadros de áudio na Apple TV e os encaminha ao app Siri, onde eles são tratados com as mesmas proteções à privacidade de todas as entradas de áudio da Siri.

Perfis da Apple TV para casas com HomeKit

Quando um usuário de uma casa com HomeKit adiciona seu perfil ao proprietário da Apple TV da casa, esse usuário recebe acesso aos programas de TV, músicas e podcasts. Os ajustes de cada usuário relacionados ao uso de seu perfil na Apple TV são compartilhados com a conta do iCloud do proprietário usando a criptografia de ponta a ponta do iCloud. Cada usuário é dono de seus dados, que são compartilhados somente para leitura do proprietário. Casa usuário da casa pode alterar esses valores no app Casa e a Apple TV do proprietário usa esses ajustes.

Quando um ajuste está ativado, a conta do iTunes do usuário é disponibilizada na Apple TV. Quando um ajuste está desativado, a conta e os dados referentes a esse usuário são apagados na Apple TV. O compartilhamento inicial do CloudKit é iniciado pelo dispositivo do usuário e o token usado para estabelecer o compartilhamento seguro do CloudKit é enviado através do mesmo canal seguro usado para sincronizar os dados entre usuários da casa.

HealthKit

Visão geral do HealthKit

O HealthKit armazena e agrega dados dos apps de saúde e preparo físico e de instituições de saúde. O HealthKit também funciona diretamente com dispositivos de saúde e preparo físico, como monitores de batimento cardíaco compatíveis com Bluetooth Low Energy (BLE) e o coprocessador de movimento integrado a muitos dispositivos iOS. Todas as interações do HealthKit com apps de saúde e preparo físico, instituições de saúde e dispositivos de saúde e preparo físico exigem a permissão do usuário. Esses dados são armazenados na classe de Proteção de Dados "Protegido Exceto se Aberto". O acesso aos dados é descontinuado 10 minutos após o bloqueio do dispositivo e os dados se tornam acessíveis na próxima vez que o usuário digitar o código ou usar o Touch ID ou Face ID para desbloquear o dispositivo.

O HealthKit também agrega dados de gerenciamento, como permissões de acesso de apps, nomes de dispositivos conectados ao HealthKit e informações de programação usadas para abrir apps quando novos dados estiverem disponíveis. Esses dados são armazenados na classe de Proteção de Dados "Protegido Até a Primeira Autenticação do Usuário". Arquivos temporários de registro armazenam registros de saúde gerados quando o dispositivo está bloqueado, como quando o usuário está se exercitando. Esses dados são armazenados na classe de Proteção de Dados "Protegido Exceto se Aberto". Quando o dispositivo é desbloqueado, os arquivos de registro temporário são importados para os bancos de dados de saúde primários e depois apagados quando a combinação é concluída.

Os dados do app Saúde podem ser armazenados no iCloud. A criptografia de ponta a ponta de dados do app Saúde requer o iOS 12 ou posterior e autenticação de dois fatores. Caso contrário, os dados do usuário ainda estarão criptografados no armazenamento e transmissão, mas não estarão criptografados de ponta a ponta. Depois que o usuário ativar a autenticação de dois fatores e atualizar para o iOS 12 ou posterior, seus dados do app Saúde são migrados para a criptografia de ponta a ponta.

Se o usuário usar o iTunes (no macOS 10.14 ou anterior) ou o Finder (macOS 10.15 ou posterior) para fazer o backup de seu dispositivo, os dados de Saúde são armazenados apenas se o backup for criptografado.

Registros de saúde clínica e integridade dos dados de Saúde

Registros de saúde clínica

Os usuários podem iniciar uma sessão em sistemas de saúde compatíveis dentro do app Saúde para obter uma cópia de seus registros de saúde clínica. Ao conectar um usuário a um sistema de saúde, o usuário autentica usando credenciais de cliente OAuth 2. Após a conexão, os dados dos registros de saúde clínica são baixados diretamente da instituição de saúde através de uma conexão protegida com TLS v1.3. Uma vez baixados, os registros de saúde clínica são armazenados em segurança juntamente com outros dados do app Saúde.

Integridade dos dados de saúde

Os dados armazenados no banco de dados incluem metadados para rastrear a proveniência de cada registro. Esses metadados incluem um identificador de app que indica qual app armazenou o registro. Além disso, um item de metadados opcional pode conter uma cópia do registro assinada digitalmente. O objetivo é fornecer integridade de dados para registros gerados por um dispositivo confiável. O formato usado para a assinatura digital é a Sintaxe de Mensagem Criptográfica (CMS), especificado no RFC 5652.

Acesso de apps de terceiros a dados de Saúde

O acesso à API do HealthKit é controlado por direitos e os apps devem atender às restrições sobre como os dados são usados. Por exemplo, apps não têm permissão para usar dados de saúde para publicidade. Os apps também precisam fornecer aos usuários uma política de privacidade que detalhe o uso dos dados de saúde.

O acesso aos dados de saúde por apps é controlado pelos ajustes de Privacidade do usuário. Os usuários são solicitados a conceder acesso aos dados de saúde a pedidos dos apps, de maneira semelhante aos apps Contatos, Fotos e outras fontes de dados do iOS. Entretanto, no caso de dados de saúde, o acesso para ler e gravar é concedido aos apps separadamente, assim como para cada tipo de dado de saúde. Os usuários podem visualizar e revogar as permissões concedidas para acesso aos dados de saúde em Ajustes > Saúde > Acesso a Dados e Dispositivos.

Se a permissão para gravar dados for concedida, os apps também podem ler os dados que gravam. Se a permissão para ler dados for concedida, eles podem ler dados gravados por todas as fontes. Entretanto, os apps não podem determinar o acesso concedido a outros apps. Além disso, os apps não podem afirmar categoricamente se receberam acesso de leitura aos dados de saúde. Quando um app não possui acesso de leitura, nenhuma consulta retorna dados – a resposta gerada é a mesma que um banco de dados vazio retornaria. Isso impede que apps deduzam o estado de saúde do usuário ao aprender quais tipos de dados o usuário está rastreando.

Ficha Médica de usuários

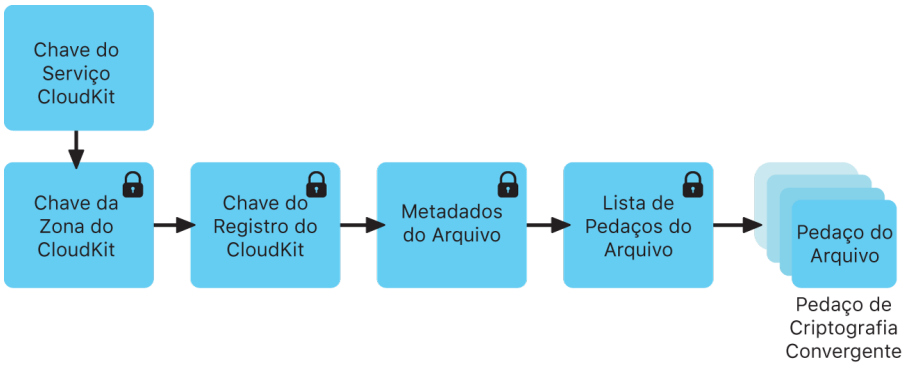
O app Saúde oferece aos usuários a opção de preencher uma ficha médica com informações que podem ser importantes durante uma emergência médica. As informações são digitadas ou atualizadas manualmente e não são sincronizadas com as informações dos bancos de dados de saúde.

As informações da Ficha Médica podem ser visualizadas ao tocar no botão Emergência, na tela Bloqueada. As informações são armazenadas no dispositivo usando a classe de Proteção de Dados "Sem Proteção", para que sejam acessadas sem que seja necessário digitar o código do dispositivo. A Ficha Médica é um recurso opcional que permite que os usuários decidam como equilibrar segurança e privacidade. Tais dados recebem backup no Backup do iCloud e não são sincronizados entre dispositivos que usam o CloudKit.

CloudKit

O CloudKit permite que os desenvolvedores de apps armazenem dados de valores de chaves, dados estruturados e recursos no iCloud. O acesso ao CloudKit é controlado pelo uso de direitos do app. O CloudKit oferece suporte a bancos de dados públicos e privados. Bancos de dados públicos são usados por todas as cópias do app (normalmente para recursos típicos) e não são criptografados. Bancos de dados privados armazenam os dados do usuário.

Assim como o iCloud Drive, o CloudKit usa chaves baseadas em conta para proteger as informações armazenadas no banco de dados privado do usuário e, de forma semelhante a outros serviços do iCloud, os arquivos são divididos em blocos, criptografados e armazenados em serviços de terceiros. O CloudKit usa uma hierarquia de chaves, semelhante à Proteção de Dados. As chaves únicas por arquivo são embaladas por chaves de Registro do CloudKit. As chaves de Registro, por sua vez, são protegidas por uma chave de zona, que é protegida pela Chave de Serviço do CloudKit do usuário. A Chave de Serviço do CloudKit é armazenada na conta do iCloud do usuário e disponibilizada somente depois de sua autenticação no iCloud.



Criptografia de ponta a ponta do CloudKit.

SiriKit

A Siri usa o sistema de extensões de apps para se comunicar com apps de terceiros. A Siri no dispositivo pode acessar as informações de contato do usuário e a localização atual do dispositivo. Mas antes de fornecer dados protegidos a um app, a Siri verifica as permissões de acesso do app, controladas pelo usuário. De acordo com essas permissões, a Siri passa apenas o fragmento relevante do enunciado original do usuário para a extensão do app. Por exemplo, se um app não tiver acesso a informações de contato, a Siri não resolverá um relacionamento em um pedido do usuário como "Use o App de Pagamento para pagar 10 reais à minha mãe". Nesse caso, o app veria apenas o termo literal "minha mãe".

Porém, se o usuário tiver concedido ao app acesso às informações de contato, o app receberia informações resolvidas sobre a mãe do usuário. Se houver referência a um relacionamento no corpo de uma mensagem, como em "Diga à minha mãe no AppMensagens que meu irmão está bem", a Siri não resolve "meu irmão", independentemente das permissões do app.

Os apps que fazem uso do SiriKit podem enviar um vocabulário específico do app ou do usuário à Siri, como os nomes dos contatos do usuário. Essas informações permitem que o reconhecimento de fala e entendimento de linguagem natural da Siri reconheçam o vocabulário desse app e são associadas a um identificador aleatório. As informações personalizadas permanecem disponíveis durante todo o uso do identificador ou até que o usuário desative a integração do app à Siri nos Ajustes, ou até que o app que utiliza o SiriKit seja desinstalado.

No caso de um enunciado como "Quero uma viagem até a casa da minha mãe usando o RideShareApp", a solicitação requer dados de localização dos contatos do usuário. Para essa solicitação apenas, a Siri fornece as informações necessárias à extensão do app, independentemente dos ajustes de permissão do usuário relacionados à localização ou às informações de contato para o app.

DriverKit

O macOS 10.15 usa extensões do sistema para ajudar desenvolvedores a manter extensões dentro de seus apps em vez de exigir extensões do kernel ("kexts"). Isso facilita a instalação e aumenta a estabilidade e a segurança do macOS. O DriverKit é o framework que permite que desenvolvedores criem drivers de dispositivo que os usuários podem instalar no Mac. Os drivers criados com o DriverKit são executados no espaço do usuário, não como extensões do kernel, melhorando a segurança e a estabilidade do sistema.

O usuário simplesmente baixa o app (instaladores não são necessários ao usar extensões do sistema ou o DriverKit) e a extensão é ativada apenas quando necessário. Elas substituem as kexts em vários casos de uso que requerem privilégios de administrador para realizar instalações em /Sistema/Biblioteca ou /Biblioteca.

Recomenda-se que administradores de TI que usam drivers de dispositivos, soluções de armazenamento na nuvem, rede e apps de segurança que exigem extensões de kernel passem para versões mais novas que se baseiem em extensões do sistema. Essas versões mais novas reduzem consideravelmente a possibilidade de pânico no kernel no Mac, além de diminuir a superfície de ataque. Essas novas extensões são executadas no espaço do usuário, não precisam de privilégios especiais para instalação e são removidas automaticamente quando o app associado é movido para o Lixo.

O framework DriverKit fornece classes de C++ para serviços de E/S, correspondência de dispositivos, descritores de memória e filas de despacho. Ele também define tipos de números, coleções, strings e outros tipos comuns adequados para E/S. O usuário os utiliza com frameworks de drivers específicos de famílias como USBDriverKit e HIDDriverKit.

ReplayKit

Gravação de filmes com ReplayKit

O ReplayKit é um framework que permite que desenvolvedores adicionem recursos de gravação e transmissão ao vivo a seus apps. Além disso, ele também permite que usuários usem a câmera frontal e o microfone do dispositivo para comentar em suas gravações e transmissões.

Gravação de filmes

Há várias camadas de segurança integradas à gravação de um filme:

- *Diálogo de permissões:* antes da gravação ser iniciada, o ReplayKit apresenta um alerta de consentimento ao usuário, solicitando que ele reconheça sua intenção de gravar a tela, usar o microfone e a câmera frontal. Esse alerta é apresentado uma vez por processo de app, sendo apresentado novamente se o app permanecer em segundo plano por mais de oito minutos.
- *Captura de tela e áudio:* a captura de tela e áudio ocorre fora do processo do app, no daemon replayd do ReplayKit. Isso garante que o conteúdo gravado nunca fique acessível ao processo do app.
- *Captura de tela e áudio dentro de apps:* permite que um app obtenha buffers de vídeo e amostra, o que é protegido por meio do diálogo de permissões.
- *Criação e armazenamento de filmes:* o arquivo de filme é gravado em um diretório acessível apenas aos subsistemas do ReplayKit e nunca fica acessível a nenhum app. Isso impede que as gravações sejam usadas por terceiros sem o consentimento do usuário.
- *Pré-visualização e compartilhamento pelo usuário final:* o usuário é capaz de pré-visualizar e compartilhar o filme com a interface oferecida pelo ReplayKit. A interface é apresentada fora do processo por meio da infraestrutura de Extensões do iOS e tem acesso ao arquivo de filme gerado.

Transmissão com ReplayKit

Há várias camadas de segurança integradas à gravação de um filme:

- *Captura de tela e áudio:* o mecanismo de captura de tela e áudio durante a transmissão é idêntico ao da gravação de filmes, ocorrendo no replayd.
- *Extensões de transmissão:* para que serviços de terceiros participem da transmissão do ReplayKit, é necessário que eles criem duas novas extensões que estejam configuradas pelo com.apple.broadcast-services:
  - Uma extensão de interface que permita ao usuário configurar a transmissão;
  - Uma extensão de envio que gerencie o envio de dados de vídeo e áudio para os servidores de retaguarda do serviço.

A arquitetura garante que os apps hosts não tenham privilégios de transmitir conteúdo de vídeo e áudio – apenas o ReplayKit e as extensões de transmissão de terceiros possuem acesso.

- *Seletor de transmissão:* com o seletor de transmissão, o usuário inicia transmissões do sistema diretamente do app com a mesma interface definida pelo sistema, a qual pode ser acessada através da Central de Controle. A UI é uma extensão que reside dentro do framework ReplayKit, implementado através da SPI UIRemoteViewController. Ele não pode ser processado pelo app host.
- *Extensão de envio:* a extensão de envio implementada por serviços de transmissão de terceiros para gerenciar conteúdo de vídeo e áudio durante uma transmissão usa buffers de amostra brutos não codificados. durante esse modo de gerenciamento, os dados de vídeo e áudio são serializados e passados à extensão de envio do terceiro em tempo real por uma conexão XPC direta. Os dados de vídeo são codificados ao extrair o objeto IOSurface do buffer de amostra do vídeo, codificá-lo com segurança como um objeto XPC, enviá-lo através do XPC para a extensão de terceiros e descodificá-lo com segurança de volta em um objeto IOSurface.

Câmera e ARKit

A Apple projetou câmeras tendo em mente a privacidade, e os apps de terceiros devem obter o consentimento do usuário antes de acessarem a Câmera. No iOS e iPadOS, quando um usuário concede acesso à Câmera a um app, esse app pode acessar imagens em tempo real das câmeras frontais e traseiras. Os apps não podem usar a câmera sem transparência de que ela está sendo usada.

As fotos e vídeos gravados com a câmera podem conter outras informações, como onde e quando foram gravados, a profundidade de campo e overcapture. Se o usuário não desejar que as fotos e vídeos feitos com o app Câmera incluam localização, ele pode acessar Ajustes > Privacidade > Serviços de Localização > Câmera para controlar isso a qualquer momento. Se o usuário não desejar que as fotos e vídeos incluam a localização ao serem compartilhados, pode desativar a localização no menu Opções na folha de compartilhamento.

Para oferecer uma posição melhor na experiência de RA do usuário, apps que usam ARKit podem usar informações do ambiente real ou de rastreamento de rosto da outra câmera. O rastreamento do ambiente real usa algoritmos no dispositivo do usuário para processar informações desses sensores e determinar sua posição em relação a um espaço físico. O rastreamento do ambiente real ativa recursos como a Direção Óptica no app Mapas.

Gerenciamento Seguro de Dispositivos

Visão geral do gerenciamento seguro de dispositivos

O iOS, iPadOS, macOS e tvOS oferecem suporte a políticas e configurações de segurança flexíveis de fácil aplicação e gerenciamento. Através delas, as organizações podem proteger informações corporativas e garantir o cumprimento dos requisitos empresariais pelos funcionários, mesmo que eles usem dispositivos próprios (como parte de um programa "traga o seu próprio dispositivo" (BYOD), por exemplo).

As organizações podem usar recursos como proteção por senha, perfis de configuração, apagamento remoto e soluções de gerenciamento de dispositivos móveis (MDM) de terceiros para gerenciar uma gama de dispositivos, ajudando a manter os dados corporativos em segurança, mesmo quando esses dados são acessados pelos funcionários em seus dispositivos pessoais.

Com o iOS 13, iPadOS 13.1 e macOS 10.15, os dispositivos Apple oferecem uma nova opção de registro de usuários elaborada especificamente para programas BYOD. O registro de usuários dá mais autonomia para os usuários em seus próprios dispositivos, ao mesmo tempo que aumenta a segurança dos dados corporativos ao armazená-los em um volume APFS separado e protegido por criptografia. Isso oferece um melhor equilíbrio de segurança, privacidade e experiência do usuário nos programas BYOD.

Modelo de emparelhamento

O iOS e ipadOS usam um modelo de emparelhamento para controlar o acesso a um dispositivo a partir de um computador host. O emparelhamento estabelece um relacionamento de confiança entre o dispositivo e o host conectado, simbolizado pela troca de chaves públicas. O iOS e iPadOS também usam essa demonstração de confiança para ativar funcionalidades adicionais com o host conectado, como a sincronização de dados. No iOS 9 ou posterior, os serviços:

- Que exigem emparelhamento não podem ser iniciados até que o dispositivo seja desbloqueado pelo usuário
- Não são iniciados a não ser que o dispositivo tenha sido desbloqueado recentemente
- Podem (como no caso da sincronização de fotos) exigir que o dispositivo seja desbloqueado para iniciar

O processo de emparelhamento requer que o usuário desbloqueie o dispositivo e aceite o pedido de emparelhamento do host. No iOS 9 ou posterior, o usuário também é solicitado a digitar sua senha e, depois disso, o host e o dispositivo trocam e salvam chaves públicas RSA de 2048 bits. Em seguida o host recebe uma chave de 256 bits capaz de desbloquear uma keybag de guarda armazenada no dispositivo. As chaves trocadas são usadas para iniciar uma sessão SSL criptografada, a qual é exigida pelo dispositivo antes que ele envie dados protegidos ao host ou inicie um serviço (sincronização via iTunes ou Finder, transferência de arquivos, desenvolvimento com Xcode, etc.). Para usar essa sessão criptografada em todas as comunicações, o dispositivo exige conexões de um host via Wi-Fi, devendo, portanto, ter sido emparelhado anteriormente via USB. O emparelhamento também ativa diversos recursos de diagnóstico. No iOS 9, os registros de emparelhamento expiram se não forem usados por mais de seis meses. No iOS 11 ou posterior, esse intervalo é encurtado para 30 dias.

Alguns serviços, incluindo com.apple.pcapd, são restritos ao uso somente via USB. Além disso, o serviço com.apple.file_relay requer que um perfil de configuração assinado pela Apple esteja instalado. No iOS 11 ou posterior, a Apple TV pode usar o protocolo Secure Remote Password para estabelecer um relacionamento de emparelhamento via conexão sem fio.

O usuário pode usar as opções “Redefinir Ajustes de Rede” ou “Redefinir Localização e Privacidade” para limpar a lista de hosts confiáveis.

Gerenciamento de ajustes de código e senha

Por padrão, o código do usuário pode ser definido por um PIN numérico. Nos dispositivos iOS e iPadOS com Touch ID ou Face ID, o tamanho mínimo do código é de quatro dígitos. Códigos maiores e mais complexos são recomendados, já que são mais difíceis de adivinhar ou atacar.

Os administradores podem exigir códigos complexos e outras políticas por meio do gerenciamento de dispositivos móveis (MDM), Microsoft Exchange ActiveSync ou ao requisitar que os usuários instalem perfis de configuração manualmente. Uma senha de administrador é necessária para a instalação do payload da política de código no macOS. Algumas políticas de código são:

- Permitir valor simples
- Exigir valor alfanumérico
- Tamanho mínimo de código e senha
- Número mínimo de caracteres complexos
- Tempo máximo de uso de código e senha
- Histórico de códigos e senhas
- Tempo limite de bloqueio automático
- Período de tolerância para bloqueio do dispositivo
- Número máximo de tentativas erradas
- Permitir Touch ID ou Face ID

Exigência de configurações

Um perfil de configuração é um arquivo XML que permite que administradores distribuam informações de configuração para dispositivos iOS, iPadOS, macOS e tvOS. No iOS, iPadOS e tvOS, a maioria dos ajustes definidos por um perfil de configuração instalado não podem ser alterados pelo usuário. Se o usuário apagar um perfil de configuração, todos os ajustes definidos pelo perfil também serão removidos. Dessa forma, os administradores podem aplicar os ajustes ao atrelar políticas ao Wi-Fi e acesso de dados. Por exemplo, um perfil de configuração que fornece configurações de e-mail também pode especificar uma política de código do dispositivo. Os usuários não poderão acessar e-mails caso seus códigos não cumpram os requisitos definidos pelo administrador.

Ajustes do perfil

Um perfil de configuração contém uma série de ajustes em payloads específicos que podem ser especificados, incluindo, entre outros:

- Políticas de código e senha
- Restrição de recursos do dispositivo (por exemplo, desativar a câmera)
- Ajustes de Wi-Fi
- Ajustes de VPN
- Ajustes da conta
- Ajustes do serviço de diretório LDAP
- Ajustes do serviço de calendário CalDAV
- Credenciais e chaves
- Atualizações de software

Assinatura e criptografia do perfil

Um perfil de configuração pode ser assinado para validar sua origem e criptografado para garantir sua integridade e proteger o conteúdo. Os perfis de configuração do iOS e iPadOS são criptografados por meio do Cryptographic Message Syntax (CMS) especificado no RFC 3852, com compatibilidade com 3DES e AES-128.

Instalação de perfis

Os usuários podem instalar perfis de configuração diretamente nos dispositivos com o Apple Configurator 2. Os perfis também podem ser baixados pelo Safari, enviados como anexos em um e-mail, transferidos via AirDrop ou pelo app Arquivos no iOS e iPadOS, ou enviados por uma conexão sem fio com uma solução de gerenciamento de dispositivos móveis (MDM). Quando um usuário configura um dispositivo no Apple School Manager ou Apple Business Manager, o dispositivo baixa e instala um perfil para o registro no MDM.

Remoção de perfis

A remoção de perfis de configuração depende da forma como foram instalados. A sequência a seguir indica como um perfil de configuração pode ser removido:

1. Todos os perfis podem ser removidos por meio do apagamento de todos os dados do dispositivo.

2. Se o perfil for atribuído ao dispositivo pelo Apple School Manager ou Apple Business Manager, ele pode ser removido pela solução MDM e, opcionalmente, pelo usuário.
3. Se o perfil for instalado por uma solução MDM, ele pode ser removido por essa solução MDM específica ou pelo usuário que estiver cancelando o registro no MDM ao remover o perfil de configuração de registro.
4. Se o perfil for instalado em um dispositivo supervisionado pelo Apple Configurator 2, essa instância supervisora do Apple Configurator 2 pode remover o perfil.
5. Se o perfil for instalado em um dispositivo supervisionado manualmente ou pelo Apple Configurator 2 e o tiver um payload de senha de remoção, o usuário deve digitar a senha de remoção para remover o perfil.
6. Todos os outros perfis podem ser removidos pelo usuário.

   Uma conta instalada por um perfil de configuração pode ser removida por meio da remoção do perfil. As contas do Microsoft Exchange ActiveSync, incluindo as instaladas por meio de um perfil de configuração, podem ser removidas pelo Microsoft Exchange Server por meio do envio do comando de apagamento remoto exclusivo da conta.

Em dispositivos supervisionados, um perfil de configuração também pode ser bloqueado em um dispositivo para impedir completamente sua remoção ou para permitir a remoção somente com um código. Já que vários usuários empresariais usam seus próprios dispositivos iOS e iPadOS, os perfis de configuração que vinculam um dispositivo a uma solução MDM podem ser removidos, embora tal ação também remova todas as informações de configuração gerenciada, dados e apps.

Gerenciamento de dispositivos móveis (MDM)

Os sistemas operacionais da Apple oferecem suporte ao gerenciamento de dispositivos móveis (MDM), que permite a organizações configurar e gerenciar de forma segura implantações de dispositivos Apple em larga escala. Os recursos de MDM têm como base tecnologias existentes dos sistemas operacionais, como perfis de configuração, registro via conexão sem fio e o serviço de Notificações Push da Apple (APNs). Por exemplo, o APNs é usado para despertar o dispositivo para que ele se comunique diretamente com sua solução MDM através de uma conexão segura. Nenhuma informação confidencial ou proprietária é transmitida através do APNs.

Por meio do uso do MDM, os departamentos podem registrar dispositivos Apple em ambientes empresariais, configurar e atualizar ajustes via conexão sem fio, monitorar a conformidade com as políticas corporativas, gerenciar as políticas de atualização de software e até mesmo apagar ou bloquear remotamente dispositivos gerenciados.

Além dos registros tradicionais de dispositivos aos quais o iOS, iPadOS, macOS e tvOS oferecem suporte, um novo tipo de registro foi adicionado ao iOS 13, iPadOS 13.1 e macOS 10.15 — o Registro do Usuário. Os registros de usuários são registros de MDM que visam especificamente implantações do tipo “traga o seu próprio dispositivo” (BYOD), nas quais o dispositivo é de propriedade pessoal, embora seja usado em um ambiente gerenciado. Os registros de usuários concedem à solução MDM privilégios limitados em relação aos registros de dispositivos não supervisionados, além de proporcionarem a separação criptográfica entre os dados do usuário e os da empresa.

Tipos de registro

- *Registro do Usuário:* o Registro do Usuário é projetado para dispositivos de propriedade do usuário e é integrado a IDs Apple Gerenciados para estabelecer a identidade do usuário no dispositivo. IDs Apple Gerenciados fazem parte do perfil de Registro do Usuário, e o usuário deve autenticar com sucesso para que o registro seja concluído. IDs Apple Gerenciados podem ser usados ao mesmo tempo que o ID Apple pessoal com o qual o usuário já iniciou a sessão, sendo que os dois não interagem entre si.
- *Registro do Dispositivo:* o Registro do Dispositivo permite que organizações registrem dispositivos manualmente e gerenciem vários aspectos do seu uso, incluindo a capacidade de apagá-los. Se um usuário remover o perfil de MDM, todos os ajustes e apps que são gerenciados pela solução MDM são removidos.
- *Registro Automático do Dispositivo:* o Registro Automático do Dispositivo permite que organizações configurem e gerenciem dispositivos Apple a partir do momento que os dispositivos são tirados da caixa (conhecido como implantação sem toque). Esses dispositivos se tornam supervisionados e o perfil do MDM não pode ser removido pelo usuário. O Registro Automático do Dispositivo foi projetado para dispositivos de propriedade da organização.

Registro Automático do Dispositivo

As organizações podem registrar automaticamente dispositivos iOS, iPadOS, macOS e tvOS no gerenciamento de dispositivos móveis (MDM) sem que seja preciso tocá-los fisicamente ou prepará-los antes que os usuários os obtenham. Depois de se registrar em um dos serviços, o administrador inicia a sessão no site do serviço e vincula o programa à sua solução MDM. Os dispositivos comprados podem então ser atribuídos a usuários por meio do MDM. Durante o processo de configuração do dispositivo, a segurança de dados sigilosos pode ser aumentada por meio da aplicação de medidas de segurança apropriadas. Por exemplo:

- Fazer com que os usuários se autentiquem como parte do fluxo de configuração inicial no Assistente de Configuração do dispositivo Apple durante a ativação
- Fornecer uma configuração preliminar com acesso limitado e exigir configuração adicional do dispositivo para acessar dados sigilosos

Depois da atribuição do usuário, quaisquer configurações, restrições ou controles específicos do MDM são instalados automaticamente. Todas as comunicações entre os dispositivos e os servidores Apple são criptografadas em trânsito por meio de HTTPS (TLS).

O processo de configuração para os usuários pode ser simplificado ainda mais por meio da remoção de etapas específicas do Assistente de Configuração dos dispositivos, para que os usuários possam começar a usá-los rapidamente. Os administradores também podem controlar se o usuário pode remover o perfil de MDM do dispositivo e assegurar a implementação de restrições ao longo do ciclo de vida do dispositivo. Depois que o dispositivo foi retirado da caixa e ativado, ele pode ser registrado na solução MDM da organização — e todos os ajustes de gerenciamento, apps e livros são instalados conforme definido pelo administrador do MDM.

Apple School Manager e Apple Business Manager

O Apple School Manager e o Apple Business Manager são serviços oferecidos para que os administradores de TI possam implantar dispositivos Apple que uma organização tenha comprado diretamente da Apple ou através de Revendedores Autorizados Apple e operadoras participantes. Quando usados com uma solução de gerenciamento de dispositivos móveis (MDM), os administradores, funcionários, a equipe e professores podem configurar os ajustes do dispositivo e comprar e distribuir apps e livros. O Apple School Manager pode ser integrado a Sistemas de Informações de Estudantes (SISs), SFTP e Microsoft Azure AD por meio de autenticação federada, de forma que os administradores possam criar contas rapidamente a partir de listas de pessoal e turmas de escolas.

Dispositivos com iOS 11 ou posterior e tvOS 10.2 ou posterior também podem ser adicionados ao Apple School Manager e Apple Business Manager após a data da compra usando o Apple Configurator 2.

A Apple Inc. mantém certificações em conformidade com o ISO/IEC 27001 e 27018 para permitir que clientes da Apple analisem obrigações contratuais e de regulamentação. Essas certificações fornecem a nossos clientes uma declaração independente sobre as práticas de Privacidade e Segurança de Informações da Apple nos sistemas analisados. Para obter mais informações, consulte o artigo de Suporte da Apple Certificações dos Serviços de Internet da Apple.

Nota: para saber se um programa da Apple está disponível em um país ou região específica, consulte o artigo de Suporte da Apple: Disponibilidade de programas da Apple e métodos de pagamento para educação e negócios.

Apple Configurator 2

O Apple Configurator 2 possui um design flexível, seguro e focado no dispositivo, permitindo que o administrador configure de forma fácil e rápida um ou dezenas de dispositivos iOS, iPadOS e tvOS conectados ao Mac via USB antes de entregá-los aos usuários. Com o Apple Configurator 2, o administrador pode atualizar softwares, instalar apps e perfis de configuração, renomear e alterar a imagem da mesa de dispositivos, exportar informações sobre o dispositivo e documentos e muito mais.

Os administradores também têm a opção de adicionar dispositivos iOS, iPadOS e tvOS ao Apple School Manager ou Apple Business Manager por meio do Apple Configurator 2, mesmo que os dispositivos não tenham sido comprados diretamente na Apple, em Revendedores Autorizados Apple ou em uma operadora de celular autorizada. Quando o administrador configura um dispositivo que foi registrado manualmente, ele se comporta como qualquer outro dispositivo registrado, com supervisão obrigatória e registro no gerenciamento de dispositivos móveis (MDM). No caso de dispositivos que não foram comprados diretamente, o usuário possui um período de 30 dias para remover o dispositivo do registro, supervisão e MDM. O período de 30 dias tem início após a ativação do dispositivo.

Supervisão de dispositivos

Durante a configuração do dispositivo, uma organização pode configurá-lo para que ele seja supervisionado. A supervisão evidencia que o dispositivo é de propriedade da organização, o que possibilita controle adicional sobre sua configuração e definição de restrições. Com o Apple School Manager ou Apple Business Manager, a supervisão pode ser ativada remotamente no dispositivo como parte do processo de registro do gerenciamento de dispositivos móveis (MDM) para dispositivos iOS, iPadOS, macOS e tvOS ou ativada manualmente por meio do Apple Configurator 2 para dispositivos iOS, iPadOS e tvOS. No iOS, iPadOS e tvOS, para que um dispositivo seja supervisionado, ele deve ser apagado.

Os seguintes dispositivos podem ser supervisionados:

- iPhone, iPad e iPod touch com iOS 5 ou posterior
- Apple TV com tvOS 10.2 ou posterior

Os seguintes dispositivos são supervisionados automaticamente após o registro no Apple School Manager ou Apple Business Manager:

- Dispositivos iOS com iOS 13 ou posterior
- iPad com iPadOS 13.1 ou posterior
- Apple TV com tvOS 13 ou posterior
- Computadores Mac com macOS 10.15 ou posterior

Restrições de dispositivos

As restrições podem ser ativadas — ou em alguns casos, desativadas — por administradores para impedir que usuários acessem um certo app, serviço ou função do dispositivo. As restrições são enviadas para os dispositivos em um payload de restrições, o qual faz parte de um perfil de configuração. As restrições podem ser aplicadas a dispositivos iOS, iPadOS, macOS e tvOS. Certas restrições em um iPhone podem ser espelhadas em um Apple Watch emparelhado.

Bloqueio de Ativação

O gerenciamento do Bloqueio de Ativação permite que uma organização se beneficie da funcionalidade antifurto desse recurso ao mesmo tempo que oferece a capacidade de remover o Bloqueio de Ativação de dispositivos de propriedade da organização. O gerenciamento do Bloqueio de Ativação pode ser usado em um iPhone, iPad, iPod touch e computadores Mac que apareçam no Apple School Manager ou Apple Business Manager e estejam registrados em uma solução de gerenciamento de dispositivos móveis (MDM).

Dependendo do dispositivo, uma organização pode escolher entre ativar ou permitir o Bloqueio de Ativação. A ativação do Bloqueio de Ativação significa que a solução MDM (e não o usuário) contata os servidores da Apple para bloquear ou desbloquear o dispositivo. Em contrapartida, ao permitir o Bloqueio de Ativação, os usuários podem bloquear os dispositivos de propriedade da organização com suas contas do iCloud.

Ative ou desative o Bloqueio de Ativação no iPhone, iPad e iPod touch

O Bloqueio de Ativação pode ser *ativado* por uma solução MDM a qualquer momento em dispositivos no Apple School Manager ou Apple Business Manager sem que os usuários possam desativá-lo ou sem exigir que os usuários ativem o Buscar em seus dispositivos.

Isso é especialmente útil para usuários com IDs Apple Gerenciados do Apple School Manager ou Apple Business Manager, já que IDs Apple Gerenciados não podem usar o serviço Buscar. Depois de ativado, o MDM é usado para remover remotamente o dispositivo do Bloqueio de Ativação quando desejado ou, se a organização tiver a posse física do dispositivo, ela pode:

- Digitar o código de acesso do Bloqueio de Ativação do MDM na tela do Bloqueio de Ativação.
- Digitar o nome de usuário e a senha do Gerente de Dispositivos do Apple School Manager ou Apple Business Manager que criou o token de registro de dispositivo que vincula a solução MDM ao Apple School Manager ou Apple Business Manager.

Permita o Bloqueio de Ativação no iPhone, iPad, iPod touch e Mac

Organizações podem usar uma solução MDM para *permitir* o Bloqueio de Ativação em um dispositivo supervisionado. Isso permite que ela se beneficie da funcionalidade antifurto desse recurso, permitindo ainda que um usuário o contorne caso ele não possa autenticar com seu respectivo ID Apple por algum motivo, inclusive se o usuário tiver saído da organização.

Pelo fato de o Bloqueio de Ativação não ser permitido por padrão em dispositivos supervisionados, a solução MDM pode armazenar um código de acesso quando o Bloqueio de Ativação estiver ativado. Esse código de acesso pode ser usado para suspender o Bloqueio de Ativação automaticamente quando o dispositivo precisar ser apagado e atribuído a um novo usuário. A solução MDM pode recuperar um código de acesso e *permitir* que o usuário ative o Bloqueio de Ativação no dispositivo com base no seguinte:

- Se o Buscar estiver *ativado* quando a solução MDM permitir o Bloqueio de Ativação, o Bloqueio de Ativação é ativado nesse momento.
- Se o Buscar estiver *inativo* quando a solução MDM ativar o Bloqueio de Ativação, o Bloqueio de Ativação será ativado na próxima vez que o usuário ativar o Buscar.

No iOS e iPadOS, os códigos de acesso estão disponíveis por até 15 dias *após* o dispositivo ser supervisionado pela primeira vez ou até que uma solução MDM recupere — e depois limpe — o código explicitamente. Se a solução MDM não recuperar o código de acesso em 15 dias, ele se torna irrecuperável.

Nota: em computadores Mac com macOS 10.15, o Bloqueio de Ativação não pode ser ativado por um MDM, mas o usuário pode ser impedido de ativar o Bloqueio de Ativação quando ele ativar o Buscar. Se computadores Mac com um chip Apple T2 Security estiverem usando um MDM aprovado pelo usuário e forem atualizados para o macOS 10.15, o Bloqueio de Ativação também não é permitido por padrão. O gerenciamento do Bloqueio de Ativação em instalações (e não atualizações) do macOS 10.15 exige que o dispositivo seja adicionado ao Apple School Manager ou Apple Business Manager e registrado no MDM.

Códigos de acesso e chaves reservas

Os códigos de acesso e chaves reservas que a solução MDM usa para gerenciar o Bloqueio de Ativação são cruciais para a capacidade de suspender o Bloqueio de Ativação. Esses códigos de acesso e chaves reservas devem ser guardados em segurança e ter backups feitos regularmente. Caso o fornecedor do MDM mude, torna-se crítico manter uma cópia desses códigos de acesso e chaves reservas ou suspender o Bloqueio de Ativação em todos os dispositivos registrados.

Modo Perdido, apagamento remoto e bloqueio remoto

Modo Perdido

Se um dispositivo iOS ou iPadOS supervisionado com iOS 9 ou posterior for perdido ou roubado, um administrador de MDM pode ativar remotamente o Modo Perdido nesse dispositivo. Quando o Modo Perdido está ativado, o usuário atual tem sua sessão encerrada e o dispositivo não pode ser desbloqueado. A tela mostra uma mensagem que pode ser personalizada pelo administrador, como por exemplo o número de telefone para o qual ligar caso o dispositivo seja encontrado. Quando o dispositivo é colocado em Modo Perdido, o administrador pode solicitar que ele envie sua localização atual e, opcionalmente, reproduza um som. Quando um administrador desativa o Modo Perdido, que é a única maneira de sair do modo, o usuário é informado dessa ação por meio de uma mensagem na tela Bloqueada ou um alerta na tela de Início.

Apagamento remoto e bloqueio remoto

Os dispositivos iOS, iPadOS e macOS podem ser apagados remotamente por um administrador ou usuário (o apagamento remoto imediato está disponível apenas se o FileVault do Mac estiver ativado). O apagamento remoto imediato é executado através do descarte seguro da chave de mídia do Armazenamento Apagável, o que torna todos os dados ilegíveis. O comando de apagamento remoto pode ser iniciado via gerenciamento de dispositivos móveis (MDM), Microsoft Exchange ActiveSync ou iCloud. No Mac, o computador atesta o recebimento e realiza o apagamento. Com o bloqueio remoto, o MDM requer que um código de seis dígitos seja aplicado ao Mac, bloqueando o acesso de qualquer usuário até que esse código seja digitado.

Quando um comando de apagamento remoto é acionado via MDM ou iCloud, o dispositivo atesta seu recebimento e realiza o apagamento. No caso de apagamento remoto por meio do Microsoft Exchange ActiveSync, o dispositivo verifica com o Microsoft Exchange Server antes de realizar o apagamento. O apagamento remoto não é possível em duas situações:

- Com Registro do Usuário
- Com o uso do Microsoft Exchange ActiveSync quando a conta foi instalada com Registro do Usuário

Os usuários também podem usar o app Ajustes para apagar dispositivos iOS e iPadOS que estiverem em sua posse. E, conforme já mencionado, os dispositivos podem ser configurados para serem apagados automaticamente após uma série de tentativas malsucedidas de digitação do código.

iPad Compartilhado

Visão geral do iPad Compartilhado

O iPad Compartilhado é um modo multiusuário para uso em implantações do iPad. Ele permite que usuários compartilhem um iPad ao mesmo tempo que mantém uma separação de documentos e dados para cada usuário. Cada usuário obtém sua própria localização de armazenamento reservada e privada, a qual é implementada como um volume APFS protegido pelas credenciais do usuário. O iPad Compartilhado requer o uso de um ID Apple Gerenciado emitido e de propriedade de uma organização, e permite que um usuário inicie a sessão em qualquer dispositivo de propriedade da organização configurado para o uso de vários usuários. Os dados dos usuários são particionados em diretórios separados, cada um em seu próprio domínio de proteção de dados e protegido por permissões UNIX e sandbox. No iPadOS 13.4 ou posterior, usuários também podem iniciar a sessão em uma sessão temporária. Quando o usuário finaliza a sessão em uma sessão temporária, seu volume APFS é apagado e o espaço reservado para o volume retorna ao sistema.

Início de Sessão no iPad Compartilhado

Os IDs Apple Gerenciados tanto nativos quanto federados são aceitos ao iniciar uma sessão no iPad Compartilhado. Ao usar uma conta federada pela primeira vez, o usuário é redirecionado para o portal de início de sessão do provedor de identidade. Depois de autenticar, um token de acesso de curta duração é emitido para os IDs Apple Gerenciados armazenados e o processo de início de sessão continua de forma semelhante ao processo de início de sessão nativo de IDs Apple Gerenciados. Após o início de sessão, o Assistente de Configuração do iPad Compartilhado solicita ao usuário que defina um código (credencial) usado para proteger os dados locais no dispositivo e para autenticação na tela de início de sessão no futuro. Como em um dispositivo de usuário único, no qual o usuário iniciaria a sessão uma única vez no seu ID Apple Gerenciado com a conta federada e desbloquearia o dispositivo com o código, no iPad Compartilhado, o usuário inicia a sessão uma única vez com a conta federada e, a partir de então, usa o código estabelecido.

Quando um usuário inicia a sessão sem a autenticação federada, o ID Apple Gerenciado é autenticado com o Serviço de Identidade da Apple (IDS) pelo protocolo SRP. Se a autenticação for bem-sucedida, um token de acesso de curta duração específico do dispositivo é concedido. Se o usuário já tiver usado o dispositivo antes, ele já terá uma conta de usuário local, a qual é desbloqueada com a mesma credencial.

Se o usuário não tiver usado o dispositivo antes ou estiver usando o recurso de sessão temporária, o iPad Compartilhado fornece um novo ID de usuário UNIX, um volume APFS para armazenar os dados pessoais do usuário e chaves locais. Pelo fato de o armazenamento ser alocado (reservado) para o usuário quando da criação do volume APFS, pode não haver espaço suficiente para criar um volume novo. Nesse caso, o sistema identificará um usuário existente cujos dados tenham sido completamente sincronizados com a nuvem e o despejará do dispositivo para que o novo usuário possa iniciar a sessão. Na improvável eventualidade de que nenhum usuário existente tenha terminado de enviar seus dados à nuvem, o início de sessão do usuário novo falha. Para iniciar a sessão, o novo usuário precisará aguardar o término da sincronização dos dados de um usuário ou fazer com que um administrador apague à força uma conta de usuário existente, o que implica risco de perda de dados.

Se o dispositivo não estiver conectado à internet (se o usuário não tiver um ponto de acesso Wi-Fi, por exemplo), a autenticação pode usar a conta local como base durante um número limitado de dias. Nesse caso, apenas os usuários com contas locais previamente existentes ou uma sessão temporária podem iniciar a sessão. Depois que esse tempo limite expira, os usuários são obrigados a autenticar online, mesmo que uma conta local exista.

Depois que a conta local de um usuário for desbloqueada ou criada, caso tenha sido autenticada remotamente, o token de curta duração emitido pelos servidores da Apple é convertido em um token do iCloud que permite iniciar a sessão no iCloud. Em seguida, os ajustes do usuário são restaurados e seus documentos e dados são sincronizados do iCloud.

Enquanto a sessão do usuário estiver ativa e o dispositivo permanecer on-line, os documentos e dados são armazenados no iCloud conforme forem criados ou modificados. Além disso, um mecanismo de sincronização em segundo plano garante que as alterações sejam enviadas ao iCloud ou a outros serviços da web através de sessões NSURLSession em segundo plano, após o usuário finalizar a sessão. Depois que a sincronização em segundo plano desse usuário for concluída, o volume APFS do usuário é desmontado e não pode ser montado novamente sem que o usuário inicie a sessão novamente.

Sessões temporárias não sincronizam dados com o iCloud e, embora uma sessão temporária possa iniciar a sessão em um serviço de sincronização de terceiros, como Box ou Google Drive, não há nenhuma possibilidade de continuar sincronizando os dados quando a sessão temporária termina.

Término de sessão no iPad Compartilhado

Quando um usuário finaliza a sessão no iPad Compartilhado, sua keybag é bloqueada imediatamente e todos os apps são encerrados. Para acelerar o caso de um usuário novo que inicia a sessão, o iPadOS posterga temporariamente algumas ações ordinárias de finalização de sessão e apresenta uma janela de início de sessão ao usuário novo. Se um usuário inicia a sessão durante esse tempo (aproximadamente 30 segundos), o iPad Compartilhado realiza a limpeza postergada como parte do início de sessão na conta do usuário novo. Porém, se o iPad Compartilhado permanecer ocioso, ele acionará a limpeza postergada. Durante a fase de limpeza, a Janela de Início de Sessão é reiniciada como se outra finalização de sessão tivesse ocorrido.

Quando uma sessão temporária termina, o iPad Compartilhado realiza a sequência completa de finalização de sessão e apaga imediatamente o volume APFS da sessão temporária.

Tempo de Uso

O Tempo de Uso é um recurso — no iOS 12 ou posterior, iPadOS e macOS 10.15 ou posterior e alguns recursos do watchOS — que permite que um usuário entenda e controle seu próprio uso de apps e páginas web, assim como o de suas crianças. Embora o Tempo de Uso não seja um recurso de segurança novo, é importante entender como ele protege a segurança e a privacidade dos dados coletados e compartilhados entre dispositivos.

No Tempo de Uso, há dois tipos de usuários: adultos e crianças.

Recurso	Sistema operacional compatível
Visualizar dados sobre uso	iOS iPadOS macOS
Aplicar restrições adicionais	iOS iPadOS macOS
Definir limites de uso da web	iOS iPadOS macOS
Definir limites de uso de apps	iOS iPadOS macOS watchOS
Configurar o Repouso	iOS iPadOS macOS watchOS

Para um usuário que gerencia o uso de seu próprio dispositivo, os controles e dados de uso do Tempo de Uso podem ser sincronizados entre dispositivos associados à mesma conta do iCloud usando a criptografia de ponta a ponta do CloudKit. Isso requer que a conta do usuário tenha autenticação de dois fatores ativada (a sincronização fica desativada por padrão). O Tempo de Uso substitui o recurso Restrições encontrado em versões anteriores do iOS.

No iOS 13, iPadOS 13.1 e macOS 10.15, os usuários do Tempo de Uso e as crianças gerenciadas compartilham automaticamente os dados de uso entre dispositivos se a autenticação de dois fatores estiver ativada em suas contas do iCloud. Quando um usuário limpa o histórico do Safari ou apaga um app, os dados de uso correspondentes são removidos do dispositivo e de todos os dispositivos sincronizados.

Pais e Tempo de Uso

Pais e mães também podem usar o Tempo de Uso em dispositivos iOS, iPadOS e macOS para entender e controlar o uso de seus filhos. Se o pai ou mãe é organizador da família (no Compartilhamento Familiar do iCloud), pode visualizar os dados e gerenciar os ajustes do Tempo de Uso para seus filhos. Os filhos são informados quando seus pais ativam o Tempo de Uso e também podem monitorar seu próprio uso. Quando os pais ativam o Tempo de Uso para seus filhos, definem um código de modo que os filhos não possam fazer alterações. Ao completarem 18 anos (dependendo do país ou região), os filhos podem desativar esse monitoramento.

Os dados de uso e ajustes de configuração são transferidos entre os dispositivos dos pais e dos filhos por meio do protocolo Serviço de Identidade da Apple (IDS), criptografado de ponta a ponta. Os dados criptografados podem ser armazenados brevemente em servidores IDS até serem lidos pelo dispositivo receptor (por exemplo, assim que o iPhone, iPad ou iPod touch for ligado, caso estivesse desligado). Tais dados não podem ser lidos pela Apple.

Análise do Tempo de Uso

Se o usuário ativar a opção Compartilhar Análise, somente os dados anonimizados a seguir serão coletados, para que a Apple possa entender melhor como o Tempo de Uso está sendo usado:

- Se o Tempo de Uso foi ativado durante o Assistente de Configuração ou posteriormente nos Ajustes
- Alteração no uso de uma Categoria após a criação de um limite para ela (em até 90 dias)
- Se o Tempo de Uso está ativado
- Se o Repouso está ativado
- Quantas vezes a consulta “Pedir Mais Tempo” foi usada
- Número de limites de apps
- Número de vezes que os usuários visualizaram o uso nos ajustes do Tempo de Uso, por tipo de usuário e por tipo de visualização (local, remota, widget)
- Quantas vezes os usuários ignoram um limite, por tipo de usuário
- Quantas vezes os usuários apagam um limite, por tipo de usuário

Nenhum dado específico de uso de apps ou da web é coletado pela Apple. Quando um usuário vê uma lista de apps nas informações de uso do Tempo de Uso, os ícones dos apps são obtidos diretamente da App Store, que não retém quaisquer dados dessas solicitações.

Certificações de segurança e privacidade da Apple

Visão geral de certificações de segurança e privacidade da Apple

A Apple mantém certificações e declarações independentes sobre seu hardware, software (incluindo sistemas operacionais e apps) e serviços para fornecer uma revisão independente das práticas de segurança e privacidade da Apple a usuários. Em caso de dúvidas sobre as Certificações de Segurança e Privacidade da Apple, contate security-certifications@apple.com.

Certificações de hardware

Para obter informações sobre as certificações públicas relacionadas ao *hardware e componentes de firmware associados*, consulte:

- Certificações de segurança do chip Apple T2 Security
- Certificações de segurança do Processador do Secure Enclave

Certificações de software

Para obter informações sobre as certificações públicas relacionadas aos *sistemas operacionais da Apple*, consulte:

- Certificações de segurança dos produtos iOS
- Certificações de segurança dos produtos iPadOS
- Certificações de segurança dos produtos macOS
- Certificações de segurança dos produtos tvOS
- Certificações de segurança dos produtos watchOS

Certificações de serviços

Para obter informações sobre as certificações públicas relacionadas aos serviços de internet da Apple, consulte:

- Certificações dos Serviços de Internet da Apple

Garantia de segurança da Apple

A Apple se empenha em uma abordagem completa em relação a certificações de segurança para oferecer as garantias apropriadas a clientes em todas as plataformas Apple. No entanto, nem todas as áreas técnicas têm padrões de certificação de segurança completos aceitos globalmente. No caso de diversas certificações bem definidas e globalmente aceitas, a Apple se empenha e conquista certificações anuais, de acordo com cada lançamento principal de um OS. Para cobrir áreas de menor representação, a Apple tem se engajado no desenvolvimento de padrões de segurança emergentes. A missão é desenvolver uma cobertura de certificação de segurança completa, aceita globalmente, entre hardware, software e serviços da Apple.

Certificações e validações de hardware e software

Com o desenvolvimento e gerenciamento completos de toda a plataforma, desde o silício até o sistema operacional, serviços e apps, a Apple começa com os **elementos básicos de certificação** que são amplamente aplicados entre diversas plataformas quando apropriados. Um desses elementos básicos é a validação do corecrypto usado em todas as implantações do módulo criptográfico de software e hardware dos sistemas operacionais desenvolvidos pela Apple. Um segundo elemento básico é a certificação do **Processador do Secure Enclave**, que agora é integrado a vários dispositivos Apple. Um terceiro é a certificação do **Elemento Seguro**, encontrado em todos os iPhones e computadores Mac com Touch ID. Esses elementos básicos de certificação de hardware constituem o alicerce para certificações de segurança da plataforma mais amplas.

Validações de Módulos Criptográficos FIPS 140-2/3 (ISO/IEC 19790)

Os módulos criptográficos dos sistemas operacionais da Apple têm sido repetidamente validados pelo Programa de Validação de Módulos Criptográficos (CMVP) como em conformidade com o FIPS (Federal Information Processing Standard) 140-2 dos EUA em cada versão principal dos sistemas operacionais desde 2012. Depois de cada versão principal, a Apple envia todos os módulos ao CMVP para validação criptográfica completa. Esses módulos validados oferecem operações criptográficas aos serviços fornecidos pela Apple e estão disponíveis para serem usados por apps de terceiros.

A Apple obtém o **Nível de Segurança 1** a cada ano para os módulos baseados em software: “CoreCrypto Module on Intel” e “CoreCrypto Kernel Module on Intel” no macOS, “CoreCrypto Module on ARM” e “CoreCrypto Kernel Module on ARM” no iOS, iPadOS, tvOS, watchOS e firmware do chip Apple T2 Security integrado ao Mac.

A Apple obteve o Nível de Segurança 2 do FIPS para o módulo de hardware integrado identificado como “Apple Secure Enclave Processor (SEP) Secure Key Store (SKS) Cryptographic Module”, permitindo o uso aprovado pelo governo de chaves geradas e gerenciadas pelo SEP. A Apple continuará buscando níveis mais altos para o módulo de hardware a cada lançamento principal sucessivo dos sistemas operacionais conforme for adequado.

O **FIPS 140-3** foi aprovado pelo Departamento de Comércio dos EUA em 2019. A diferença mais marcante desta versão do padrão é o uso do padrão ISO/IEC 19790:2015 e do padrão de teste associado ISO/IEC 24759:2017. O CMVP iniciou um programa de transição e indicou que, a partir de 2020, os módulos criptográficos começarão a ser validados usando o FIPS 140-3 como base. Os módulos criptográficos da Apple terão como objetivo atender e mudar para o padrão FIPS 140-3 o mais breve possível.

No caso de módulos criptográficos atualmente em processos de teste e validação, o CMVP mantém duas listas distintas que podem conter informações sobre as validações propostas. Em módulos criptográficos sendo testados por laboratórios qualificados, a Lista de Implementação Sendo Testada (em inglês) pode incluir o módulo. Depois de enviado pelo laboratório para validação pelo CMVP, o módulo criptográfico pode aparecer na Lista de Módulos em Processo (em inglês). Consulte essas duas listas de processos primeiro, caso tenha dúvidas sobre seus estados de validação logo após o lançamento principal de um OS.

Certificações do Produto (Common Criteria ISO/IEC 15408)

O Common Criteria (ISO/IEC 15408) é um padrão usado por várias organizações como base para realizar avaliações de segurança de produtos de TI.

Para certificações que possam ser mutualmente reconhecidas sob o CCRA (Common Criteria Recognition Arrangement), consulte o Portal do Common Criteria (em inglês). O padrão Common Criteria também pode ser usado fora do CCRA por esquemas de validação nacionais e privados.

O objetivo, conforme declarado pela comunidade do Common Criteria, é que um conjunto de padrões de segurança aprovados internacionalmente forneça uma avaliação clara e confiável das capacidades de segurança de produtos de Tecnologia da Informação. Ao fornecer uma avaliação independente da capacidade de um produto em atender aos padrões de segurança, a Certificação Common Criteria oferece a clientes mais confiança em produtos de Tecnologia da Informação e leva a decisões mais informadas.

Através do CCRA (Common Criteria Recognition Arrangement), países membros e regiões concordaram em reconhecer a certificação de produtos de Tecnologia da Informação com o mesmo nível de confiança. A adesão a esse grupo, além da profundidade e largura de Perfis de Proteção (PPs), continua crescendo anualmente para avaliar tecnologias emergentes. Esse acordo permite que o desenvolvedor de um produto busque uma única certificação sob qualquer um dos Esquemas de Autorização.

PPs anteriores foram arquivados e estão sendo substituídos pelo desenvolvimento de Perfis de Proteção direcionados, os quais se concentram em soluções e ambientes específicos. Em um esforço combinado para garantir o reconhecimento mútuo contínuo entre todos os membros do CCRA, a Comunidade Técnica Internacional (iTC) continua direcionando todos os desenvolvimentos e atualizações de PPs rumo a Perfis de Proteção Colaborativos (cPP), os quais são desenvolvidos desde o início com o envolvimento de diversos esquemas.

O documento que expressa os requisitos de segurança avaliados em um produto de TI é chamado de “Alvo de Segurança” (ST) e, para receber a garantia especificada, o dispositivo deve ser configurado conforme a descrição no documento guia associado à avaliação.

A garantia obtida ao usar os padrões Common Criteria é expressa com requisitos de garantia de segurança que podem ser especificados em um Perfil de Proteção (PP) ou ST. Níveis de Garantia da Avaliação (EAL) agrupam conjuntos de exigências de garantia da segurança usados comumente e podem ser especificados em PPs e STs para serem compatíveis com a possibilidade de comparação.

A Apple começou,desde o início de 2015, a buscar certificações sob essa nova estrutura do Common Criteria com PPs selecionados. Desde 2015, a Apple obtém certificações Common Criteria (ISO/IEC 15408) para cada versão principal do iOS e ampliou a cobertura para incluir a garantia fornecida por novos Perfis de Proteção (PPs). Essas incluem o seguinte:

iOS e iPadOS em dispositivos móveis (iPhone e iPad)

- Certificação de Dispositivo Móvel
  - Perfil de Proteção Fundamental de Dispositivo Móvel *(certificação da plataforma)*
  - Módulo PP do Agente de MDM *(gerenciamento MDM da plataforma)*
  - Pacote Funcional de TLS *(toda a comunicação de entrada e saída da plataforma via TLS)*
  - Módulo PP do Cliente de VPN *(VPN Sempre Ativa usando IKEv2 para IPSEC)*
  - Pacote Ampliado para Clientes de LAN Sem Fio *(acesso sem fio autenticado e criptografado)*
- Certificações de Apps
  - Software de aplicativo*(Contatos)*
  - Pacote Ampliado para Navegadores Web *(navegador Safari)*

A Apple assumiu um papel ativo nas comunidades técnicas focadas em avaliar tecnologias de segurança móveis. Essas incluem as Comunidades Técnicas Internacionais (iTC) responsáveis por desenvolver e atualizar Perfis de Proteção Colaborativos (cPPs). A Apple continua avaliando e buscando certificações perante PPs e cPPs disponíveis atualmente e em desenvolvimento.

As certificações da plataforma Apple para o mercado norte americano são geralmente realizadas com a NIAP (National Information Assurance Partnership), a qual mantém uma lista de projetos atualmente em avaliação, mas ainda não certificados. Além dos certificados de plataforma gerais listados, outros certificados CC foram emitidos para demonstrar requisitos de segurança específicos para alguns mercados.

Certificações de Serviços

A Apple Inc. mantém certificações em conformidade com padrões como o ISO/IEC 27001 e 27018 para permitir que clientes da Apple analisem obrigações contratuais e de regulamentação. Essas certificações fornecem a nossos clientes uma declaração independente sobre as práticas de Privacidade e Segurança de Informações da Apple nos sistemas analisados.

- Certificações dos Serviços de Internet da Apple

Glossário

Termo	Definição
AES	Advanced Encryption Standard (Padrão de Criptografia Avançado).
AES-XTS	Um modo do AES definido no IEEE 1619-2007 para a criptografia de mídias de armazenamento.
Aleatorização do Layout de Espaço de Endereço (ASLR)	Técnica empregada pelo iOS para dificultar o êxito do aproveitamento mal-intencionado por erros de software. A garantia de imprevisibilidade de endereços e offsets da memória, impossibilita o hardcode desses valores pelo código de aproveitamento. No iOS 5 ou posterior, a posição de todos os apps e bibliotecas do sistema também é aleatorizada, assim como todos os apps de terceiros compilados como executáveis de posição independente.
APFS	Apple File System.
Armazenamento Apagável	Área dedicada do armazenamento NAND, usada para armazenar chaves criptográficas, que pode ser endereçada diretamente e apagada com segurança. Mesmo não fornecendo proteção caso um ataque físico ao dispositivo ocorra, as chaves armazenadas no Armazenamento Apagável podem ser usadas como parte de uma hierarquia de chaves para facilitar o apagamento rápido e invocar segurança.
Autorização do Software do Sistema	Combina chaves criptográficas integradas ao hardware com um serviço on-line para assegurar que apenas softwares legítimos da Apple, adequados a dispositivos compatíveis, sejam fornecidos e instalados durante a atualização.
Bits de núcleo de software	Bits dedicados no mecanismo de Secure Enclave EAS que são afixados ao UID ao gerar chaves a partir do UID. Cada bit de núcleo de software tem um bit de bloqueio correspondente. A ROM de Inicialização do Secure Enclave e o SO podem alterar independentemente o valor de cada bit de núcleo de software, contanto que o bit de bloqueio correspondente não tenha sido definido. Uma vez que o bit de bloqueio tenha sido definido, não é possível modificar o bit de núcleo de núcleo de software nem o bit de bloqueio. Os bits de núcleo de software e seus bloqueadores são redefinidos quando o Secure Enclave é reinicializado.
Boot Camp	O Boot Camp permite a instalação do Microsoft Windows no Mac.

Termo	Definição
Chave de mídia	Parte da hierarquia de chave de criptografia que ajuda a fornecer um apagamento seguro e instantâneo. No iOS, iPadOS, tvOS e watchOS, a chave de mídia embala os metadados no volume de dados (sendo assim, sem ela, o acesso a todas as chaves únicas por arquivo não é possível, deixando inacessíveis os arquivos protegidos pela Proteção de Dados). No macOS, a chave de mídia embala o material das chaves, todos os metadados e dados no volume protegido pelo FileVault. Em ambos os casos, o apagamento da chave de mídia deixa os dados criptografados inacessíveis.
Chave do sistema de arquivos	Chave que criptografa os metadados de cada arquivo, incluindo sua chave de classe. Mantida no Armazenamento Apagável, priorizando facilitar o apagamento rápido em detrimento da confidencialidade.
Chave única por arquivo	A chave de 256 bits usada para criptografar um arquivo no sistema de arquivos com AES128-XTS, onde os 256 bits são divididos para fornecer tanto a chave de ajuste de 128 bits quanto a chave de cifra de 128 bits. A chave única por arquivo é embalada por uma chave de classe e armazenada nos metadados do arquivo.
Chaves	Infraestrutura e conjunto de APIs usadas pelo iOS e apps de terceiros para armazenar e obter senhas, chaves e outras credenciais sensíveis.
Circuito integrado (CI)	Também chamado de “microchip”.
CKRecord	Um dicionário de pares chave-valor que contêm dados salvos ou transferidos do CloudKit.
Cofre da Dados	Um mecanismo — aplicado pelo kernel — para proteger contra o acesso não autorizado a dados, independentemente de o app que os solicita usar sandbox.
Controlador de memória	O subsistema no SoC que controla a interface entre o SoC e sua memória principal.
Controlador do SSD	Subsistema de hardware que gerencia a mídia de armazenamento (unidade de estado sólido).
DMA	O acesso direto à memória permite que subsistemas de hardware acessem a memória principal.
ECDSA	Algoritmo de assinatura digital baseado em criptografia de curva elíptica.
Elliptic Curve Diffie-Hellman Exchange (ECDHE)	Elliptic Curve Diffie-Hellman Exchange com chaves temporárias. A ECDHE permite que duas partes concordem com uma chave secreta de modo que impeça que a chave seja descoberta por um interceptador observando as mensagens entre as duas partes.
Embalagem de chaves	Criptografia de uma chave com outra. O iOS usa a embalagem de chaves NIST AES, conforme o RFC 3394.
eSPI	Barramento de Interface Periférico Serial aprimorada para comunicação serial síncrona.

Termo	Definição
Firmware da UEFI	Interface de Firmware Extensível Unificada, uma tecnologia de substituição da BIOS para conectar um firmware ao sistema operacional de um computador.
Gerenciador de Inicialização de Baixo Nível (LLB)	Em computadores Mac com arquitetura de inicialização de dois estágios, código invocado pela ROM de Inicialização, que por sua vez, carrega o iBoot, como parte da cadeia de inicialização segura.
Gerenciamento de dispositivos móveis (MDM)	Um serviço que permite ao usuário gerenciar remotamente dispositivos registrados. Depois do registro de um dispositivo, o usuário pode usar o serviço de MDM através da rede para configurar ajustes e realizar outras tarefas no dispositivo sem interação com o usuário.
iBoot	Código que carrega o XNU, como parte da cadeia de inicialização segura. Dependendo da geração do SoC, o iBoot pode ser carregado por LLB ou diretamente pela ROM de Inicialização.
ID de Grupo (GID)	Semelhante ao UID, mas comum a cada processador de uma classe.
ID Exclusivo (UID)	Chave AES de 256 bits gravada em cada processador durante o processo de manufatura. Não pode ser lida por firmware ou software e é usada apenas pelo mecanismo AES de hardware do processador. Para obter a chave em si, seria preciso montar um ataque físico altamente sofisticado e caro contra o silício do processador. O UID não está relacionado a nenhum outro identificador do dispositivo, incluindo, entre outros, o UDID.
Identificação Exclusiva de Chip (ECID)	Um identificador de 64 bits exclusivo ao processador de cada dispositivo iOS. Quando uma ligação é atendida em um dispositivo, o toque de dispositivos próximos emparelhados com o iCloud é interrompido com um breve anúncio por meio de Bluetooth Low Energy (BLE) 4.0. Os bytes do anúncio são criptografados pelo mesmo método dos anúncios do Handoff. Usado como parte do processo de personalização, ele não é considerado um segredo.
Identificador Uniforme de Recursos (URI)	String de caracteres que identifica um recurso baseado na web.
Joint Test Action Group (JTAG)	Ferramenta padrão de depuração de hardware usada por programadores e desenvolvedores de circuitos.

Termo	Definição
Keybag	Estrutura de dados usada para armazenar uma coleção de chaves de classe. Cada tipo (usuário, dispositivo, sistema, backup, guarda ou Backup do iCloud) possui o mesmo formato. Um cabeçalho contendo: Versão (definida como quatro no iOS 12 ou posterior), Tipo (sistema, backup, guarda ou Backup do iCloud), UUID da Keybag, um HMAC caso a keybag esteja assinada e o método usado para embalar as chaves de classe — trançamento com o UID ou PBKDF2, juntamente com o sal e a contagem da iteração. Uma lista de chaves de classe: UUID da Chave, Classe (qual arquivo ou classe da Proteção de Dados das Chaves), tipo de embalagem (apenas chave derivada do UID; chave derivada do UID e chave derivada do código), chave de classe embalada e uma chave pública para classes assimétricas
Mapeamento do ângulo de fluxo dos sulcos	Representação matemática da direção e largura dos sulcos extraídos de parte de uma impressão digital.
Mecanismo de criptografia AES	Um componente de hardware dedicado que implementa o AES.
Modo de Atualização do Firmware do Dispositivo (DFU)	Modo no qual o código ROM de Inicialização aguarda por recuperação via USB. A tela fica preta quando no modo DFU, mas ao conectar-se a um computador com o iTunes aberto, o seguinte diálogo é apresentado: "O iTunes detectou um (iPad, iPhone ou iPod touch) em modo de recuperação. O usuário precisa restaurar esse (iPad, iPhone ou iPod touch) para poder utilizá-lo com o iTunes."
Modo de Recuperação	O modo de Recuperação é usado para restaurar um dispositivo iOS ou Apple TV se o iTunes (apenas para dispositivos iOS) não reconhecer o dispositivo do usuário ou disser que está no modo de Recuperação, a tela estiver parada no logotipo da Apple por vários minutos sem uma barra de progresso ou a tela de conexão com o iTunes aparecer.
Modo DFU do T2	Modo de Atualização do Firmware do Dispositivo do chip Apple T2 Security.
Módulo de segurança de hardware (HSM)	Computador especializado inviolável que resguarda e gerencia chaves digitais.
NAND	Memória flash não volátil.
Perfil de provisão	Arquivo plist assinado pela Apple que contém um conjunto de entidades e direitos permitindo a instalação e o teste de apps em um dispositivo iOS. Um Perfil de Provisão de desenvolvimento lista os dispositivos escolhidos por um desenvolvedor para distribuição ad hoc. Um Perfil de Provisão de distribuição contém o ID do app de apps empresariais.
Proteção da Integridade do Coprocessador do Sistema (SCIP)	Coprocessadores do sistema são CPUs no mesmo SoC do processador do aplicativo.
Proteção de Dados	Mecanismo de proteção de arquivos e Chaves para iOS. Também pode referir-se às APIs que os apps usam para proteger arquivos e itens das Chaves.

Termo	Definição
Recompensa de Segurança da Apple	Uma recompensa oferecida pela Apple a pesquisadores que relatem uma vulnerabilidade que afete os sistemas operacionais mais recentes disponíveis e, nos casos relevantes, o hardware mais recente.
Registro de Progresso de Inicialização (BPR)	Um conjunto de avisos de hardware de SoC que o software pode usar para rastrear os modos de inicialização em que o dispositivo entrou, como modo DFU ou modo de Recuperação. Uma vez que um aviso de Registro de Progresso de Inicialização é emitido, não pode ser apagado. Isso permite que um software posterior obtenha um indicador confiável do estado do sistema.
ROM de Inicialização	Primeiro código executado pelo processador de um dispositivo ao ser inicializado. Por ser parte integral do processador, não pode ser alterado pela Apple ou por um atacante.
Serviço de Identidade da Apple (IDS)	Diretório da Apple de chaves públicas do iMessage, endereços APNs, números de telefone e endereços de e-mail usados para buscar chaves e endereços de dispositivos.
Serviço de Notificações Push da Apple (APNs)	Serviço mundial fornecido pela Apple que entrega notificações push para dispositivos iOS e iPadOS.
Sistema do Chip (SoC)	Circuito integrado (CI) que incorpora vários componentes em um único chip. O processador do aplicativo, o Secure Enclave e outros coprocessadores são componentes do SoC.
Trançamento	Processo pelo qual o código de um usuário é transformado em uma chave criptográfica e fortificado com o UID do dispositivo. Isso assegura que ataques de força bruta tenham que ser realizados em um dispositivo específico, diminuindo assim a probabilidade da ocorrência (que não pode ser feita em paralelo). O algoritmo do trançamento (PBKDF2) usa AES chaveado com o UID do dispositivo como função pseudoaleatória (PRF) em cada iteração.
XNU	Núcleo dos sistemas operacionais iOS e macOS. É considerado confiável e exige medidas de segurança como assinatura de código, sandbox, verificação de direitos e ASLR.

Histórico de Revisão do Documento

Data	Resumo
Abril de 2020	Atualizado para: • iOS 13.4 • iPadOS 13.4 • macOS 10.15.4 • tvOS 13.4 • watchOS 6.2 Atualizações: • Desconexão do microfone do iPad adicionado à Desconexão do microfone por hardware no Mac e iPad. • Cofres de Dados adicionado a Como a Apple protege as informações pessoais dos usuários. • Atualizações a Uso do Bootstrap Token, Configuração do usuário, Configuração da organização e Ferramentas de linha de comando. • Adições à Ferramenta de Remoção de Malware em Proteção contra malware. • Atualizações à Visão Geral do iPad Compartilhado, Início de Sessão no iPad Compartilhado e Término de sessão no iPad Compartilhado. • Novo tópico de Visão geral de certificações de segurança e privacidade da Apple. • Atualizações à Visão geral de certificações de segurança e privacidade da Apple e Garantia de segurança da Apple.
Dezembro de 2019	Os documentos Manual de Segurança do iOS, Visão Geral da Segurança no macOS e Visão Geral do Chip Apple T2 Security foram combinados Atualizado para: • iOS 13.3 • iPadOS 13.3 • macOS 10.15.2 • tvOS 13.3 • watchOS 6.1.1 Controles de Privacidade, Siri e Sugestões da Siri, e Prevenção de Rastreamento Inteligente do Safari foram removidos. Consulte https://www.apple.com/br/privacy/ para obter as informações mais recentes sobre esses recursos.

Data	Resumo
Maio de 2019	Atualizado para o iOS 12.3 • Compatível com TLS 1.3 • Descrição revisada da segurança do AirDrop • Modo DFU e modo de Recuperação • Requisitos de código para conexão de acessórios
Novembro de 2018	Atualizado para o iOS 12.1 • FaceTime em Grupo
Setembro de 2018	Atualizado para o iOS 12 • Secure Enclave • Proteção da Integridade do Sistema Operacional • Express Card com reserva de energia • Modo DFU e modo de Recuperação • Acessórios do HomeKit TV Remote • Tíquetes por proximidade • Cartões de ID de estudante • Sugestões da Siri • Atalhos na Siri • App Atalhos • Gerenciamento de senha de usuário • Tempo de Uso • Certificações de Segurança e Programas
Julho de 2018	Atualizado para o iOS 11.4 • Políticas de biometria • HomeKit • Apple Pay • Bate-papo de Negócios • Mensagens no iCloud • Apple Business Manager
Dezembro de 2017	Atualizado para o iOS 11.2 • Apple Pay Cash
Outubro de 2017	Atualizado para o iOS 11.1 • Certificações de Segurança e Programas • Touch ID/Face ID • Notas Compartilhadas • Criptografia de ponta a ponta do CloudKit • Atualização de TLS • Apple Pay, Pagamento na web com o Apple Pay • Sugestões da Siri • iPad Compartilhado

Data	Resumo
Julho de 2017	Atualizado para o iOS 10.3 • Secure Enclave • Proteção de Dados de Arquivos • Keybags • Certificações de Segurança e Programas • SiriKit • HealthKit • Segurança de Rede • Bluetooth • iPad Compartilhado • Modo Perdido • Bloqueio de Ativação • Controles de Privacidade
Março de 2017	Atualizado para o iOS 10 • Segurança do Sistema • Classes de Proteção de Dados • Certificações de Segurança e Programas • HomeKit, ReplayKit, SiriKit • Apple Watch • Wi-Fi, VPN • Início de sessão único • Apple Pay, Pagamento na web com o Apple Pay • Provisão de cartões de crédito, débito e pré-pagos • Sugestões do Safari
Maio de 2016	Atualizado para o iOS 9.3 • IDs Apple Gerenciados • Autenticação de dois fatores para ID Apple • Keybags • Certificações de Segurança • Modo Perdido, Bloqueio de Ativação • Notas Seguras • Apple School Manager • iPad Compartilhado

Data	Resumo
Setembro de 2015	Atualizado para o iOS 9 • Bloqueio de ativação do Apple Watch • Políticas de código • Suporte à API do Touch ID • A Proteção de dados no A8 usa AES-XTS • Keybags para atualização de software não supervisionada • Atualizações de certificação • Modelo de confiança de app empresarial • Proteção de Dados para favoritos do Safari • Segurança de Transporte em Apps • Especificações VPN • Acesso Remoto ao iCloud para o HomeKit • Cartões de Fidelidade no Apple Pay, app da administradora do cartão no Apple Pay • Indexação local do Spotlight • Modelo de Emparelhamento do iOS • Apple Configurator 2 • Restrições

Apple
One Apple Park Way
Cupertino, CA 95014
apple.com

BR028-00205