



SUPLEMENTO DE INFORMAÇÕES

Autenticação multifatorial

Versão: 1.0

Data: fevereiro de 2017

Autor: PCI Security Standards Council

Índice

Visão geral	1
MFA e PCI DSS	1
Terminologia	1
Fatores de autenticação	2
Independência dos mecanismos de autenticação	2
Autenticação fora de banda	3
Tokens criptográficos	3
Proteção dos fatores de autenticação	5
Multietapas x multifatores	5
Uso de SMS para autenticação	6
Leis e regulamentações	6
Cenários comuns de autenticação	7
Cenário 1	7
Cenário 2	8
Cenário 3	9
Cenário 4	10

Visão geral

O objetivo da autenticação multifatorial (multi-factor authentication, MFA) é fornecer um grau mais elevado de garantia da identidade do indivíduo que tenta acessar um recurso, como localização física, dispositivo de computação, rede ou banco de dados. A MFA cria um mecanismo multicamadas que um usuário não autorizado teria de derrubar para obter acesso.

Este documento descreve os princípios aceitos pela indústria e as melhores práticas associadas à autenticação multifatorial. A orientação encontrada nele destina-se a qualquer organização que avalie, implemente ou atualize uma solução de MFA, bem como a provedores de soluções de autenticação multifatorial.

MFA e PCI DSS

O PCI DSS exige que a MFA seja implementada conforme definido no Requisito 8.3 e em seus sub-requisitos¹. A orientação sobre o objetivo desses requisitos é fornecida na coluna Orientação do padrão, que inclui *“a autenticação multifatorial exige que um indivíduo apresente, no mínimo, duas formas separadas de autenticação (conforme descrito no Requisito 8.2), antes de o acesso ser concedido”*. A orientação adicional neste documento não estende o requisito do PCI DSS além daquilo que está declarado no padrão.

Embora o Requisito 8.3 do PCI DSS não exija que as organizações validem sua implementação de MFA a todos os princípios descritos neste documento de orientação, eles podem ser incorporados em uma revisão futura do padrão. Portanto, as organizações são fortemente incentivadas a avaliar todas as implementações de MFA novas e atuais para manter a conformidade com esses princípios.

Terminologia

Além dos termos definidos no *Glossário de termos, abreviações e acrônimos do PCI DSS*, as seguintes siglas são mencionadas:

Termo	Descrição
SE	Acrônimo para Elemento seguro (Secure Element). Plataforma de hardware inviolável, capaz de hospedar aplicativos com segurança e armazenar dados confidenciais e criptográficos.
TEE	Acrônimo para Ambiente confiável de execução (Trusted Execution Environment). Software que fornece recursos de segurança como execução isolada.
TPM	Acrônimo para Módulo de plataforma confiável (Trusted Platform Module). Módulo dedicado e fisicamente isolado do restante do microcontrolador do sistema de processamento, projetado para garantir o hardware ao integrar chaves criptográficas nos dispositivos. Ele oferece instalações para a geração segura de chaves criptográficas e limitação de seu uso.

¹ Refere-se ao PCI DSS v3.2

Fatores de autenticação

O processo de autenticação geral para MFA requer pelo menos dois dos três métodos de autenticação descritos no Requisito 8.2 do PCI DSS:

- a) **Algo que você sabe**, como uma senha ou frase de senha. Este método envolve a verificação de informações que um usuário fornece, como uma senha/frase de senha, PIN ou as respostas para perguntas secretas (resposta a desafio).
- b) **Algo que você tem**, como um dispositivo de token ou um smartcard. Este método envolve a verificação de um item específico que um usuário tem em sua posse, como um token de segurança física ou lógico, um token de senha única (one-time password, OTP), um alarme remoto (keyfob), um cartão de acesso de funcionário ou um cartão SIM de telefone. Para autenticação móvel, um smartphone frequentemente fornece o fator de posse em conjunto com um aplicativo de OTP ou um material criptográfico (ou seja, certificado ou uma chave) que se encontra no dispositivo.
- c) **Algo que você é**, como a biometria. Este método envolve a verificação de características inerentes ao indivíduo, como a realizada por meio de exames de retina, da leitura da íris, da impressão digital ou da veia dos dedos, do reconhecimento facial ou de voz, da geometria da mão e até da geometria do lóbulo da orelha.

Outros tipos de informações, como geolocalização e hora, podem ser adicionalmente incluídos no processo de autenticação; no entanto, pelo menos dois dos três fatores identificados acima sempre devem ser usados. Por exemplo, dados de geolocalização e de hora podem ser usados para restringir o acesso remoto à rede de uma entidade de acordo com o cronograma de trabalho de um indivíduo. Embora o uso desses critérios adicionais possa reduzir ainda mais o risco de sequestro da conta ou de atividade mal-intencionado, o método de acesso remoto ainda precisa exigir autenticação através de pelo menos dois dos seguintes fatores: algo que você sabe, algo que você tem e algo que você é.

Independência dos mecanismos de autenticação

Os mecanismos de autenticação usados para a MFA devem ser independentes uns dos outros, de tal forma que o acesso a um fator não conceda acesso a nenhum outro, e o comprometimento de qualquer fator não afete a integridade ou a confidencialidade de qualquer outro fator. Por exemplo, se o mesmo conjunto de credenciais (por exemplo, nome de usuário/senha) for usado como um fator de autenticação e também para obter acesso a uma conta de e-mail onde um fator secundário (por exemplo, senha única) é enviado, esses fatores não são independentes. Da mesma forma, um certificado de software armazenado em um laptop (algo que você tem) que é protegido pelo mesmo conjunto de credenciais usadas para efetuar login no laptop (algo que você sabe) pode não oferecer independência.

O problema com credenciais de autenticação incorporadas no dispositivo é uma possível perda de independência entre fatores — ou seja, a posse física do dispositivo pode conceder acesso a um segredo (algo que você sabe), bem como um token (algo que você tem), como o próprio dispositivo, ou um certificado ou token de software armazenado ou gerado no dispositivo. Dessa forma, a independência dos fatores de autenticação é frequentemente realizada através da separação física dos fatores; entretanto, ambientes de execução altamente robustos e isolados (como um Ambiente confiável de execução [Trusted Execution Environment, TEE], Elemento seguro [Secure Element, SE] e Módulo de plataforma confiável [Trusted Platform Module, TPM]) também podem ser capazes de atender aos requisitos de independência.

Autenticação fora de banda

Fora de banda (Out-of-band, OOB) se refere a processos de autenticação onde os métodos de autenticação são transmitidos através de diferentes redes ou canais.

Onde os fatores de autenticação são transmitidos através de um único dispositivo/canal — por exemplo, inserir credenciais por meio de um dispositivo que também recebe, armazena ou gera um token de software — um usuário mal-intencionado que estabeleceu o controle do dispositivo tem a capacidade de capturar ambos os fatores de autenticação.

A transmissão de uma senha única (one-time password, OTP) para um smartphone foi tradicionalmente considerada um método eficaz fora da banda. No entanto, se o mesmo telefone for usado para enviar a OTP — por exemplo, por meio de um navegador da Web — a eficácia da OTP como fator secundário é efetivamente anulada.

A transferência fora de banda dos mecanismos de autenticação é um controle adicional que pode aumentar o nível de garantia para a autenticação multifatorial. Em vez da capacidade de usar comunicação fora da banda, o processo de autenticação deve estabelecer controles para garantir que o indivíduo que tente usar a autenticação seja, na verdade, o usuário legítimo em posse do fator de autenticação.

Tokens criptográficos

Tokens criptográficos podem ser incorporados em um dispositivo ou armazenados em mídias separadas e removíveis. A seguinte orientação é baseada na NIST SP800-164² e na NIST SP800-157³, e considera alguns fatores de forma comuns que são frequentemente usados com dispositivos de computação móvel.

² NIST Special Publication 800-164 (Draft), *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)*. URL: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf (acessado em 07 de novembro de 2016).

³ NIST Special Publication 800-157 *Guidelines for Derived PIV Credentials*. URL:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf> (acessado em 07 de novembro de 2016)

Tokens criptográficos de hardware removíveis (não incorporados)

Nesta categoria de dispositivos, uma chave privada reside em um módulo criptográfico de hardware (ou token de segurança física), fisicamente separado do dispositivo de computação móvel. O acesso ao dispositivo de computação móvel ou criptograma armazenado no token não concede acesso ao outro, mantendo, assim, a independência dos fatores de autenticação.

Cada um dos fatores de forma descritos abaixo suporta um elemento seguro (secure element, SE), um componente criptográfico inviolável que fornece segurança e confidencialidade em dispositivos móveis.

- **Cartão SD com módulo criptográfico** – Um formato de cartão de memória não volátil para uso em dispositivos portáteis, como telefones celulares e tablets.
- **UICC removível com módulo criptográfico** – A configuração do Cartão de circuito integrado universal (Universal Integrated Circuit Card, UICC) se baseia na especificação do cartão GlobalPlatform v2.2.1 [GP-SPEC] e fornece armazenamento e processamento, bem como recursos de entrada/saída.
- **Token USB com módulo criptográfico** – Um token Universal Serial Bus (USB) é um dispositivo que se conecta à porta USB em várias plataformas de computação de TI, incluindo dispositivos móveis e computadores pessoais. Os tokens USB normalmente incluem armazenamento incorporado e também podem incluir recursos de processamento criptográfico — por exemplo, mecanismos criptográficos para verificar a identidade dos usuários. Implementações de token USB que contêm um elemento de segurança integrado (um cartão de circuito integrado ou ICC [integrated circuit card]) são adequadas para uso no processo de autenticação.

Tokens criptográficos incorporados

Uma credencial de autenticação e sua chave privada associada podem ser usadas em módulos criptográficos que são incorporados em dispositivos móveis⁴. Esses módulos podem estar na forma de um módulo criptográfico de hardware, que é um componente do dispositivo móvel, ou na forma de um módulo criptográfico de software, que é executado no dispositivo.

Os módulos criptográficos de hardware são preferidos em relação ao software devido à sua imutabilidade, superfícies de ataque menores e comportamento mais confiável; sendo assim, eles podem fornecer um grau mais elevado de confiabilidade para que eles executem suas funções confiáveis.

Proteger e usar a credencial de autenticação e a chave privada correspondente no software possivelmente poderá aumentar o risco de que a chave seja roubada ou comprometida.

⁴ Draft NIST Interagency Report 7981, Mobile, PIV, and Authentication. URL: http://csrc.nist.gov/publications/drafts/nistir-7981/nistir7981_draft.pdf (acessado em 07 de novembro de 2016)

Proteção dos fatores de autenticação

Para prevenir o uso indevido, a integridade dos mecanismos de autenticação e a confidencialidade dos dados de autenticação precisam ser protegidas. Os controles definidos no Requisito 8 do PCI DSS fornecem garantia de que os dados de autenticação estão protegidos contra acesso e uso não autorizados. Por exemplo:

- Senhas e outros dados referentes a “algo que você sabe” devem ser difíceis de adivinhar ou resistentes a ataques de força bruta, e devem ser protegidos contra divulgação para partes não autorizadas.
- Dados biométricos e outros dados referentes a “algo que você é” devem ser protegidos contra replicação não autorizada ou uso por terceiros com acesso ao dispositivo no qual os dados estão presentes.
- Cartões inteligentes, certificados de software e outros dados referentes a “algo que você tem” não devem ser compartilhados e devem ser protegidos contra replicação ou posse por partes não autorizadas.

Quando quaisquer elementos de autenticação dependerem de um dispositivo de consumo multiuso — por exemplo, telefones celulares e tablets — controles também devem estar em vigor para mitigar o risco do dispositivo sendo comprometido.

Multietapas x multifatores

O PCI DSS exige que todos os fatores na autenticação multifatorial sejam verificados antes do mecanismo de autenticação conceder o acesso solicitado. Além disso, nenhum conhecimento prévio quanto ao sucesso ou à falha de qualquer fator deve ser fornecido ao indivíduo até que todos os fatores tenham sido apresentados. Se um usuário não autorizado puder deduzir a validade de qualquer fator de autenticação individual, o processo geral de autenticação se torna uma coleção de etapas subsequentes de autenticação de fator único, mesmo que um fator diferente seja usado para cada etapa. Por exemplo, se um indivíduo enviar credenciais (por exemplo, nome de usuário/senha) que, uma vez validadas com sucesso, levem à apresentação do segundo fator para validação (por exemplo, biometria), isso seria considerado uma autenticação “multietapas”.

É possível que a autenticação multietapas e multifatorial estejam presentes em um ambiente. Por exemplo, um indivíduo pode executar uma etapa de autenticação para efetuar login em um computador antes de iniciar um processo de MFA separado para obter acesso ao CDE. Um exemplo desse cenário seria um usuário remoto que inseriu credenciais para efetuar login no seu laptop corporativo. O usuário pode, então, iniciar uma conexão VPN à rede da empresa usando uma combinação de credenciais e um smartcard físico ou token de hardware.

Uso de SMS para autenticação

O PCI DSS depende das normas da indústria, como NIST, ISO e ANSI, que abrangem todos os setores, não apenas o de pagamentos. Embora a NIST atualmente permita o uso de SMS, a organização informou que a autenticação fora de banda usando SMS ou voz se tornou obsoleta e pode ser removida das versões futuras de sua publicação⁵.

Leis e regulamentações

As organizações precisam estar cientes das leis locais e regionais que também podem definir requisitos para o uso de MFA. Por exemplo, pode haver requisitos adicionais com relação à autenticação do consumidor usada para iniciar pagamentos ou realizar transações de alto risco, como a Diretriz da União Europeia sobre Serviços de Pagamento (European Union Directive on Payment Services, PSD2) e o Manual de Exame de TI do Conselho Federal de Exame das Instituições Financeiras (Federal Financial Institutions Examination Council, FFIEC). Além disso, algumas leis ou regulamentações podem ter requisitos de MFA mais rigorosos do que aqueles exigidos pelo PCI DSS.

O PCI SSC incentiva todas as organizações a estarem cientes do impacto potencial que as leis e regulamentações locais podem ter sobre suas implementações de MFA. Os requisitos do PCI DSS para autenticação multifatorial não substituem as leis locais ou regionais, regulamentações governamentais ou outros requisitos legais.

⁵ DRAFT NIST Special Publication 800-63B Digital Authentication Guideline. URL: <https://pages.nist.gov/800-63-3/sp800-63b.html> (acessado em 07 de novembro de 2016)

Cenários comuns de autenticação

Esta seção explora alguns cenários comuns de autenticação e considerações para autenticação multifatorial.

Cenário 1

Um indivíduo usa um conjunto de credenciais (senha A) para efetuar login em um dispositivo e também para acessar um token de software armazenado no dispositivo. O indivíduo então estabelece uma conexão com o CDE/a rede corporativa, fornecendo um conjunto diferente de credenciais (senha B) e a OTP gerada pelo token do software como autenticação.

O sistema de autenticação concede o acesso solicitado se ambos os fatores fornecidos forem válidos:

- Algo que você sabe – Senha B
- Algo que você tem – Token de software

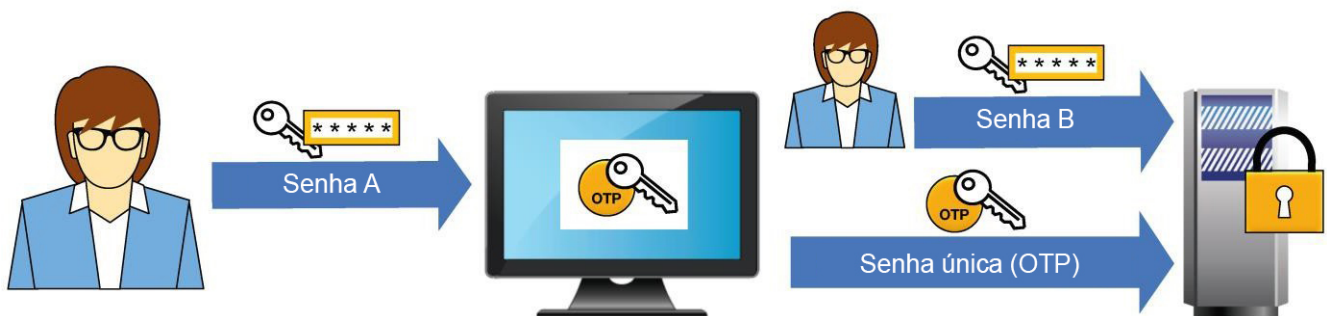


Figura 1: Cenário 1

Para garantir que a independência dos fatores de autenticação seja mantida, este cenário exige que o token do software ("algo que você tem") esteja incorporado ao dispositivo físico de tal forma que ele não possa ser copiado ou usado em nenhum outro dispositivo.

Além disso, a segurança física sobre o dispositivo se torna um controle de segurança exigido como prova de posse do dispositivo. Caso contrário, se o acesso ao token do software for apenas um reflexo da capacidade de efetuar login no dispositivo (local ou remotamente), o processo geral de autenticação é um uso duplo de "algo que você sabe".

Cenário 2

Neste cenário, o indivíduo usa um conjunto de credenciais (por exemplo, nome de usuário/senha ou biometria) para efetuar login no dispositivo; essas credenciais também fornecem acesso a um token de software armazenado no dispositivo. Para iniciar uma conexão com o CDE/a rede corporativa, o usuário inicia uma janela do navegador que preenche previamente um conjunto diferente de credenciais (por exemplo, armazenadas em cache no dispositivo ou usando o gerenciador de senhas) juntamente com o token do software.



Figura 2: Cenário 2

Este cenário não fornece independência entre fatores de autenticação, pois um único conjunto de credenciais (senha A) fornece acesso a ambos os fatores (senha B e token de software).

Cenário 3

Neste cenário, o indivíduo usa um conjunto de credenciais (por exemplo, nome de usuário/senha) para efetuar login no computador. A conexão com o CDE/a rede corporativa requer o conjunto inicial de credenciais e uma OTP gerada por um token de software que reside em um dispositivo móvel.

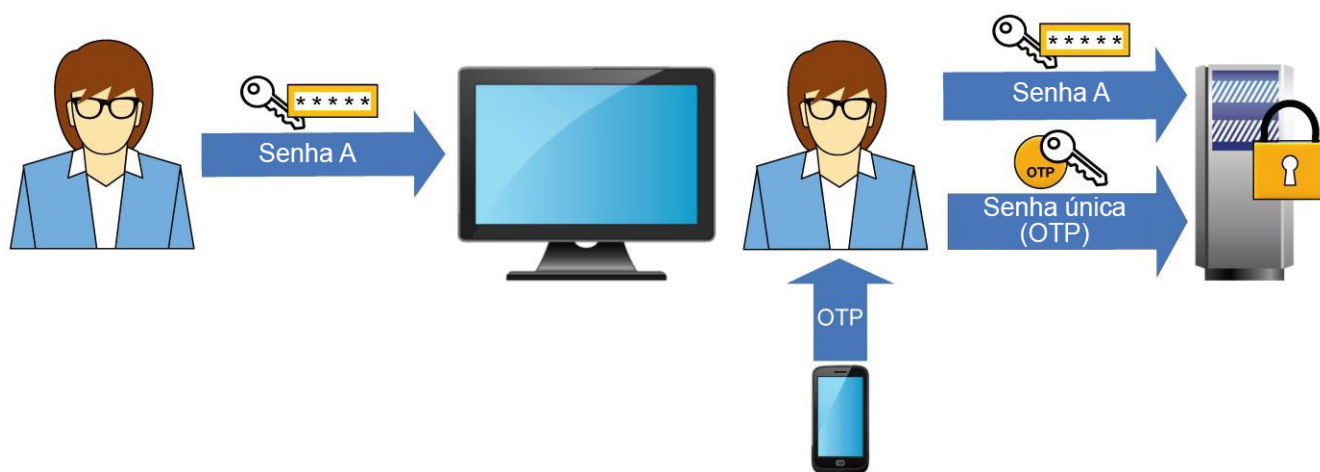


Figura 3: Cenário 3

Ainda que o indivíduo use a mesma senha (algo que você sabe) para fazer autenticação tanto no laptop quanto no CDE/na rede corporativa, o token de software que reside em um celular fornece um segundo fator (algo que você tem) que mantém a independência entre os mecanismos de autenticação.

Se o dispositivo móvel também for usado para iniciar a conexão com o CDE/a rede corporativa, controles de segurança adicionais seriam necessários para demonstrar a independência dos mecanismos de autenticação.

Cenário 4

Neste cenário, o indivíduo usa a autenticação multifatorial (por exemplo, senha e biometria) para efetuar login em um smartphone ou laptop. Para estabelecer uma conexão sem console com o CDE/a rede corporativa, o indivíduo então fornece um único fator de autenticação (por exemplo, uma senha diferente, certificado digital ou resposta assinada a desafio).



Figura 4: Cenário 4

Neste cenário, o dispositivo (smartphone ou laptop) deve ser protegido e controlado para garantir que a autenticação multifatorial seja devidamente implementada e sempre executada antes de iniciar a conexão com o CDE/a rede corporativa. Isso inclui a garantia de que os usuários não possam alterar ou desativar as configurações de segurança — por exemplo, desativar ou ignorar a autenticação multifatorial — e que a independência dos fatores de autenticação seja mantida.

Além disso, controles adicionais podem ser necessários para impedir que uma parte não autorizada obtenha o uso construtivo da “confiança” estabelecida entre o dispositivo e o CDE/a rede corporativa. Um exemplo de uso construtivo seria um usuário mal-intencionado executar um processo no dispositivo que lhe permita interagir com o CDE/a rede corporativa sem ter conhecimento da senha ou da biometria usada pelo usuário legítimo.

Quando o usuário gerencia seu próprio dispositivo, por exemplo, em um ambiente BYOD (bring your own device, traga seu próprio dispositivo), o dispositivo gerenciado pelo usuário deve manter um ambiente de execução robusto e isolado (como TEE, SE ou TPM) que não possa ser afetado negativamente ou burlado pelo usuário. Caso contrário, a empresa não teria garantia de que a MFA está devidamente implementada e aplicada no dispositivo.