Indústria de cartões de pagamento (PCI)
Requisitos de segurança de POI para PTS

Dúvidas técnicas frequentes para uso com a versão 6

Setembro de 2020

Sumário

TERMO DE RECONHECIMENTO: A versão em inglês deste documento, conforme disponibilizada no site da PCI SSC, para todos os efeitos, é considerada a versão oficial destes documentos e, na medida em que houver ambiguidades ou inconsistências entre a redação do presente texto e do texto em inglês,a versão em inglês disponibilizada no local mencionado prevalecerá

Avaliação de dispositivo de POI: dúvidas frequentes

Essas dúvidas técnicas frequentes respondem as dúvidas referentes à aplicação dos requisitos de segurança para dispositivos de POI físicos e lógicos do PCI (Payment Card Industry), conforme abordado no manual *Requisitos de segurança de dispositivos de ponto de interação para PTS do PCI*. Essas dúvidas frequentes trazem mais esclarecimentos oportunos para aplicação dos requisitos de segurança. As dúvidas frequentes fazem parte desses requisitos e devem ser devidamente levadas em consideração durante o processo de avaliação.

Atualizações: as novas ou as dúvidas modificadas para maior clareza estão em **vermelho.**

Dúvidas gerais

Q 1 **Se um aplicativo para dispositivos incluir avisos para dados não vinculados a um PIN e o dispositivo aplicar controles compatíveis com o Requisito B15 do PCI, ele poderá ser especificado como dispositivo de avisos controlado pelo adquirente, sendo o aplicativo excluído dos identificadores do dispositivo?**

A *Sim, se o aplicativo não afetar nenhum dos recursos necessários para cumprimento os requisitos do PCI. Não é preciso que os códigos internos do dispositivo, que não oferecem e não afetem a segurança, sejam representados pelos identificados do dispositivo aprovado.*

Q 2 **Supõe-se que a superfície da área incluída no invólucro esteja visível sem necessidade de desmontar o dispositivo?**

A *Não. Os componentes envasados do dispositivo, e críticos no que diz respeito à segurança, estão dentro do invólucro do dispositivo e, portanto, é improvável que possam ser vistos sem a abertura do invólucro.*

Q 3 **É admissível que um dispositivo contenha componentes e complementos removíveis disponibilizados pelo fornecedor?**

A *Todos os componentes removíveis (escudos de privacidade, bases de encaixe, módulos de interface etc.) devem ser avaliados por um laboratório aprovado para determinar que não apresentam nenhum risco a mais para a segurança. No entanto, os componentes individuais não receberão aprovação separada.*

Q 4 **Fevereiro (atualização) de 2014: o uso de capas protetoras de teclado afeta o status de aprovação do dispositivo?**

A *Sim. Em geral, as capas não são aceitas no programa de aprovação de dispositivos devido à possibilidade de exploração do teclado ou ocultação de indícios de adulteração. As capas podem ser usadas de forma que não cubram nenhuma parte da área de introdução do PIN. Por exemplo, em dispositivos touchscreen, onde a tela sensível ao toque é usada para captura de assinatura e introdução PIN, as capas podem ser usadas para proteger a área de assinatura, impedindo o desgaste excessivo da mesma. Neste exemplo, somente a área usada para a captura da assinatura pode ser protegida. O material utilizado deve ser transparente, não basta ser translúcido, para não obstruir a área de introdução da chave, qualquer que seja o ângulo de visão.*

Q 5 **Dezembro (atualização) de 2017: o uso de capas protetoras afeta o status de aprovação do dispositivo?**

A *Sim. Em geral, as capas não são aceitas no programa de aprovação de dispositivos devido à possibilidade de ocultação de indícios de adulteração. As capas podem ser usadas de forma que não cubram nenhuma parte da área de MSR ou ICCR. Por exemplo, não é permitido que as capas usadas para proteção na ocorrência de queda do dispositivo móvel ou a inclusão de cordões de transporte cubram o ICCR ou o MSR. As interfaces devem estar claras e visíveis para o consumidor, de modo que os fios ou os indícios de adulteração não fiquem ocultos. O material utilizado deve ser transparente, não basta ser translúcido. As capas para a área de introdução do PIN devem estar em conformidade com o que foi esclarecido nas dúvidas frequentes anteriores. Se o POI tiver sido aprovado para uso com capa protetora, a política de segurança deverá disponibilizar uma imagem da capa protetora aprovada, devidamente instalada e testada pelo laboratório.*

Q 6 **Maio (atualização) de 2018: a introdução do código de autenticação (por exemplo, senha) usado para liquidação/balanço em caixas eletrônicos exige o uso de EPP seguro, ou pode usar um mecanismo alternativo como, por exemplo, o teclado na parte de trás do caixa eletrônico?**

A *Não é necessário que o código de autenticação usado para liquidação/balanço no caixa eletrônico seja inserido via EPP, e é permitido usar o teclado instalado na parte traseira do caixa eletrônico. No entanto, em circunstância alguma é permitido utilizar as chaves usadas para criptografia dos PINs dos titulares de cartão em conexão com alguma transação financeira para criptografar esse código de autenticação. As chaves de criptografia do PIN utilizadas para proteção dos PINs dos titulares de cartão não devem ser utilizadas para proteger o código de autenticação da liquidação, seja esse valor inserido na parte traseira ou via PPE. Seria necessário utilizar uma chave de dados separada para qualquer tipo de proteção do código de autenticação da liquidação.*

Lembre-se de que os códigos de autenticação inseridos para colocar o EPP em estado confidencial, como aqueles usados para permitir o carregamento manual de chaves, devem ser inseridos por meio de uma interface segura, ou seja, via EPP.

Q 7 **Alguns dispositivos são enviados com firmware que podem ser convertidos em uma versão compatível, mas que não são compatíveis da forma como são enviados. Quando isso é aceito?**

A *Isso só é aceito quando a conversão não pode ser revertida. Somente é permitido converter um dispositivo em uma versão que esteja em conformidade. Não deve ser capaz de converter uma versão que esteja em conformidade em uma versão não conforme. A conversão deve ser realizada no carregamento inicial das chaves secretas da entidade adquirente. A transformação deve resultar na zeroização de todas as chaves secretas da entidade adquirente que existiam anteriormente. É necessário que a versão compatível do firmware possa ser claramente diferenciada da versão não compatível. Não basta anexar um sufixo (um ou mais caracteres) a uma versão atual do firmware. Em vez disso, a conversão deve gerar um número de versão de ordem elevada, que possa ser claramente diferenciada pelos compradores desses dispositivos. Somente a versão que estiver em conformidade deve ser aprovada e relacionada.*

Q 8 **Alguns ataques são tecnicamente simples, pois não exigem uma identificação extensa, como a detecção de comunicação em interfaces padrão como USB/Ethernet entre dispositivos. Então, como o cálculo do valor do ataque deve ser realizado?**

A *Para ataques tecnicamente simples que não exigem ampla identificação, por exemplo a detecção de comunicação em interfaces padrão como USB/Ethernet entre dispositivos, todos os fatores de custo além do tempo e da experiência devem ser desconsiderados. Além disso, o tempo de ataque e a experiência somente devem ser considerados para identificação da configuração geral do dispositivo e da propriedade a ser atacada (por exemplo, o tipo de interface).*

Q 9 **UPT Versão 1 ficou indisponível para novas avaliações após abril de 2011. Sob quais condições é permitido um delta para um UPT aprovado com a Versão 1?**

A *Um fornecedor com uma aprovação geral do UPT com a versão 1 pode receber deltas no dispositivo em questão para alterações sofridas pelos componentes de OEM utilizados, incluindo a substituição de componentes de OEM por um modelo diferente, por exemplo, um ICCR de OEM aprovado em separado, produzido por um fornecedor, é substituído no UPT de fator de forma final por outro modelo, mesmo sendo de um fornecedor diferente. Isso se aplica enquanto o fornecedor continuar tendo controle sobre a montagem final e a fabricação do UPT.*

As alterações que ocorrem no próprio fator de forma final (por exemplo, caixa), devido à complexidade da integração, devem ser submetidas a testes como uma nova avaliação em comparação com uma versão dos requisitos que não tenha sido retirada do uso para novas avaliações.

No entanto, de maneira geral, todos os requisitos de segurança afetados serão avaliados, inclusive aqueles que antes não se aplicavam, por exemplo, se o novo invólucro introduzir outros dispositivos na interface do titular do cartão não presentes na avaliação original.

Q 10 **Faz alguma diferença se o fornecedor dos componentes de OEM for também o fornecedor que receber a aprovação geral do UPT, em comparação com um cenário em que o fornecedor de OEM vende seus componentes/módulo de entrada para outros fornecedores, tais como os fornecedores de quiosque ou bombas de combustível automáticas (AFD) que buscam a aprovação geral do UPT?**

A *Não. Os componentes de OEM podem ser fabricados por qualquer fornecedor, mesmo que esse fornecedor seja diferente do fornecedor do UPT. No entanto, se os fornecedores forem diferentes, esses componentes já devem ter sido aprovados pela PCI ou o fornecedor de OEM deve conceder permissão ao fornecedor do UPT para que esses componentes sejam avaliados como parte da aprovação geral do UPT.*

Q 11 **Junho de 2012: durante a avaliação, determina-se que um novo dispositivo inclui a pilha de IP idêntica, previamente avaliada e aprovada sob a versão mais recente do módulo Requisitos para protocolos abertos. É obrigatório refazer todos os testes de protocolos abertos?**

A *Se o fornecedor puder disponibilizar provas que corroboram a afirmação de que a pilha de IP é 100% idêntica, inclusive a mesma versão de vários componentes e protocolos IP, serviços IP e protocolos de segurança IP idênticos, não haverá necessidade de realizar novos testes. O relatório deve documentar como foi realizada a confirmação de que a pilha de IP é idêntica e deve incluir as informações da pilha de IP, entre elas a versão do componente, os protocolos IP, os serviços IP e os protocolos de segurança IP compatíveis.*

Q 12 **Julho de 2014: os dispositivos POI podem ser aprovados com compatibilidade com protocolos abertos. Os fornecedores oferecem uma política de segurança prescrita pela PCI e outras orientações de segurança para a implementação adequada dos protocolos abertos que fazem parte da aprovação. Se a entidade que estiver implementando o dispositivo fizer alterações que não estiverem de acordo com as orientações de segurança, necessárias para implantar o dispositivo em conformidade com o módulo de protocolos abertos, esse fato afetará a aprovação? Por exemplo: adicionar outros serviços ou protocolos que não estavam presentes na orientação ou usar ou substituir, de outra forma, a pilha de IP por uma inserida no aplicativo.**

A *Sim, esse fato invalidaria o status da aprovação do dispositivo para todas as implementações que promovam tais alterações. Qualquer alteração desse tipo deve resultar na obrigatoriedade de que o dispositivo seja submetido com êxito a uma avaliação delta para manter a aprovação.*

O módulo de protocolos abertos destina-se a garantir que os protocolos e serviços abertos em dispositivos de POI não tenham vulnerabilidades que possam ser exploradas de forma remota e permitam o acesso a dados ou recursos confidenciais no dispositivo. Nessa situação, não importa com que tipo de rede (pública ou privada) o dispositivo é usado.

O fornecedor define quais protocolos e serviços são aceitos pelo dispositivo e oferece orientações para uso. Os protocolos e serviços são avaliados pelo laboratório. Adicionar ou ativar outros serviços e protocolos ou não seguir as orientações de segurança emitidas após a avaliação invalidaria o status de aprovação do dispositivo para a implementação em questão.

Q 13 **Janeiro de 2015: há uma série de dúvidas frequentes sobre o uso de tecnologias sem fio, tais como Bluetooth e Wi-Fi. Qual é o propósito dessas dúvidas frequentes, e além disso, a PCI tem algum requisito específico para outros tipos de tecnologias de comunicação?**

A *O propósito das FAQs sobre todas as comunicações sem fio para os dispositivos de POI é garantir que as interfaces do POI estejam protegidas, de forma que:*

- *Não seja fácil interceptar os dados dos cartões.*
- *Não seja fácil interceptar para ataque (como o MITM) ou usar as interfaces de comando com o terminal como vetores de ataque dentro do dispositivo.*
- *O comprometimento da interface não leve a, permita ou facilite o maior comprometimento dos ativos de segurança do POI.*

A PCI não estipula ou exige o uso de qualquer tecnologia de comunicação específica, no entanto, toda a implementação deve atender aos requisitos acima por intermédio de algum aspecto das camadas físicas ou lógicas de comunicação. A comunicação física ou direta com fio muitas vezes consegue isso pela natureza de sua interface física. As comunicações sem fio não têm essa facilidade e, portanto, devem utilizar-se da segurança nas camadas do link ou aplicativo, pelo uso de um protocolo de segurança, para estabelecer um caminho confiável para todas as comunicações via link sem fio. Esse protocolo de segurança deve ter sido testado e aprovado sob o módulo de protocolos abertos da avaliação da PTS da PCI no que diz respeito ao dispositivo em questão. Além disso, entre os exemplos de implementações do protocolo de segurança aceitáveis estão o WPA2 (implementado na camada do link) ou túneis de VPN criptografados (implementados na camada do aplicativo).

Q 14 Dezembro (atualização) de 2016: os dispositivos de PTS podem ser usados como transmissores de sinalização (iBeacon ou sinalização BLE)?

A *Os sinalizadores para qualquer versão de BLE (por exemplo, 4.0, 4.1) são permitidos, desde que as seguintes condições existam e sejam validadas por um laboratório aprovado por PTS:*

- *O sinalizador está previsto como interface de dispositivo no relatório de PTS do POI.*
- *O provisionamento pelo ar (OTA) não é permitido em nenhum momento. O provisionamento e a atualização dos sinalizadores devem ser coerentes com os atuais padrões de PTS. (ou seja, seções J, B4 ou B4.1)*
- *Deve ser mencionado na política de segurança.*
- *Os sinalizadores somente transmitem. O laboratório deve confirmar que não é possível utilizar a comunicação de BLE para responder a nenhuma solicitação externa, nem para conectar, parear ou oferecer, de qualquer outra forma, comunicação bidirecional a qualquer outro dispositivo.*
- *O fornecedor disponibiliza documentação sobre o uso seguro e o provisionamento do sinalizador e essa documentação indica claramente que o sinalizador é usado somente para transmissão, e que o provisionamento OTA não é permitido.*
- *O fornecedor documentará a finalidade do uso da recurso de sinalização,ou seja, seu uso pretendido. A documentação deve informar quais dados são transmitidos e garantir que nenhum dado confidencial possa ser transmitido.*
- *O dispositivo de PTS não pode, jamais, receber transmissões do sinalizador.*

Q 15 Em relação a quais requisitos os leitores de cartões seguros devem ser validados?

A *Os leitores de cartões seguros devem cumprir, conforme aplicável, os requisitos do ICCR e/ou MSR definidos no Apêndice B dos requisitos de segurança do POI para PTS da PCI e todos os outros requisitos relativos à proteção dos dados de conta, conforme indicado no Apêndice B. Além disso, a aplicabilidade de todos os requisitos de proteção de dados de conta não definidos deve ser considerada. Na maioria dos casos, eles não serão aplicáveis e não exigirão nenhuma avaliação além dessa determinação.*

Se o dispositivo for capaz de comunicar-se por meio de uma rede IP ou usar um protocolo de domínio público (por exemplo, Wi-Fi ou Bluetooth, entre outros), os requisitos especificados no módulo de protocolos abertos também deverão ser cumpridos. Outros requisitos, como B1, autotestes e B7, números aleatórios podem ser aplicados dependendo do recurso do dispositivo. Em todos os casos, se um requisito de segurança for afetado, o dispositivo deverá ser avaliado em relação a ele.

Q 16 Fevereiro de 2014: pode-se usar um SCR (leitor de cartão seguro) para aceitação de PIN offline?

A *Os SCRs ou outros dispositivos de POI que incluam um ICCR ou um leitor híbrido devem ter "Offline" indicado sob o suporte do PIN para serem usados para aceitação de PIN offline.*

Q 17 Fevereiro de 2014: se um SCR processa PINs, ou seja, aceita a autenticação do PIN offline por meio de um componente de ICCR, ou formata e criptografa um PIN block para envio online diretamente para o host, ele deve ser avaliado com um dispositivo específico de entrada do PIN?

A *Sim, deve ser validado em conjunto com um dispositivo específico de entrada do PIN,por exemplo, PED ou EPP,para validar a segurança da interação, incluindo o estabelecimento da relação entre as chaves. O dispositivo de entrada do PIN deve ser previamente aprovado ou receber aprovação simultânea com o SCR no mesmo ou em uma avaliação laboratorial simultânea separada.*

Q 18 Junho de 2012: os requisitos de aprovação dos dispositivos SCR ou que não aceitam PIN não incluem DTR A1 do PTS da PCI, que exigem mecanismos ativos de resposta em caso de adulteração. É possível atender aos requisitos de segurança física de um dispositivo SCR ou que não aceita PIN usando somente características de resistência à adulteração e de indícios de adulteração, se for possível mostrar que o custo do ataque ultrapassa os níveis mínimos necessários para cada um dos requisitos de teste de segurança física?

A *Não, é obrigatório que todos os dispositivos implementem mecanismos ativos para detecção de adulteração, de forma a atender aos requisitos de segurança física do PTS da PCI. Os dispositivos SCR e que não aceitam PIN devem ter mecanismos de detecção de adulteração ativos de forma permanente, para que monitorem a ocorrência de invasões e reajam a esses eventos, apagando imediatamente as informações confidenciais de dentro do dispositivo, tornando-o inoperante.*

Os dispositivos não conseguirão atender aos requisitos de POI para PTS se não tiverem um mecanismo de reação contra adulteração ativo para zeroizar chaves secretas e privadas durante os ataques de penetração, independentemente de quais módulos do padrão de POI para PTS o dispositivo foi projetado para cumprir. A penetração do dispositivo deve fazer com que todas as chaves secretas e privadas sejam apagadas de forma imediata e automática, de modo que se torne inviável recuperar o material de chaveamento. Isso se aplica aos dispositivos, mesmo que não aceitem PINs do cliente ou que não sejam projetados para proteger os PINs do cliente. As chaves criptográficas secretas ou privadas, que nunca são usadas para criptografar ou descriptografar dados, ou que não são usadas para autenticação, não estão incluídas nesse requisito, pois essas chaves jamais seriam envolvidas na proteção dos PINs de clientes ou dos dados de cartões de clientes.

Q 19 Julho de 2013: os dispositivos com ICCR somente podem ser aprovados para recebimento de PIN online se aceitarem qualquer método de entrada do PIN offline (ou seja, se o dispositivo aceitar PIN criptografado e/ou em texto simples)?

A *Os dispositivos com ICCR que não são avaliados em relação aos requisitos de ICCR para uso offline não podem ter a versão aprovada do suporte para firmware para aceitação de PINs offline. Além disso, os dispositivos compatíveis com PIN online devem ser avaliados quanto ao PIN online, ou a aceitação do PIN online na versão aprovada do firmware deve ser desativada.*

Q 20 Junho de 2012: se o dispositivo for compatível com várias interfaces com recursos de IP, será necessário que os testes sejam realizados em todas as interfaces com recursos de IP pelo laboratório durante a avaliação?

A *Se o dispositivo aceitar várias interfaces com recursos de IP e a pilha de IP (incluindo todos os protocolos IP, serviços IP e protocolos de segurança IP) for idêntica para todas as interfaces, somente será necessário realizar testes em uma das interfaces com recursos de IP.*

Q 21 **Dezembro de 2013: os requisitos de PTS da PCI não impõem nenhum fator de forma específico para os dispositivos. Existe alguma restrição aos tipos de sistemas ou dispositivos que podem ser aprovados no âmbito do programa de PTS da PCI?**

A *O PTS da PCI não determina os fatores de forma dos dispositivos para permitir que os fornecedores desenvolvam soluções inovadoras para atender às necessidades do mercado. No entanto, somente os dispositivos projetados para interação direta com os clientes podem receber a aprovação em relação ao PTS. Os subcomponentes, tais como os microprocessadores, as "latas" do leitor de cartão magnético, os dispositivos que aceitam ICC e outros, que são projetados para integração em outro dispositivo que impediria a visão direta e a interação do sistema aprovado pelo titular do cartão, não podem ser aprovados sob os requisitos do PTS da PCI.*

Q 22 **Julho (atualização) de 2014: as interfaces dos teclados numéricos de PDV do PIN podem ser aprovados para operação offline quando validados para conformidade com um leitor de cartão externo aprovado em relação ao PTS (neste caso, um PED aprovado com relação ao PTS atuando como leitor de cartão externo ou leitor de cartão seguro). Quais detalhes devem ser especificados para tal configuração?**

A *A especificação do teclado numérico de PDV do PIN deve detalhar com qual PED ou SCR específico, aprovado em relação ao PTS, o teclado numérico do PIN é capaz de executar a validação do PIN offline. O hiperlink para o PED ou SCR aprovado será incluído como componente aprovado. Sempre que houver vários dispositivos com os quais for possível operar, será necessário enumerar todos eles. O uso do dispositivo com um leitor não especificado invalida a aprovação offline.*

Q 23 **Outubro (atualização) de 2018: com a descoberta do ataque de Padding Oracle on Downgraded Legacy Encryption (POODLE), o SSL ainda é um protocolo permitido?**

A *Ainda é possível manter a compatibilidade com o protocolo SSL, no entanto o fornecedor deve documentar (para dispositivos com versão 4 e superior, incluindo a política de segurança publicada no site da PCI) que ele é inerentemente fraco e deve ser removido, salvo se obrigatório, de forma provisória, para facilitar a interoperabilidade como parte do plano de migração. Para SSL 3 ou versões mais antigas do TLS, se compatível, todos os conjuntos de cifras que fizerem uso de DES ou RC4 devem ser removidos. Ambos os objetivos podem ser alcançados modificando-se o código-fonte para remover a compatibilidade com SSL e conjuntos de cifras não permitidos e/ou pela modificação do arquivo de configuração. Em ambos os casos, as informações sobre a versão do código, incluindo, se pertinente, o arquivo de configuração modificado, devem ser possíveis de identificar como parte do firmware aprovado.*

Além disso, para todas as novas avaliações de POI com o conjunto de protocolos de internet, os dispositivos devem ser compatíveis com TLS 1.2 ou superior. Além disso, todas as avaliações delta para dispositivos de POI v3, v4, v5 ou v6, que afetem o módulo de protocolos abertos, devem atender aos mesmos critérios.

A PCI exige que os dispositivos somente aceitem conjuntos de cifras para uso em TLS 1.2 ou superior, que ofereçam pelo menos 112 bits de segurança. Podem-se usar o conjuntos de cifras que compõem o AES e outros algoritmos aprovados pelo NIST. Os conjuntos de cifras que fazem uso do TDEA (3DES) não são mais aceitos devido à quantidade limitada de dados que podem ser processadas em uma única chave, ou seja, o tamanho do bloco de 64 bits não oferece proteção adequada em aplicativos como o TLS, onde grandes quantidades de dados são criptografados na mesma chave.

Q 24 **Maio (atualização) de 2018: os dispositivos de entrada do PIN podem integrar-se fisicamente no mesmo dispositivo com outras funcionalidade, como aparelhos celulares, recursos de PDA ou terminal de PDV. As configurações portáteis dos dispositivos de entrada do PIN podem acomodar o anexo (por exemplo, por meio de um encaixe deslizante, um invólucro ou uma ou conector de áudio) para telefones celulares, PDAs ou terminais de POS, onde o dispositivo conectado se comunica com o PED. Essa configuração aparece como um único dispositivo, com interfaces separadas para entrada por parte do funcionário e do titular do cartão. Quais considerações devem ser levadas em conta para ambas as configurações?**

A *Para qualquer dispositivo onde se espera que o titular do cartão utilize a mesma interface para a entrada do PIN que o funcionário usaria para a função telefone, PDA, aplicação de pagamento etc., ou onde há várias interfaces em um único dispositivo integrado, o dispositivo integrado deve ser reforçado de forma física e lógica, de acordo com os requisitos de segurança de POI para PTS.*

Em uma configuração portátil com um dispositivo anexado, há risco de o titular do cartão inserir o PIN na interface incorreta. Além disso, a interface de comunicação entre o PED e o dispositivo conectado pode dar a esse último o acesso a funções de MSR, sem controles criptográficos, permitindo o skimming dos dados da conta do cartão. Neste modelo de integração, então:

- *Ambos os dispositivos são avaliados e validados como compatíveis com os requisitos de POI para PTS, ou*
- *O dispositivo de PED, que também deve controlar os leitores de cartão, deve implementar e ser validado em relação ao módulo de SRED de POI para PTS. O PED deve sempre aplicar funções de SRED para criptografia de dados de cartão. O PED somente tem permissão para atuar em um estado: criptografar todos os dados da conta. Não pode ser configurado para inserir um estado em que os dados da conta não sejam criptografados.*

Q 25 **Julho de 2015: os PEDs portáteis que se conectam a telefones celulares, PDAs ou terminais de PDV por meio de um encaixe deslizante, um invólucro ou um conector de áudio são necessários para oferecer compatibilidade com o SRED. Isso se aplica aos PEDs que se conectam via tecnologias sem fio, como Bluetooth ou Wi-Fi, aos telefones celulares e tablets?**

A *Sim. Além disso, para os dispositivos que não implementam criptografia de SRED, a política de segurança deve indicar claramente que o sistema não pode ser implementado para conexão com tablets ou telefones celulares, e que qualquer uso nesse sentido violará a aprovação do dispositivo. Os sistemas que têm aprovação de SRED devem observar que as funções de SRED devem ser ativadas e aplicadas para esses casos de uso, para manter sua aprovação.*

Q 26 **Maio (atualização) de 2018: os dispositivos de entrada do PIN que se conectam a telefones celulares, PDAs ou terminais de PDV por meio de encaixes deslizantes, invólucros, conectores de áudio ou conexão sem fio, são necessários para oferecer compatibilidade com SRED. Isso se aplica aos PEDs que são integrados a outros dispositivos (como tablets ou telefones celulares) que aparecem como um único dispositivo?**

A *Sim. O dispositivo integrado é aquele em que dois dispositivos física e eletronicamente distintos (por exemplo, um PED e um dispositivo comercial pronto para uso (COTS), como um telefone celular) aparecem como um único dispositivo como camuflagem para mascarar a conectividade.*

Nessas configurações, há risco de o titular do cartão inserir o PIN na interface errada. Além disso, a interface de comunicação entre o PED e o dispositivo integrado pode dar a este último

o acesso a funções de leitura de cartão, sem controles criptográficos, permitindo o skimming dos dados da conta do cartão. Neste modelo de integração, então:

- *Tanto os dispositivos PED quanto os sem PED são avaliados e validados como compatíveis de acordo com os requisitos de POI para PTS, ou*
- *O PED, que também deve controlar os leitores de cartão, deve ser implementado e validado em relação ao módulo de SRED de POI para PTS e ser física e eletronicamente distinto do sistema sem PED (por exemplo, não é permitido que o firmware do PED seja executado dentro do mesmo processador que o firmware do dispositivo sem PED). O PED deve sempre aplicar funções de SRED para criptografia de dados de cartão. O PED somente tem permissão para atuar em um estado: criptografar todos os dados da conta. Não pode ser configurado para inserir um estado em que os dados da conta não estejam criptografados.*

A política de segurança deve indicar também que o dispositivo sem PED não foi avaliado em relação ao programa PTS da PCI e é necessário haver orientações de segurança para garantir o funcionamento seguro da solução. Será incluída mais uma observação ao portal, esclarecendo que o dispositivo sem PED não foi avaliado no âmbito do programa PTS.

Q 27 Julho de 2017: para fins de aceitação da PCI, o padrão de esboço é um documento que foi publicado como esboço para uso experimental (por exemplo, ISO FDIS) ou foi publicado como esboço para comentários públicos (por exemplo, esboços do NIST).

A *No entanto, o ANSI (X9) não faz nenhum destes dois e são necessários mais esclarecimentos. Para fins de aceitação da PCI, o padrão de esboço do ANSI (X9) é aquele que foi eliminado do grupo de trabalho atribuído ao X9 (por exemplo, X9F1, X9F4 ou X9F6). Antes deste ponto, os procedimentos dos grupos de trabalho permitem que os membros publiquem documentos em vários estágios do "esboço" que podem entrar em conflito entre si e podem não refletir um consenso do grupo de trabalho. A violação do algoritmo invalida qualquer padrão de esboço ou final.*

Q 28 Maio de 2018: é permitido que o aplicativo do terminal analise os dados de entrada, alterando dinamicamente seu comportamento na execução? Por exemplo, os navegadores ou clientes de e-mail podem processar e exibir HTML5, Java, JavaScript ou qualquer outra linguagem de programação?

A *Sim, desde que os dados estejam sendo processados, verificados e exibidos pelo firmware.*

Q 29 Outubro de 2018: há requisitos mínimos para a versão do Android a ser usada em dispositivos do PTS?

A *Sim, espera-se que a versão do Android seja oficialmente aceita com, no mínimo, as correções de segurança. Todos os relatórios, incluindo deltas, em que a versão do Android não for aceita com as correções de segurança comuns serão rejeitados. Se essas correções não forem disponibilizadas pela Google, as comprovações das correções de segurança (implementadas no mínimo mensalmente) disponibilizadas pelo fornecedor deverão ser documentadas no relatório oferecido pela PCI. Espera-se que sejam apresentadas como comprovações a validação do código de atualização feita pelo laboratório para pelo menos duas correções anteriores, bem como a validação feita pelo laboratório indicando que essas correções remediaram as vulnerabilidades conhecidas atualmente na versão do Android que está sendo utilizada.*

Os fornecedores devem estar cientes de que isso significa que a consideração sobre o futuro status da correção de qualquer versão do Android que estiver sendo utilizada deve ser feita durante os estágios iniciais do projeto do dispositivo, para evitar a rejeição inesperada dos dispositivos quando uma versão do Android não for mais compatível durante o desenvolvimento de uma solução.

Q 30 Outubro de 2018: Os DTRs estabelecem que "os relatórios baseados em comprovações, que demonstram a conformidade do dispositivo por meio de testes sólidos, são fundamentais para o dispositivo ser aprovado." Quais são as expectativas mínimas para testes/comprovação de teste da resistência de qualquer dispositivo a ataques que envolvam penetração/modificação física?

A *Embora as comprovações de corte e/ou perfuração do dispositivo (caixa externa, partes internas) seja uma atividade de teste primária na maioria das avaliações, o corte e/ou a perfuração sozinhos raramente são suficientes para demonstrar resistência satisfatória para todos/quaisquer requisitos de segurança onde um caminho de ataque viável tenha elementos de penetração física/modificação. É necessário que o laboratório de avaliação apresente também comprovações sólidas da resistência do dispositivo a ataques físicos que tentem contornar, por exemplo (entre outros), interruptores anti-adulteração, malhas, PCBs, circuitos anti-adulteração, teclados, telas, leitores de cartões, placas etc., e esses componentes das peças do dispositivo e/ou os componentes que os conectam.*

Requisitos A1 de POI

Q 1 **Quais vulnerabilidades devem ser levadas em consideração no que diz respeito às telas sensíveis ao toque?**

A *Se as laterais estiverem acessíveis, um ataque de sobreposição que empregar uma segunda tela transparente e sensível ao toque poderá trazer problemas. A conexão/caminho da tela sensível ao toque para o processador (e qualquer dispositivo usado para decodificar os sinais entre eles) precisa ser verificado para confirmar que é seguro. Os chanfros ao redor da tela sensível ao toque são especialmente perigosos porque podem ocultar o acesso às áreas que são motivo de preocupação descritas acima.*

A API de firmware e os aplicativos (se aplicável) devem ser examinados com atenção para determinar as condições sob as quais é permitida a entrada de dados de texto simples. Exemplo: não deve ser possível, salvo nos dispositivos com tela controlada por mensagens do adquirente, que um terceiro exiba uma imagem (JPEG) que indique "pressione enter quando estiver pronto para inserir o PIN" e, em seguida, um teclado de texto simples apareça na próxima tela. É necessário ter ainda mais cautela com os dispositivos que contêm uma tela de toque devido ao desejo de fazer com que esses dispositivos sejam intuitivos para os usuários e, para isso, executar muitos aplicativos diferentes, sem autenticação e não controladas. Isto se aplica especialmente aos dispositivos que se destinam a ser segurados com as mãos, devido à tendência em considerá-los como se fossem PDAs que podem realizar transações de débito.

Q 2 **Em caso de violação, o dispositivo deve tornar-se imediatamente inoperável e apagar, de forma automática e imediata, todas as informações secretas que puderem estar armazenadas no dispositivo, de modo que seja inviável recuperar essas informações secretas. As instruções determinam que não há necessidade de as chaves secretas ou privadas serem zeroizadas na existência de uma ou ambas as condições a seguir:**

- **Se alguma dessas chaves não for zeroizada, será necessário então ter outros mecanismos em vigor para desativar o dispositivo. Além disso, essas chaves devem ser protegidas de acordo com o que estabelece o Requisito A6.**
- **As chaves nunca são usadas para criptografar ou descriptografar dados e não são usadas para autenticação.**

Alguma outra condição se aplica?

A *As chaves (secretas ou privadas) jamais serão usadas para criptografar ou descriptografar outras chaves. As chaves que podem ser usadas para baixar outras chaves para tornar o dispositivo operável devem ser zeroizadas ou tornadas inoperáveis para uso no download de novas chaves. Por exemplo, ambos as KEKs simétricas utilizadas para carregamento de chaves usando técnicas simétricas e chaves privadas associadas ao carregamento de chaves por técnicas assimétricas. O dispositivo deve impor que os dispositivos adulterados sejam obrigatoriamente retirados do uso para inspeção, recarga de chaves e recolocadas em funcionamento. Não basta confiar em controles de procedimentos para isso.*

Q 3 **O dispositivo faz uso de uma chave gerada de forma aleatória e internamente no processador seguro para proteger outras chaves. Essa chave é armazenada em segurança e fica protegida dentro de um registro no mesmo processador seguro. O processador seguro reside em uma área segura do dispositivo. Essa chave é usada para criptografar outras chaves, que são armazenadas criptografadas fora do processador seguro, por exemplo, na memória flash, que também reside na área segura do dispositivo. Em caso de adulteração, o dispositivo apaga a chave gerada internamente, mas deixa intactas as outras chaves criptografadas por esta chave, que não podem mais ser usadas porque o dispositivo não pode descriptografá-las. De acordo com o A1, o dispositivo deve zeroizar também essas chaves criptografadas em caso da adulteração?**

A *Não é necessário que o dispositivo zeroize essas chaves criptografadas, desde que sejam criptografadas com algoritmos e tamanhos de chaves apropriados, conforme definido no Requisito B9.*

Q 4 **Maio (atualização) de 2018: o Requisito A1 afirma que um dispositivo emprega mecanismos de detecção de violação e de resposta que fazem com que ele se torne imediatamente inoperável. Se o dispositivo for adulterado, ele ainda poderá ser usado para processar transações com cartão de pagamento sem PIN?**

A *Os dispositivos de aceitação de PIN que sofrerem alguma adulteração devem cessar imediatamente o processamento de todas as transações com cartão de pagamento baseadas em PIN. Se for implementada, somente uma redefinição deverá ser aceita, a menos que o dispositivo seja removido para inspeção e conserto. Toda intervenção que permitir a realização de transações deve exigir a presença de alguém no local que confirme que não houve adulteração no dispositivo, e estará sujeita às seguintes condições:*

- *Uso de técnicas de controle duplo;*
- *Proporcionar controle e rastreabilidade, incluindo o registro de IDs dos usuários, carimbo de data e hora e ações realizadas;*
- *As informações confidenciais necessárias para a autorização (por exemplo, senhas/códigos de autenticação) são inicializadas ou utilizadas de forma a impedir a repetição no mesmo dispositivo ou em outro dispositivo.*

Requisitos A2 de POI

Q 1 Quais vulnerabilidades devem ser levadas em consideração para telas sensíveis ao toque?

A *Se as laterais estiverem acessíveis, um ataque de sobreposição que empregar uma segunda tela transparente e sensível ao toque poderá trazer problemas. A conexão/caminho da tela sensível ao toque para o processador (e qualquer dispositivo usado para decodificar os sinais entre eles) deverá ser verificada para confirmar que é seguro. Os chanfros ao redor da tela sensível ao toque são especialmente perigosos porque podem ocultar o acesso às áreas que são motivo de preocupação descritas acima.*

A API para firmware e aplicativos (se aplicável) deve ser examinada com atenção para determinar as condições sob as quais é permitida a entrada de dados de texto simples. Exemplo: não deve ser possível, salvo nos dispositivos com tela controlada por mensagens do adquirente, que um terceiro exiba uma imagem (JPEG) que indique "pressione enter quando estiver pronto para inserir o PIN" e, em seguida, um teclado de texto simples apareça na próxima tela. É necessário ter ainda mais cautela com os dispositivos que contem com uma tela de toque devido ao desejo de fazer com que esses dispositivos sejam intuitivos para os usuários e, para isso, executar muitos aplicativos diferentes, sem autenticação e não controladas. Isto se aplica especialmente aos dispositivos que se destinam a ser segurados com as mãos, devido à tendência em considerá-los como se fossem PDAs que podem realizar transações de débito.

Requisitos A4 de POI

Q 1 Dezembro de 2011: quais são as exigências para a segurança das chaves públicas e das funções de gerenciamento de chaves em dispositivos de classe para aprovação do SCR?

A *As chaves públicas devem ser protegidas contra alterações dentro do dispositivo, para impedir ataques que comprometam a segurança do sistema por meio deste vetor de ataque. Os dispositivos projetados para ter conformidade com as classes de aprovação do SCR e que dependem de chaves públicas para proporcionar segurança ou autenticação a funções como atualizações de firmware, devem ser avaliados pelo laboratório para PTS da PCI no que diz respeito ao Requisito A4.*

Requisitos A5 de POI

Q 1 Quais padrões e métodos são usados para medir as "emissões eletromagnéticas"?

A *Os fornecedores devem levar em consideração que as emissões eletromagnéticas podem trazer risco para os dados do PIN e devem projetar os dispositivos de forma a resolver esse risco. Existem muitos métodos para proteger e minimizar emissões eletromagnéticas. O fornecedor deve descrever, por escrito, para o laboratório como o projeto do dispositivo trata do problema das emissões eletromagnéticas. O laboratório examinará as provas disponibilizadas pelo fornecedor para determinar se as provas corroboram a afirmação do fornecedor. As provas podem incluir o próprio dispositivo, documentos de projeto, resultados de testes de terceiros e aprovações. Os testes serão realizados conforme o necessário.*

Q 2 **Maio de 2017: há situações em que o relatório de avaliação não precisa informar o custo do ataque?**

A *Sim, no caso do A5 (monitoramento durante a entrada do PIN), quando os testes de qualquer característica externa disponível para monitoramento que satisfaça, comprovadamente, as etapas pertinentes dos testes do DTR não tiverem detectado nenhum vazamento, deve-se explicar por que razão um cenário de ataque não pode ser viável por menos de 26 pontos, com um mínimo de 13 para exploração inicial. Nessa situação, não é necessário apresentar nenhum cálculo formal do ataque.*

Requisitos A7 de POI

Q 1 **Julho de 2017: os avaliadores normalmente usam a análise do código-fonte e também os testes da implementação para confirmar que há métodos de proteção de canais laterais implementados. Como o avaliador deve proceder quando as proteções estão presentes no código criado pelo fornecedor do chip e somente são disponibilizadas ao fornecedor do POI como biblioteca e não como código-fonte?**

A *O avaliador deve tratar o dispositivo como uma caixa preta e estender os testes para além do que seria necessário se o código-fonte estivesse disponível para determinar se o dispositivo é resistente a ataques. O apêndice de avaliação dos padrões para análise de canal lateral do PTS da PCI nos Requisitos de teste derivado oferecem orientação.*

O relatório deve estipular claramente quais materiais foram disponibilizados para a avaliação e o que foi especificamente testado, os detalhes das contramedidas em vigor e implementadas, incluindo o código que foi analisado. Se não forem disponibilizados materiais, o caso deverá ser tratado como avaliação da uma caixa preta, tal como definido no parágrafo anterior e comunicado como tal.

Requisitos A8, B15 e C2.4 de POI

Q 1 **O objetivo de A8, B15 e C2.4 é eliminar a possibilidade de que os valores do PIN sejam inseridos em um momento impróprio e manipulados pelo dispositivo de maneira insegura. Uma maneira de o fornecedor atender ao A8, B15 ou C2.4 é permitindo somente a entrada de valores do PIN. Seria aceitável permitir a entrada de dados numéricos se os dados numéricos fossem formados por três ou menos caracteres e, portanto, não pudessem representar o valor do PIN?**

A *Isso pode ser aceito se não houver nenhuma maneira de o dispositivo aceitar a entrada do valor do PIN em um momento inapropriado. Por exemplo, não deve ser possível para o dispositivo permitir a entrada de três caracteres, mudar automaticamente os estados sem que o titular do cartão pressione "enter" ou alguma outra tecla de controle e, em seguida, aceitar o restante do valor do PIN.*

Q 2 **Quais são as restrições se o dispositivo puder exibir mensagens não controladas e o teclado for usado para inserir dados que não incluam o PIN?**

A *Todos as solicitações de entrada de dados que não incluem o PIN estão sob o controle da unidade criptográfica e devem ser específicas para que o titular do cartão não insira o PIN em um momento inapropriado. Uma mensagem não controlada, seguida por uma solicitação ambígua, para entrada de dados que não incluem o PIN, pode levar o titular do cartão a inserir seu PIN em um momento inadequado. Por exemplo, se o dispositivo exibir a mensagem não controlada "Pronto para o PIN" e, em seguida, solicitar dados de texto simples ao exibir "Inserir dados", o titular do cartão poderá inserir seu PIN nesta solicitação de dados que não se refere ao PIN.*

Q 3 **É aceitável que mensagens não controladas sejam exibidas simultaneamente com solicitações para digitação de dados?**

A *Não. Todo texto, incluindo imagens, além de números e pontuação, exibido junto com uma solicitação é considerado uma solicitação e deve cumprir todos os requisitos que regem essas mensagens.*

Q 4 **O projeto de alguns dispositivos adéqua-se às solicitações de exibição controladas pelo fornecedor ou pelo adquirente, no que diz respeito ao gerenciamento de quem recebe a custódia das chaves criptográficas que protegem as atualizações das mensagens. É necessário que esse dispositivo tenha identificadores diferentes?**

A *Se o dispositivo tiver que ser especificado como dispositivo de solicitação de exibição controlado pelo adquirente e pelo fornecedor, será necessário que haja uma diferenciação para que os clientes possam distinguir entre os dois (por exemplo, diferentes versões de hardware e/ou firmware).*

Q 5 **Para os dispositivos que implementam solicitações controladas pelo adquirente, é obrigatório usar um dispositivo criptográfico seguro para implementar o controle duplo obrigatório para gerenciar essas mensagens?**

A *O controle duplo deve ser aplicado por um SCD. O SCD pode ser o próprio PED ou outro dispositivo. Se um SCD diferente do PED impõe o controle duplo, o fornecedor deve disponibilizar o SCD a terceiros ou descrever como se deve usar o SCD para atender ao B15. A descrição deve incluir um exemplo de um SCD atual específico, que pode ser comprado e usado para cumprir atender ao B16. O PED deve ter uma API compatível com o SCD. É necessário desenvolver a solução completa. Não basta oferecer instruções detalhadas que exijam que os usuários desenvolvam parte da solução.*

Q 6 **Dezembro (atualização) de 2017: para os PEDs projetados com várias interfaces de aceitação de dados, onde houver um teclado rígido dedicado para a entrada do PIN (e outros dados confidenciais), e a outra interface for uma interface de toque não destinada a aceitar a entrada de nenhum dado confidencial, quais controles serão necessários para a segunda interface?**

A *Nesse tipo de projeto, é necessário aplicar os seguintes controles na interface "não confidencial", além da atual restrição de que os aplicativos não devem solicitar a entrada de dados confidenciais:*

- *O firmware deve ser desenvolvido de forma que não seja possível inserir nenhum dado confidencial na interface "não confidencial".*

- *Se as coordenadas de toque x/y forem enviadas para os aplicativos autenticados no dispositivo, o fornecedor deverá oferecer orientação aos desenvolvedores de aplicativos para que jamais enviem coordenadas de toque. Além disso, o fornecedor deve analisar também todos os aplicativos e NÃO assiná-los/autenticá-los se eles tiverem sido escritos de forma a enviar coordenadas de toque, não permitindo, assim, que eles sejam carregados; ou*
- *Se o PED autenticar o terminal que recebe as coordenadas x/y e se o link de comunicação entre essas instâncias for criptografado com segurança (por exemplo usando um túnel TLS v1.2), o dispositivo poderá disponibilizar as coordenadas de toque x/y exclusivamente para os aplicativos ou servidores que tiverem sido autenticados pelo dispositivo.*

Requisitos A8 de POI

Q 1 **O cálculo da possibilidade de ataque de 18 por dispositivo pode incluir o custo dos kits de desenvolvimento que disponibilizam informações para programação de aplicativos?**

A *Não. O dispositivo deve incluir proteções que exijam que o invasor alcance uma possibilidade de ataque de pelo menos 18 para derrotá-las. Os controles administrativos sobre as informações de programação dos aplicativos não são adequados para atender a esse requisito.*

Q 2 **Os dispositivos de tela de toque oferecem várias possibilidades para a entrada de dados: layout tradicional do teclado numérico do PIN, layout QWERTY, captura de assinatura, reconhecimento de caligrafia etc. O A6 se aplica a todos esses métodos de entrada de dados, ou somente ao teclado numérico tradicional do PIN?**

A *O A6 se aplica a todos os métodos de entrada de dados que podem ser usados pelo titular do cartão para revelar seu PIN, incluindo o layout QWERTY, a captura de assinatura e o reconhecimento de caligrafia.*

Requisitos A9 de POI

Q 1 **O Requisito A9 estipula que o dispositivo deve oferecer um meio para impedir a observação visual dos valores do PIN enquanto são inseridos pelo titular do cartão. Quais métodos são aceitos?**

A *Os Requisitos de segurança do POI oferecem várias opções que podem ser usadas em separado ou em conjunto para fornecer proporcionar privacidade durante o processo de digitação do PIN. Essas são as opções:*

- *Uma barreira para blindagem física (privacidade). Lembre-se de que, caso seja possível destacar o escudo de privacidade, será necessário que haja um guia do usuário junto com o dispositivo, que declare que o escudo de privacidade deve ser usado para cumprir a ISO 9564. Opcionalmente, o guia do usuário pode também fazer referência aos requisitos do dispositivo da PCI;*
- *Projetado de forma que o titular do cartão possa fazer a proteção usando o seu próprio corpo, para impedir a observação durante a entrada do PIN, por exemplo, um dispositivo portátil;*
- *Ângulo de visão limitado (por exemplo, um filtro polarizador ou um teclado numérico recuado para entrada do PIN);*
- *O gabinete que faz parte do caixa eletrônico ou quiosque, a mão ou o corpo do titular do cartão (aplica-se exclusivamente a dispositivos portáteis); e*
- *O ambiente do dispositivo instalado.*

Q 2 **Setembro (atualização) de 2016: a aprovação do dispositivo será afetada de alguma forma se o método de privacidade avaliado pelo laboratório não for utilizado?**

A *É comum que os desenvolvedores de dispositivos argumentem que os mecanismos de proteção de privacidade podem ser volumosos ou intrusivos, que dificultam a tarefa de ver a tela do dispositivo ou, para os usuários menos hábeis, interferem no pagamento com cartão e na entrada do PIN. No entanto, para manter a aprovação do dispositivo, além de qualquer proteção de responsabilidade associada ao comprometimento imputável ao uso do referido dispositivo, é obrigatório que o dispositivo cumpra os requisitos de proteção da privacidade, conforme avaliado pelo laboratório, e com base nos quais a aprovação se baseou. Os dispositivos implementados que não utilizarem os requisitos de proteção da privacidade avaliados pelo laboratório de testes deixarão de ser considerados dispositivos aprovados. Essa informação deve ser divulgada na política de segurança do dispositivo.*

Q 3 **Setembro de 2016: os fornecedores devem oferecer um escudo de privacidade que proteja a privacidade do titular do cartão durante a entrada do PIN ou, opcionalmente, o fornecedor pode empregar critérios de proteção da privacidade menos restritivos, desde que disponibilize regras e orientações sobre como o ambiente em que o dispositivo está instalado pode impedir a observação visual. Isso afeta as informações divulgadas da política de segurança?**

A *Sim. A política de segurança deve estipular as regras e orientações, com base nas quais o dispositivo foi avaliado, no que diz respeito à forma como o ambiente em que o dispositivo está instalado, pode impedir a observação visual. A política deve divulgar também que a implementação que não empregar essas considerações, que foram avaliadas pelo laboratório e nas quais a aprovação baseou-se, invalidará a aprovação do dispositivo.*

Se o dispositivo vier com um escudo de privacidade removível, a política de segurança deverá divulgar que a implementação sem o escudo invalidará a aprovação, a menos que o dispositivo seja implementado de acordo com as instruções estabelecidas na política de segurança validada pelo laboratório, para implementar o dispositivo com as proteções oferecidas pelo ambiente onde ele está instalado. A política deve divulgar também que a implementação que não empregar essas considerações, que foram avaliadas pelo laboratório e nas quais a aprovação baseou-se, invalidará a aprovação do dispositivo.

Requisitos A10 de POI

Q 1 **Setembro de 2013: o dispositivo pode ser validado para SRED se receber dados de conta inseridos em um módulo ou dispositivo não integrado, por exemplo, quando o dispositivo recebe dados de conta inseridos por chave em outro dispositivo?**

A *O módulo ou dispositivo externo, onde os dados da conta são capturados, pode receber aprovação de SRED se avaliado em conjunto com o dispositivo de POI. A aprovação de SRED dependeria de ambos os dispositivos atenderem a todos os requisitos de SRED aplicáveis, incluindo a proteção de chaves criptográficas. Os dados da conta (conforme definido no glossário dos* Requisitos de segurança de POI para PTS da PCI) que *percorrem o caminho de comunicação partindo do ponto externo de captura devem ser criptografados de acordo com esses requisitos. Ambos os dispositivos faziam parte da lista de aprovação, e a substituição do dispositivo externo por outro que não seja validado para SRED invalida a aprovação de SRED como uma função oferecida.*

Se o dispositivo externo não puder atender aos requisitos de SRED, o dispositivo principal, mesmo que proteja de outra forma os dados da conta de acordo com o SRED, não poderá receber a designação de SRED onde puder receber dados da conta do dispositivo em questão, sejam esses dados recebidos criptografados ou não. Nessa situação, para que o dispositivo principal receba a aprovação de SRED, o firmware do dispositivo principal não deve aceitar o recebimento dos dados da conta capturados externamente.

Requisitos A11 de POI

Q 1 **Novembro de 2012: onde for utilizada uma lista de permissões para controlar se os dados de PAN saem do dispositivo em texto simples ou em texto criptografado, a atualização da lista de permissões tem que estar sob o controle direto do fornecedor?**

A *Não, o vendedor pode oferecer os mecanismos ao adquirente para que este controle diretamente a atualização das listas de permissões, de forma coerente com as mensagens de exibição controladas pelo adquirente,ou seja, o uso de técnicas de controle duplo e provisões para permitir a auditoria e o registro.*

O fornecedor pode, opcionalmente, disponibilizar documentação para o usuário detalhando o gerenciamento de chaves criptográficas seguindo esses princípios e implementando o uso de um dispositivo criptográfico seguro para o gerenciamento dessas chaves. O processo existe acima do dispositivo, no entanto o dispositivo deve ainda assim impor a aplicação, por exemplo, validar o MAC ou a assinatura digital.

Requisitos A13 de POI

Q 1 **O que se deve entender por "espaço suficiente para manter um dispositivo de captura de PIN"?**

A *Não é permitida a existência de nenhum espaço que possa ser acessado via abertura para cartão inteligente (ICC) grande o suficiente para ocultar um dispositivo de captura de PIN. O dispositivo em questão poderia fazer uso da tecnologia de ICC. Portanto não deve haver nenhum espaço que possa ser acessado via abertura para cartão grande o suficiente para esconder um chip de ICC e bateria pequena.*

Q 2 Qual é o volume de espaço permitido no A13?

A *O A13 visa impedir que algum dispositivo de captura de PIN seja inserido no dispositivo pela abertura do cartão. O volume do espaço acessível via abertura do cartão que pode ser utilizado por invasores pode variar de acordo com a geometria do espaço e com os métodos de ataque. Por esse motivo, o requisito não proíbe um volume específico. Em vez disso, a viabilidade da colocação de dispositivos espiões deve ser considerada durante a avaliação da conformidade com o A14. Exemplos destas considerações:*

- *É necessário que existam pontos de contato para que o dispositivo espião se conecte.*
- *O dispositivo espião e os fios não devem obstruir a operação normal.*
- *A colocação do dispositivo espião não deve produzir indícios de adulteração que seriam percebidos pelo titulares típicos dos cartões.*

Q 3 Maio de 2018: a nova classe de aprovação de SCRP aumenta o nível de proteção obrigatório para a interface de E/S do ICC para 26 pontos. Por que isso é necessário quando outras classes de aprovação continuam permitindo que os dispositivos que atendam a um nível de proteção de 20 pontos seja considerado compatível?

A *A intenção da classe de aprovação do SCRP é garantir que os dados do cartão do cliente sejam protegidos e criptografados com criptografia avançada, para serem enviados por meio do dispositivo de ambiente COTS, passado para os sistemas de back-end para processamento de pagamentos. Essa é uma parte importante da segurança total da entrada do PIN baseada em software no PIN de COTS (SpOC), na solução do sistema COTS, e ajuda a impedir ataques da correlação e a reduzir a ameaça de comprometimento do PIN no dispositivo COTS. Como a proteção do sinal de E/S do ICC exige proteção da interface física para o cartão do cliente por meio do processador de segurança, que realiza a criptografia desses dados exigindo um aumento nos mínimos dos pontos de ataque para isso, portanto causa um aumento na proteção geral exigida no SCRP como um todo que, por sua vez, tem um efeito de continuidade para reduzir o risco de roubo de PIN no dispositivo COTS.*

Outras classes de aprovação em que os cartões ICC são aceitos podem não processar PINs de modo algum, ou serem obrigadas a garantir a conformidade com outros cálculos de custo de ataque e mínimos dentro dos requisitos de PTS da PCI e portanto não dependerem tanto da separação dos dados dos cartões dos clientes e dos dados do PIN. Por isso os pontos de ataque podem permanecer em 20 pontos para os outros casos de uso.

Requisitos A14 de POI

Q 1 O D2 destina-se a tratar da abertura do leitor ICC ou de todo o leitor?

A *O D2 foi criado com o entendimento de que a abertura (ranhura) é um ponto de ataque em potencial para a inserção de um mecanismo de exploração.*

Q 2 Alguns projetos de dispositivos trazem componentes (por exemplo, escudo de privacidade) que estão próximos à abertura para cartão IC, e podem ser usados para ocultar algum cabo. Quais critérios são usados para determinar a conformidade quando da existência desses componentes?

A *Considera-se que o projeto está em conformidade com o A14 quando uma parte do cabo entre a abertura e o componente de ocultação estiver visível.*

Requisitos B1 de POI

Q 1 **Se um dispositivo aplicar um firmware na cabeça de leitura do MSR para criptografar dados da conta, esse firmware estará sujeito à verificação de autenticidade, conforme definido no Requisito B1?**

A *Não. A verificação de autenticidade, conforme definido no Requisito B1, destina-se ao gerenciamento de firmware que estiver direta ou indiretamente envolvido na proteção dos PINs dos titulares de cartão, conforme definido nos diversos requisitos de segurança. No entanto, o firmware na cabeça de leitura deve ser projetado de modo que não possa ser atualizado.*

Q 2 **Em quais circunstâncias o dispositivo pode não utilizar a verificação de autenticidade no autoteste de seu firmware?**

A *A verificação de autenticidade no teste do firmware do dispositivo não será obrigatória se (todos se aplicam):*

- *A verificação de autenticidade do firmware, internamente e de acordo com o B2 ou externamente com procedimentos apropriados dentro de um ambiente seguro sob o controle do fornecedor, é realizada sempre que o firmware é implementado na área segura em questão;* ***e***
- *O esforço para modificar ou substituir, deliberadamente, o firmware ou partes dele para ter acesso a informações confidenciais (acesso ao dispositivo de memória) deve ser tratado como um cenário de ataque estabelecido nos Requisitos A1, A4 e A6 e atender às respectivas possibilidades de ataque;* ***e***
- *É realizada uma verificação periódica de integridade, de acordo com o Requisito B1, no firmware, garantindo que alterações aleatórias serão detectadas. Se a autenticidade criptográfica não for realizada, a verificação de integridade deve ser de base criptográfica. Embora seja possível empregar um algoritmo que faça uso de uma chave secreta, como os hashes com chave, ele não é necessário para atender aos critérios de integridade.*

Essas condições se aplicam independentemente de qualquer propriedade não reconfigurável da memória do dispositivo.

Se o firmware for autenticado externamente, o nível de segurança deverá ser igual ao das instalações de injeção de chave.

Requisitos B2 de POI

Q 1 **Quais partes podem ter as chaves usadas para a autenticação criptográfica das atualizações do firmware?**

A *O firmware é responsabilidade do fornecedor do dispositivo e, como tal, as chaves criptográficas que o autenticam dentro do dispositivo devem permanecer exclusivamente com o fornecedor ou com seu representante indicado.*

Q 2 **As atualizações de firmware devem ser autenticadas de forma criptográfica e, se a autenticação falhar, a atualização será rejeitada e excluída. Há alguma circunstância que permita a atualização do firmware sem autenticação?**

A *Alguns chipsets não foram projetados para atualizações de firmware, somente para aceitar substituição do firmware. A exclusão do firmware e das chaves criptográficas atuais durante a substituição não permite a autenticação do novo firmware.*

Nesses casos, será permitido atualizar o firmware sem autenticação se o processo exigir que o dispositivo seja devolvido às instalações do fornecedor resultando na zeroização segura de todas as chaves secretas e privadas contidas no dispositivo.

Q 3 **Dezembro de 2011: se o dispositivo aceitar a atualização do firmware, o dispositivo deve autenticar criptograficamente o firmware e, se o firmware não for confirmado, a atualização do firmware deverá ser rejeitada e excluída. O dispositivo pode carregar completamente o novo firmware antes de verificar sua autenticidade e substituir a cópia principal do código autenticado atual se ele mantiver uma cópia de segurança protegida do código autenticado atual?**

A *Sim, desde que o que se segue seja verdadeiro:*

- *O novo código é autenticado criptograficamente antes da execução.*

  Se a autenticação do novo código falhar, a cópia de segurança do código será autenticada criptograficamente e, se a cópia de segurança for autenticada com êxito, o dispositivo inicializará a partir da cópia de segurança e essa cópia será usado então para substituir o novo código cuja autenticação falhou.

- *Se a autenticação de ambas as versões do firmware falhar, a falha do dispositivo ocorrerá de maneira segura.*

Q 4 **Fevereiro de 2017: se o dispositivo utilizar assinaturas digitais para autenticar as atualizações de firmware (em conformidade com o B2), será necessário a aplicação de um protocolo seguro para atender ao B22?**

A *O B2 estipula que o firmware carregado no dispositivo deve ser autenticado independentemente de como o arquivo for entregue ao dispositivo.*

O B2 garante que a plataforma de gerenciamento entrega os arquivos ao dispositivo com segurança e que não é possível utilizar a interface como vetor de ataque no dispositivo.

- *Para o acesso remoto, ou seja, os arquivos são entregues ao dispositivo por uma rede privada ou pública, o uso de um protocolo de segurança é obrigatório e deve ser validado.*

- *Para o acesso manual, ou seja, quando o operador tem controle físico do terminal e dos arquivos, e os arquivos não são entregues por meio de uma rede, o dispositivo garante que não é possível explorar a interface (por exemplo, restringindo o acesso/recurso na interface, exigindo direitos administrativos, utilizando técnicas de autenticação criptográfica etc.).*

O B22 afirma que trata-se exclusivamente do acesso remoto e não inclui elementos manuais. A existência de um protocolo de segurança seria obrigatória para garantir que a interface não possa ser explorada.

Requisitos B2.2 de POI

Q 1 **Março de 2011: os aplicativos autenticadas podem ser desenvolvidos pelo fornecedor do POI ou por outros terceiros. Os aplicativos devem ser desenvolvidos com técnicas coerentes com o PA-DSS e devem ser autenticadas criptograficamente pelo POI. Há alguma outra consideração?**

A *Sim. A técnica utilizada para gerenciar o mecanismo de autenticação (por exemplo, assinaturas digitais) deve empregar um dispositivo de criptográfico seguro (SCD) e técnicas de duplo controle. Para terceiros, o fornecedor do dispositivo deve fornecer o SCD aos terceiros ou descrever como o SCD deve ser usado para atender ao B7. A descrição deve incluir um exemplo de um SCD atual específico, que pode ser comprado e utilizado em conformidade com o B5. O POI deve ter uma API compatível com o SCD. A solução completa deve ser desenvolvida em sua totalidade. Não é permitido disponibilizar instruções detalhadas que exijam que os usuários desenvolvam parte da solução.*

Requisitos B4 de POI

Q 1 **O requisito B4 exige que um PIN seja criptografado imediatamente. Normalmente, isso significa que o processador seguro forma e criptografa o PIN Block antes de executar qualquer outra operação. No entanto, alguns projetos de dispositivos colocam um microprocessador entre o teclado e o processador seguro. Em quais condições, se houver alguma, esse tipo de projeto seria permitido?**

A *Esse tipo de projeto será considerado compatível se o microprocessador, o processador seguro e o caminho entre eles estiver completamente dentro do limite de proteção do dispositivo. Este limite é estabelecido pelo método escolhido para atender ao A1.*

Um método alternativo para atender ao requisito seria que o microprocessador criptografasse imediatamente o PIN antes de passá-lo para o processador seguro, que então o descriptografaria e criaria o PIN Block criptografado. Lembre-se de que neste tipo de projeto, o software do microprocessador utilizado para criptografar os dados do PIN está sendo usado para atender aos requisitos da PCI. Portanto, este software deve ser considerado um "firmware" conforme indicado pelos requisitos da PCI. Dessa forma, os Requisitos B3 e B4 se aplicariam a esse firmware.

Q 2 **É comum que a criptografia dos teclados do PIN utilizados em caixas eletrônicos aceite o uso de um comando para iniciar a entrada do PIN e outro comando para criptografar o PIN. Isso é permitido no B4?**

A *Sim. É permitido que o EPP permita que um comando inicie a entrada do PIN e um segundo comando inicie a criptografia do PIN. No entanto, não pode ser possível que o comando de criptografia seja usado para criptografar o PIN várias vezes para gerar o PIN criptografado do EPP com chaves criptográficas distintas ou para gerar do PIN em texto simples. Além disso, o valor do PIN de texto simples somente deve existir em memória protegida contra adulteração ou equivalente.*

Q 3 **Setembro de 2012: os dispositivos aceitam a criptografia do PIN várias vezes como parte de uma série de transações. O B4 estipula que as criptografias devem utilizar a mesma chave criptográfica para essa série. A série de transações pode ser criptografada por uma série de chaves se a chave atual for uma derivação de uma chave anterior?**

A *O requisito tem como objetivo impedir que os adversários utilizem a chave autorizada para enviar a transação online para autorização e outra chave para registrar a transação para recuperação posterior. Nesse respeito, pode ser utilizada uma metodologia de chave exclusiva por transação (UKPT), para a série de transações, em que as chaves fazem parte da mesma série e toda a hierarquia é garantida da mesma forma, inviabilizando, no projeto, a inserção de uma chave não autorizada.*

Q 4 **Abril de 2013: o B4 exige que os PINs online sejam criptografados imediatamente após a entrada do PIN. Estipula ainda que os PINs de texto simples não devem existir durante mais de um minuto, a contar da conclusão da entrada do PIN do titular do cartão. Em todos os casos, o apagamento do PIN de texto simples deve ocorrer antes que os mecanismos de detecção de violação possam ser desativados pelos métodos de ataque descritos no A1. Há alguma circunstância em que o PIN de texto simples possa existir por mais de um minuto?**

A *Alguns caixas eletrônicos implementaram tecnologias de depósito inteligentes para aprimorar a experiência do cliente. O resultado disso foi que algumas transações de depósito demoram mais de um minuto, fazendo com que o PIN seja apagado do buffer após um minuto e que o titular do cartão tenha que reiniciar a transação e, em alguns casos, não consiga concluí-la. Nesses casos, os aplicativos dos caixas eletrônicos exigem a mudança da solicitação para nova entrada do PIN se o tempo da transação esgotar, em vez de exigir que toda a transação seja reiniciada.*

A fim de oferecer um tempo suficiente para a mudança desses aplicativos, a PCI concederá três anos, a contar da publicação destas dúvidas frequentes, para que esses aplicativos sejam modificados. Durante esse período de três anos, o PIN não criptografado pode permanecer no buffer por até cinco minutos. No entanto, o PIN deve permanecer protegido para que não seja comprometido, empregando os métodos de ataque descritos no A1. Além disso, o laboratório de testes deve levar em consideração a falta de criptografia oportuna na concepção dos ataques.

Este período de suspensão somente se aplica à criptografia dos teclados numéricos de PIN projetados para em caixas eletrônicos.

Requisitos B5 de POI

Q 1 É aceitável que os componentes da chave XOR (OU exclusivo) durante o carregamento de chaves satisfaça os requisitos de autenticação do B5?

A *O XOR dos componentes da chave, por si só, não é suficiente para constituir a autenticação. É obrigatória a existência de algum tipo de autenticação dos usuários que utilizam a função de carregamento de chave ou autenticação do comando de carregamento de chave.*

Q 2 Maio (atualização) de 2018: em quais circunstâncias é permitida a entrada da chave via teclado do dispositivo?

A *As chaves secretas de componente único de texto simples não podem ser inseridas no dispositivo via teclado. Os componentes das chaves de texto simples podem ser inseridos via teclado de acordo com a norma ISO 11568-2. As chaves criptografadas também podem ser inseridas via teclado. A inserção dos componentes da chave ou das chaves criptografadas deve ser restrita a indivíduos autorizados. As funções utilizadas para inserir as chaves somente devem estar disponíveis quando o dispositivo estiver em estado confidencial. O acesso às funções confidenciais deve ser restrito por meio do uso de senhas/códigos de autenticação ou outras informações secretas.*

Q 3 Os menus de manutenção que oferecem serviços como o ajuste de contraste do LCD, autotestes, manutenção da impressora e testes de teclas constituem "serviços suscetíveis"?

A *Se os serviços prestados nessas funções normalmente não permitidas não afetarem a segurança do terminal ou dos dados dos titulares de cartão, não são considerados serviços suscetíveis. Somente os serviços que podem comprometer a segurança do terminal são serviços suscetíveis.*

Q 4 Para os dispositivos que exigem o uso de dados de autenticação para acesso a funções suscetíveis, com os dados de autenticação estáticos, os dados de autenticação podem ser enviados com o dispositivo?

A *Os dados de autenticação somente podem ser enviados com o dispositivo quando os dados de autenticação estão em embalagens invioláveis, como o uso de embalagens para envio de PIN. Caso contrário, é necessário utilizar canais de comunicação separados com destinatários pré-designados.*

Q 5 Março de 2011: as chaves secretas de texto simples ou privadas e seus componentes podem ser injetados no teclado do PIN por meio de um carregador de chaves (que deve ser algum tipo de dispositivo criptográfico seguro). Há alguma restrição para o carregamento de chaves por essa metodologia?

A *Sim, o carregamento de chaves de texto simples, secretas ou privadas e seus componentes por meio de dispositivos para carregamento de chaves é restrito a instalações de carregamento de chaves seguras. O segredo de texto simples ou o carregamento de chaves privadas dos dispositivos sem supervisão implementados no campo deve ficar restritos aos componentes das chaves inseridos por meio do teclado numérico do PIN. Se criptografadas, essas chaves podem ser carregadas por meio de outra interface, como uma porta serial ou USB.*

Q 6 **Dezembro de 2011: os dispositivos podem ter funções para zeroizar chaves secretas e privadas no dispositivo. Essas funções são consideradas serviços suscetíveis que exigem autenticação?**

A *Sim, a zeroização intencional de chaves secretas ou privadas em um evento contra adulteração é a execução de funções que não estão disponíveis durante o uso normal. Isso exige que a autenticação seja coerente com as implementações de outros serviços suscetíveis, como o uso de PINS/frases secretas. Se implementado, o dispositivo deve forçar a alteração dos valores de autenticação padrão na configuração do dispositivo. O mecanismo de autenticação pode, opcionalmente, empregar técnicas de controle duplo.*

Q 7 **Junho (atualização) de 2015: os dispositivos podem ter funções para zeroizar chaves secretas e privadas no dispositivo. Este recurso é considerado um serviço suscetível, que exige autenticação. Em alguns casos, há um efeito ascendente onde as alterações de software devem ocorrer nos pontos da interface, tais como plataformas de caixas eletrônicos, aplicativos, interruptores e hosts que se conectam aos EPPs. Há alguma situação em que este requisito possa ser dispensado?**

A *Todos os dispositivos que implementarem este recurso devem atender ao requisito. No entanto, o dispositivo pode fazer isso implementando um novo comando de exclusão autenticada ao conjunto de comandos do EPP, além dos comandos já existentes. A programação deve ser feita como opção "um ou outro", de modo que ambos os métodos não fiquem disponíveis ao mesmo tempo. Quando a opção autenticada é selecionada, esta ação bloqueia definitivamente os comandos não-autenticados.*

Em todos os casos, é necessário especificar um período de validade limitado para forçar as alterações de software ascendentes a serem implementadas dentro de um período estipulado. A PCI concederá um período de três anos, a contar da publicação destas dúvidas frequentes, para modificação desses aplicativos. Este período de suspensão somente se aplica à criptografia dos teclados numéricos de PIN projetados e utilizados em caixas eletrônicos.

A partir de 1º de janeiro de 2017, todos os EPPS recém-aprovados devem aceitar exclusivamente o recurso de exclusão autenticada. Não há necessidade de que os EPPs aprovados antes de janeiro de 2017, com recurso para exclusão não autenticada, sejam atualizados para que passem a aceitar o recurso de exclusão autenticada, de forma a manter a conformidade com a PCI.

Requisitos B7 de POI

Q 1 **Janeiro de 2015: é obrigatório, de acordo com o DTR B21, que o POI gere o número imprevisível (NI) do EMV para qualquer transação baseada em PIN utilizando o gerador interno de números aleatórios, conforme testado de acordo com o requisito B7. É obrigatório também que as transações não baseadas em PIN gerem o NI com o gerador de números aleatórios do POI?**

Sim, é necessário utilizar o gerador de números aleatórios do POI para gerar todos os valores aleatórios e imprevisíveis, que são usados para a segurança dos dados do cartão e das transações de PIN. Quando o POI é utilizado para gerar o NI do EMV, o gerador de números aleatórios do POI deve ser usado para gerar valores do NI do EMV, independentemente do método de verificação do titular do cartão implementado para a transação em questão. Lembre-se de que o processo de geração de NI do EMV pode incorporar outros dados, tais como registros internos e dados da transação (veja, por exemplo, o algoritmo de geração de NI do EMV em http://www.emvco.com .

Requisitos B9 de POI

Q 1 **É permitido que um dispositivo tenha a capacidade de usar chaves mestras, tanto como chaves de criptografia quanto para chave de sessão e como chaves fixas, ou seja, a chave mestra poderia ser usada para criptografar PIN blocks e descriptografar chaves de sessão?**

A *Não. A chave deve ser usada para uma finalidade exclusiva, conforme exigência da ANSI X9.24 e ISO 11568.*

Q 2 **É permitido utilizar a mesma técnica de autenticação para carregamento de chaves criptográficas e firmware?**

A *A técnica pode ser a mesma, no entanto os segredos utilizados para autenticação devem ser diferentes. Exemplo: se forem usadas assinaturas de RSA, a chave de RSA privada, utilizada para assinatura das chaves criptográficas para carregamento, deve ser diferente da chave privada utilizada para assinatura do firmware.*

Q 3 **É permitido utilizar a criptografia do modo ECB de TDES para chaves de sessão no emprego da técnica de chave mestra/chave de sessão?**

A *Sim. É permitido utilizar o modo ECB de TDES para criptografar chaves de sessão.*

Q 4 **É permitido carregar componentes de chave de TDES de 128 bits de comprimento duplo em dispositivos com valores de bits inferiores (por exemplo, duas partes de 64 bits mantidas pelo guardião de chaves 1 e duas partes de 64 bits mantidas pelo guardião de chaves 2)?**

A *Sim, desde que as chaves de TDES criptográficas de 128 bits (e componentes das chaves) sejam geradas e gerenciadas como chaves de TDES de 128 bits de comprimento duplo completas durante todo o ciclo de vida, de acordo com a ANSI X9.24 e ISO 11568.*

Por exemplo, seria permitido gerar um componente de chave de TDES de 128 bits, de comprimento completo, mas carregá-lo no dispositivo como um componente constituído por duas metades de 64 bits.

Não seria permitido gerar chaves de 64 bits ou componentes de chaves em separado e, depois, concatená-los para uso como chave de comprimento duplo após a geração.

Se forem utilizados valores de verificação de chave para garantir a integridade da chave, é necessário calcula-los sobre todo o componente da chave de 128 bits ou da chave resultante de 128 bits, mas nunca sobre uma parte da chave ou do componente da chave. Além disso, a chave resultante que estiver dentro do dispositivo deverá ser recombinada de acordo com os requisitos da PCI e padrões ANSI/ISO. O mesmo acontece para as chaves de comprimento triplo. É necessário utilizar todo o componente da chave de 192 bits ou a chave de 192 bits resultante para calcular os valores de verificação de chave.

Q 5 **Em quais condições o dispositivo pode permitir que as chaves criptográficas de texto simples de um único componente sejam carregadas via teclado?**

A *Nenhuma. O dispositivo não deve aceitar a entrada de chaves criptográficas de texto simples de componente único via teclado. Os componentes da chave de comprimento completo e as chaves criptografadas podem ser carregados via teclado se os requisitos que regem as funções suscetíveis forem atendidos* ***(PCI B5, B6)*** *.*

Q 6 **ISO 11568-2 *Cifras simétricas, seu gerenciamento de chaves e ciclo de vida* e ANSI X9.24-1 *Gerenciamento de chaves simétricas para serviços financeiros de varejo, parte 1: como utilizar técnicas simétricas* estipulam que nenhuma chave existente no dispositivo de origem das transações deve existir em nenhum outro dispositivo desse tipo. Isso se aplica a todas as chaves secretas e privadas contidas no dispositivo?**

A *A intenção do requisito é que o comprometimento de uma chave em um dispositivo de origem da transação (por exemplo, um dispositivo de EPP ou POS) não afete a segurança de outro dispositivo semelhante. A este respeito, toda chave privada ou secreta presente ou utilizada, de outra forma, nos dispositivos de origem da transação deve ser exclusiva desse dispositivo, salvo pelo acaso. Isso inclui chaves utilizadas para criptografia de PIN, validação de firmware, controle de mensagens de exibição ou proteção de qualquer uma dessas mesmas chaves durante o carregamento no dispositivo ou armazenamento dentro do dispositivo. Lembre-se de que cada uma dessas funções exige a sua própria chave exclusiva.*

Este requisito se aplica a chaves controladas ou originadas pelo fornecedor e pelo adquirente. Não estão inclusas aqui as chaves públicas presentes ou utilizadas pelo dispositivo.

Q 7 **Os dispositivos podem aceitar o carregamento remoto de chaves secretas do adquirente empregando técnicas assimétricas. Todo protocolo de carregamento remoto de chaves deve disponibilizar um mecanismo para minimizar a probabilidade de ataques man-in-the-middle, onde um dispositivo pode ser falsificado para comunicação com um host ilegítimo. Um mecanismo comum é "vincular" o host ao dispositivo, de modo que o dispositivo não aceite comunicações que não tiverem sido assinadas digitalmente pelo host legítimo e autenticadas pelo dispositivo. Há diversos cenários onde pode tornar-se necessário mudar os hosts e/ou os pares de chaves assimétricas do host. Ao desvincular de um dispositivo os pares de chaves do host, o que pode ser feito de forma manual no dispositivo ou remota via comando autenticado e assinado digitalmente, há alguma disposição especial a ser feita?**

A *No recebimento de uma instrução válida para desvincular um par de chaves do host de um dispositivo, o dispositivo deve zeroizar todas as chaves secretas de qualquer entidade adquirente atual. A maioria dos cenários que envolve a necessidade de desvincular um host é oriunda de mudanças na entidade adquirente. Porém, em todos os casos, o dispositivo deve ser inicializado com novas chaves secretas da entidade adquirente antes de recolocar o dispositivo em operação.*

Q 8 **O TR-31 define três chaves. Uma chave de proteção de bloco de chaves (KBPK), uma chave de criptografia de bloco de chaves (KBEK) e uma chave de MAC de bloco de chaves (KBMK). A KBPK é usada para calcular a KBEK e a KBMK. A KBPK pode ser usada para qualquer outra finalidade?**

A *Não. Para atender ao requisito que estabelece que a chave seja usada para um único propósito, conforme definido na ANSI X9.24, a chave de proteção do bloco de chaves deve ser utilizada exclusivamente para calcular a KBEK e a KBMK, e não deve ser utilizada para nenhuma outra finalidade. Somente a KBPK é utilizada para gerar a chave KBEK e KBMK. Nenhuma outra chave é utilizada para esse fim.*

Q 9 **Será necessário empregar o TR-31, ou uma metodologia equivalente, sempre que uma chave simétrica for baixada de um host remoto criptografado por uma chave simétrica compartilhada. Há alguma outra circunstância em que o TR-31 ou uma metodologia equivalente se aplique ou não se aplique?**

A *Os dispositivos deverão aceitar o TR-31 ou outra metodologia equivalente para carregamento de chaves sempre que for realizado o carregamento de uma chave simétrica criptografada por outra chave simétrica. Isso se aplica quando as teclas simétricas são carregadas manualmente (ou seja, via teclado), por meio de um dispositivo de injeção de chave ou de um host remoto. Não se aplica quando o carregamento das chaves simétricas de texto não criptografado ou seus componentes é realizado empregando técnicas padrão de controle duplo.*

Q 10 **Em apoio à conversão de dispositivos implementados para o uso do TR-31, o status de uma chave carregada anteriormente para outra finalidade, tal como uma KEK, pode ser redefinido para chave de proteção do bloco de chave do TR-31?**

A *Não. O carregamento da chave em uma abertura (registro) deve definir a abertura para a sua devida função. Se a função da abertura for alterada, ou se uma nova tecla de texto não criptografado for carregada na abertura, sem autenticação, via controle duplo, todas as outras chaves no dispositivo (ou pelo menos todas as chaves que foram previamente protegidas pela chave que estava anteriormente na abertura) deverão ser apagadas. Este mecanismo ajuda a garantir que o dispositivo não possa ser ocupado para fins ilegítimos.*

Q 11 **Maio (atualização) de 2018: é obrigatório ter o TR-31 ou o suporte equivalente como opção para qualquer dispositivo que permita o carregamento de chaves simétricas, criptografadas por outra chave simétrica, como uma opção de configuração. Para implementar o TR-31 ou equivalente nos dispositivos que estão implementando atualmente uma outra metodologia simétrica que não o TR-31, quais características o dispositivo deve ter para permitir essa migração?**

A *O dispositivo deve aplicar o seguinte, caso pertinente:*

- *A conversão de uma metodologia menos segura (diferente do TR-31 ou não equivalente ao TR-31) para uma metodologia mais segura (TR-31 ou equivalente) deve ser irreversível.*
- *É necessário inserir a KBPK de texto simples (ou equivalente), via teclado, como dois ou mais componentes e exigir o uso de pelo menos duas senhas/códigos de autenticação. As senhas/códigos de autenticação devem ser inseridos via teclado ou transmitidos criptografados para o dispositivo.*

  Essas senhas/códigos de autenticação devem ser exclusivos por dispositivo (e por guardião), salvo pelo acaso, ou se forem o padrão do fornecedor, eles devem ter uma data de vencimento pré-estabelecida e forçar a mudança após o primeiro uso. As senhas/códigos de autenticação que são exclusivos por dispositivo podem ser alterados opcionalmente pelo adquirente, mas essa ação não é obrigatória. As senhas/códigos de autenticação devem ter pelo menos sete caracteres.

  A entrada de componentes de chaves sem o uso de pelo menos duas senhas/códigos de autenticação separados provoca a zeroização das chaves secretas pré-existentes do adquirente, ou seja, a invocação da função/comando de carregamento de chaves provoca a zeroização antes do carregamento real da nova chave. Para os dispositivos que aceitam hierarquias de chaves de vários adquirentes (por exemplo, dispositivos multiadquirentes), somente a hierarquia (por exemplo, chave mestra do terminal (TMK) específica e chaves habituais) associada à chave que está sendo carregada deve ser zeroizada. Em todos os casos, os valores de autenticação (senhas, códigos de autenticação ou semelhantes) de cada usuário em um determinado dispositivo devem ser diferentes para cada usuário.

- *O carregamento de uma KBPK de texto simples (ou equivalente) por meio de um carregador de chaves deve ser feito pelo emprego de um controle duplo e pela exigência do uso de duas ou mais senhas/códigos de autenticação antes da injeção da chave. Essas senhas/códigos de autenticação são inseridos diretamente via teclado do dispositivo pertinente ou são transmitidos criptografados para o dispositivo e devem ter pelo menos sete caracteres de comprimento. Essas senhas/códigos de autenticação devem ser exclusivos por dispositivo (e por guardião), salvo pelo acaso, ou se forem o padrão do fornecedor, eles devem ter uma data de vencimento pré-estabelecida e forçar a mudança após o primeiro uso. Não é permitido usar, em hipótese alguma, chaves de texto simples ou seus componentes via conexão de rede.*

  A injeção de chaves secretas de texto simples ou seus componentes, quando o próprio dispositivo receptor não exige o uso de pelo menos duas senhas/códigos de autenticação para injeção, provoca a zeroização das chaves secretas pré-existentes do adquirente. Para os dispositivos que aceitam hierarquias de chaves de vários adquirentes (por exemplo, dispositivos multiadquirentes), somente a hierarquia (por exemplo, chave mestra do terminal (TMK) específica e chaves habituais) associada à chave que está sendo carregada deve ser zeroizada. Em todos os casos, os valores de autenticação (senhas, códigos de autenticação ou semelhantes) de cada usuário em um determinado dispositivo devem ser diferentes para cada usuário.

- *O carregamento da KBPK no dispositivo criptografado por uma chave simétrica equivalente, diferente do TR-31 ou não equivalente ao TR-31, é proibido. No entanto, a KBPK pode ser carregada por meio de técnicas assimétricas.*

Q 12 A Orientação do DTR B9 afirma: "o dispositivo pode incluir mais de um esquema de troca de chaves e armazenamento em conformidade. Isso não pressupõe que o dispositivo deva aplicar o TR-31 ou um esquema equivalente, mas que deve ser capaz de implementar tal esquema como opção de configuração." Se o uso do TR-31 como mecanismo de troca de chaves for opcional, deverá haver uma alteração explícita da configuração do dispositivo para ativar/desativar o TR-31 como o esquema "ativo" para troca de chaves?

A *Sim, é obrigatório haver uma mudança de configuração explícita. A mudança é considerada um serviço suscetível e deve atender aos requisitos do B5, proteção de serviços suscetíveis.*

Q 13 Agosto de 2011: quando o dispositivo é convertido ou implementa, de outra forma, o TR-31, a conversão deve ser unilateral. Nos dispositivos com suporte a várias hierarquias de chaves independentes, como aquelas projetadas para aceitar vários adquirentes, a implementação se aplica a todas as hierarquias de chaves no dispositivo?

A *Não. Os dispositivos compatíveis com várias hierarquias independentes podem implementar o TR-31 (ou equivalente) a cada hierarquia.*

Q 14 Há alguma restrição sobre como a chave mestra do terminal é carregada no dispositivo?

A *A chave mestra inicial do terminal (TMK) deve ser carregada no dispositivo empregando técnicas assimétricas de carregamento de chaves ou técnicas manuais, por exemplo, o teclado do dispositivo, cartões IC, dispositivo de carregamento de chaves etc. O carregamento subsequente da chave mestra do terminal pode empregar técnicas assimétricas, técnicas manuais ou a TMK existente para criptografar a TMK substituta para download. As chaves não podem ser recarregadas por nenhuma metodologia em caso de comprometimento do dispositivo, que deve ser retirado do uso.*

Q 15 Alguns dispositivos permitem o uso de uma função de dados de descriptografia que, se não for controlada, poderá permitir a livre emissão de informações confidenciais, tais como chaves ou PINs. Como o dispositivo deve impedir a saída de dados confidenciais?

A *Ele deve ser gerenciado por pelo menos uma dessas cinco técnicas:*

- *As informações de uso de qualquer chave baixada devem ser vinculadas de forma criptografada ao valor da chave por meio de métodos aceitos, e o dispositivo deve impor que a chave seja usada exclusivamente para o uso pretendido.*
- *A inclusão de um novo tipo de chave (entrada) após a configuração inicial do dispositivo provoca a zeroização de todas as outras chaves secretas. Os dispositivos que aceitam técnicas de distribuição remota de chaves com técnicas assimétricas só devem aceitar o uso dessas técnicas para o carregamento de TMKs. O emprego de técnicas de distribuição remota de chaves para chaves habituais (por exemplo, PIN, dados, MAC etc.) não deve ser aceito, salvo se as informações de uso das chaves estiverem criptograficamente vinculadas a cada chave individual.*
- *Os tipos de chave de dados baixados não devem ser aceitos pelo dispositivo, salvo se forem criptografados por uma chave mestra de terminal diferente das chaves suscetíveis, como os tipos de chaves PEK ou MAC.*
- *O dispositivo não oferece nenhum suporte para descriptografar dados ou função semelhante.*
- *O dispositivo deve garantir que, em hipótese alguma, chaves com diferentes finalidades tenham o mesmo valor. Essa exigência deve ser mantida até que o dispositivo seja desativado (ou até que as TMKs aplicáveis mudem).*

Q 16 Maio (atualização) de 2018: as chaves secretas ou seus componentes podem ser usados para outros fins, tais como senhas/códigos de autenticação para permitir o uso de serviços suscetíveis?

A *Não. O uso de chaves secretas ou seus componentes para outros fins viola a exigência de que as chaves sejam usadas para o seu propósito exclusivo, por exemplo, criptografia de chaves ou criptografia de PIN etc.*

Q 17 Setembro (atualização) de 2016: os requisitos de segurança de PIN da PCI estipulam que todas as chaves armazenadas nos dispositivos criptográficos utilizados (ou que poderiam ser utilizados) para qualquer fim criptográfico, em conexão com a aquisição de dados de PIN removidos do serviço, sejam destruídas. Se for necessário para cumprir o disposto acima, o dispositivo deverá ser fisicamente destruído para que não possa ser recolocado em serviço ou permitir a divulgação de quaisquer dados ou chaves secretas. Isso se aplica exclusivamente às chaves simétricas?

A *Não. Aplica-se a todas as chaves secretas ou privadas usadas pelo dispositivo para criptografia de PIN, validação de firmware, controle de mensagens de exibição ou para proteção de qualquer uma dessas mesmas chaves durante o carregamento no dispositivo ou armazenamento dentro do dispositivo, incluindo as chaves privadas utilizadas em conexão com a distribuição de chaves remotas por meio de técnicas assimétricas. Este requisito se aplica a chaves controladas ou originadas pelo fornecedor e pelo adquirente. Não estão inclusas aqui as chaves públicas presentes ou utilizadas pelo dispositivo.*

O fornecedor deve disponibilizar instruções para desativação, e mecanismos associados, para tornar essas chaves irrecuperáveis por adversários, de forma que possa ser verificada por parte do laboratório de avaliação. Essas técnicas incluem, entre outras:

- *Comandos de menu específicos para zeroizar chaves armazenadas*
- *Indução de eventos de adulteração para zeroização dessas chaves*
- *Criptografia por chave de força igual ou maior, que esteja ela mesma zeroizada, ou seja, somente os criptogramas das chaves protegidas podem ser recuperados.*

Q 18 **Maio de 2018: a ANSI TR-34 descreve dois protocolos para implementar a distribuição de chaves simétricas empregando técnicas assimétricas. As duas técnicas são descritas como método com duas passagens e método com uma passagem e devem ser empregadas da seguinte forma:**

- **O método com duas passagens é apropriado para onde o POI e o servidor de distribuição de chaves (KDH) puderem se comunicar em tempo real. Ele emprega valores de uso único (nonces) para impedir ataques repetidos.**
- **O método de uma passagem é apropriado para ambientes onde a comunicação em tempo real do POI e do KDH não será possível,ou seja, o POI não pode iniciar a sequência de mensagens do protocolo criptográfico. Nesses ambientes, o KDH vai gerar a mensagem criptográfica que poderá ser transportada para o POI por meio de canais não confiáveis e não em tempo real. Ele inclui o uso de carimbos de data e hora em vez de valores de uso único aleatórios para impedir ataques repetidos.**

A inserção de chaves mal intencionadas em dispositivos de POI por um segundo KDH, sob o mesmo PKI, será possível onde o POI já tiver trocado as credenciais com um primeiro KDH. A fim de impedir este ataque, a associação (ou método equivalente conforme observado na orientação do DTR B9) é necessária para todos os dispositivos de POI, além de ser um pré-requisito para os protocolos de troca de chave de duas e uma passagens.

Os dispositivos POI são obrigados a aceitar ambos os métodos?

A *Não, o dispositivo pode aceitar apenas um deles. O fornecedor deve descrever na política de segurança do dispositivo, que é publicada no site da PCI, se o dispositivo aceita somente um dos métodos ou ambos, e os ambientes e circunstâncias sob as quais é apropriado implementar os métodos aceitos.*

Q 19 **Setembro de 2020: O Requisito de segurança d3 PIN 18-3 exige a implementação de blocos de chave. Os métodos interoperáveis incluem os que estão definidos no ASC X9 TR-31 e ISO 20038. O requisito permite também qualquer método equivalente, pelo qual o método equivalente inclui o vínculo criptográfico das informações sobre o uso de chaves ao valor da chave, empregando os métodos aceitos. Como os métodos equivalentes são determinados?**

A *Métodos equivalentes devem ser sujeitados a uma avaliação por parte de peritos independentes e esta avaliação deve estar disponível publicamente para avaliação por parte de outros profissionais da área:*

- *A avaliação feita pelo perito independente deve incluir provas de que, no método equivalente, a chave criptografada e seus atributos no bloco de chaves têm proteção de integridade, de modo que computação inviabilize a possibilidade de que a chave seja usada se a chave ou seus atributos tiverem sido modificados. As modificações incluem, entre outras:*
  - *Alteração ou substituição de quaisquer bits nos atributos ou na chave criptografada*
  - *Troca de quaisquer bits do bloco de chaves protegido com bits de outra parte do bloco*

- *O especialista independente deve ser qualificado por meio de uma combinação de educação, treinamento e experiência em criptografia, para realizar avaliações técnicas objetivas que sejam independentes de quaisquer vínculos com fornecedores e interesses especiais. Veja abaixo a definição mais detalhada sobre o especialista independente.*
- *O laboratório de PTS confirmará que todos os fornecedores de dispositivos que implementaram essa metodologia o fizeram seguindo todas as diretrizes da referida avaliação e análise por outros profissionais da área, incluindo todas as recomendações para o gerenciamento de chaves associadas.*

O especialista independente tem todas as qualificações a seguir:

- *Uma ou mais credenciais profissionais aplicáveis à área, por exemplo, qualificações no nível de PhD em uma disciplina relevante ou certificação governamental em criptografia por um órgão autorizado (por exemplo, NSA, CES ou GCHQ) e*
- *Tem dez ou mais anos de experiência no assunto em questão e*
- *Assina um código de conduta ética e estaria sujeito a processos de conformidade ética, se necessário, e*
    - *Publicou pelo menos dois artigos em publicações revisadas por outros profissionais da área sobre o assunto em questão, ou*
    - *Reconhecimento por seus colegas na área (p. ex., reconhecido como pesquisador ou pesquisador destacado (Fellow ou Distinguished Fellow), ou reconhecimento profissional semelhante por um órgão apropriado, como ACM, BCS, IEEE, IET, IACR).*

A independência exige que a organização não esteja sujeita a controle, restrição, modificação ou limitação por uma determinada fonte externa. Especificamente, a independência exige que uma pessoa, empresa ou corporação que atue como criptologista ou especialista semelhante para mais de uma empresa cliente não seja funcionário regular dessa empresa, não trabalhe exclusivamente para uma empresa e, quando for remunerado, que o seja em cada caso atribuído, por tempo consumido e despesas incorridas.

Q 20 Setembro de 2020: os dispositivos devem ser compatíveis com a metodologia de derivação de chaves ANSI TR-31 para chaves TDES e, para chaves AES, devem ser aceitar a metodologia TR-31 ou ISO 20038. Em ambos os casos, podem-se utilizar métodos equivalentes quando sujeitos à avaliação por parte de peritos independentes e a referida revisão estiver disponível publicamente, conforme descrito. Quais características aplicadas no TR-31 e ISO 20038 devem ser levadas em consideração para determinação da equivalência?

A *A "equivalência" deve ser demonstrada no contexto das provas de segurança. O método equivalente deve, comprovadamente, realizar as funções de integridade das chaves, restringindo o uso das chaves, evitando a reutilização e mantendo o sigilo delas. Especificamente, um esquema de blocos de chaves equivalente deve oferecer, no mínimo, as seguintes propriedades:*

a) *Deve impedir que o carregamento de PIN, MAC e/ou chaves de dados, ou de quaisquer chaves utilizadas para gerenciá-las dentro da hierarquia de chaves, seja usado para outra finalidade. IPEK, KEKs e chaves de derivação devem ser identificados exclusivamente quando aceitas.*
b) *Deve impedir a determinação do comprimento das chaves variáveis.*
c) *Deve garantir que a chave somente possa ser usada em algoritmo específico (tal como o TDES ou o AES, mas não para ambos).*
d) *Deve garantir que a chave modificada ou um bloco de chaves possa ser rejeitado antes do uso, independentemente da utilidade da chave após a modificação. A modificação inclui a alteração de quaisquer bits da chave, bem como a reordenação ou a manipulação de chaves de DES exclusivas individuais dentro do bloco de chave de TDES.*
e) *Se forem aceitos diversos formatos de bloco de chaves, com alguns deles oferecendo as proteções acima e outros não, será necessário que sejam legíveis por humanos, no bloco de chaves, antes do carregamento/utilização do formato implementado. Por exemplo, observando os comandos enviados para o dispositivo.*
f) *Ele deve aceitar todos os algoritmos simétricos implementados pelos dispositivos, que devem usar os blocos de chave.*
g) *Se houver compatibilidade com algoritmos assimétricos, o tipo do algoritmo, os formatos do teclado e preenchimento e os formatos de assinatura deverão estar identificados no bloco de chaves.*
h) *Os modos de operação devem ser os aprovados pelo NIST, com chaves separadas, usadas para confidencialidade e autenticidade. Nenhuma das chaves utilizadas deve estar relacionada de forma reversível.*

O bloco de chaves equivalente pode, opcionalmente, aceitar outras características, tais como:

i. *Um número de versão de chave que impeça o uso de chaves mais antigas ou vencidas.*
ii. *Compatibilidade com chave 'direcional' (chaves unidirecionais), para que seja possível identificar a chave MAC como "somente para verificar" ou a chave de dados como "somente para criptografar".*
iii. *Compatibilidade para propósitos com chaves que não sejam PIN, MAC e dados.*
iv. *Suporte para TDES e AES (quando os dispositivos que implementam os blocos de chaves aceitarem somente um desses algoritmos, somente transitórios, os novos dispositivos devem ser compatíveis com AES).*

v. *Implementar controles de confidencialidade sobre todos os metadados de chaves que não forem o comprimento da chave.*

vi. *Suporte para algoritmos assimétricos.*

Q 21 **Setembro de 2020: os dispositivos de POI devem, obrigatoriamente, ser compatíveis com a metodologia de derivação de chaves ANSI TR-31 para chaves TDES e, para chaves AES, devem ser compatíveis com a metodologia TR-e/31 ou ISO 20038. TR-31 e ISO 20038 são métodos para colocar as chaves em pacotes (os blocos de chave) para transporte ou armazenamento, no entanto, eles fazem uso de mecanismos simétricos para isso e, para o transporte de chaves, exigem uma chave de troca de chaves simétricas pré-compartilhada para uso como chave de proteção de bloco de chaves. Se não for estabelecida previamente uma chave simétrica com um dispositivo de POI para distribuição remota de chaves, e forem usados métodos assimétricos, a compatibilidade com uma metodologia de bloco de chaves será obrigatória?**

A *Sim. É necessário utilizar um método como o ASC X9 TR 34: método interoperável para distribuição de chaves simétricas por meio de técnicas assimétricas: Parte 1 — Utilização de transporte com chave unilateral para chaves públicas baseadas em fatoração. No TR-34, semelhante ao TR-31 e ISO 20038, o bloco de chaves é composto por três partes:*

- *O cabeçalho do bloco de chaves (KBH) que contém informações do atributo sobre a chave e o bloco de chaves*
- *Os dados confidenciais que estão sendo trocados/armazenados*
- *O método de vínculo do bloco de chaves.*

No entanto, o TR-34 emprega métodos assimétricos para o Método de vínculo de blocos de chaves, em vez dos métodos simétricos utilizados no TR-31 ou ISO 20038, que exigem que a chave simétrica tenha sido previamente trocada entre o dispositivo de POI e o KDH.

Requisitos B10 de POI

Q 1 **Junho (atualização) de 2016: o Requisito B10 afirma que qualquer método utilizado para produzir textos criptografados, que tenha como base modos de operação "fora do padrão" (por exemplo, modo de criptografia baseado em Feistel (FFX) para preservação de formato) deve ser aprovado por, pelo menos, uma organização de avaliação de segurança independente (por exemplo, um órgão de normalização) e submetido à avaliação de peritos independentes. Como esse requisito é atendido quando o método não faz parte de uma norma publicada?**

A *Todos os dados de conta devem ser criptografados utilizando, exclusivamente, algoritmos de criptografia aprovados pelo ANSI X9 ou ISO (por exemplo, AES, TDES). Além disso, o modo de operação utilizado deve:*

1. *Estar descrito na ISO/IEC 10116:2006 (ou equivalente) e seguir as diretrizes de preenchimento seguro.*

OU

2. *Existir em um projeto de norma de um organismo de normalização aplicável à indústria de pagamentos financeiros, ou seja, ANSI, ISO ou NIST*

E

3. *Ser submetido a uma avaliação por parte de peritos independentes e a referida avaliação estar disponível publicamente e ser avaliada pelo laboratório de avaliação de PTS da PCI.*

A avaliação por parte de um perito independente deve incluir provas de que este FPE oferece proteção contra a "recuperação de mensagens", conforme definido em Bellare, M., Ristenpart, T., Rogawway, P., & Stegers, T. (2009, agosto). Criptografia de preservação de formato. Em áreas específicas na criptografia (págs. 295 a 312). Springer Berlin Heidelberg (https://eprint.iacr.org/2009/251.pdf).

O perito independente deve ser qualificado por meio de uma combinação de educação, treinamento e experiência em criptografia, para realizar avaliações técnicas objetivas que sejam independentes de quaisquer vínculos com fornecedores e interesses especiais. Veja a definição mais detalhada sobre o especialista independente no glossário.

O laboratório de PTS confirmará que o fornecedor do dispositivo implementou a solução de FPE seguindo todas as diretrizes da referida avaliação e análise por outros profissionais da área, incluindo todas as recomendações para o gerenciamento de chaves associadas.

Requisitos B12 de POI

Q 2 O dispositivo pode usar uma chave de criptografia de chaves para criptografar ou descriptografar informações de marcação da chave junto com uma chave?

A *Sim, as informações associadas da marcação da chave, como o algoritmo, o vencimento das chaves, seu uso ou o MAC da chave podem ser criptografadas ou descriptografadas junto com a chave utilizando uma chave de criptografia de chaves. A chave e sua marcação são vinculadas por um modo de encadeamento de criptografia, conforme definido na IS0 10116.*

Requisitos B15 de POI

Q 1 Qual é a definição de "unidade criptográfica"?

A *A unidade criptográfica é o microprocessador que criptografa o PIN block. Esse processador está sujeito* aos *requisitos do dispositivo da PCI* e, *portanto, é considerado seguro quando está dentro de um dispositivo considerado em conformidade. Isso significa que é permitido utilizar um microcontrolador de uso geral desde que esteja dentro de um dispositivo considerado em conformidade com os requisitos do dispositivo da PCI.*

Q 2 É permitido utilizar um diodo emissor de luz (LED) controlado exclusivamente pelo criptoprocessador, como indicação ou solicitação para a entrada do PIN?

A *Não. Os titulares de cartões esperam que a solicitação do PIN seja exibida na mesma tela que as outras mensagens. Se isso não acontecer, há uma possibilidade maior de os titulares de cartões serem enganados.*

Q 3 A exibição de dígitos do PIN de texto simples pelo dispositivo se qualificaria como prova de adulteração?

A *Não. O titular do cartão pode não saber o comportamento típico de um determinado dispositivo e pode não reconhecer que o dispositivo está violando o Requisito B3.*

Q 4 **Se o terminal contar com uma tela sob seu controle e um teclado com a sua própria tela, a unidade criptográfica do dispositivo deverá controlar ambas as telas?**

A *Sim. Se um único dispositivo tiver duas telas que poderiam solicitar dados ao titular do cartão, ambas seriam regidos pelo B15. Isso significa que o terminal e o teclado são um único dispositivo, que deve atender aos requisitos da PCI.*

Q 5 **As chaves criptográficas utilizadas para atualizar as instruções na tela devem ser gerenciadas de acordo com os princípios de controle duplo e de conhecimento dividido, e nenhuma chave secreta ou privada utilizada deve ser exibida na parte transparente e externa do dispositivo criptográfico seguro. Os dados de autenticação utilizados para ativar o uso de uma chave de assinatura ou de codificação de autenticação de mensagens podem percorrer ambientes desprotegidos, por exemplo, a RAM desprotegida de um computador?**

A *Os dados de autenticação podem aparecer na parte transparente externa do dispositivo criptográfico seguro. No entanto, o fornecedor deve disponibilizar instruções ao laboratório para uso de uma sala segura, PC dedicado, implementação de técnicas de controle duplo, procedimentos de inspeção de equipamentos etc.*

Q 6 **Quais requisitos de registro devem ser atendidos pelo dispositivo criptográfico seguro, de acordo com o B15?**

A *Os registros devem disponibilizar material comprovativo suficiente para demonstrar ao laboratório que existem técnicas e mecanismos de controle especificados pelo fornecedor.*

Q 7 **Maio (atualização) de 2018: os tokens de autenticação de USB ou cartões inteligentes podem ser considerados como dispositivos criptográficos seguros, necessários para impor o controle duplo de acordo com o B15?**

A *O uso de tokens duplos, por si só, não atenderia ao requisito. Seria necessário que os tokens aplicassem o uso de senhas/códigos de autenticação, e teriam que contar com segurança para proteger seus conteúdos.*

Q 8 **Maio de 2011: se o dispositivo estiver em conformidade com o B15, quais são os requisitos para controlar as atualizações dessas instruções?**

A *O B15 é avaliado quando o dispositivo utiliza atualizações de firmware para controlar a mudança das instruções da tela. Portanto, a atualização das instruções para os dispositivos que apresentam conformidade com o B15 exige a criação de uma nova versão do firmware e uma consequente mudança no número da versão do firmware do PED.*

Não é permitido a existência de instruções controladas pelo fornecedor atualizadas de forma independente do firmware, sem a geração de uma nova versão do firmware. É permitido que as atualizações das instruções façam uso de uma chave criptográfica separada para isso, utilizada para outras atualizações de firmware, no entanto qualquer método de atualização separado deve ser avaliado pelo laboratório para confirmar a sua conformidade com os Requisitos E2 e B2. Em todos os momentos, as chaves criptográficas utilizadas para atualizar instruções e o firmware devem diferir daquelas utilizadas para atualizar códigos não relacionados ao firmware, como aplicativos.

Q 9 **Maio de 2011: se o dispositivo estiver em conformidade com o B15, significa que preciso reenviar o dispositivo para avaliação pelo laboratório sempre que mudar as instruções?**

A *Se houver caracteres curinga adequados na lista de versões do firmware para acomodar as novas versões das instruções que foram revisadas anteriormente e confirmadas como sendo adequadas por um laboratório da PCI, não será necessário que um laboratório da PCI avalie cada uma das alterações.*

Q 10 **Maio de 2011: o Requisito B15 não especifica nenhuma possibilidade mínima de ataque. Quais são os requisitos sobre a segurança física dos dispositivos, que permitem que as instruções na tela sejam atualizadas por terceiros utilizando controles baseados em criptografia?**

A *Todas as instruções que puderem ser utilizadas para solicitar a entrada de dados em texto simples pelo titular do cartão devem ser protegidas contra um potencial de ataque de pelo menos 18 pontos da PCI, com um mínimo de 9 para exploração. Isso inclui instruções que possam ser atualizadas por terceiros com controles baseados em criptografia.*

Q 11 **Março de 2015: os teclados numéricos do PIN, projetados para uso nos caixas eletrônicos, geralmente aceitam o estado seguro (criptografa os dados inseridos) e não seguro. A transição entre os estados exige autenticação?**

A *Sim. É necessário empregar os mecanismos criptográficos de acordo com o Apêndice D dos requisitos de teste derivados do POI. Especificamente:*

- *É obrigatório ter um canal seguro entre a interface do teclado numérico do PIN e o controlador (caixa automático) para controlar mudanças entre o PIN e os modos de entrada de dados de texto simples*
- *Para telas sensíveis ao toque, o gerenciamento dos "botões" do teclado é feito de forma segura, para evitar a determinação do PIN do cliente pela exploração de possíveis diferenças no teclado exibido e a organização dos botões numéricos na interface de toque.*

Isso não significa que o dispositivo deva forçar a implementação, mas sim que deve oferecer suporte para a implementação.

Requisitos B17 de POI

Q 1 **Agosto de 2011: o sistema operacional do dispositivo deve conter somente os componentes necessários e deve ser configurado de forma segura e executado com privilégio mínimo. O que é considerado "sistema operacional" para a PCI?**

A *No âmbito do PTS da PCI, qualquer software subjacente que preste serviços para execução de códigos no dispositivo é considerado parte do sistema operacional. Exemplos de tais serviços incluem inicialização e reinicialização do sistema (boot), camadas de abstração de hardware, gerenciamento de memória, multitarefa, primitivos de sincronização, sistemas de arquivos, drivers de dispositivos e pilhas de rede. Os serviços que oferecem segurança ou podem afetar a segurança são, além disso, considerados firmware.*
Os sistemas operacionais podem variar de bibliotecas de camadas de abstração de hardware e micronúcleos incorporados a sistemas operacionais complexos e com vários usuários.

Requisitos B18 de POI

Q 1 **Quais são os métodos aceitos para atender a esse requisito?**

A *O uso de técnicas aceitas para gerenciamento de chaves normalmente satisfaz este requisito:*

- *Quando se utiliza a técnica de gerenciamento de chaves mestras/sessão, essa exigência é cumprida porque a substituição das chaves exige que o invasor conheça a chave mestra contida no dispositivo.*
- *Este requisito é satisfeito quando se utiliza a técnica de gerenciamento de chaves DUKPT porque as chaves do PIN são derivadas de informações secretas contidas no dispositivo.*

No entanto, quando o dispositivo se destina a aceitar vários adquirentes e o adquirente é selecionado pelo usuário (ou seja, comerciante pressionando um botão), o dispositivo deve confirmar que foi realizada a seleção do adquirente correto.

Q 2 **É permitido que um dispositivo compatível com várias hierarquias de chaves atenda ao B18 garantindo que aplicativos específicos só possam acessar chaves associadas a elas?**

A *Sim. É permitido desde que cada aplicativo somente possa acessar chaves de uma única hierarquia de chaves.*

Q 3 **Quais são os meios permitidos para a seleção de chaves criptográficas externas?**

A *As chaves podem ser selecionadas por meio do teclado do dispositivo, ou comandos enviados de outro dispositivo, como as caixas registradoras eletrônicas. Todos os comandos enviados de outro dispositivo devem ser autenticados criptograficamente para proteção contra ataques man-in-the-middle e de repetição.*

Q 4 **Se uma chave selecionada externamente não for a chave criptográfica utilizada para criptografar diretamente o PIN block, a autenticação dessa seleção será obrigatória?**

A *Se a seleção externa estiver associada à criptografia do PIN, a autenticação será aplicada. Por exemplo, seria necessário autenticar a seleção externa da chave mestra na qual uma chave de sessão será descriptografada para uso na criptografia do PIN block.*

Q 5 **É permitido que as chaves do PIN sejam selecionadas externamente, indiretamente, selecionando o adquirente se a seleção do adquirente for realizada com um comando autenticado criptograficamente? Supõe-se a existência de várias hierarquias de chaves relacionadas à criptografia do PIN em cada adquirente.**

A *Sim. Desde que haja um mecanismo que garanta que as chaves de cada adquirente estejam associadas exclusivamente a esse adquirente.*

Q 6 **Maio (atualização) de 2018: a seleção de chaves externas inclui a seleção realizada por servidores locais ou remotos. Em que circunstâncias os dispositivos que aceitam várias hierarquias de chaves não são obrigados a aplicar a autenticação de cada comando de seleção de chave externa?**

A *Se um aplicativo puder selecionar chaves de várias hierarquias de chaves, o dispositivo deverá impor a autenticação dos comandos usados para seleção de chaves externas. Se o dispositivo permitir que o aplicativo somente selecione chaves de uma única hierarquia, a autenticação do comando não será obrigatória.*

Opcionalmente, a autenticação não é obrigatória em nenhuma das duas circunstâncias a seguir:

- *As hierarquias de chaves para criptografia de PIN somente são estabelecidas diretamente pelo fornecedor em suas instalações seguras ou em uma instalação autorizada, operada por um terceiro, que normalmente execute o carregamento de chaves em nome do fornecedor e esteja registrado para tal de acordo com as regras aplicáveis da bandeira de pagamento; e, subsequente à saída da instalação, é fisicamente e/ou logicamente impossível carregar outras hierarquias de chaves sem retornar à instalação.*
- *Somente é permitido estabelecer as principais hierarquias de acordo com o Requisito B7. As novas hierarquias de chaves devem ser autenticadas usando controle duplo (senhas/códigos de autenticação) por meio do carregador de chaves ou diretamente pelo EPP ou PED do PDV. As atuais hierarquias de chaves podem ser substituídas sem o uso de autenticação se o carregamento resultar na zeroização das chaves secretas pré-existentes,ou seja, a invocação da função/comando de carregamento de chaves provoca a zeroização antes do carregamento real da nova chave. Além disso, as hierarquias de chaves existentes podem ser substituídas ou novas hierarquias de chaves podem ser estabelecidas empregando a distribuição remota de chaves por meio de técnicas assimétricas que estejam em conformidade com os Requisitos de segurança de PIN da PCI, Anexo A.*

Q 7 **Quando o B18 não se aplica aos dispositivos de instrução na tela controlados pelo adquirente?**

A *O B18 não se aplica aos dispositivos de instruções na tela B, controlados pelo adquirente, que não incluem comandos para seleção de chaves externas ou não podem conter várias chaves relacionadas à criptografia do PIN.*

Requisitos B20 de POI

Q 1 Junho (atualização) de 2015: a aprovação do dispositivo será afetada de alguma forma se o laboratório que avaliou a política de segurança for trocado pelo fornecedor?

A *A partir do V4, o conteúdo da política de segurança faz parte da avaliação do dispositivo pelo laboratório e constitui uma entrada integral na qual a aprovação do dispositivo se baseia. Os programadores seguem a política de segurança para garantir que não violem as condições de aprovação do dispositivo. Toda alteração à política de segurança, que afetar os requisitos de segurança do dispositivo, deve ser avaliada para que o dispositivo mantenha sua aprovação. Além disso, toda alteração nos recursos oferecidos pelo dispositivo que afetar as informações que devem, obrigatoriamente, estar contidas na política de segurança, deve estar refletida em uma atualização no documento da política de segurança indicada.*

Dependendo da natureza das alterações, isso pode se refletir nas atualizações (por exemplo, nos apêndices) de uma política de segurança atual ou como outras políticas de segurança publicadas no site. Em todos os casos, todas as versões dos produtos aprovados devem ser abordadas nas políticas de segurança publicadas no site da PCI.

Q 2 Outubro (atualização) de 2018: os Requisitos do laboratório de PTS da PCI proíbem que o laboratório de PTS crie qualquer documentação de fornecedor. Há algum caso em que um laboratório de PTS possa ajudar um fornecedor na criação da documentação?

A *Em alguns casos, o laboratório de PTS pode revisar a política de segurança para realizar edições na gramática, na formatação ou na ortografia de um dispositivo que estiver sob avaliação. Isso pode ser feito para ajudar o fornecedor a elaborar um documento que seja suficiente para ser enviado à PCI. Nesse caso, o laboratório de PTS oferecerá o seguinte como parte do envio do relatório de avaliação:*

- *Uma versão alterada, com mudanças marcadas da política de segurança editada, exibindo o texto original criado pelo fornecedor, bem como o texto atualizado.*
- *Uma cópia clara da política de segurança editada para publicação.*

Requisitos B21 de POI

Q 1 A ISO 9564 estipula que, se o PIN tiver que ser enviado ao cartão IC em forma criptografada, o dispositivo deverá criptografar o PIN com uma chave de criptografia autenticada do cartão IC e enviar o PIN criptografado ao cartão IC. Há alguma restrição sobre o carregamento de chaves por essa metodologia?

A *O dispositivo deve proteger a integridade de todas as chaves públicas (ICC, emissor aplicável e bandeira de pagamento) empregando as técnicas definidas na ISO 11568. Em todos os casos, a autenticação deverá ocorrer em um componente seguro do dispositivo, como o teclado do PIN ou ICCR. Isso inclui a autenticação das chaves públicas do ICC, bem como a chave pública do emissor associado na cadeia de certificados até a chave da bandeira de pagamento aplicável.*

Requisitos B23 de POI

Q 1 **Junho de 2012: a orientação afirma que o modo de criptografia é definido como sendo quando a criptografia do dispositivo do recurso dos dados da conta está ativada e operacional. O dispositivo pode expor todos ou alguns dados da conta livremente quando estiver no modo de criptografia?**

A *Sim, mesmo para os dispositivos que aceitam somente o modo de criptografia. Por exemplo, o dispositivo pode implementar listas de autorização autenticadas com criptografia para geração de dados da conta livremente, mesmo que essa lista de autorização faça com que todos os dados da conta sejam emitidos livremente. A ausência da lista de autorização faz com que todos os dados da conta sejam criptografados.*

Requisitos E2 de POI

Q 1 **Muitos dispositivos são projetados para que terceiros possam criar e carregar aplicativos. Os fornecedores geralmente permitem isso disponibilizando a terceiros as ferramentas necessárias para criar e carregar aplicativos. Como o fornecedor pode garantir que não será responsabilizado pelo controle do aplicativo?**

A *Se os aplicativos não forem considerados firmware, não será necessário que sejam controlados pelo fornecedor. O projeto do dispositivo deve impedir que os aplicativos afetem as funções e os recursos regidos pelos requisitos. São exemplos de funções que não devem ser influenciadas por aplicativos que "não são firmware": gerenciamento de chaves (seleção de chaves, autenticação de chaves, geração de chaves, carregamento de chaves etc.), autotestes, tempo entre criptografia de PIN blocks, acesso a serviços suscetíveis, limites de serviços suscetíveis, atualização e autenticação de firmware, resposta na ocorrência de adulteração etc.*

A alteração das instruções por parte de terceiros é um caso especial que pode ser afetada por aplicativos que não são firmware, desde que o POI do PCI B15 seja atendido.

Os aplicativos de SRED desenvolvidos por terceiros também são uma exceção. Devem atender a todos os critérios aplicáveis no módulo de SRED, incluindo todas as dúvidas frequentes associadas.