PROPOSTA DE PORTABILIDADE DE PSC
Autoria: AC Soluti

Problemática

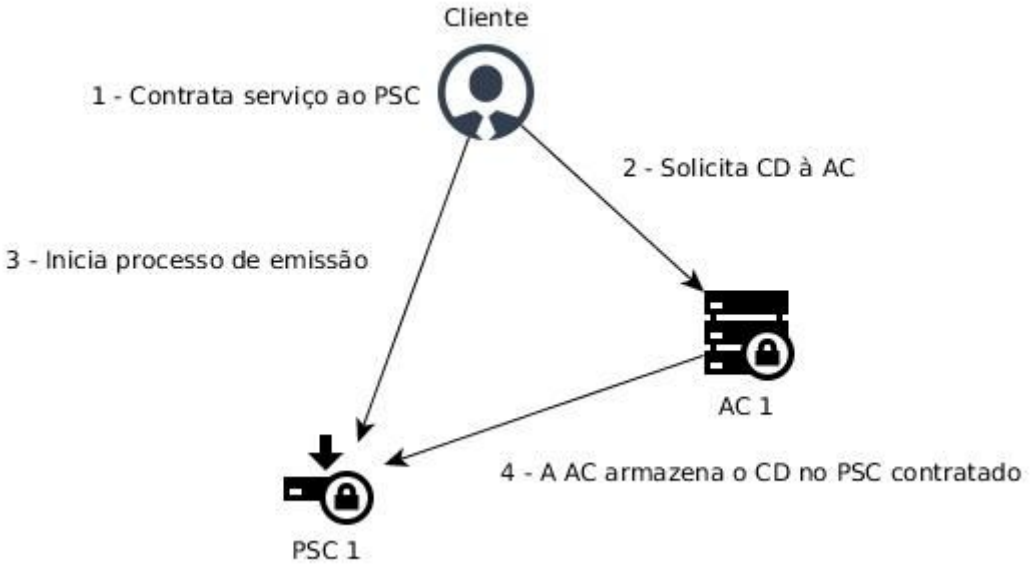
Entendemos que a exportação de chaves armazenadas em HSM apresenta uma vulnerabilidade desnecessária. Mesmo com a utilização de protocolos que suportam o processo de exportação, o controle da chave durante o processo apresenta riscos tanto para o titular quanto para o PSC que receberá as chaves exportadas. Nenhum controle externo é tão seguro quanto a fronteira criptográfica física e lógica de um HSM. Qualquer exportação que dependa de chaves de transporte que nasceram fora do próprio HSM é vulnerável.

Objetivo

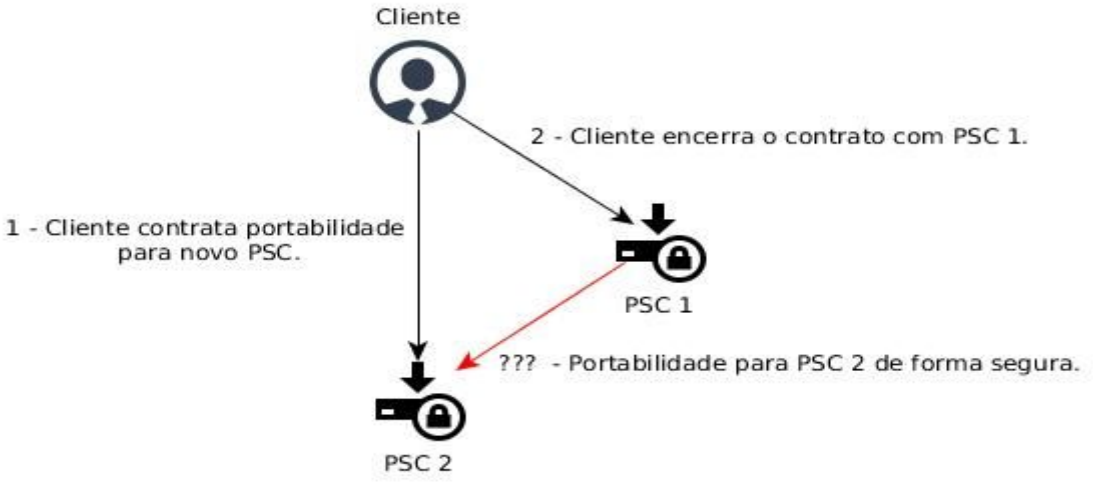
Esta proposta tem como objetivo permitir a portabilidade de um usuário (subscritor) entre diferentes PSC (Prestadores de Serviço de Confiança) mitigando o riscos apresentados. Esta proposta destina-se aos PSC de armazenamento de certificados digitais e não aos PSC de assinatura, verificação e guarda de documentos.

Cenário

Titular subscritor do serviço do PSC (**usuário**) contratou PSC1 (**PSC de origem**) para a guarda de sua chave, usada em um certificado digital emitido pela AC1 (**AC de origem**). Consideramos que o usuário contratou o PSC1. A AC1 foi contratada pelo próprio usuário ou pelo PSC1 para emissão do certificado. A emissão ocorreu após usuário comparecer a uma AR da AC1. A remuneração de cada parte (PSC1, AC1, AR) depende do modelo comercial, de livre negociação entre cada parte e entre o usuário.



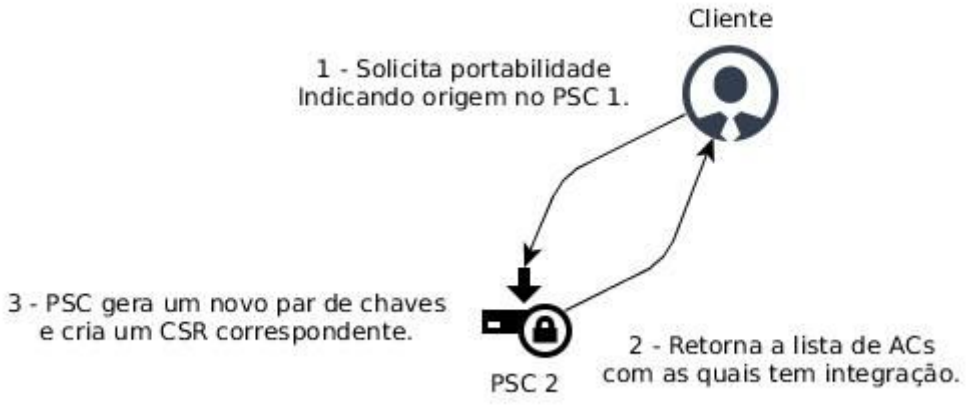
Em algum momento durante a validade do seu certificado digital, o usuário decide encerrar o contrato com o PSC1 e contratar o PSC2 (**PSC de destino**). A isso daremos o nome de **Portabilidade de PSC**. O usuário não terá que comparecer novamente a uma AR pois seu certificado digital emitido pela AC1 ainda está válido.



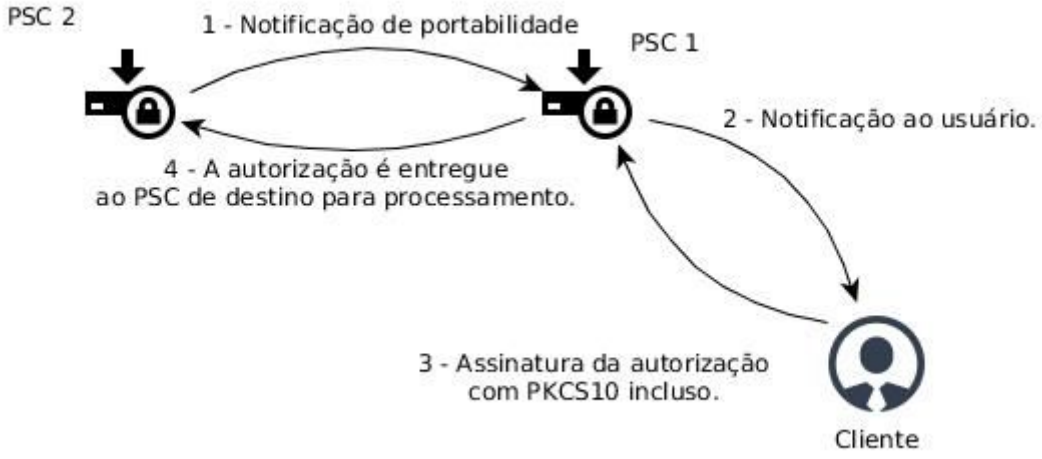
Proposta

Para que essa portabilidade seja possível, sem que a chave do tipo A3/A4 precise ser exportável, propomos que o usuário receba **uma nova chave (e novo certificado)**, da forma que descrevemos a seguir.

1. Ao contratar o PSC2, o usuário deverá informar que quer fazer a portabilidade de PSC, indicando que seu certificado digital válido está atualmente no PSC1.
2. PSC2 apresenta uma lista de AC (com as quais o PSC2 tem contrato/convênio) para que o usuário escolha em qual deseja emitir seu novo certificado (podendo inclusive ser a própria AC1).
3. PSC2 procede com geração da nova chave do usuário e geração do CSR/PKCS#10.



4. PSC2 (destino) aciona PSC1 para solicitar assinatura da autorização de portabilidade.
    a. PSC1 notifica usuário a respeito do pedido de portabilidade, para que o usuário faça a assinatura da autorização.
    b. Usuário faz a assinatura digital da autorização após autenticação no PSC1.
    c. A autorização de portabilidade deverá conter o CSR/PKCS#10 da nova chave.
    d. PSC1 devolve para o PSC2 a autorização assinada.



5. PSC2 aciona a AC2 (**AC de destino**) para iniciar o processo de emissão automática de um certificado digital fruto de portabilidade.
    a. Ao fazer isso, o PSC2 encaminhará à AC2 a autorização de portabilidade assinada pelo usuário, incluindo o CSR/PKCS#10 da nova chave.

6. AC2 emite automaticamente o novo certificado e o entrega ao PSC2.
    a. O prazo final de validade do novo certificado deverá ser o mesmo do certificado de origem (o que assinou a autorização de portabilidade).
    b. Os dados presentes no CN e otherName devem ser os mesmos do certificado de origem.

7. PSC2 comunica ao PSC1 a conclusão do processo de portabilidade.
    a. PSC1 informa ao usuário fim do processo de portabilidade.
    b. PSC1 elimina de sua base a chave do usuário.

Nesse processo, a AC2 (AC de destino) deve ser remunerada. Se não for o usuário a custear essa portabilidade, o PSC2 poderá fazê-lo. Em todo caso, essa questão será definida livremente entre as partes envolvidas.

O DOC-ICP 17 diz que:

A utilização de Prestadores de Serviços de Confiança para estes serviços elencados é facultativa. Certificados digitais dos usuários finais armazenados em dispositivos normatizados conforme estabelecido no DOC-ICP-04 [xx] e assinaturas digitais padrão ICP-Brasil feitas pela chave do usuário em outros sistemas são válidas conforme ditame legal da ICP-Brasil.

Nós gostaríamos de sugerir o seguinte:

A utilização de Prestadores de Serviços de Confiança para estes serviços elencados é facultativa. Certificados digitais dos usuários finais armazenados em dispositivos normatizados conforme estabelecido no DOC-ICP-04 [xx] e assinaturas digitais padrão ICP-Brasil feitas pela chave do usuário em outros sistemas, desde que estes validem o certificado digital utilizado, segundo as LCRs publicadas no momento da assinatura, são válidas conforme ditame legal da ICP-Brasil.

O acréscimo acima evitaria que assinadores de mercado quaisquer, que implementassem os padrões de assinatura da ICP-Brasil, mas que não fizessem a checagem mínima de validação do certificado, não fossem aceitos.

DOC-ICP 17.01

Na página 14, está escrito:

i) É vedado qualquer tipo de acesso remoto ao ambiente de nível 3.

A intenção aqui era falar de acesso remoto *adm*inistrativo, certo?

Na página 15, está escrito:

b) Esse acesso às chaves dos usuários deve ser de uso e controle exclusivo do titular da chave privada, sem a possibilidade de ingresso por outros titulares no mesmo HSM, qualquer funcionário e sistema do PSC ou dependentes de outras soluções e chaves criptográficas;

O texto acima ficou confuso. Sugestão:

Esse acesso às chaves dos usuários deve ser de uso e controle exclusivo do titular da chave privada. Qualquer funcionário ou outro sistema do PSC não devem ter acesso às chaves privadas dos usuários.

A propósito, a ideia é criar tantas contas de usuários quantas forem necessárias dentro do HSM? Isso é escalável? Ou os usuários serão cadastrados numa base, que será controlada por um sistema do PSC, e este fará o acesso às chaves dos usuários após a devida autenticação dos usuários no sistema do PSC? Não seria um sistema do PSC quem se autenticaria no HSM e acessaria as chaves dos usuários finais? Isso vai ao encontro do que já foi pontuado por outras empresas que

responderam à Consulta Pública (vide parecer DigitalSign, item 6.1, alínea “c”). Provavelmente será necessário rever o texto acima.

Na página 15, está escrito:

d) Deverá ser feita, em outro ambiente, a cópia das chaves dos usuários finais, observados os mesmos requisitos de armazenamento do ambiente principal.

Na página 15, também está escrito:

a) As chaves dos usuários finais e os respectivos certificados gerados, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, devem estar armazenados dentro dos espaços (*slots*), ou equivalente, da fronteira criptográfica e segura física de um HSM homologado na ICP-Brasil, endereçados por conta de usuário;

Pergunta: Se as chaves só podem estar armazenadas dentro de um HSM, e, muito provavelmente elas serão não-exportáveis, como será feita a cópia das chaves dos usuários finais para outro ambiente? Via replicação automática entre os HSM? Isso gera dependência de fornecedor! Para um PSC privado, a dependência de fornecedor pode não ser um grande problema na hora da aquisição, mas e se um produto for descontinuado? Se uma empresa parar de fabricar evoluções de um HSM?

Não seria importante permitir que as chaves fiquem armazenadas em cofre, em formato padrão (PKCS), para garantir independência de fabricantes do HSM?

Outra pergunta seria: As chaves privadas devem ser armazenadas no formato não exportável? Provavelmente sim. Só que isso não foi ressaltado em nenhum lugar do documento. Talvez seja bom frisar.

Raissa Medeiros
Adm. de Redes
GESET
Caixa Econômica Federal

Prezados,

A ANCert em consulta ao seu núcleo de estudos técnicos, entende que a norma pretendida fere cabalmente o parágrafo único do Art. 6º da Medida Provisória 2.200/01, visto que jamais o titular do certificado digital estará de fato em posse, uso ou conhecimento exclusivo de sua chave privada, uma vez que haverá sempre um intermediário (PSC) entre o titular e as suas prerrogativas exclusivas trazidas pela norma. Atualmente os hardwares criptográficos individualizados e físicos e até mesmo a possibilidade de uso dos certificados ICP-Brasil em dispositivos móveis, garantem que a norma citada esteja sendo cumprida, permitindo ao titular seu real e exclusivo controle sobre a chave privada.

Na computação em nuvem, há a ***impossibilidade prática*** de qualquer ente ou mesmo usuário do serviço de nuvem saber o que de fato está se processando na nuvem, por exemplo: há impossibilidade prática de se checar e garantir que o código fonte apresentado para auditoria dos serviços é o mesmo código fonte que de fato opera na nuvem.

Impossível também saber ou conhecer o computador físico (hardware) que está sendo realizada esta guarda de chaves privadas a geração e verificação de assinaturas digitais e armazenamento de documentos dos usuários do serviço.

Ressalta-se que um Prestador de Serviços em nuvem, poderá se utilizar para isso de servidores físicos (hardwares) que podem estar alocados em qualquer local do mundo, onde a jurisdição estatal brasileira não teria seu alcance efetivo afim de solucionar uma eventual lide jurídica envolvendo o tema, no qual fosse necessária uma perícia física no servidor em que o serviço está alocado, por exemplo, podendo causar dificuldade e até impossibilidade da comprovação técnica em que se funda o nexo causal do eventual dano.

Neste contexto a solução proposta apresenta-se como uma relação de confiança semiológica com o prestador de serviços que se encontra apoiada e baseada unicamente no normativo técnico apresentado e na sua garantia oferecida através do sistema de homologação, auditorias de conformidade e fiscalização da AC Raiz.

Frise-se também que há um risco ao se estabelecer que haja grande concentração de valor agregado da informação a disposição do provedor de serviço ao centralizar muitos certificados digitais e transações dos particulares em seu poder, sendo que o sistema atual já prevê essa descentralização e também dissolução do risco ao instituir o Parágrafo único do Art. 6º da Medida Provisória 2.200/01.

Em relação aos serviços de oferta de criação, validação, verificação de assinaturas digitais e guarda destas transações na solução em nuvem, entendemos pelas vulnerabilidades apontadas acima que a solução não poderia em principio oferecer todas as garantias

possíveis de sigilo que as relações civis possuem e demandam, expondo a risco o direito à privacidade.

Diante de todo o exposto e sendo a União através do Comitê Gestor da ICP-Brasil em conjunto com o Instituto Nacional de Tecnologia da Informação na qualidade de AC Raiz, os garantidores últimos de qualquer dano frente a responsabilidade solidária imposta ao Sistema Nacional de Certificação Digital bem como da higidez e segurança jurídica e social que a dimensão da Infra Estrutura de Chaves Públicas hoje atinge e suporta, entendemos por recomendável que a utilização de solução de HSM em Nuvem nos moldes propostos seja permitida apenas para assinaturas previstas pelo parágrafo 2º do Art. 10 da Medida Provisória 2200-2, não devendo ser atribuídas as garantias de fé pública presunção de veracidade decorrentes do uso do certificados digitais ICP-Brasil a este tipo de solução.

Concluímos portanto que: A homologação de serviços em nuvem para custodia e operação de certificados digitais emitidos para pessoas físicas ou jurídicas sob o regime normativo na ICP-Brasil, só faz sentido se desses serviços estiverem excluídos toda e qualquer operação com as correspondentes chaves privadas, ou seja, operações de geração, custódia, intermediação para acesso ou utilização de tais chaves pelo titular. Pois, do contrário, a autarquia que homologasse, e o agente homologado para prestar tais serviços no âmbito da ICP-Brasil, estariam juntos violando frontalmente, de forma cabal e irretorquível, o disposto no parágrafo único do art. 6 da Medida Provisória 2200-2, em prejuízo dos titulares de certificados sob tutela desse regime. Com o agravante desse prejuízo ser de natureza auto-incriminante, frente ao disposto no parágrafo 2 do art 10 do mesmo diploma legal, em contexto onde essa autarquia é justamente o ente público responsável por zelar pelo cumprimento dessa norma fundadora e constituinte da dimensão jurídica da ICP-Brasil.

Cordialmente,

ASSOCIAÇÃO NACIONAL DE AUTORIDADES DE CERTIFICAÇÃO DIGITAL - ANCert

Resposta à Consulta Pública da ICP-Brasil para Certificação Digital na Nuvem com HSM/PSC

www.kryptus.com contato@kryptus.com

Tabela de Conteúdo

1 Comentários relacionados à Resolução

1.1 Art 3º - Seção 2.1.6.1

Texto original: 2.1.6.1 Os PSC deverão ser entidades opcionais com capacidade técnica para realizar (i) o armazenamento de certificados digitais para usuários finais no âmbito da ICP-Brasil ou (ii) fornecer serviços de assinatura digital, verificação da assinatura digital e, se for o caso, armazenamento de documentos assinados digitalmente no padrão ICP-Brasil ou (iii) ambos, conforme regulamento operacional específico.

Comentários: Uma das propostas é o armazenamento seguro de documentos eletrônicos como podemos verificar no texto extraído do *briefing* da consulta "A proposta é que se ofereça, caso assim o usuário deseje, um serviço de assinatura digital padronizado e de armazenamento dos documentos eletrônicos. "

A proposta não deixa claro se o armazenamento dos documentos eletrônicos será realizado dentro de um HSM ou não.

O conjunto par de chaves criptográficas com certificado ICP-Brasil ocupa cerca de 5KB de espaço de armazenamento. Um documento típico ocupa pelo menos 100KB de disco. Como resultado, o espaço disponível para armazenamento no HSM esgotará 20 vezes mais rápido.

Acreditamos que o intuito do texto era indicar que os PSC devem armazenar o documento assinado digitalmente, mas não necessariamente no HSM, acreditamos que seria mais interessante deixar isso explícito de alguma forma.

A resolução também sugere que "2.1.6.2 Caberá à AC Raiz, por meio de Instrução Normativa, determinar os procedimentos técnicos e operacionais de um PSC.".

Sugestão: A Kryptus sugere que a Instrução Normativa torne opcional o armazenamento de documentos assinados digitalmente no HSM ou que a resolução aponte que apenas chaves criptográficas e certificados deverão obrigatoriamente ser armazenados em HSM.

2 Comentários relacionados ao DOC-ICP-17

2.1 Seção 4.4.2

Texto original: 4.4.2. Proteção de arquivo

A DPPSC deve estabelecer que todos os registros arquivados devem ser classificados e armaz4.

REQUISITOS OPERACIONAIS

Comentário: O texto parece estar incompleto.

3 Comentários relacionados ao DOC-ICP-17-01

3.1 Seção 6.1 - Item a)

Texto original: a) As chaves dos usuários finais e os respectivos certificados gerados, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, devem estar armazenados dentro dos espaços (slots), ou equivalente, da fronteira criptográfica e segura física de um HSM homologado na ICP-Brasil, endereçados por conta de usuário;

Comentários: A Kryptus aproveita para enaltecer a decisão do ITI de regulamentar a geração de chaves criptográficas em HSMs e mantê-las armazenadas em HSMs durante todo o ciclo de vida da chave.

A segurança de sistemas computacionais é baseada em diversos mecanismos, sendo um deles a proteção física. Não utilizar desse mecanismo que está disponível no mercado ou utilizá-lo parcialmente, apresenta a redução do grau de segurança das soluções que envolvem certificação digital.

Essa proposta vai de encontro com o exposto pelo ITI no *briefing*: “A proposta é que, também, toda parte de autenticação do usuário fique dentro da fronteira física criptográfica do HSM e que as chaves dos usuários, mantendo o altíssimo nível de segurança, se utilize de um protocolo interoperável (KMIP – Key Management Interoperability Protocol); ”.

Não será possível manter o nível de segurança almejado sem a iniciativa de armazenar chaves e certificados nos HSMs.

3.2 Seção 6.1 - Item c)

Texto original: 6.1 c) [...] Os mecanismos de autenticação devem empregar método ou protocolo de validação que proteja os dados por meio de criptografia. Esta funcionalidade será apensada aos requisitos técnicos na renovação de homologação dos HSM;

Comentários: O item comenta que os dados devem ser protegidos por meio de criptografia, mas não deixa claro se são dados de assinatura (HASH ou documento digital), chave privada ou dados de autenticação.

O texto também não deixa claro se a proteção é dos dados em trânsito ou no armazenamento do HSM.

Dado que o *briefing* contém o texto “A proposta é que, também, toda parte de autenticação do usuário fique dentro da fronteira física criptográfica do HSM”, o

nosso entendimento é que os dados de autenticação devem ser protegidos utilizando protocolos seguros como o TLS 1.2, por exemplo.

Quanto ao armazenamento dos dados de autenticação, entendemos que também devem ser protegidos por HSM que é equipamento dotado de segurança física, provendo o nível de segurança almejado pelo ITI.

Quanto à utilização do mecanismo em HSMs que trabalham com o protocolo KMIP, a Kryptus ressalta que é uma solução excelente não só pelo nível de segurança provido para as aplicações na ICP-Brasil, mas também pela escalabilidade da solução.

O KMIP trabalha diretamente a nível de protocolo, facilitando a escalabilidade, alta disponibilidade e balanceamento de carga das soluções que o utilizam.

Sugestão 1: 6.1 c) [...] Os mecanismos de autenticação devem empregar método ou protocolo de validação que proteja a transmissão e o armazenamento dos dados de autenticação por meio de criptografia. Esta funcionalidade será apensada aos requisitos técnicos na renovação de homologação dos HSM;

Sugestão 2: 6.1 c) [...] Os mecanismos de autenticação devem empregar método ou protocolo de validação que proteja a transmissão e o armazenamento dos dados de autenticação e proteja a transmissão dos dados de assinatura (HASH ou documento digital) por meio de criptografia. Esta funcionalidade será apensada aos requisitos técnicos na renovação de homologação dos HSM;

3.3 Seção 6.2.1

Texto original: 6.2.1 Os HSMs devem suportar o protocolo *Key Management Interoperability Protocol* – KMIP, versão 1.3 ou superior, devendo seguir, além dos relatados neste documento, os seguintes requisitos:

Comentários: A Kryptus gostaria de enaltecer a decisão do ITI de regulamentar a utilização do protocolo KMIP como protocolo de comunicação da solução.

O KMIP não é um padrão que foi criado para substituir arquiteturas e padrões arcaicos voltados para token. O padrão PKCS#11 por exemplo, foi criado pensando na utilização de smartcards e tokens, possuindo laços fracos de interoperabilidade.

3.3.1 História

O KMIP teve sua primeira versão lançada em outubro de 2010 1. O objetivo era aproximar dispositivos de fabricantes diferentes em um mundo onde as chaves criptográficas estão se espalhando rapidamente: "*But with encryption comes the need to properly manage the encryption keys. With encryption increasing across multiple enterprise applications it became harder to easily manage the keys from the different enterprise cryptographic applications. Better standards were needed to create uniform interfaces for the centralized encryption key manager."* 2

Desde então o KMIP passou por várias revisões, estando hoje na versão 1.4 que foi concluída em fevereiro de 2017. Existe um draft da versão 2.0 que deve ser lançada em 2018.

O KMIP é atualizado, mantido e definido por um comitê técnico da OASIS 3. Esse comitê é formado por empresas como: Kryptus, Thales, Safenet/Gemalto, HPE, Oracle, IBM, entre outras.

3.3.2 Escalabilidade

O KMIP foi pensado como uma solução para a nuvem, pois é um protocolo de rede que permite trabalhar com equipamentos de modelos diferentes, fabricantes diferentes, em posições diferentes do globo, obtendo os mesmos resultados. Sendo possível aplicar técnicas de alta disponibilidade e balanceamento de carga facilmente.

Já o PKCS#11 exige que o Cliente possua um driver (módulo PKCS#11) que foi feito para um computador específico. A Kryptus, em sua experiência, notou que o lado servidor do PKCS#11 (dispositivo criptográfico: token, smartcard, HSM, etc.) geralmente possui implementações diferentes, tornando custosa a escalabilidade da solução.

3.3.3 Interoperabilidade

As soluções baseadas em PKCS#11 possuem interoperabilidade duvidosa, pois é comum encontrar dispositivos diferentes que não funcionam da mesma forma. É justo pensar que a troca do módulo PKCS#11, que é o conector do padrão, faria com que a solução funcionasse da mesma forma em dispositivos diferentes, mas na prática isso não acontece.

Outro problema recorrente é a necessidade de utilizar um módulo específico para a plataforma do cliente, basicamente esse módulo é um driver. Se o cliente desejar trocar a plataforma computacional, pode esbarrar em barreiras como a inexistência da implementação do módulo para a sua solução. Como o cliente final será um usuário comum, padrões muito dependentes de plataforma se tornam inviáveis.

O KMIP é um protocolo de rede, portanto os dados que trafegam no canal de comunicação devem ser enviados seguindo exatamente como a especificação define. Por se tratar de uma camada de rede inferior, é possível trocar de modelo, versão ou fabricante de equipamento, investindo pouco em integração e testes da solução.

A OASIS promove testes de interoperabilidade do KMIP na conferência RSA que acontece anualmente na cidade de São Francisco nos Estados Unidos. Os testes acontecem desde 2010 e reunem diversos fabricantes de dispositivos criptográficos e de gerenciamento de chaves. A última edição contou com a participação da Kryptus, SafeNet/Gemalto, Cryptsoft, Fornetix, HPE, Hancom Secure, IBM, Oracle e QuintessenceLabs 4.

3.3.4 Implementações existentes

A lista de implementações existentes do KMIP possui cerca de 28 aplicativos e dispositivos.

A lista de produtos KMIP disponíveis comercialmente está na casa de 76 dispositivos de diversos fabricantes internacionais.

3.4 Seção 6.2.1.1

Texto original: 6.2.1.1 Os PSC devem definir um conjunto de operações que se aplicam aos objetos gerenciados que por sua vez consistem em atributos, como mostrado na tabela a seguir.

Comentários: A Kryptus acredita ser importante notar que nem todos as operações listadas são necessárias para a operação de um PSC. A sugestão é que o texto seja modificado para indicar explicitamente que a tabela é um exemplo.

Outro ponto importante é que os comandos *Notify* e *Put* são *server-to-client* e seu mecanismo não é especificado pela especificação, portanto o comportamento pode variar de um equipamento para outro. Sugerimos a retirada desses comandos da tabela para não gerar confusão.

Sugestão de texto: 6.2.1.1 Os PSC devem definir um conjunto de operações que se aplicam aos objetos gerenciados que por sua vez consistem em atributos, como mostrado na tabela exemplo a seguir.

3.5 Seção 6.2.1.6

Texto original: 6.2.1.6 Os atributos podem ser configurados, modificados e apagados.

Comentários: De acordo com a especificação do KMIP, nem todos os atributos podem ser configurados, modificados e apagados.

O atributo *Cryptographic Parameters* por exemplo, pode ser modificado e apagado pelo cliente, ao contrário do atributo *Cryptographic Length*, que não pode ser modificado ou apagado pelo cliente.

Sugestão de texto: 6.2.1.6 Os atributos podem ser configurados, modificados e apagados quando a especificação do KMIP permitir a modificação e exclusão pelo Cliente.

4 Comentários relacionados à resposta da DigitalSign

4.1 Item 2)

Texto original: 2) No que concerne à obrigatoriedade da utilização do protocolo KMIP, de referir que neste momento é essencialmente usado para gestão de chaves de encriptação e/ou autenticação, e não conhecemos nenhum HSM certificado internacionalmente que implemente este protocolo.

Para além disso, e pela sua natureza, ainda tem limitações severas nas componentes de uso de funções criptográficas necessárias para os processos de assinatura digital.

Pensamos que no futuro este protocolo pode vir eventualmente a ser mais um standard de facto, mas neste momento achamos que não faz sentido vedar a utilização dos protocolos internacionais que efetivamente são os standards atuais, tais como o PKCS#11, Java (JCA/JCE), Microsoft CAPI e CNG, OpenSSL, etc. e nos quais se baseiam todas as soluções de PKI atualmente existentes no mercado.

Comentários: A DigitalSign afirma não conhecer nenhum HSM certificado internacionalmente que implemente o protocolo KMIP. Podemos listar pelo menos dois aqui: Kryptus kNET HSM 5 e Thales e-Security keyAuthority 6.

A respeito das limitações do protocolo, a Kryptus terá que discordar. O KMIP é um padrão que é definido e atualizado pelo comitê técnico formado por membros da OASIS. Esse comitê é formado por membros de empresas que comercializam HSMs: Kryptus, Thales, SafeNet/Gemalto, IBM, HPE, Oracle, etc.

O KMIP passa por atualizações constantes, implementando funcionalidades e necessidades de mercado que são coletadas pelos fabricantes membros do comitê técnico.

Outro ponto interessante é que o protocolo KMIP se adequa às APIs de mercado citadas (PKCS#11, JCA/JCE, MS-CAPI, MS-CNG e OpenSSL) por ser um protocolo de comunicação. As APIs de mercado como a própria denominação indica, são interfaces de programação com chamadas de função bem definidas. O KMIP é um protocolo de rede que pode ser utilizado abaixo das APIs de mercado, garantindo a continuidade e adaptação de sistemas legados.

4.2 Item 3)

Texto original: 3) Sobre o processo de autenticação (com recurso a duplo fator), na Europa está em vigor legislação (e está para ser publicada muito brevemente nova legislação que vem reforçar ainda mais esses requisitos – Versao final para publicação em anexo II) que também obriga um duplo fator de autenticação.

No entanto, para garantir uma completa independência dos fabricantes, e cientes das limitações dos HSMs, a opção foi pela necessidade da utilização conjunta de um HSM homologado e de um SAM, conforme descritivo acima e no Anexo I a este documento.

Este módulo (SAM), que é responsável pelo processo de autenticação do usuário e pela verificação da integridade dos dados a serem assinados, pode correr em um sistema/equipamento distinto do HSM.

Este módulo também tem de ser homologado, no entanto é um processo bem mais simplificado.

Também, o facto de ser independente do HSM, torna o processo bem mais simples e económico, pois qualquer nova funcionalidade inserida nos HSMs é muito dispendiosa e demorada pois tem de passar todas as certificações internacionais.

Em última análise, pela proposta do ITI, qualquer alteração aos requisitos de autenticação (devido à evolução tecnológica, legal ou outra) obrigará à substituição dos HSM (que aumenta enormemente os custos), ao invés de apenas haver a necessidade de atualizar/trocar um componente do sistema.

Comentários: A DigitalSign sugere a utilização do módulo SAM para a autenticação duplo fator ao invés de utilizar o HSM, o que vai contra um dos princípios básicos da proposta do ITI que podemos encontrar no *briefing*: “A proposta é que, também, toda parte de autenticação do usuário fique dentro da fronteira física criptográfica do HSM”.

A Kryptus concorda que a inclusão de funcionalidades de autenticação duplo fator com KMIP implica na (re-)homologação dos equipamentos em normas internacionais, mas acreditamos ser irrelevante no escopo da ICP-Brasil, cuja norma vigente para homologação de HSMs é o MCT 7.

Outra questão importante é que já existem diversos fabricantes oferecendo HSMs com implementações de Execução Segura de código, possibilitando a modificação da implementação do mecanismo de duplo fator sem a re-homologação do equipamento.

Por fim, quando um HSM é homologado na ICP-Brasil, significa que está apto a ser utilizado para aquelas funções, sendo desnecessário modificar a funcionalidade e homologar o equipamento novamente.

Quanto à evolução tecnológica da autenticação duplo fator, nos parece ser uma preocupação desnecessária. Os mecanismos de autenticação duplo fator são usados em larga escala em aplicações de uso geral como a suíte de serviços da Google 7, autenticação em sistemas bancários 8, redes sociais como o Facebook 9 e até mesmo na indústria de jogos online 10. Ou seja, já existem mecanismos sólidos para autenticação duplo fator.

A respeito da adição de um componente de sistema que não é o HSM (o SAM é citado como possibilidade). Essa adição implica na criação de um novo Manual de Condutas Técnicas para a homologação desse sistema e levaria a ICP-Brasil ao mesmo problema, em que o módulo de autenticação terá que ser re-homologado quando for necessário incluir novas funcionalidades. Acreditamos ser mais interessante manter o sistema no HSM, que provê segurança física e lógica ao processo de autenticação.

5 Referências Bibliográficas

1 OASIS. Key Management Interoperability Protocol Specification Version 1.0. http://docs.oasis-open.org/kmip/spec/v1.0/os/kmip-spec-1.0-os.html

2 Townsend Security. A Brief History of KMIP. https://info.townsendsecurity.com/a-brief-history-of-kmip

3 OASIS. OASIS Key Management Interoperability Protocol (KMIP) TC. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip

4 OASIS. RSA 2017 Features Huge Demonstration of Support for Cyber Threat Intelligence, Encryption, and Cryptography Standards as 24 OASIS Member Companies Collaborate. https://www.oasis-open.org/news/pr/rsa-2017-features-huge-demonstration-of-support-for-cyber-threat-intelligence-encryption-and

5 Kryptus. kNET HSM. http://hsm.kryptus.com

6 Thales. keyAuthority. https://www.thalesesecurity.com/products-and-services/products-and-services/key-management-systems/keyauthority

7 Google. Verificação em duas etapas do Google. https://www.google.com/landing/2step/

8 Bradesco. Token no celular. https://banco.bradesco/html/classic/promocoes/mtoken/index.shtm

9 Facebook. What is two-factor authentication and how does it work? https://www.facebook.com/help/148233965247823

10 Blizzard. Keep your Account Secure with the Blizzard Authenticator http://us.battle.net/heroes/en/blog/20815191/keep-your-account-secure-with-the-blizzard-authenticator-6-6-2017

São Paulo, 28 de setembro de 2017.

AO ITI

Referente: Consulta pública - Certificado Digital em Nuvem (HSM/PSC da ICP-Brasil)

Pelo presente gostaríamos de agradecer a oportunidade em contribuir com o avanço da infraestrutura de chaves públicas ICP-Brasil e indicar abaixo nossas preocupações após rever a referida consulta pública.

Causa-nos preocupação a obrigatoriedade da utilização de um novo protocolo (KMIP) em HSMs e soluções já certificadas e em uso há mais de 10 anos na ICP-Brasil e outras soluções de mercado. Os equipamentos HSM já certificados e em uso pelas Autoridades Certificadoras tem demonstrado alto nível de segurança e não percebemos nenhum interesse pelo mercado, especialmente as Autoridades Certificadoras em alterar o que está em funcionamento. Ainda mais que a obrigatoriedade ocorra nas revalidações das certificações dos equipamentos já validados e testados, certamente causará ao mercado um certo estranhamento pois é de difícil convencimento e de fato não há nenhum ganho nesse tipo de aplicação, visto sua ampla utilização no Brasil e internacionalmente. Para tal sugerimos a criação de um novo e exclusivo MCT para essa aplicação de certificados em nuvem, uma vez que a aplicação difere da proposta corrente de uma AC.

O protocolo KMIP é relativamente novo, criado há pouco mais de 5 anos e ainda deve sofrer melhorias ao longo do tempo, especialmente comparado a outros mais maduros e muito mais utilizados como PKCS#11, JCE, Open-SSL, CSP. Equipamentos HSM de mercado, que visam segurança não operam com KMIP, cujo objetivo de interoperabilidade ainda deixa a parte de segurança em segundo plano.

Os protocolos que vem sendo utilizados pelo mercado conforme indicamos no parágrafo acima atendem à interoperabilidade sem expor aos problemas de segurança que advém com a expansão da fronteira criptográfica como autenticação de usuário conforme sugerida no documento publicado na consulta pública. Além do fato da obrigatoriedade de uma autenticação de segundo fator ocorrer dentro dos módulos, que embora à primeira vista parece ser interessante, poderá de fato confundir a finalidade real dos equipamentos, trazendo à tona vulnerabilidades de difícil reparação, pela própria certificação do equipamento, especialmente em acoplamentos de serviços publicados em nuvem e disponíveis à toda sorte de ataque.

É latente a discussão em diversos setores do mercado e há muita dúvida em relação aos benefícios das condições que estarão sendo impostas. Mais uma vez reiteramos que a obrigatoriedade nas revalidações das certificações dos equipamentos já validados e testados deve ser evitada e que a expansão da fronteira criptográfica como autenticação de usuário trará novas brechas de segurança que devem ser profundamente avaliadas. Por essa razão sugerimos que a discussão seja mais ampla dando mais tempo a todos os participantes para apresentarem suas preocupações e sugestões de forma a evoluir o sistema da ICP Brasil de maneira segura. Sobretudo por não termos percebido em nenhum de nossos parceiros no mercado brasileiro a preocupação ou pressa em utilizar um novo protocolo como o KMIP que acarretará mudanças profundas em condutas técnicas já bem estabelecidas no Brasil.

Mantemo-nos à disposição para quaisquer esclarecimentos que fizerem necessários e agradecemos a oportunidade que nos foi apresentada.

Atenciosamente,

_____

Anselmo Cimatti Netto.
Diretor de Operações

SafeNet Tecnologia em Informática Ltda.
Rua Bahia, 277 – 2º andar – Alphaville Industrial – CEP: 06465-110 – Barueri — SP
Tel: +55 (11) 3787-8100 - www.safenet-inc.com

Consulta Pública

Submission Date	2017-09-29 16:53:35
Nome:	Fabio Arrebola
E-mail	arrebola@evaltec.com.br

Comentários

No DOC-ICP-17:
1. As seções 4.1 e 4.5 parecem idênticas. Isso está correto?
2. Nas seções 4.1 e 4.2 do DOC-ICP-17, deixar a definição da forma de acesso aos serviços de armazenamento de chaves e geração, validação e armazenamento de assinaturas digitais à cargo do Provedor de Serviços de Confiança (PSC) traz flexibilidade, mas parece ir contra a padronização. O ponto aqui é que deixar essas definições à cargo do PSC pode ocasionar problemas de interoperabilidade, especialmente para as aplicações subscritoras. Basta imaginar um cenário em que um subscritor consome serviços de múltiplos PSCs, ou ainda um cenário de descredenciamento de um PSC. O ônus da interoperabilidade recai sobre o subscritor.
3. Na seção 4.3.1.1 não seria importante incluir a necessidade de registro de eventos do ciclo de vida do certificado e chave privada?
4. Ainda em relação aos requisitos operacionais, não seria importante incluir interfaces para que o usuário final titular do certificado tenha controle do ciclo de vida, incluindo a destruição da sua chave privada?
5. Adicionalmente, surge a pergunta, será permitida a cópia de segurança da chave privada do usuário final? E a replicação em sistema de contingência?
6. Não ficou claro qual seria o conteúdo da seção 7 sobre Políticas de Assinatura. O que ela deveria descrever?

No DOC-ICP-17-01:
1. No item c) da seção 6.1 exigir que o HSM provenha duplo fator de autenticação ao titular é sim importante para proporcionar maior segurança ao processo, mas requer cuidado. Parece haver indefinição entre os fatores de autenticação e a proposta de um TOKEN opaco. A seção 6.2.2 precisa de mais clareza.
2. Em adição à observação anterior, outra pergunta que vem à mente é: qual(is) HSM(s) homologado(s) atualmente possui(em) esse tipo de funcionalidade (suporte a duplo fator de autenticação)? Parece ser mais prudente que o segundo fator de autenticação seja controlado por uma camada de software que componha o PSC do que por um elemento de hardware. Se o objetivo do documento é padronização do serviço de armazenamento de chaves ele poderia indicar quais padrões devem ser utilizados para cada um dos eventuais fatores de autenticação adicionais à tradicional combinação entre usuário e senha.
3. Ainda em relação à questão da autenticação, não seria mais prudente permitir que a autenticação do usuário final seja controlada por uma camada de software que componha o PSC, e que seja distinta do HSM?
4. No item 6.2.1 exigir que o HSM suporte o protocolo KMIP parece ser uma diretiva muito rígida. Isso porque há grande sobreposição entre o KMIP e PKCS#11. Assim, grande parte das funcionalidades necessárias para o ciclo de vida e de uso de uma chave privada poderiam ser implementados sem a necessidade do KMIP. Portanto, já que não houve clareza sobre qual(s) o(s) motivo(s) embasa(m) a exigência do KMIP, podem esclarecer os motivos da escolha?
5. Em adição à observação anterior, outra pergunta que vem à mente é: qual(is) HSM(s) homologado(s) atualmente possui(em) esse tipo de funcionalidade? Parece que o ônus cai sobre o fabricante do HSM.
6. Por fim, ainda em relação ao item #3, talvez valha a pena definir um protocolo padrão (KMIP ou PKCS#11), possibilitando, opcionalmente o oferecimento de outros protocolos adicionais.

Comentários gerais:
1. Qual a intersecção, se é que há alguma, entre a proposta de padronização do serviço de assinatura digital e os Manuais de Conduta Técnica (MCTs) e as homologações de software de assinatura digital realizadas pelo LEA? Isto é, os serviços de geração e verificação de assinaturas digitais estão sujeitos às mesmas homologações?
2. O termo “Certificação Digital em Nuvem” pode dar origem à más interpretações, e eventualmente poderia ser trocado por termo mais apropriado. Para o público em geral o termo “em nuvem” dá a conotação de que qualquer provedor de infraestrutura em âmbito nacional ou internacional poderia ser utilizado. No entanto, conforme proposta de acréscimo à redação do item 2.1.6 do DOC-ICP-03, há a restrição que as instalações operacionais e recursos de segurança física e lógica estejam localizadas em território nacional.
3. Ainda sobre terminologia, para evitar problemas de interpretação o termo mais adequado não seria “armazenamento de chave privada associada a certificado digital de usuário final” ao invés de “armazenamento de certificado digital de usuário final”. Vide exemplos em DOC ICP 17 item 1.1.2, 1.1.3, 2.1.1.2, 4.3.1.1 etc.

Consulta Pública

Submission Date	2017-09-29 16:46:42
Nome:	ANCert - Associação Nacional de Autoridades de Certificação Digital
E-mail	presidencia@ancertbrasil.org.br

Comentários

Prezados,
A ANCert em consulta ao seu núcleo de estudos técnicos, entende que a norma pretendida fere cabalmente o parágrafo único do Art. 6º da Medida Provisória 2.200/01, visto que jamais o titular do certificado digital estará de fato em posse, uso ou conhecimento exclusivo de sua chave privada, uma vez que haverá sempre um intermediário (PSC) entre o titular e as suas prerrogativas exclusivas trazidas pela norma. Atualmente os hardwares criptográficos individualizados e físicos e até mesmo a possibilidade de uso dos certificados ICP-Brasil em dispositivos móveis, garantem que a norma citada esteja sendo cumprida, permitindo ao titular seu real e exclusivo controle sobre a chave privada.

Na computação em nuvem, há a impossibilidade prática de qualquer ente ou mesmo usuário do serviço de nuvem saber o que de fato está se processando na nuvem, por exemplo: há impossibilidade prática de se checar e garantir que o código fonte apresentado para auditoria dos serviços é o mesmo código fonte que de fato opera na nuvem.

Impossível também saber ou conhecer o computador físico (hardware) que está sendo realizada esta guarda de chaves privadas a geração e verificação de assinaturas digitais e armazenamento de documentos dos usuários do serviço.

Ressalta-se que um Prestador de Serviços em nuvem, poderá se utilizar para a execução dos serviços de servidores físicos (hardwares) que podem estar alocados em qualquer local do mundo, onde a jurisdição estatal brasileira não teria seu alcance efetivo afim de solucionar uma eventual lide jurídica envolvendo o tema, no qual fosse necessária uma perícia física no servidor em que o serviço está alocado, por exemplo, podendo causar dificuldade e até impossibilidade da comprovação técnica em que se funda o nexo causal do eventual dano.

Neste contexto a solução proposta apresenta-se como uma relação de confiança semiológica com o prestador de serviços que se encontra apoiada e baseada unicamente no normativo técnico apresentado e na sua garantia oferecida através do sistema de homologação, auditorias de conformidade e fiscalização da AC Raiz.

Frise-se também que há um risco ao se estabelecer que haja grande concentração de valor agregado da informação a disposição do provedor de serviço ao centralizar muitos certificados digitais e transações dos particulares em seu poder, sendo que o sistema atual já prevê essa descentralização e também dissolução do risco ao instituir o Parágrafo único do Art. 6º da Medida Provisória 2.200/01.

Em relação aos serviços de oferta de criação, validação, verificação de assinaturas digitais e guarda destas transações na solução em nuvem, entendemos pelas vulnerabilidades apontadas acima que a solução não poderia em principio oferecer todas as garantias possíveis de sigilo que as relações civis possuem e demandam, expondo a risco o direito à privacidade do consumidor que é hipossuficiente em termos de conhecimento técnico sobre a tecnologia embarcada na solução.
Diante de todo o exposto e sendo a União através do Comitê Gestor da ICP-Brasil em conjunto com o Instituto Nacional de Tecnologia da Informação na qualidade de AC Raiz, os garantidores últimos de qualquer dano frente a responsabilidade solidária imposta ao Sistema Nacional de Certificação Digital bem como da higidez e segurança jurídica e social que a dimensão da Infra Estrutura de Chaves Públicas hoje atinge e suporta, entendemos por recomendável que a utilização de solução de HSM em Nuvem nos moldes propostos seja permitida apenas para assinaturas previstas pelo parágrafo 2º do Art. 10 da Medida Provisória 2200-2, não devendo ser atribuídas as garantias de fé pública presunção de veracidade presentes no parágrafo 1º do mesmo Art. 10, decorrentes do uso do certificados digitais ICP-Brasil a este tipo de solução.

CONCLUÍMOS PORTANTO QUE: A homologação de serviços em nuvem para custodia e operação de certificados digitais emitidos para pessoas físicas ou jurídicas sob o regime normativo na ICP-Brasil, só faz sentido se desses serviços estiverem excluídos toda e qualquer operação com as correspondentes chaves privadas, ou seja, operações de geração, custódia, intermediação para acesso ou utilização de tais chaves pelo titular. Pois, do contrário, a autarquia que homologasse, e o agente homologado para prestar tais serviços no âmbito da ICP-Brasil, estariam juntos violando frontalmente, de forma cabal e irretorquível, o disposto no parágrafo único do art. 6 da Medida Provisória 2200-2, em prejuízo dos titulares de certificados sob tutela desse regime. Com o agravante desse prejuízo ser de natureza auto-incriminante, frente ao disposto no parágrafo 2 do art 10 do mesmo diploma legal, em contexto onde essa autarquia é justamente o ente público responsável por zelar pelo cumprimento dessa norma fundadora e constituinte da dimensão jurídica da ICP-Brasil.

Atenciosamente,

ANCert.

Consulta Pública

Submission Date	2017-09-29 14:45:16
Nome:	BRy Tecnologia
E-mail	cristian@bry.com.br

Comentários

1. Introdução

A BRy Tecnologia vem através desta manifestação posicionar-se em relação à Consulta Pública “Certificado Digital em Nuvem (HSM/PSC da ICP-Brasil)”, visando compartilhar sua experiência e conhecimento na gestão de Certificados e prestação de serviços de Certificação Digital em nuvem, para o aprimoramento da proposta do ITI.

Entendemos que a hospedagem de certificados em nuvem é de fato tendência e futuro da Certificação Digital, e aplaudimos a ICP-Brasil e ITI por trazer o assunto a tona de maneira construtiva, buscando estabelecer parâmetros mínimos de interoperabilidade e segurança.

Consideramos que será necessário detalhar e posteriormente discutir novamente diversos pontos do normativo que não estão suficientemente claros ou nos quais há necessidade de maior pesquisa e detalhamento.

Nesta resposta, discutimos pontos chave que identificamos no tempo disponível para manifestação, sobre os quais pensamos ser relevante existir reconsideração, tendo como premissas a garantia de maior segurança técnica e jurídica, interoperabilidade, viabilidade econômica e promoção de livre-concorrência, que terão como resultado a almejada massificação e redução de custos da Certificação Digital.

1.1 PSC é descrito como serviço à AC, porém o serviço é prestado ao Titular
A resolução proposta trata o PSC como um serviço à Autoridades Certificadoras, e não aos Titulares de Certificado, como se vê em itens como:

(Resolução) “Art. 4 (...) 2.2.7.3.2. O PSC que já estiver credenciado na ICP-Brasil poderá prestar serviço, no caso de armazenamento de certificados digitais dos usuários finais, a qualquer Autoridade Certificadora, devendo apenas a AC contratante comunicar ao ITI com 5 (cinco) dias de antecedência, alterar a sua PC e publicar o fato em sua página web.”

(Resolução) “Art 12. (...) 1.3.3.2. PSC poderão ser entidades utilizadas pelas AC, ou a própria AC, nesta PC ou na DPC implementada pela AC e se classificam em três categorias, conforme o tipo de atividade prestada”.

Entendemos que a escolha da forma de geração e armazenamento da chave criptográfica associada ao Certificado Digital é de responsabilidade exclusiva do titular, e isso está firmado de forma inquestionável no conjunto normativo. Publicamos no nosso blog corporativo em fevereiro deste ano (2017) texto discutindo o assunto (https://blog.bry.com.br/certificados-em-hsm-na-icp-brasil/) e reiteramos abaixo a importância de não restringir este direito e dever do titular.

O conjunto normativo proposto não justifica adequadamente a escolha da definição do serviço PSC como um serviço Autoridades Certificadoras, e entendemos que esta forma de definição pode limitar ou dificultar a atuação de prestadores de serviço com plena capacidade técnica e operacional para ser um PSC, mas que não sejam Autoridades Certificadoras, bem como limitar os modelos de negócio a serem oferecidos ao titular, em última instância, resultando em prejuízo a este tanto no exercício do seu dever e direito de responsabilidade sobre a segurança do seu Certificado Digital, bem como na disponibilidade de alternativas que lhe sejam mais vantajosas.

Entendemos que o fornecimento do serviço de armazenamento de certificado em nuvem é prestado ao titular, e não à AC. ACs, tipicamente, vendem certificados A3 com token/smartcard, com smartcard+leitora, mas também somente o certificado A3, ficando o titular livre para escolher o fornecedor de hardware de sua escolha com o fornecedor que preferir e confiar. Não vemos motivo para, de forma similar, não tratar o serviço de armazenamento de certificados como um serviço prestado diretamente ao Titular. Muito pelo contrário, entendemos que é importante que o serviço seja assim considerado.

A AC fornecedora do Certificado Digital pode, claro, formar parcerias estratégicas com PSCs para venda de Certificados em Nuvem em suas lojas, de maneira idêntica as parcerias que ocorrem hoje entre ACs e fornecedores de tokens/smartcards. Esta questão não parece precisar ser criada ou sequer incentivada na normatização, sendo que é de comum interesse entre PSCs e Autoridades Certificadoras que essas parcerias sejam formadas e existam, e é questão puramente comercial e estratégica das entidades envolvidas. Não nos parece, igualmente, ser necessário prever na PC das ACs este fato, uma vez que estas já tipicamente prevem a responsabilidade do titular no seguro acionamento da geração de chaves e também preveem o armazenamento de Certificados A3 em equipamento HSM homologado pela ICP-Brasil conforme DOC-ICP-04.

Todo o direcionamento à interoperabilidade almejado pelo uso do protocolo KMIP, que está sendo proposto pelo ITI, vai no sentido da maior segurança do Titular na escolha de prestação de serviço, e propicia maior participação e concorrência entre os participantes do mercado, tendo como resultado final a massificação, melhoria e redução de custos na ICP-Brasil. Entendemos que estabelecer o serviço de PSC como um serviço ao Titular, e não à AC, auxilia na promoção destes objetivos, sem de forma alguma restringir que ACs e PCS formem alianças para oferta de seus respectivos serviços em conjunto.

Propomos a seguinte alteração de redação como base para tal fundamentação:

(Resolução) “Art. 4 (...) 2.2.7.3.2. O PSC que já estiver credenciado na ICP-Brasil poderá prestar serviço, no caso de armazenamento de certificados digitais dos usuários finais, a qualquer usuário da ICP-Brasil.”
(Resolução) “Art 12. (...) 1.3.3.2. PSC poderão ser entidades utilizadas pelos titulares de Certificados Digitais e se classificam em três categorias, conforme o tipo de atividade prestada”.

1.2 Autenticação de duplo fator não é bem definida

(DOC-ICP-17.01) “6.2.2 Para a operação duplo fator de autenticação do titular da chave privada, deve ser criada uma nova extensão ao tipo de credencial, conforme relatado a seguir:”

Os subitens de 6.2.2 não deixam claro qual é o mecanismo de segundo fator de autenticação que se propõe. A especificação de uma entidade TOKEN não é suficiente, sem adequadas referências, para inferir qual o tipo de autenticação.

Sugere-se fortemente, entretanto, que o DOC-ICP não limite o tipo de segundo fator de autenticação a um específico, mas sim especifique requisitos mínimos para tal autenticação; Existem autenticações biométricas, semânticas, OTP, OATH, tokens de autenticação, FIDO, entre outras existentes ou que venham a ser implementadas, e limitar a um mecanismo específico limitará a oportunidade de fornecedores inovarem no fornecimento de soluções mais avançadas, seguras e usáveis para os titulares, bem como a inovação com novos mecanismos que venham a ser criados.

Consulta Pública

Submission Date	2017-09-29 14:13:29
Nome:	Renato Fonseca
E-mail	renato@evalsaude.com.br
Comentários	Prezados, Possuímos componentes que estão disponíveis em mais de 100 clientes no segmento da saúde. Assim, nos preocupa as restrições relacionadas à segurança física no capítulo 7 sobre o SERVIÇO DE ASSINATURA DIGITAL, VERIFICAÇÃO DE ASSINATURA DIGITAL E ARMAZENAMENTO DE DOCUMENTOS ASSINADOS. Pois, sistemas oferecidos como serviço pela Internet hoje, já possuem garantias de segurança, o que permite viabilizar o processamento em larga escala sem estas restrições. Na nossa interpretação sobre o documento, existe uma forte tendência sobre vincular um mesmo PSC para o serviço de armazenamento com o serviço de assinatura digital. Compreendemos que a integração deste dois serviços pode diminuir a exposição dos canais de comunicação, entretanto, pode exigir que um PSC acumule duas funções, não privilegiando a expertise de empresas que tenham focos diferentes. Os equipamentos HSM com modelo de rede já dispõem de controles de segurança em sua comunicação, o uso por meio de Internet notavelmente aumentará o espectro de potenciais ataques, mas não exclui o fato de que o equipamento é desenhado para acesso. O software sendo responsável pelo mecanismo autenticação com múltiplos fatores, permite flexibilização sobre o modelo a ser utilizado pelos titulares. Cabendo a estes julgar a melhor forma de implementação, cientes dos benefícios e riscos associados. Por exemplo, em um projeto onde o dispositivo de controle de acesso físico em um hospital possa compor os fatores de autenticação, isto trará a unificação de funções em dispositivos já disponíveis, reduzindo o investimento das instituições. Propomos a criação de diferentes níveis de serviço de armazenamento de certificados digitais, de modo a permitir que diferentes aplicações sejam clientes destes repositórios com requisitos diferentes dada a necessidade da aplicação. Hoje existem requisitos específicos para os tipos de certificados digitais de assinatura, sigilo e carimbo de tempo, ou seja, os A1 até A4, S1 até S4 e T1 até T4. Isto pode afetar os itens 3.1.1.L, 6.1.A, 6.1.D, 6.2.4 entre outros. Assim, em um nível de segurança específico, avaliar a possibilidade de um HSM permitir que chaves sejam protegidas por chaves mestras no HSM, porém armazenadas em outro repositório. Em resumo, propomos sejam elaborados requisitos específicos, independentes, para os serviços de armazenamento e assinatura e que existam níveis de serviço para permitir a flexibilidade de desenho de projetos de aplicações. Atenciosamente, E-VAL Saúde

Consulta Pública

Submission Date	2017-09-28 23:04:39
Nome:	Douglas Nunes da Silva
E-mail	douglas@webdocbi.com.br
Comentários	De acordo como feito no padrão europeu, assim, o monopolismo de certificadores acabará. Novas oportunidade de negócio serão geradas. A disposição.

Consulta Pública

Submission Date	2017-09-28 11:00:09
Nome:	Sidnei Yokoyama
E-mail	sidnei@dicas.org.br
Comentários	Solicito a verificação de possibilidade de prorrogação de prazo por mais uma semana para que tenha tempo para finalizar o estudo das documentações. Cordialmente, Sidnei

Consulta Pública

Submission Date	2017-09-28 10:11:09
Nome:	Marcos de Carvalho Monteiro
E-mail	mcm@tjrj.jus.br
Comentários	Não ficou claro se no caso de um órgão publico desejar adquirir um HSM para armazenamento de certificados digitais de Pessoa Física de seus funcionários (A3 ou A1), ele se enquadra como um PSC devendo cumprir todas as exigências legais dispostas na resolução.

Consulta Pública

Submission Date	2017-09-28 07:07:08
Nome:	Paulo Bitar
E-mail	bitar@rd2buzz.com
Comentários	Gostaríamos que fosse avaliado o Projeto apresentado ao ITI em 15/10/2015 feito pela RD2Buzz para a ANAHP e APM, o qual dá lastro a consulta em andamento.

Consulta Pública

Submission Date	2017-09-27 13:09:04
Nome:	Alexandre Matos
E-mail	alexandre.matos@estacio.br
Comentários	De acordo com o padrão europeu no Brasil.

Consulta Pública

Submission Date	2017-09-28 07:07:08
Nome:	Paulo Bitar
E-mail	bitar@rd2buzz.com
Comentários	Gostaríamos que fosse avaliado o Projeto apresentado ao ITI em 15/10/2015 feito pela RD2Buzz para a ANAHP e APM, o qual dá lastro a consulta em andamento.

Consulta Pública

Submission Date	2017-09-26 13:44:33
Nome:	Auta de Amorim Gagliardi Madeira
E-mail	autamadeira@yahoo.com.br
Comentários	Boa tarde. Procuro baixar o Parecer dos Processos SEFAZ/DF Governo do Distrito Federal, porém, seus LINKS enviados não abrem, de jeito nenhum. Anexos: (Clique em Visualizar Histórico) Dossie_01270010542017_25-09-2017.pdf PARECER01270010542017.pdf Tentativas feitas em duas máquinas hoje - 26-9-17. Peço p.f., me informar, DATA QUE SERÁ PULICADO O PARECER. No aguardo da sua resposta, permaneço aguardando que me informe. Att. Auta Gagliardi Madeira - OAB/DF 5585. Secretaria de Estado de Fazenda Atendimento Virtual Protocolo: 20170921-97555 Nome / Razão Social: AUTA A G MADEIRA CPF, CNPJ ou Passaporte: 041.002.982-34 Assunto: Ouvidoria Fazendária Tipo de Atendimento: Processo - informações e reclamações / solicitação de agilidade Solicitação - Data de Abertura 26/09/2017

Consulta Pública

Submission Date	2017-09-25 17:54:48
Nome:	Erick Nakano
E-mail	erick.nakano@ebiges.com
Comentários	Ressalva com relação às obrigações da PSC. Consta no documento DOC-ICP-17 Capítulo 9.1.1. Obrigações do PSC item d) tomar as medidas cabíveis para assegurar que subscritores e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações; Apesar de citar sobre direitos e obrigações que, são de suma importância, seria prudente incluir a obrigação, por parte da PSC, de tomar as medidas cabíveis para assegurar que subscritores e demais entidades envolvidas tenham conhecimento sobre procedimentos para a solicitação e acompanhamento de serviços e para aquisição e manutenção de certificados digitais.

Consulta Pública

Submission Date	2017-09-24 20:34:36
Nome:	Luiz Carlos Zancanella
E-mail	luizcarlos@safeweb.com.br
Comentários	Prezados Srs. Não dá entender o ITI não acreditar em seus próprios produtos. Ex_01: No caso desta consulta do CD em nuvem, não acreditar na segurança da criptografia para armazenamento da KR, em detrimento a segurança de barreira, não é somente não acreditar em seu próprio produto, mas também uma deturpação técnica conceitual. Mas a falta de confiança é histórica, veja Ex_02: O titular de um e-CPF não poder assinar um termo de titularidade para obtenção de outro Certificado, como um e-CNPJ, é não acreditar no Certificado Digital. obrigado pela atenção

Consulta Pública

Submission Date	2017-09-20 10:49:22
Nome:	heraldo santos leal
E-mail	heraldocobra1@gmail.com
Comentários	gostaria de ter acesso ao site para tomar conhecimento do processo

Consulta Pública

Submission Date	2017-09-19 14:25:28
Nome:	Paulo Roberto Lomba de Oliveira
E-mail	contato@taz.com.br
Comentários	POSITIVO. Otimizará tecnicamente o procedimento tornando-o mais célere, trazendo possibilidades de acréscimo de segurança da informação e proteção dos dados, por acompanhar mais na vanguarda a evolução tecnológica.

Certificado Digital em Nuvem (HSM/PSC da ICP-Brasil)

A DigitalSign é uma Autoridade Certificadora de 1º nível, que integra o ICP-Brasil desde 2013. A sua congénere Portuguesa atua no mercado Europeu desde 2001 está certificada como um "*Trusted Service Provider*" (TSP) para a emissão de certificados digitais qualificados e *TimeStamps* qualificados na Europa.

Tal como referido no briefing do projeto do ITI, a União Europeia (EU) publicou em 2014 um novo regulamento (eIDAS) relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas, tendo o mesmo entrado em pleno vigor em 01/07/2017. Nesse documento foi igualmente regulada a possibilidade de criação de assinaturas eletrónicas à distância (remotas), com o objetivo de simplificar e massificar o uso da certificação digital, ao mesmo tempo que se consegue uma segurança mais efetiva no processo.

A DigitalSign Portugal foi uma das entidades ouvida e envolvida na especificação dos requisitos desse projeto, dos quais se destacam os seguintes:

- A autenticação do usuário deve ser feita com recurso a pelo menos dois fatores de autenticação, tal como também consta do presente projeto da ICP-Brasil.
- Em todos os pedidos de assinatura, o TSP tem de garantir não só a correta autenticação do usuário, mas também a integridade e a origem dos dados a serem assinados.
- O ambiente onde é feita essa autenticação/verificação, a assinatura dos dados e o armazenamento das chaves/certificados é denominado como "*Qualified Signature Creation Device*" (QSCD), e contém dois componentes essenciais:
    - "*Signature Activation Module*" (SAM), responsável pela autenticação do usuário e verificação da integridade e origem dos dados a serem assinados.
      Este sistema, sendo independente do HSM, deve possuir proteções contra violação, e está sujeito a um processo de homologação autónomo, por laboratórios acreditados e segundo nova norma em anexo II.
    - "*Cryptographic Module*" (HSM), responsável pela gestão das chaves criptográficas e certificados dos usuários, assim como pelas funções criptográficas de assinatura.
      Este sistema, deve possuir homologação standard internacional.

A visão geral dos componentes básicos do sistema é apresentada no Anexo I a este documento.

No Anexo II partilhamos o índice do documento de especificação de requisitos (*Protection Profile – norma CEN EN 419241-2 - Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing*), de forma a evidenciar a complexidade e abrangência dos aspetos de segurança inerentes aos processos e sistemas usados na assinatura remota.

Informações mais detalhadas sobre o documento em causa podem ser consultadas em: https://standards.cen.eu/dyn/www/f?p=204:110:0:::FSP_PROJECT,FSP_ORG_ID:60568,6205&cs=1FFBE4E2990FEECD37BAA0F24FB514076

A DigitalSign Portugal foi um dos primeiros TSPs a disponibilizar o serviço de assinatura remota dentro do espaço europeu, através de uma solução devidamente homologada.

Feita esta introdução, passamos a expor alguns aspetos, para os quais gostaríamos de propor uma análise mais profunda com vista à sua redefinição:

1) Após análise da documentação disponível sobre este projeto de certificado digital em nuvem, nota-se uma clara separação das componentes de "armazenamento do certificado/chave e respetivo controlo por parte do usuário" e da "assinatura digital".

   Entendemos as motivações dessa separação, no entanto isso poderá levar a situações em que o PSC-A possui uma plataforma de assinatura e o PSC-B faz o armazenamento de chaves – caso haja um processo judicial de repudiação de uma assinatura fraudulenta, tornar-se-á impossível aferir qual dos PSCs será o responsável pela não observância das regras, pois o PSC-A é responsável por mostrar o documento e calcular o respetivo *hash*, enquanto o PSC-B é responsável por garantir o acesso à chave, mas não verifica a integridade nem a origem dos dados a assinar.

   Esta situação de indefinição não é desejável e poderá colocar em causa a credibilidade de toda a infraestrutura ICP-Brasil. Sugerimos, assim, que esta separação não seja possível, para estarem alinhados com as normas internacionais e reduzirem riscos, tornando claras as responsabilidades.

2) No que concerne à obrigatoriedade da utilização do protocolo KMIP, de referir que neste momento é essencialmente usado para gestão de chaves de encriptação e/ou autenticação, e não conhecemos nenhum HSM certificado internacionalmente que implemente este protocolo.

   Para além disso, e pela sua natureza, ainda tem limitações severas nas componentes de uso de funções criptográficas necessárias para os processos de assinatura digital.

   Pensamos que no futuro este protocolo pode vir eventualmente a ser mais um standard de facto, mas neste momento achamos que não faz sentido vedar a utilização dos protocolos internacionais que efetivamente são os standards atuais, tais como o PKCS#11, Java (JCA/JCE), Microsoft CAPI e CNG, OpenSSL, etc. e nos quais se baseiam todas as soluções de PKI atualmente existentes no mercado.

3) Sobre o processo de autenticação (com recurso a duplo fator), na Europa está em vigor legislação (e está para ser publicada muito brevemente nova legislação que vem reforçar ainda mais esses requisitos – Versao final para publicação em anexo II) que também obriga um duplo fator de autenticação.

   No entanto, para garantir uma completa independência dos fabricantes, e cientes das limitações dos HSMs, a opção foi pela necessidade da utilização conjunta de um HSM homologado e de um SAM, conforme descritivo acima e no Anexo I a este documento.

   Este módulo (SAM), que é responsável pelo processo de autenticação do usuário e pela verificação da integridade dos dados a serem assinados, pode correr em um sistema/equipamento distinto do HSM.

   Este módulo também tem de ser homologado, no entanto é um processo bem mais simplificado.

   Também, o facto de ser independente do HSM, torna o processo bem mais simples e económico, pois qualquer nova funcionalidade inserida nos HSMs é muito dispendiosa e demorada pois tem de passar todas as certificações internacionais.

Em última análise, pela proposta do ITI, qualquer alteração aos requisitos de autenticação (devido à evolução tecnológica, legal ou outra) obrigará à substituição dos HSM (que aumenta enormemente os custos), ao invés de apenas haver a necessidade de atualizar/trocar um componente do sistema.

Dado o exposto, e com base em toda a experiência nacional e internacional da DigitalSign, cremos que para este serviço atingir os objetivos propostos, há fatores que devem ser acautelados, dos quais destacamos:

- ***Time to market***: é necessário garantir uma rápida implementação destas funcionalidades com ferramentas existentes e não estar à espera para definir novos standards cujos fabricantes internacionais de HSM e software de PKI não irão adotar no curto prazo, pois os custos de desenvolvimento são altos e um processo de homologação certificação é dispendioso.

- **Promoção da concorrência**, seja ela por parte dos prestadores de serviços, seja por parte dos fabricantes de hardware e software – ora, com esta abordagem todos os produtos internacionalmente homologados e fiáveis ficam de fora, e dessa forma não prevemos que se atinjam os objetivos de facilidade e redução dos custos, ficando a ICP Brasil dependente unicamente de fabricantes locais…

- **Fazer um alinhamento global**, aderindo aos padrões internacionais – a criptografia não é uma tecnologia brasileira, é uma tecnologia Internacional, e quando se refere como boas práticas os padrões europeus, por exemplo, devem aceitar-se esses padrões ou transpô-los integralmente para as regras do Brasil, e não optar pela definição de padrões que apenas são usados no Brasil, isolando-se a ICP-Brasil das normas internacionalmente aceites.

  De referir que o regulamento eIDAS e toda a normalização técnica levada a cabo pelo CEN e ETSI está a ser aceite como a referência (*standard de facto*) por muitos outros países fora da comunidade Europeia, designadamente na Ásia, África, Rússia e mesmo Estados Unidos da América, e estes países estão a implementar os regulamentos na íntegra.

  Como exemplo recente dos problemas provocados pelo desalinhamento da ICP-Brasil com as normas internacionais, temos a autorização no Brasil do uso dos certificados A1 (que internacionalmente não têm uma equiparação legal a uma assinatura manuscrita) e que levou a que a Adobe excluísse estes certificados da AATL.

  Outro exemplo foi a necessidade de redesenhar toda a estrutura de emissão de certificados SSL – com os custos inerentes – devido ao facto de não se terem acautelado inicialmente as regras internacionais.

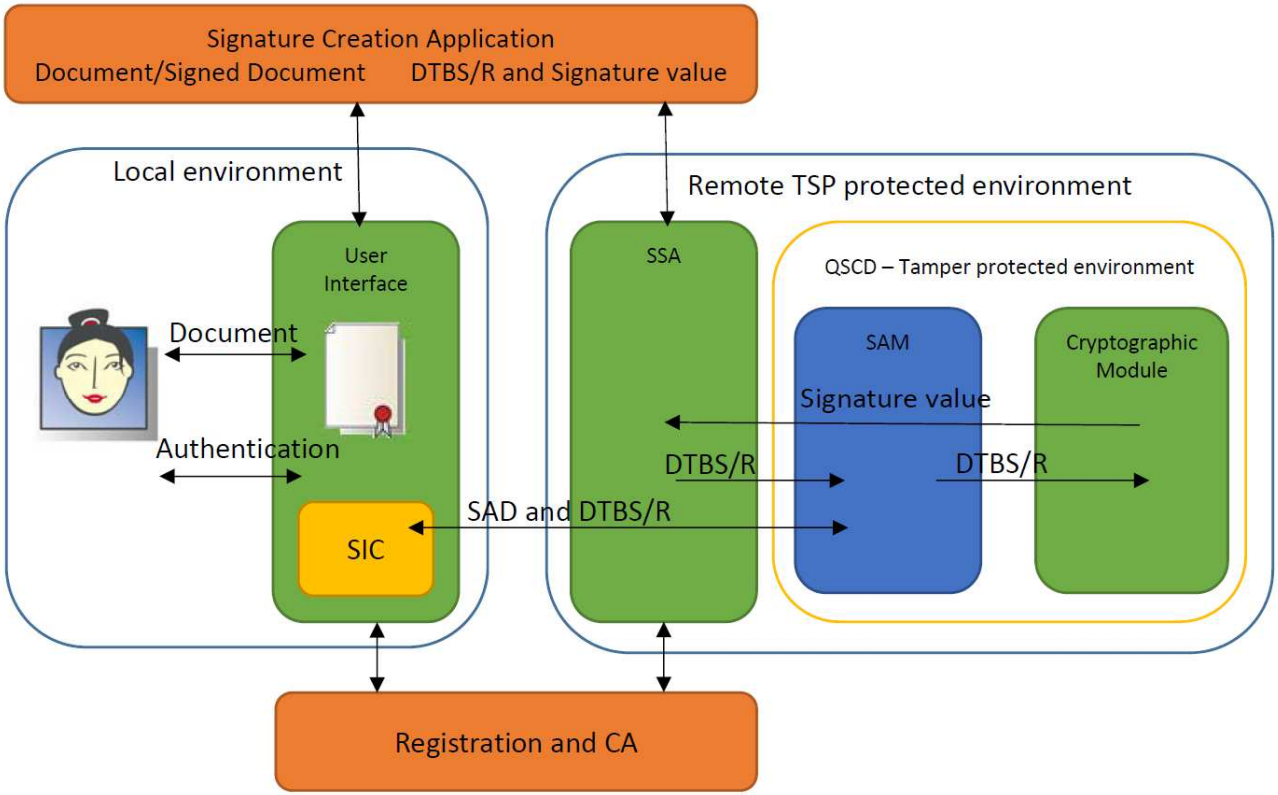
Esperando que esta nossa análise e sugestões possa contribuir para uma melhoria efetiva deste projeto de certificado digital em nuvem, reiteramos os nossos cumprimentos e disponibilizamo-nos para futuros esclarecimentos que julguem necessários.

São Paulo, 22 de setembro de 2017.

_____

DIGITALSIGN CERTIFICAÇÃO DIGITAL LTDA.

Anexo I - Componentes Básicos do Sistema de Assinatura Remota



Legenda:

SIC: Signer's Interaction Component
SAD: Signature Activation Data
DTBS/R: Data To Be Signed Representation
SSA: Server Signing Application
QSCD: Qualified Signature Creation Device
SAM: Signature Activation Module

Anexo II – Índice da norma CEN EN 419241-2

Contents

List of Tables

List of Figures

6. REQUISITOS PARA ARMAZENAMENTO DE CERTIFICADOS DIGITAIS

6.1 Armazenamento dos certificados digitais.

a) As chaves dos usuários finais e os respectivos certificados gerados, para os tipos de

certificados que obrigatoriamente devem ser gerados e armazenados em hardware

criptográficos, devem estar armazenados dentro dos espaços (slots), ou equivalente, da

fronteira criptográfica e segura física de um HSM homologado na ICP-Brasil, endereçados

por conta de usuário;

Sugestão:

> Entendemos que, neste item, o emprego do termo “físico” referindo-se à fronteira criptográfica do equipamento restrinja o uso de recursos avançados de armazenamento e proteção das chaves implementados pela Thales no repositório conhecido como *Security World*, que está sim, invariavelmente vinculado à proteção do hardware criptográfico (HSM) através do emprego de criptografia forte, portanto dentro da fronteira criptográfica segura do equipamento, mas que não necessariamente utiliza a memória interna do hardware seguro como repositório das chaves enquanto as mesmas se encontrem simplesmente armazenadas (inertes), e não em uso.
>
> Recomendamos, portanto, que a redação deste item seja modificada para exibir:
>
> “a) As chaves dos usuários finais e os respectivos certificados gerados, para os tipos de certificados que obrigatoriamente devem ser gerados e armazenados em hardware criptográficos, devem estar armazenados dentro dos espaços (slots), ou equivalente, da fronteira criptográfica segura de um HSM homologado na ICP-Brasil, endereçados por conta de usuário;”.

c) O HSM deve prover mecanismos de duplo fator de autenticação ao titular para acesso à

chave privada. Cada fator deve ser de uma classe diferente (conhecimento, posse, push

notifications ou biometria). Os mecanismos de autenticação devem empregar método ou

protocolo de validação que proteja os dados por meio de criptografia. Esta funcionalidade

será apensada aos requisitos técnicos na renovação de homologação dos HSM;

Sugestão:

Entendemos que o emprego de duplo fator de autenticação para acesso à chave privada seja de fundamental importância na estratégia de controle de acesso dos usuários e portanto celebramos a atenção da norma a este ponto, entretanto entendemos que este recurso não esteja vinculado apenas e diretamente ao hardware criptográfico (HSM), mas sim ao sistema de autenticação oferecido pelo PSC, composto de hardware e software. A razão para esta sugestão é que os recursos de duplo fator de autenticação providos pelos HSMs são geralmente orientados à administração do dispositivo e podem oferecer obstáculos à escalabilidade da solução, pela forma como são implementados e pelos custos dos referidos recursos, além de estarem restritos àqueles recursos implementados pelo hardware, sem possibilidade de expansão e reforço, pelo sistema do PSC, como por exemplo, métodos de autenticação por biometria, hoje não implementados por nenhum modelo de HSM disponível no mercado. A melhor forma de implementar tal recurso, portanto, é vinculá-lo ao sistema do PSC e não ao HSM, permitindo que os recursos de duplo fator de autenticação dos HSMs sejam expandidos e reforçados através da integração dos sistemas do PSC com o HSM através das APIs (*Application Porgram Interface)* oferecidas pelo hardware.

Recomendamos, portanto, que a redação deste item seja modificada para exibir:

“c) O sistema do PSC deve prover mecanismos de duplo fator de autenticação ao titular para acesso à chave privada. Cada fator deve ser de uma classe diferente (por exemplo, conhecimento, posse, ou biometria). Os mecanismos de autenticação devem empregar método ou protocolo de validação que proteja os dados por meio de criptografia.”

6.2 Protocolo e Rede

6.2.1 Os HSMs devem suportar o protocolo Key Management Interoperability Protocol – KMIP,

versão 1.3 ou superior, devendo seguir, além dos relatados nesse documento, os seguintes

requisitos:

...

6.2.2 Para a operação duplo fator de autenticação do titular da chave privada, deve ser criada uma

nova extensão ao tipo de credencial, conforme relatado a seguir:

...

Sugestão:

> O protocolo *KMIP* tem o objetivo de se tornar uma interface única padrão de comunicação entre sistemas criptográficos em geral (não necessariamente hardwares criptográficos), simplificando os mecanismos de gerenciamento de chaves (*key management*). Embora o propósito seja nobre e prometa trazer ganhos para o mercado, a realidade é que por se tratar ainda de um padrão relativamente novo e não estabelecido como padrão *de facto*, ainda se apresenta apenas como recurso adicional para a imensa maioria dos sitemas que utilizam chaves ccriptográficas, não sendo implementado como opcão de integração nativa por nenhum dos grandes fabricantes internacionais de HSMs. Mais uma vez celebramos a atenção desta norma às tendências do mercado, entretanto entendemos que especificar este padrão como única opção de integração para gestão dos objetovs criptográficos dos HSMs seja excessivamente restritivo, e ofereça um obstáculo imediato à criação dos PSC e, portanto, aos esforços de flexibilização e massificação de uso da certificação digital. Ainda neste tema, uma vez que o paddrão KMIP seja mantido como uma opção de integração para gestão de chaves, o mesmo deveria referir-se ao sistema do PSC e não especificamente aos HSMs, uma vez que não há qualquer problema de segurança identificado com as opções atuais de integração oferecidas pelos fabrricantes de hardwares criptográficos. Resumindo, tornar o KMIP a única interface de integração para gestão das chaves criptográficas nos HSMs neste momento aumentará exponencialmente a complexidade dos requisitos mínimos para o sistema do PSC e inviabilizará a participação dos grandes fabricantes internacionais de HSMs, enfraquecendo esta norma e comprometendo diretamente o objetivo principal de massificação desta tecnologia.
>
> Recomendamos que os referidos itens sejam eliminados da norma.

6.2.3 Poderá ser arquitetado um pool de HSM para operação, replicação e gerenciamento das

chaves dos usuários finais, devendo seguir, além dos relatados nesse documento, os seguintes

requisitos.

a) Especificação e estabelecimento de uma comunicação segura (sessão SSL/TLS) entre os HSM;

Sugestão:

A utilização de um canal de comunicação SSL/TLS não é a única alternativa segura de replicação de objetos entre dispositivos HSMs. Entendemos que especificá-lo desta forma se mostre altamente restirivo àqueles fabricantes que implementam este recurso e exclui outros fabricantes que implementam recursos tão seguros quanto este para replicação de objetos criptográficos entre os dispositivos HSM.

Recomendamos, portanto, que a redação deste item seja modificada para exibir:

“a) Especificação e estabelecimento de uma comunicação segura (sessão SSL/TLS) entre os HSMs ou mecanismo equivalente”;