Reposta a manifestação da AC SOLUTI.

A AC SOLUTI propõe uma solução para portabilidade de um usuário entre diferentes PSC.

Na manifestação, a AC SOLUTI descreve uma forma de se realizar a portabilidade sem a exportação da chave privada, emitindo um novo par de chaves. Ademais, sugere que nesse caso não é necessário novo comparecimento em uma AR para os processos de identificação (aproveitando o já realizado) e que só se destrua a chave privada no PSC 1, emitida por uma AC 1, e se crie outra no PSC 2. Para isso, o usuário comunica que quer realizar a portabilidade, o PSC 2 indica uma lista de AC a qual tem convênio e esse conjunto procede a criação de uma nova chave, inclusive com um procedimento de assinar as requisições como é feito na emissão de um certificado. Com a autorização e assinatura da requisição da nova chave, o PSC 1 se comunica com PSC 2, entregando a autorização assinada, gerando um novo certificado, que conterá a mesma validade do anterior e os mesmos dados publicados. Inclui, inclusive, que nesse processo a AC 2 (AC destino) deve ser remunerada, se não pelo usuário, pelo PSC 2.

ITI: A proposta indica uma forma de “portabilidade” de chave do usuário. Entretanto, o versado não resolve o problema de alta dependência da solução PSC a um fabricante de HSM, nem quando um PSC (acontece o mesmo em uma AC) for descredenciado ou descredenciar-se, por conta própria, da ICP-Brasil. Nesse cenário, os problemas continuam. Não é crível que, podendo mitigar esse problema, a ICP-Brasil tenha que realizar um *recall* de todos os usuários do PSC ou então daqueles que possuem certificados na cadeia de AC. Existe ainda o problema atrelado ao custo desse processo, que no entendimento do ITI, não pode ser do usuário, até em vista do Código de Defesa do Consumidor, ou que por qualquer motivo ele seja prejudicado por um mau funcionamento do PSC.
É importante também lembrar que o PSC, assim como a AC Raíz e ACs subsequentes respondem solidariamente pela infraestrutura. É fundamental que todos estudem uma forma de mitigar o problema relatado.
A proposta do ITI para resolver essa questão acima mencionada e entregar uma solução de portabilidade ao usuário, ou seja, que ele decida em qual PSC a sua chave deve ficar, ataca ambas as questões. De forma segura, até então, e controlada pelo usuário e não pelo PSC, é possível exportar a chave do usuário, em um movimento semelhante ao que já é feito no *backup* de chave de AC.
Uma proposta que está em teste é a seguir transcrita:

Portabilidade de chaves privadas de usuários: PSC 1 - PSC 2

a) Glosário:

CP_rU_i: Chave privada do usuário 'i', armazenada no HSM 1, a ser exportada e importada para o HSM 2;

$CP_rH_e^2$: Chave privada do HSM 2, a ser utilizada para importação de chaves privadas de usuários gravadas no HSM 1;

$CP_uH_e^2$: Chave Pública do HSM 2, utilizada para exportação de chaves privadas de usuários armazenadas no HSM 1, a serem importadas pelo HSM 2. $CP_uH_e^2$ deve ser armazenada no repositório do ITI, seguindo procedimentos já estabelecidos ($CP_uH_e^2$ pode ser transformada em um certificado digital);

CS_i: Chave simétrica a ser gerada pelo HSM 1, para exportação da chave privada do usuário 'i', CP_rU_i. CS_i é utilizada para cifração da chave privada do usuário 'i';

$Algo_s$: Algoritmo criptográfico simétrico, de sigilo, pode ser o AES ou Serpent, com modo de operação CTR e tamanho de chave 256 bits.

b) Usuário deve solicitar, assinando digitalmente, uma requisição, que estará disponível no sítio dos PSCs, de portabilidade de sua chave privada, de exportação no PSC atual e de importação no PSC de destino.

c) Os PSCs receberão essa requisição e autorizarão essa portabilidade com os três perfis (administrador, auditor e operador). Assim que receber a autorização do usuário, PSC 1 e PSC 2 devem iniciar os procedimentos de exportação e importação.

d) Os PSCs devem estabelecer uma conexão ponta a ponta em um canal seguro de comunicação (HTTPS com dupla autenticação por certificado digital ICP-Brasil).

e) Modo Operacional:

i. Procedimentos preliminares:

[a] Cada PSC gera um par de chaves ([CP_uH_e , CP_rH_e] - pública e privada) em cada um de seus HSMs. Este par tem como propósito prover portabilidade entre HSMs de quaisquer PSCs. Este par de chaves deve ser utilizado em possível exportação de chaves privadas de usuário, Cp_rU_i e também na assinatura das requisições para envelopamento utilizando a sua chave pública. Por analogia, para a chave CP_uH_e, 'C' significa 'Chave', P_u chave Pública, e H_e significa chave gerada pelo HSM para exportação de chave do usuário 'i', CP_rU_i. De forma similar, CP_rH_e e CP_rU_i têm significados equivalentes;

[b] CP_uH_e é armazenada em repositório do ITI, e CP_rH_e é mantida no HSM de origem;

ii. Para Exportação de chaves privadas dos usuários contidas no HSM 1 para o HSM 2:
[c] No PSC importa-se para o HSM 1 a chave pública do HSM 2, $CP_uH_e^2$, do repositório do ITI;

[d] No HSM 1 gera-se uma chave de sessão simétrica, CS_i, distinta, para cada chave privada de usuário a ser exportada;

[e] No HSM 1 cifra-se a chave simétrica, CS_i, com a chave pública do HSM 2, $CP_uH_e^2$, de destino, para exportação da chave do usuário 'i', CP_rU_i;

[f] No HSM 1 cifra-se a chave privada do usuário 'i', CP_rU_i, antes do procedimento de exportação de chaves, com a chave simétrica gerada, CS_i, com o algoritmo de sigilo padrão AES ou Serpent, com o modo de operação CTR e tamanho de chave de 256 bits;

[g] No HSM 1 apaga-se cada chave de sessão simétrica gerada, CS_i, após o procedimento de cifração do item 'f' ter sido executado;

[h] Após a cifração da chave privada do usuário 'i', CP_rU_i, ter sido realizada com sucesso, exporta-se essa chave, e a chave Cs_i cifrada, para o HSM 2;

iii. Para importação de chaves privadas dos usuários contidas no HSM 1 para o HSM 2:

[i] O administrador do HSM 2, de destino, cria novo usuário e o habilita;

[j] O usuário importa do HSM 1 sua chave privada e a chave simétrica cifrada, itens 'e' e 'f';

[k] No HSM 2, de destino, recebe-se a chave privada CP_rU_i e a chave simétrica CS_i cifradas, do usuário 'i';

[l] No HSM 2 decifra-se a chave simétrica, CS_i, com a chave privada do HSM 2, $CP_rH_e^2$;

[m] Em seguida, no HSM 2 decifra-se a chave privada do usuário 'i', CP_rU_i, que estava no HSM 1, com a chave simétrica CS_i, com o algoritmo criptográfico padrão AES ou Serpent, com o modo de operação CTR e tamanho de chave de 256 bits;

[n] No HSM 2 grava-se a chave privada do usuário 'i', CP_rU_i, já decifrada, e importada do HSM 1;

[o] No HSM 2 destrói-se a chave simétrica CS_i;

[p] O PSC 2 encaminha para o PSC 1 mensagem indicando que a importação ocorreu satisfatoriamente. Então, o HSM 1 apaga a chave privada do usuário 'i', CP_rU_i.

Reposta a manifestação de Raíssa Medeiros, GESET, Caixa Econômica Federal

Sugere-se que seja incrementado na norma o seguinte: “desde que estes validem o certificado digital utilizado, segundo as LCRs publicadas no momento da assinatura,”.
ITI: Os processos de validação de uma assinatura no padrão ICP-Brasil, conforme descrito na DPC, já imputam a checagem da LCR ou OCSP. Para um PSC é obrigatório, e será verificado no ato de credenciamento, seguir esses padrões ICP-Brasil.

Pergunta se a vedação de acesso remoto é administrativo.
ITI: Era importante que se descrevesse o que a manifestante entende como administrativo, mas é vedada, nas operações que rodam no nível 3, qualquer acesso feito de forma remota nos servidores e suas operações, por qualquer tipo de perfil, administrativo, operacional ou auditoria.

Sugere-se o texto: “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.”
ITI: No caso concreto, é necessário ser mais do que o sugerido em texto pela manifestante, como, por exemplo, a vedação de sistemas e uma chave de acesso criada pelo próprio HSM para que o usuário tenha controle da sua chave privada, por isso o texto da norma encontra-se desta forma. Caso esse não tenha ficado claro, faremos as alterações.

Respondendo as perguntas:
(...) a ideia é criar tantas contas de usuários quantas forem necessárias dentro do HSM?
ITI: Sim.
Isso é escalável?
ITI: É escalável, depende da capacidade do HSM ou de soluções em *pool*.
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?
ITI: Não, todos os usuários serão criados dentro do HSM, em *slots* exclusivos.
Não seria um sistema do PSC quem se autenticaria no HSM e acessaria as chaves dos usuários finais?
ITI: Não, os endereços dos usuários são dentro do HSM e o próprio possui acesso direto e exclusivo daquele espaço.

Outras perguntas: 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?

ITI: Existe em andamento um estudo para que se faça um procedimento seguro com chaves exportáveis, conforme referência do próprio DOC-ICP-10. É possível ver esse procedimento na resposta feita a AC SOLUTI. A cópia da chave, ou backup da chave, pode ser feito como em uma AC.

Via replicação automática entre os HSM? Isso gera dependência de fornecedor!

ITI: Não, ao contrário, se não adotarmos um procedimento de exportação de chave com segurança e interoperabilidade nos PSCs, assim como pode acontecer para AC, a solução ficará totalmente independente do fornecedor. A ideia é mitigar esse problema.

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?

ITI: Exatamente por isso estamos propondo um protocolo de portabilidade.

Se uma empresa parar de fabricar evoluções de um HSM?

ITI: Conforme respondido anteriormente.

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

ITI: Padrão PKCS 11, atualmente, faz com que tenhamos dependência dos fabricantes, visto as nuanças em que são criados as credenciais de usuários. Por isso estamos há alguns meses estudando o protocolo KMIP, mitigando a dependência que hoje existe na ICP-Brasil.

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.

ITI: Conforme respondido anteriormente, isso já está colocado nas normas do PSC. O protocolo KMIP é uma interface de interoperabilidade.

Resposta a manifestação da ANCERT

Serão transcritos os parágrafos e respondido um a um.

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.

ITI: Respeitando a manifestação exarada, mas não concordamos e não se aplica a verdade fática de procedimentos técnicos com a inicial e conclusão da ANCERT nesse ponto. É importante dizer que não existe a palavra “posse” na MP 2.200/01 e tecnicamente posse não é controle, são conotativamente palavras distintas. Seria difícil a interpretação e consecução técnica se a MP, por algum motivo, colocasse a palavra posse, porque a chave privada é algo lógico e não material. É importante notar que a MP também não descreve sobre *hardware* criptográfico. O usuário terá, e ampla literatura técnica versa sobre, dos manuais dos fabricantes a solução credenciadas, total e exclusivo controle, uso e conhecimento da sua chave privada, em conformidade plena a MP. Todas as interfaces, inclusive a proposta KMIP, permitem essa conclusão. Não há dúvida sobre essa questão.

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.

ITI: Nesse ponto não ficou muito claro o que a ANCERT colacionou, mas tentaremos interpretar. Na solução PSC é exatamente o contrário. O usuário saberá sim o que está sendo processado, conforme escrito em norma. Aliás, nesse cenário, ao contrário do que se apresenta em *smart card* ou *token*, o usuário poderá monitorar qualquer acesso ou assinatura. A ICP-Brasil conhecerá a solução

do PSC de ponta a ponta. Sobre o código fonte, é exatamente ao contrário. Com *smart card* e *token* existe uma dificuldade enorme para se saber qual "código fonte" está realmente sendo usado e comercializado, o que em HSM isso não ocorre, devido ao maior controle de fiscalização, auditoria e produtos certificados. Enfim, ganha-se, como dito, mais segurança, controle, uso e conhecimento sobre a chave privada do usuário final.

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.

ITI: Também nesse ponto, na solução PSC acontece exatamente ao contrário do manifestado pela ANCERT. Será possível conhecer, ativamente, o HSM em que a solução opera.

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.

ITI: É exatamente o contrário. Os ambientes e *hardwares* de uma PSC obrigatoriamente estarão em território nacional, respeitando toda legislação e normas do Brasil.k

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.

ITI: A semiologia da solução PSC encontra-se respaldada na legislação e nas normas técnicas, alvissareiras na sua propositura de segurança. Indo além, a norma torna os sistemas da ICP-Brasil mais confiáveis, seguros e fáceis para o usuário, ampliando a fronteira de confiança.

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.

ITI: Sim, concorda-se sobre a concentração, mas não há relação, mais uma vez, com o parágrafo único, conforme já explicado. Por isso, a norma proposta toma extremos cuidados com o ambiente de segurança físico e lógico, que se assemelham aos encontrados em uma AC. Veja que a proposta é facultativa e o usuário detém o poder de escolhê-la. Mais do que nunca, o controle da chave privada está imbricado com as decisões do próprio usuário.

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

ITI: Não entendemos dessa forma, mas esse, sem dúvida, é um debate que pode ser ampliado. É importante aqui separar, para as questões de sigilo, o que é uma criação e validação de assinatura com guarda de documentos. O PSC será obrigado, como atualmente não acontece em diversos portais de assinatura, gerando uma grande inconsistência para as aplicações e usuário, a utilizar de padrões e políticas de assinaturas ICP-Brasil, garantindo maior valor probante das assinaturas digitais. Sobre o sigilo dos documentos esse sim um debate que deve ser feito. Na solução PSC o usuário determina se quer que seus documentos assinados sejam armazenados no PSC. O PSC deve obedecer a legislação vigente sobre documentação sigilosa, confidencial, privada ou pública.

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.

ITI: Importante salientar que a ICP-Brasil não pode regular algo que não faz parte do seu sistema. Outro adendo a ser feito: o § 2º do art.10 é tecnicamente e pericialmente frágil por tentar, de forma incorreta, refletir algo do processo civil. Ademais, não há conclusão pericial de autoria quando se analisa somente documentos eletrônicos assinados com certificados não ICP-Brasil. O conjunto mínimo de segurança física, lógica, de algoritmos, de identificação e de processos da ICP-Brasil que conseguem atingir essa questão.

ITI: A conclusão exposta foi respondida ao longo do texto.

Resposta a manifestação da Krytpus.

ITI: Sobre o primeiro ponto manifestado na consulta, chegou-se a conclusão que todo objeto público poderá ser armazenado fora do HSM. O armazenamento de um documento assinado é um serviço que pode ser oferecido pelo PSC, desde que haja concordância expressa do usuário e que respeite a legislação vigente sobre armazenamento de documentos digitais.
Foram corrigidas já as questões redacionais.
Já foram revistas também as questões de cunho técnico, tanto para as comunicações seguras quanto para as operações KMIP.
Ao final, a Kryptus faz considerações sobre a manifestação da DigitalSing, que será respondida nesse documento.

Resposta a manifestação da Gemalto/Safenet

Serão transcritos os parágrafos e respondidos um a um

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.

ITI: É importante observar que a adoção do protocolo KMIP não será, ainda, para as soluções já certificadas de AC na ICP-Brasil e sim, para uma nova entidade, com um novo propósito na ICP-Brasil. Os equipamentos nos PSC continuarão a ser certificados e todos os requisitos de segurança serão testados e aprovados. Há um enorme ganho nesse tipo aplicação. Entendendo que a Gemalto/Safenet é uma empresa fabricante de smart card e HSM, com seus produtos vendidos para entidades na ICP-Brasil, mas existe uma grave dependência desta infraestrutura com os fabricantes de HSM. Conforme já foi respondido, não se pode mais ater a uma situação de uma entidade na ICP-Brasil, por qualquer motivo, não operar mais ou ser descredenciada e as chaves não poderem ser utilizadas. A dependência total nos fabricantes faz com que usuários finais corram sérios riscos de serem prejudicados, assim como, a credibilidade da ICP-Brasil.

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.

ITI: O KMIP foi criado há pouco mais de sete anos e esperamos mesmo que ele sofra evoluções. É importante que melhorias sejam sempre implementadas. Não é verdade que o protocolo KMIP deixe em segundo planto a segurança do processo, até porque esse continuará sendo parte do da certificação de HSM da ICP-Brasil. Segurança e interoperabilidade são princípios basilares da ICP-Brasil. Estes outros protocolos citados, apesar de possuírem instruções para interoperabilidade, na prática, não acontece de maneira fácil. Ao ITI nunca foi mostrado que HSM distintos se conversam com esses outros protocolos no intuito de se promover essa interoperabilidade.

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 a toda sorte de ataque.

ITI: Conforme dito, ao ITI nunca foi demonstrado essa interoperabilidade. Caso a Gemalto/Safenet possa nos trazer relatórios ou demonstrar essa interoperabilidade, estamos a disposição. Não ficou claro a segunda parte do parágrafo, na qual é versado que o segundo fator de autenticação poderá trazer vulnerabilidades de difícil reparação. Quais seriam essas vulnerabilidades do segundo fator de autenticação dentro da fronteira criptográfica do equipamento?

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.

ITI: Revalidações de certificação são obrigatórias no âmbito de habilitação de equipamentos na ICP-Brasil. Não estamos em momento algum expandindo a fronteira criptográfica de autenticação do usuário. Temos uma situação, entendendo o lado do fabricante, que é não mais depender de soluções proprietárias.

Resposta a manifestação de Fabio Arrebola (arrebola@evaltec.com.br)

Serão transcritos os parágrafos e respondidos um a um

1. As seções 4.1 e 4.5 parecem idênticas. Isso está correto?
ITI: Já foi corrigido.

2 (…) definições de forma de acesso (…)
ITI: Na verdade não recai sobre o subscritor, visto que todas as aplicações do PSC serão declaradas e passarão pelo crivo de uma auditoria pré-operacional. Então a implementação correta e segura, de acordo com a norma, recai sobre o PSC, mas esse poderá escolher qual forma de autenticação proverá ao usuário, desde que siga as normas exaradas.

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?
ITI: O registro do ciclo de vida da chave privada se da DPC.

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?
ITI: Sim, é importante e assim será cobrado.

5. Adicionalmente, surge a pergunta, será permitida a cópia de segurança da chave privada do usuário final? E a replicação em sistema de contingência?
ITI: A cópia será para o ambiente de contingência, garantindo a devida prestação do serviço, conforme dita o documento de referência da Adobe AATL (https://helpx.adobe.com/content/dam/help/en/acrobat/kb/approved-trust-list2/_jcr_content/main-pars/download-section/download-1/aatl_technical_requirements_v2.0.pdf)

6. Não ficou claro qual seria o conteúdo da seção 7 sobre Políticas de Assinatura. O que ela deveria descrever?
ITI: Ela deve descrever quais são as políticas de assinatura que serão adotadas pelo PSC.

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.
ITI: Foi feito um descritivo melhor sobre os fatores de autenticação.

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.
ITI: Sim, os HSM podem possuir esse segundo fator, entretanto a norma trará isso como opcional e o segundo fator poderá ser aplicado a uma camada de software.

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?
ITI: Sim e assim foi feito.

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?
ITI: Os motivos que embasam essa decisão do protocolo KMIP está na independência dos fabricantes de HSM e soluções no âmbito da ICP-Brasil. Essa dependência, até para as AC, causam um grande risco a ICP-Brasil.

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.

ITI: Atualmente não possuem essa funcionalidade. Depois da divulgação do novo MCT que subsidiará os ensaios técnicos, os HSM terão seis meses para se adequar.

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.
ITI: A ideia é permitir interoperabilidade. Desconhecemos um protocolo que ofereça as funcionalidades de interoperabilidade concreta como o KMIP.

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?
ITI: Não existe obrigatoriedade de certificação de *software* na ICP-Brasil, somente do *hardware* criptográfico, que terá o seu MCT atualizado.

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.
ITI: O ITI percebeu essa dificuldade também. É a criação de uma entidade (PSC), com possibilidade de acesso remoto, mas com requisitos da ICP-Brasil.

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.
ITI: Já foi realizada essa correção.

Resposta a Bry Tecnologia.

ITI: Sobre a questão relatada de ser um serviço prestado ao usuário, em que esse terá o poder de escolher o seu PSC, ou seja, a forma como a sua chave privada será armazenada e acessada, concordamos com a colocação e já foi feita uma revisão do texto normativo nesse sentido.
Não é um serviço de Autoridade Certificadora. Outras empresas, desde que cumpram o normativo proposto, poderão solicitar o credenciamento. As restrições estão colocadas caso uma AC queira ser um PSC.
Sobre o segundo fator de autenticação, será promovido uma atualização da proposta para descrever diversos fatores de autenticação que poderão ser utilizados, mas sem a restrição de uso. O PSC poderá usar qualquer um entre os colocados em norma.

Reposta a manifestação de Renato Fonseca (renato@evalsaude.com.br)

ITI: Não existe tendência para vincular os dois serviços. É possível realizá-los de forma separada.
Os equipamentos HSM possuem diversos mecanismos de proteção, inclusive de detecção de intrusão que vão além da capacidade de um smart card ou computadores e dispositivos móveis pessoais.
Não existe a necessidade de criação de diferentes níveis de serviço de armazenamento; o propósito, neste projeto, permanece o mesmo. Chaves de HSM que são protegidas fora do perímetro criptográfico, cifradas com chaves mestras geradas dentro do HSM, é uma solução que está sendo estudada pelo ITI. Neste momento não fará parte do conjunto normativo, mas a equipe técnica já possui todos os elementos necessários e tem conversado com fabricantes que possuem essa solução.

Reposta a manifestação de Douglas Nunes da Silva (douglas@webdocbi.com.br)

ITI: Sim, uma das referências desse projeto é o regulamento europeu.

Reposta a manifestação de Sidnei Yokoyama (sidnei@dicas.org.br)

ITI: Foram dados 15 dias corridos para as manifestações. Tivemos boas contribuições.

Reposta a manifestação de Marcos de Carvalho Monteiro (mcm@tjrj.jus.br)

ITI: A norma proposta versa que caso uma solução corporativa, de acesso pela rede interna pelos funcionários da instituição, não se enquadra na solução de PSC.
A solução do PSC é para acessos não corporativos, remotos, de qualquer lugar ou dispositivo, armazenando chaves de qualquer requerente.

Reposta a manifestação de Paulo Bitar (bitar@rd2buzz.com)

ITI: Será feito uma pesquisa interna para possibilidade de avaliarmos o projeto.

Reposta a manifestação de Alexandre Matos (alexandre.matos@estacio.br)

ITI: Sim, uma das referências desse projeto é o regulamento europeu.

Reposta a manifestação de Auta de Amorim Gagliardi Madeira (autamadeira@yahoo.com.br)

ITI: A manifestação exarada trata-se de assunto não correlato ao PSC.

Reposta a manifestação de Erick Nakano (erick.nakano@ebiges.com)

ITI: Sim, foi inserido também na proposta normativa a questão de acompanhamento de serviços e ciclo de vida do certificado.

Reposta a manifestação de Luiz Carlos Zancanella (luizcarlos@safeweb.com.br)

ITI: Se entendemos bem o manifestado, fala-se em armazenamento de forma cifrada em um ambiente fora da fronteira criptográfica do HSM. Conforme já posicionado, o ITI está estudando essa implantação, mas a equipe técnica não possui elementos suficientes para propor seu uso nesse momento. Até por questões normativas (A1, A2, A3 e A4), que possivelmente teriam que ser revistas.

Sobre a questão do termo de titularidade, essa não faz parte deste projeto, mas é importante lembrar que membros, que participam do mercado, do Comitê Gestor da ICP-Brasil recusaram uma simplificação e diminuição de custos de assinatura digital do mesmo recentemente. Equipe técnica do ITI acredita também que essa é uma questão importante a ser abordada.

Reposta a manifestação de Heraldo Santos Leal (heraldocobra1@gmail.com)

ITI: Acreditamos que todos puderam ter acesso ao site ao longo dos 15 dias de consulta pública.

Reposta a manifestação de Paulo Roberto Lomba de Oliveira (contato@taz.com.br)

ITI: Sim, a ideia é trazer mais segurança, celeridade, facilidade de uso e proteção de dados na ICP-Brasil.

Reposta a manifestação da DigitalSign

A Digitalsign faz as seguintes ponderações:

1) Sugere que PSC de assinatura não seja separado de PSC de armazenamento de chaves, visto que num processo judicial de repúdio de uma assinatura fica impossível aferir qual dos PSC será o responsável pela não observância das regras uma vez que o PSC de assinatura somente mostra o documento e calcula o hash, enquanto que o PSC de armazenamento é responsável pelo acesso à chave, mas não verifica a integridade nem a origem dos dados a assinar.

ITI: Todos os PSC deverão passar por procedimento de credenciamento antes de entrar em operação no âmbito da ICP-Brasil. Os requisitos definidos para credenciamento e manutenção do credenciamento obrigam, dentre outros, registros de todas as operações realizadas por esses PSC. Nesse procedimento de credenciamento, está previsto uma avaliação de regularidade por auditoria pré-operacional, executada pelo ITI, para avaliar a conformidade dos procedimentos da candidata a PSC. Isto posto, entendemos que é possível identificar o responsável por qualquer falha de repúdio visto que ambos PSC possuirão registros de suas operações realizadas, possibilitando rastreabilidade.

Questiona a obrigatoriedade do protocolo KMIP em relação aos demais padrões, tais como: PKCS#11, JAVA, OPENSSL, entre outros. Alega desconhecer HSM com essa implementação e limitações severas em componenetes de uso de funções criptográficas necessárias no processo de assinatura digital. Acredita que em breve o KMIP se estabeleça de fato.

ITI: A obrigatoriedade para o protocolo KMIP se restringe ao PSC de armazenamento no intuito de viabilizar interoperabilidade de chaves entre os PSC, uma vez que essa interoperabilidade se torna complexa quando se adota PKCS#11. Para os PSC de assinatura, não há restrição. Caso se confirme restrições mercadológicas de HSM com KMIP, a proposta será alterada para iniciar com PKCS#11, definindo-se um prazo de transitoriedade para implementação do KMIP.

Sugere que a autenticação seja realizada com recurso de dois fatores pelo Módulo SAM (*Signature Activation Module*), responsável pelo processo de autenticação do titular e pela verificação da integridade dos dados a serem assinados, ocorrendo em sistema/equipamento distinto do HSM e

necessitando de homologação. Alega que implementação de funcionalidade no HSM é dispendiosa e demorada em razão das certificações internacionais.

ITI: A proposta contempla duplo fator de autenticação, sendo que um seja implementado pelo HSM, e o outro possa ser implementado por aplicação, podendo fazer a função do Módulo SAM. Tal solução resolve a questão de restrição mercadológica dos HSM relacionada à autenticação do titular. Podemos avaliar a sugestão de certificação do Módulo SAM com reconhecimento de certificações Common Criteria (ISO 15.408) ou FIPS.