INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

ATA DE REUNIÃO

REUNIÃO ORDINÁRIA DO COMITÊ GESTOR DA ICP-BRASIL

Aos dez dias do mês de Novembro de 2017, nas dependências do Instituto Nacional de Tecnologia da Informação – ITI, situado no endereço SCN Qd. 02 Bl.E, na cidade de Brasília/DF, com horário de início às 9h, reuniram-se os membros titulares e Suplentes do Comitê Gestor da ICP-Brasil – CG ICP-Brasil, servidores do Instituto Nacional de Tecnologia da Informação – ITI, e alguns ouvintes para participar da Reunião Ordinária do referido Comitê. Estiveram presentes: Luiz Carlos Azevedo (Coordenador Titular do Comitê Gestor da ICP-Brasil – Casa Civil da Presidência da República), Nelson do Vale de Oliveira (Suplente da Casa Civil da Presidência da República) Gastão José de Oliveira Ramos (Secretário-Executivo do CG ICP-Brasil – Instituto Nacional de Tecnologia da Informação - ITI), Cláudia Maria de Andrade (Suplente do Ministério da Fazenda), Rafael Cunha Alves Moreira (Titular do Ministério da Indústria, Comércio Exterior e Serviços), José Ney de Oliveira Lima (Suplente do Ministério do Planejamento, Desenvolvimento e Gestão), Otávio Viegas Caixeta (Titular do Ministério da Ciência, Tecnologia, Inovações e Comunicações), José Garcia da Luz (Titular do GSI/PR-Gabinete de Segurança Institucional), Julio Cosentino (Titutlar da Associação Nacional de Certificação Digital - ANCD), Nivaldo Cleto (Titular da AARB – Associação das Autoridades de Registro do Brasil), Gianni Moreira Leitão (Titular da Fenacor/CNC), Salvador Medeiros Ferrer (Titular da Febraban – Federação Brasileira de Bancos), Manuel Dantas Matos (Titular da Camara-e.net – Câmara Brasileira de Comércio Eletrônico), Antonio Sérgio Borba Cangiano (Suplente da Associação Nacional de Certificação Digital - ANCD) Rafaelo Abrita (Diretor de Auditoria, Fiscalização e Normalização do ITI), Waldeck Pinto de Araújo Júnior (Diretor de Infraestrutura de Chaves Públicas Brasileira), Alexandre Munia Machado (Procurador Federal Chefe do ITI); Edmar da Silva Araújo (Chefe de Gabinete Substituto e Assessor de Comunicação do ITI), Eduardo de Magalhães Lacerda (Assessor do Diretor-Presidente do ITI), Ruy César Ramos Filho (Assessor do Diretor-Presidente do ITI), Pedro Pinheiro Cardoso (Coordenador-Geral da Auditoria e Fiscalização do ITI), Wilson Roberto Hirata (Coordenador-Geral de Normalização e Pesquisa do ITI), José Rodrigues Gonçalves Júnior (Coordenador-Geral de Segurança da Informação do ITI), André Machado Caricatti (Coordenador-Geral de Operações do ITI), Pedro Motta (Ouvinte pelo Serpro), Priscila Figueiredo (Ouvinte/Procuradora pela camara-e.net), Patrícia Paiva (Ouvinte pela ANCD), Maurício Balassiano (Ouvinte pela ANCD), Vinícius Souza (Ouvinte pela camara-e.net), Jean Martina (Ouvinte pela Universidade Federal de Santa Catarina – UFSC), Robson Machado (Ouvinte pela camara-e.net), Paulo M. Roque (Ouvinte pela AARB – Associação das Autoridades de Registro do Brasil), Sérgio Basso (Ouvinte pela Secretaria Executiva do Comitê Gestor), André Peixoto (Ouvinte pela Secretaria Executiva do Comitê Gestor), e Sergio Fuchs (Ouvinte pelo Ministério da Fazenda) para tratar da pauta a seguir:

1. Inclusão de itens no DOC-ICP-05, versão 4.3, no DOC-ICP-05.02, versão 1.5.

Esta proposta visou a aproveitar o sistema financeiro nacional, organizado, normatizado e controlado pelo Banco Central, para prover uma maior facilidade na obtenção do certificado digital. É de conhecimento público que o setor bancário tem um robusto sistema de identificação e prevenção de fraudes que não pode ser dispensado. A proposta era aproveitar o cadastro de

cliente bancário para subsidiar a identificação e a emissão de um certificado digital padrão ICP-Brasil, sem abrir mão das premissas da legislação em vigor.

Ato: Resolução

Votação:

Favorável: Casa Civil; Ministério da Fazenda; Ministério da Indústria, Comércio Exterior e Serviços; Ministério do Planejamento, Desenvolvimento e Gestão; Ministério da Ciência, Tecnologia, Inovações e Comunicações; GSI/PR-Gabinete de Segurança Institucional; ANCD – Associação Nacional de Certificação Digital; e Febraban –Federação Brasileira de Bancos.

Contrária: camara-e.net – Câmara Brasileira de Comércio Eletrônico, Fenacor/CNC e AARB – Associação das Autoridades de Registro do Brasil.

Ausência: Ministério da Justiça e Segurança Pública

Apuração: aprovado por 8 a 3.

2. Criação do Prestador de Serviço de Confiança (PSC) na ICP-Brasil

A proposta de resolução pretendeu criar uma entidade na ICP-Brasil chamada “Prestador de Serviço de Confiança – PSC”, acrônimo e solução também encontrada na comunidade europeia (TSP – Trust Service Provider), que será credenciado, auditado e fiscalizado, conforme proposta normativa, pelo ITI.

Ato: A resolução modifica alguns DOC-ICP e cria os DOC-ICP-17 e DOC-ICP- 17.01, este último uma Instrução Normativa, que conterá os procedimentos operacionais e de segurança do PSC.

Votação:

Favorável: Casa Civil; Ministério da Fazenda; Ministério da Indústria, Comércio Exterior e Serviços; Ministério do Planejamento, Desenvolvimento e Gestão; Ministério da Ciência, Tecnologia, Inovações e Comunicações; GSI/PR-Gabinete de Segurança Institucional; ANCD – Associação Nacional de Certificação Digital; e Febraban –Federação Brasileira de Bancos, camara-e.net – Câmara Brasileira de Comércio Eletrônico, Fenacor/CNC e AARB – Associação das Autoridades de Registro do Brasil.

Ausência: Ministério da Justiça e Segurança Pública

Apuração: aprovado por 11 a 0

Após solicitação formal do representante da AARB, senhor Nivaldo Cleto, faço constar nesta ata, em anexo, manifestação por escrito acerca do tema dos bancos, encaminhada por e-mail a esta secretaria executiva.

Após solicitação formal do representante da Febraban, senhor Salvador Ferrer, faço constar nesta ata sua manifestação acerca do tema dos bancos, proferida no momento de seu voto:

“*Depois de muito trabalho, muita discussão, o voto da Febraban é favorável. Eu só gostaria que constasse na ata da reunião que existem pontos que precisarão ser discutidos e que, talvez, no momento inicial os bancos não estejam prontos para um processo rápido de massificação e que existem algumas coisas precisam ser trabalhadas”*

Após solicitação formal da representante da Fenacor, senhora Gianni Moreira, faço constar nesta ata, em anexo, manifestação por escrito acerca do tema dos bancos, encaminhada por e-mail a esta secretaria executiva.

Após solicitação formal da representante da Câmara-e.net, senhor Manuel Matos, faço constar nesta ata, sua manifestação acerca do tema da Criação do Prestador de Serviço de Confiança (PSC) na ICP-Brasil, proferida no momento de seu voto:

"Foi concedida a palavra ao Sr Manuel Matos, que salientou que a pauta em debate era composta por 3 escopos distintos (i. a criação de prestador de serviço de confiança; ii. o armazenamento de chaves privativas em HSM; e iii. a exportação das chaves privativas de usuários finais) e que não eram, necessariamente, temas relacionados, sendo possível desmembrá-los para fins de votação. Isto porque, por uma questão de proteção à Infraestrutura de Chaves Públicas Brasileira em um momento em que testemunhamos situações de fragilização de outras PKIs do mundo, como os casos da Estônia e da Espanha, somada ao inedistismo da proposta de exportação de chaves privativas de usuários finais, sem adentrar em eventuais violações à MP nº 2.200-2/2001, o conselheiro, consubstanciado em parecer de lavra do supervisor do LabSEC - Laboratório de Pesquisa e Desenvolvimento em Segurança Computacional da Universidade Federal de Santa Catarina (UFSC), Professor Ricardo Felipe Custódio, mediante solicitação formal encaminhada por este membro titular do Comitê Gestor, apresentou ofício em que foi consignado, em suma, que o LABSEC não tem como "afirmar se os testes realizados foram ou não suficientes para atender a todas as demandas apostas nos normativos em referência" e que o LABSEC entende que "seja prudente realizarmos um piloto, não somente para avaliar de forma mais ampla o processo de portabilidade". Diante de todos os fatos expostos, com vistas a evidenciar que seria plenamente possível deliberar, naquele momento, apenas sobre a criação de prestador de serviço de confiança e sobre o armazenamento de chaves privativas de usuários finais em HSM de terceiros, Manuel Matos questionou à representante do Ministério da Fazenda, Sra. Cláudia Maria Andrade, entidade que possui a maior Autoridade Certificadora Normativa da ICP-Brasil (AC RFB), sobre a necessidade, para fins de aplicações que venham a utilizar HSMs pela RFB, que sua implementação esteja vinculada ou que seja um pré-requisito a possibilidade de importação, exportação ou qualquer forma de portabilidade ou extração das chaves privativas de usuários finais. Em resposta ao questionamento, a representante do Ministério da Fazenda respondeu negativamente, no sentido de que a implementação de aplicações que utilizem HSM não depende da exportação ou exportação de chaves privativas, ressalvando que o Ministério da Fazenda entende ser necessário que os testes sejam mantidos e que continuem sendo realizados, durante o prazo de 180 dias e que, de toda sorte, para fins de mitigar riscos, seria de bom tom que fosse incluída cláusula vinculante da implementação da portabilidade à continuidade e ao êxito dos testes realizados neste período. Manuel Matos agradeceu aos esclarecimentos prestados pela Sra. Cláudia e ponderou que prudentemente, era necessário segregar os assuntos para que pudessem ser votados, deixando tema 'portabilidade de chaves privativas' para ser avaliado em um momento posterior, suportado por laudos técnicos, exaustivos testes, inclusive com diversos fornecedores e amplos debates na academia, junto aos Poderes da República e junto à sociedade civil. A partir das exposições do Sr. Manuel Matos, o Coordenador do Comitê Gestor, Sr Luiz Carlos Azevedo, sugeriu que o tema 'portabilidade' fosse reavaliado posteriormente pelo colegiado, mediante ajuste do artigo 22 da minuta de Resolução, que passaria a contemplar a seguinte redação "Art.22. Esta Resolução entra em vigor na data da sua publicação, exceto quanto ao disposto na Nota 1, do item 1.3.2, do Anexo I, deste documento, o qual entrará em vigor cento e oitenta dias após a regulamentação do Protocolo KMIP no processo de avaliação da conformidade de equipamentos no âmbito da ICP-Brasil (MCT 07 – Volumes I e II), ***absolutamente condicionada a manutenção dos testes de portabilidade durante o período de vacância e à uma nova apreciação pelo comitê gestor ICP-Brasil findo o prazo estabelecido"****. A partir do ajuste sugerido pelo Coordenador, que foi acatado pela integralidade dos presentes e que, portanto, foi incorporada a minuta de Resolução, passou-se à votação da pauta"*

Após solicitação formal da representante da Câmara-e.net, senhor Manuel Matos, faço constar

nesta ata, em anexo, manifestação por escrito acerca do tema da "exportação de chaves privadas de titulares finais de certificados digitais", de lavra do Supervisor do LabSEC - Laboratório de Pesquisa e Desenvolvimento em Segurança Computacional da Universidade Federal de Santa Catarina (UFSC) entregue fisicamente no momento das deliberação ao Chefe de Gabinete do ITI.

Após solicitação formal do representante da ANCD, senhor Julio Cosentino, faço constar nesta ata relato do decorrido da reunião acerca do tema dos bancos, com o devido registro temporal extraído do vídeo do encontro disponível em https://www.youtube.com/watch?v=dlHow05xNxo:

"O senhor Gastão Ramos, Secretário-Executivo do CG pede a palavra, cuja manifestação faço constar nesta, acerca do tema dos bancos: "Ninguém está tolhendo a atuação de ninguém, intenção é a massificação do uso do certificado digital, nem todos os bancos têm AC's ou AR's. Alguns têm, como o Banco do Brasil, a Caixa, o Banrisul e o Bradesco, e todos têm que passar pelo processo de credenciamento do ITI, ou contratar AR's que também passam pelo mesmo processo. A presente resolução preserva todos os quesitos da ICP-Brasil, nossas normas e toda nossa regulamentação.". Sr. Luiz Carlos Azevedo, Coordenador do Comitê Gestor da ICP-Brasil inicia os trabalhos e fala sobre a certificação digital para o sistema financeiro, as facilidades para que se emita certificados digitais para cientes dos bancos sem a necessidade da coleta de documentos, considerando que os bancos já possuem essas normas regulamentadas pelo Banco Central. (00.04.38) Propõe a alteração do texto da Resolução corrigindo o item 2.2.7.1 explicitando que quem emite certificados digitais são as AC's, e não os bancos. O Banco terá que solicitar a AR's de uma AC, ou a uma AR do próprio banco caso ele possua autoridades de registros. (00.07.10) Propõe alteração na redação da NOTA 16, de forma a explicitar que estão dispensadas das normas da ICP Brasil as AR's de bancos que já seguirem as normas equivalentes que o BACEN define e fiscaliza para todos os bancos, e seguem obrigadas a todas as demais normas ICP-Brasil a que não tiverem correspondência. (00.09.00) "O objetivo é a massificação do uso de certificados digitais. Hoje apenas com 3 milhões de pessoas físicas, sendo que os bancos possuem cadastros de clientes com cerca de cento e cinquenta milhões de correntistas (00.09.43). Passe-se a palavra para os participantes titulares do CGICP para as manifestações de praxe. (00.10.15) Antes disso, porém, Sr. Waldeck se manifesta dizendo que "Todos os entes da ICP Brasil estão sujeitos às normas, no entanto é um objetivo constante simplificar, reduzir custos; as AR's e AC's possuem cadastros hoje, mesmo não tendo certificados válidos, e agora com essa resolução podem utilizar esses cadastros. (00.13.20) O senhor Nivaldo se manifesta sobre a posição da AARB, que faço constar nesta: "Eu sempre participei de grupos para a massificação de certificados digitais. Participei do grupo em 2003, 2004, 2005 e, sempre colocamos que o certificado digital não deve parecer uma obrigação fiscal da Receita. Nós somos contra a NOTA 16 e solicitamos a retirada – o DOC-ICP.03.01 V.2.01, Item 2 formaliza a Segurança de Pessoal, em todos os atos normativos, não só para agentes com contrato de trabalho. Nós queremos isonomia. Existe um risco quando o cliente abre uma conta com dinheiro; é muito fácil, os bancos querem isso, no entanto as AR's ficam reféns das normas, os bancos devem seguir as mesmas normas. Esperamos que os bancos contratem as AR's, senão a categoria vai acabar. Encaminhamos retirar a NOTA 16. Encaminhamos voto da AARB para retirada do tema de pauta para discussões mais aprofundadas. Em se mantendo o assunto na pauta, que seja retirada a NOTA 16 e incluído o artigo oitavo, para que os bancos múltiplos e Caixa Econômica Federal, tenham a mesma auditoria da ICP Brasil (00.19.22)". Finalizou a fala concluindo que se não fossem acatadas as sugestões, a AARB votaria contra. Dr. Gastão Ramos, Secretário-Executivo do CG, solicitou a palavra e explicou que "o ITI não faz Resolução para atender segmento A, B, ou C, que o objetivo é massificar o uso de certificados digitais e diminuir custos, e para isso o ITI analisa novos processos e novas tecnologias, tanto que a Resolução apenas inclui os itens necessários nos DOC's existentes. Já existem bancos na ICP Brasil, todos passam pelos mesmos critérios para credenciamento, auditorias e fiscalização. Não há interesse nos bancos, eles já estão dentro da infraestrutura. E qualquer processo novo tem que ser de acordo com a ICP Brasil. Os Bancos são auditados pelo Banco Central, como a ICP Brasil faz. Apenas não redundaremos procedimentos de fiscalização e auditorias em cadastros que já estão sob a fiscalização do BACEN. Os bancos têm que prestar contas à entidade superior. Não tem direcionamento, todos têm que se adequar às normas. (00.21.44) Sobre o Artigo 4o, comenta: "É lícito aproveitar os

cadastros de bancos, AR.s para todos da cadeia. Sem perder a confiança e credibilidade, isso para reduzir custos. ITI não atua em preços, nem em modelos de negócios. Temos preocupação com toda a cadeia produtiva, atendemos os interesses da ICP Brasil". O Coordenador do Comitê Gestor, Sr. Luiz Carlos Azevedo reitera que a redação da NOTA 16 foi alterada. (00.28.50). Sr.Waldeck/DINFRA pede a palavra: "A massificação do uso do certificado digital faz a ICP -Brasil mais forte, traz mais confiança na certificação digital ICP, para toda a sociedade brasileira; a massificação e nossas aplicações". (00.29.00). O interesse é maior dos bancos que da ICP Brasil. Vejam que os bancos não estão isentos da auditoria. Será auditado pelo ITI, sem isenções – abrir conta virtualmente, não consta da norma, a emissão do certificado digital tem que ser presencial para completar as informações. A Nota 16 isenta só o que já existe normatizado na ICP Brasil e BACEN. Sra. Claudia/Ministério da Fazenda pede a palavra e registra que "A Receita Federal do Brasil faz menção de apoio à aprovação da Resolução" (00.32.24). Dr. Rafaello/DAFN faz sua intervenção: "Se os bancos ingressarem como AR.s passarão pelo processo de credenciamento, se contratarem uma AR, a AR estará sob a ICP Brasil e será fiscalizada como qualquer outro integrante da ICP Brasil. O objetivo é modernizar estruturas e ampliar a massificação do uso do CD. (00.32.33) Sr. Nivaldo/AARB, após ouvir explicações dos integrantes do ITI, fez seu encerramento diante do relato da proposta, que faço constar nesta: "Entendemos o exposto, e não somos contrários, queremos isonomia, vocês estão esclarecendo que poderemos usar os cadastros existentes das AR.s. O que nos preocupa é a competição de formiguinhas contra tubarões. Vejam que sou evangelizador de massificação do uso do certificado digital, e somos favoráveis a diminuir custos.". Sr. Salvador, representante da Febraban se manifesta: "O sistema financeiro nacional é altamente regulado, e responsável a responder por crimes de lavagem de dinheiro, por exemplo. (00.44.53) . Muitos dos interesses dos bancos não foram atendidos, mas a massificação requer para os bancos discutir aspectos técnicos e jurídicos para só assim massificar; esse é um primeiro passo (00.46.10). Sr. Luiz Carlos Azevedo, Coordenador do CG, agradece a compreensão da Febraban e encaminha para a votação (00.47.50), mencionando que todas as manifestações serão incorporadas na ata (00.48.14). Sra. Gianni, representante da Fenacor/CNC profere a leitura de seu voto e pede que o mesmo seja anexado, na íntegra à ata da reunião. Demais membros presentes proferem seus votos"

Após solicitação formal do representante da ANCD, senhor Julio Cosentino, faço constar nesta ata relato do decorrido da reunião acerca do tema da Criação do Prestador de Serviço de Confiança (PSC) na ICP-Brasil, com o devido registro temporal extraído do vídeo do encontro disponível em https://www.youtube.com/watch?v=dlHow05xNxo:

"Agradecemos a compreensão sobre o pleito da exigência pelo nível de segurança, T4, com pré-requisito para um PSC, todavia, pedimos rever o SLA de 99,9% para 99,5%, porque de outra forma, fará com que haja aumento dos custos operacionais dos PSS 's e Autoridades Certificadoras. Portanto, propomos que o SLA mínimo do PSC seja o mesmo previsto para um PSS. Ademais, visando maior cautela, sugerimos fortemente a criação de OID específico para os certificados em questão, a fim de mitigar riscos para a infraestrutura." A senhora Cláudia, representante do Ministério da Fazenda pede a palavra, dizendo que "a Receita lutou bastante pelo tema, para que certificados digitais móveis pudessem ser incorporados. É dada a palavra ao Sr. Lacerda, Assessor do ITI, que tece suas considerações acerca da portabilidade da chave privada: " Estamos realizando todos os testes de segurança e viabilidade do processo. Não concluímos os testes ainda. A norma condiciona a entrada à aprovação do MCT. A ideia é que após o relatório final dos testes de portabilidade, o ITI se posicione e atualize o MCT para depois de seis meses torná-la obrigatória. Não existe um açodamento do ITI a essa questão. O importante é que os membros do CG saibam do risco de dependência atual com relação aos fabricantes de HSM, problema que estamos buscando mitigar" (01.19.08). Foi concedida a palavra ao Sr Manuel Matos, representante da Camara-e.net, que salientou que a pauta em debate era composta por 3 escopos distintos (i. a criação de prestador de serviço de confiança; ii. o armazenamento de chaves privativas em HSM; e iii. a exportação das chaves privativas de usuários finais) e que não eram, necessariamente, temas relacionados, sendo possível desmembrá-los para fins de votação. Isto porque, por uma questão de proteção à Infraestrutura de Chaves Públicas Brasileira em um momento em que testemunhamos situações de

fragilização de outras PKIs do mundo, como os casos da Estônia e da Espanha, somada ao inedistismo da proposta de exportação de chaves privativas de usuários finais, sem adentrar em eventuais violações à MP no 2.200-2/2001, o conselheiro, consubstanciado em parecer de lavra do supervisor do LabSEC - Laboratório de Pesquisa e Desenvolvimento em Segurança Computacional da Universidade Federal de Santa Catarina (UFSC), Professor Ricardo Felipe Custódio, mediante solicitação formal encaminhada por este membro titular do Comitê Gestor, apresentou ofício em que foi consignado, em suma, que o LABSEC não tem como "afirmar se os testes realizados foram ou não suficientes para atender a todas as demandas apostas nos normativos em referência" e que o LABSEC entende que "seja prudente realizarmos um piloto, não somente para avaliar de forma mais ampla o processo de portabilidade". A Sra. Claudia/Min. Fazenda esclarece sobre a portabilidade ser ou não ser imprescindível para a Receita Federal do Brasil. "O nosso pedido é sobre o uso de HSM. Contudo, como há vários aspectos sobre segurança, em termos de importação e exportação, temos como sugestão, estabelecer prazo para decisão sobre a exportação ou não de chaves." Sr. Manuel Matos/câmara-e.net agradeceu aos esclarecimentos prestados pela Sra. Cláudia e ponderou que prudentemente, era necessário segregar os assuntos para que pudessem ser votados, deixando tema 'portabilidade de chaves privativas' para ser avaliado em um momento posterior, suportado por laudos técnicos, exaustivos testes, inclusive com diversos fornecedores e amplos debates na academia, junto aos Poderes da República e junto à sociedade civil. A representante da Fenacor/CNC, Sra. Gianni Moreira votou a favor da Resolução, condicionada à ressalva de intensificação e aprovação de testes de portabilidade acerca da proposta de uso do protocolo KMIP. O coordenador, senhor Luís Carlos Azevedo, conduziu o tema, concordando e manifestando a posição de que os testes de portabilidade do certificado digital deverão prosseguir e que após relatórios conclusivos dos mesmos, nova reunião do Comitê Gestor deverá ser requerida para aprovação das operações de importação e exportação de chaves. Enquanto isto não ocorre, o uso de HSM 's para a emissão de "certificados digitais em nuvem" não convencionará a importação e exportação de chaves, inicialmente. A partir do ajuste sugerido pelo Coordenador, que foi acatado pela integralidade dos presentes e que, portanto, foi incorporada a minuta de Resolução, passou-se à votação da pauta"

Registre-se que esta reunião ordinária do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira foi transmitida ao vivo pelo canal do ITI no Youtube. Seu teor permanece na íntegra e à disposição da sociedade no link https://www.youtube.com/watch?v=dlHow05xNxo

Nada mais havendo a tratar, o senhor coordenador deu por encerrada a reunião, da qual, para constar, eu, EDMAR DA SILVA ARAÚJO, Chefe de Gabinete substituto do ITI, à luz do artigo 10 - parágrafo único da Resolução 63 de Abril de 2009, que aprova o regimento interno do Comitê Gestor, lavrei a presente Ata, que, lida e aprovada, encaminha-se assinada digitalmente para publicação no site do ITI www.iti.gov.br

---

Documento assinado eletronicamente por **Edmar da Silva Araújo**, **Chefe de Gabinete da Presidência**, em 22/11/2017, às 11:52, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 1222470026049756493

A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0029501** e o código CRC **F566DAB8**.

PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO
INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

LISTA DE PRESENÇA DO COMITÊ GESTOR DA ICP-Brasil
10 de novembro de 2017

ÓRGÃO	DESIGNAÇÃO	REPRESENTANTE	CONTATO	ASSINATURA
ITI	SECRETÁRIO EXECUTIVO	GASTÃO JOSÉ DE OLIVEIRA RAMOS	(61) 3424-3875	
CASA CIVIL	TITULAR COORDENADOR	LUIZ CARLOS AZEVEDO	(61) 3411-1606 1034 1855	
CASA CIVIL	SUPLENTE	NELSON DO VALE OLIVEIRA	(61) 3411-2716	Nelson do Vale
MINISTÉRIO DA FAZENDA	SUPLENTE	CLÁUDIA MARIA DE ANDRADE	(61) 3412-2495 2476	Cláudia Maria de Andrade
MINISTÉRIO DA, INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS	TITULAR	RAFAEL CUNHA ALVES MOREIRA	(61) 2027-7649	
MINISTÉRIO DO PLANEJAMENTO DESENVOLVIMENTO E GESTÃO	SUPLENTE	JOSÉ NEY DE OLIVEIRA LIMA	(61) 2020-2389	
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO	TITULAR	OTÁVIO VIEGAS CAXETA	(61) 2033-7916 7436	Presente
GSI/PR - GABINETE DE SEGURANÇA INSTITUCIONAL	TITULAR	JOSÉ GARCIA DA LUZ	(61) 3411-2271	

Atualizada em 10/11/2017

CAMARA E-NET	TITULAR	MANUEL DANTAS MATOS	(11) 2539-5556 (11) 97310-1900
CAMARA E-NET	CONVIDADA	PRISCILA FIGUEIREDO	
CAMARA E-NET	CONVIDADO	ROBSON MACHADO	
CAMARA E-NET	CONVIDADO	VINÍCUS SOUZA	
AARB - ASSOCIAÇÃO DAS AUTORIDADES DE REGISTRO DO BRASIL	TITULAR	NIVALDO CLETO	(11) 3675-2230 (11) 99910-8303
AARB - ASSOCIAÇÃO DAS AUTORIDADES DE REGISTRO DO BRASIL	SUPLENTE	BRUNO LINHARES GOMES SOARES	(11) 3675-2230 (11) 99910-8303
AARB - ASSOCIAÇÃO DAS AUTORIDADES DE REGISTRO DO BRASIL	CONVIDADO	PAULO M. ROQUE	(11) 3675-2230 (11) 99910-8303
CNC – CONFEDERAÇÃO NACIONAL DO COMÉRCIO DE BENS, SERVIÇOS E TURISMO	TITULAR	GIANNI MOREIRA LEITÃO	(21) 3077-4777
FEBRABAN -FEDERAÇÃO BRASILEIRA DE BANCOS	TITULAR	SALVADOR MEDEIROS FERRER	(11) 5029-1821 (11) 97167-4799
ANCD-ASSOCIAÇÃO NACIONAL DE CERTIFICAÇÃO DIGITAL	TITULAR	JÚLIO CÉSAR ROGÉRIO COSENTINO	(61) 3224-3851

	SUPLENTE	ANTÔNIO SÉRGIO BORBA CANGIANO	(61) 3224-3851
ANCD-ASSOCIAÇÃO NACIONAL DE CERTIFICAÇÃO DIGITAL			
ANCD-ASSOCIAÇÃO NACIONAL DE CERTIFICAÇÃO DIGITAL	CONVIDADO	VICTOR ESTELLES	
ANCD-ASSOCIAÇÃO NACIONAL DE CERTIFICAÇÃO DIGITAL	CONVIDADA	PATRÍCIA PAIVA	
ANCD-ASSOCIAÇÃO NACIONAL DE CERTIFICAÇÃO DIGITAL	CONVIDADO	MAURÍCIO BALASSIANO	
UFSC	Ouvinte	Jean Gerson Martins	48 996336497
GARTNER	Convidado	Sergio Basso	
GARTNER	"	André Peixoto	
SERPRO	"	Pedro Motta	

SERGIO FUCHS

REUNIÃO DO CG DA ICP-BRASIL

Voto nº 01, de 10 de novembro de 2017.

Delibera sobre a emissão de certificados pelo Sistema Financeiro Nacional (Caixa Econômica Federal e Bancos Múltiplos)

CONSIDERANDO que o objetivo da proposta, segundo fundamentação formulada pelo Instituto Nacional de Tecnologia da Informação, é estimular a massificação do acesso e do uso do certificado digital ICP-Brasil e viabilizar que correntistas, especificamente da Caixa Econômica Federal e dos Bancos Múltiplos, possuam um meio mais célere de obter os certificados digitais nos padrões ICP-Brasil;

CONSIDERANDO que, para tanto, propõe-se que os correntistas solicitantes de certificados digitais devidamente cadastrados perante a Caixa Econômica e Bancos Múltiplos, possam usufruir de benefícios diferenciados dos demais cidadãos para fins de emissão de seu certificado digital;

CONSIDERANDO que a Constituição Federal Brasileira, no *caput* de seu artigo 5º, preconiza que "todos são iguais perante a lei", e que o artigo 37, *caput*, determina que a impessoalidade é um princípio a ser observado diuturnamente pela Administração Pública;

CONSIDERANDO, no que concerne ao objetivo salientado pelo Instituto Nacional de Tecnologia da Informação na formulação das justificativas da pauta ("estimular a massificação do acesso e do uso do certificado digital ICP-Brasil"), que o ITI e o Tribunal Superior Eleitoral (TSE), com a interveniência da Casa Civil da Presidência da República, firmaram aos 07 de novembro de 2017, acordo de cooperação técnica para permitir a criação de uma Autoridade Certificadora no âmbito do TSE, almejando atender às demandas de identificação civil segura instituídas por meio da Lei nº 13.444, de 11 de maio de 2017, que dispõe sobre a Identificação Civil Nacional (ICN), que alcançará indistintamente a todos os cidadãos;

Ante o exposto, **PROPÕE**:

Que sejam ampliados os benefícios de procedimentos diferenciados de qualificação presencial a todos os cidadãos, sejam correntistas ou não destas entidades, descaracterizando-se, portanto, a discriminação e a personificação da diferenciação que se visa conceder apenas à Caixa Econômica Federal e aos Bancos Múltiplos, para que se possa conceber a possibilidade de discussão do tema.

Contudo, em permanecendo, por decisão deste colegiado, a ofensa aos princípios constitucionais da igualdade e da impessoalidade previstos nos artigos 5º e 37 da Constituição Federal Brasileira, o voto deste membro do Comitê Gestor é pela rejeição da proposta.

Por fim, solicita que esta manifestação seja lida e anexada em sua integralidade à ata da presente reunião do Comitê Gestor da ICP-Brasil.

GIANNI MOREIRA LEITÃO
FENACOR/CNC

AARB
Associação das Autoridades de Registro do Brasil

São Paulo, 10 de novembro de 2017.

Ao

Dr. Luiz Carlos de Azevedo

Coordenador do ICP Brasil

Riscos da adoção de simplificação da emissão de certificados digitais para emissores provenientes da área financeira

Introdução

Este documento tem como objetivo expressar uma serie de preocupações das Autoridades de Registro, filiadas à AARB, sobre a adoção das medidas expostas em proposta de alteração da normativa que rege a ICP-Brasil em relação aos correntistas da rede bancária, conforme ofício enviado pela Presidência do ITI em 30/10/2017 e posteriormente ratificado em reuniões realizadas em 01/11/2017 e 06/11/2017.

Partimos da premissa que, em um mercado regulado e que tem como objetivo a prestação de serviço tão essencial à sociedade como a identificação de Pessoas Físicas e Jurídicas no ambiente da internet, o conjunto da legislação e normativas específicas têm missão muito mais abrangente do que somente estabelecer critérios técnicos e legais que orientem a **operação** da certificação digital.

A ICP-Brasil, e aí se encontra parcela importante de seu mérito e sucesso, define uma **estratégia** e uma **estrutura produtiva** para prestação de serviços, com a caracterização de seus "players" e da divisão de tarefas entre esses, assim como apoia o desenvolvimento de um **modelo de negócios** sobre o qual se estabeleceram centenas de empresas que oferecem dezenas de milhares de postos de trabalho.

Em nossa opinião as medidas propostas, por suas características, abalam as bases desta estratégia, da estrutura produtiva e do modelo de negócios constituído, além de apresentarem alguns riscos específicos à segurança do próprio sistema.

Respondendo aos apelos ao diálogo e à participação das entidades representativas do mercado na formulação das políticas para certificação digital, sempre presentes na virtuosa relação que mantemos com a Presidência e Diretorias do ITI, viemos apresentar nossa visão sobre o tema, essencial à sobrevivência de nossos negócios.

Rua Cayowaa, 233 - Perdizes
São Paulo - SP - CEP: 05018-000

Tel: (+55 11) 3675-2230

www.aarb.org.br

Riscos da concentração do mercado e suas consequências no atual mercado

A proposta operacional formulada na alteração ora em discussão oferece enorme **vantagem competitiva** a Autoridades de Registro de propriedade de instituições bancárias, que poderão contar com as informações já processadas e armazenadas pelos bancos e passar a operar dentro do fluxo de tratamento das informações cadastrais bancárias.

As outras Autoridades de Registro não contam com essa possibilidade, justamente por serem uma **terceira parte confiável e isenta**, estranha às relações deste tipo ou de qualquer outro fora do âmbito da ICP-Brasil.

Como a economia formal, que é a base de nosso público alvo, é em seu conjunto bancarizada, existe forte possibilidade de ocorrer a substituição das atuais cadeias de produção da certificação digital por esta nova cadeia simplificada que se abre, atendendo basicamente os mesmos clientes. A extensão da certificação digital para outros clientes será realizada mediante a expansão de serviços bancários específicos, que se potencialmente poderá interessar às instituições bancárias no aprimoramento de suas relações com seus clientes, não irá gerar propagação de negócios fora deste circuito.

Por outro lado, o mercado bancário é extremamente concentrado em alguns poucos bancos, como demonstra o quadro abaixo, com dados de 2010.

Instituição	Correntistas
Banco do Brasil	35.933.973
Bradesco	23.128.870
Itaú	21.920.817
Caixa Econômica	19.261.000
Santander	9.242.000
Banrisul	2.596.842
BNB	812.300
BRB	476.219
Citibank	457.731
Total	113.829.752

Cinco instituições bancárias, sendo que uma das quais já opera como Autoridade Certificadora, concentram grande parte da população que se relaciona com o sistema bancário.

A consequência, do ponto de vista produtivo, é a reprodução no mercado da certificação digital do grau de concentração que já existe na área financeira, com o desaparecimento de centenas de empresas e dezenas de milhares de postos de trabalho, vitimando justamente os precursores da construção da certificação digital no Brasil.

Isto vai na contramão do estabelecido pela Medida Provisória que institui a ICP-Brasil, que delimitou claramente as funções da Autoridade Certificadora, que desenvolve, constrói e

opera a infraestrutura tecnológica – tipicamente vocação de empresas de grande porte, das atividades das Autoridades de Registro, responsáveis pelo atendimento ao público e pelas funções de operacionalizar o sistema, vocação de pequenas e médias empresas.

A proposta em discussão poderá propiciar a expulsão de pequenas e médias empresas deste sistema, substituídas por empresas de propriedade dos grandes grupos financeiros. A possibilidade de contratação de ARs que não sejam de propriedade dos grandes grupos bancários, embora formalmente prevista na normativa, é pouco provável no caso daqueles que concentram a maior parte dos correntistas e negócios, justamente pelas atividades compartilhadas e pelo fluxo previsto.

Riscos do fim da "terceira parte confiável"

Outra premissa da ICP-Brasil é a figura da **terceira parte confiável** que, sem manter interesse nas relações instituídas entre os usuários da certificação digital e as aplicações por estes utilizadas, tem a indispensável isenção para conceder-lhes a identificação inequívoca.

Além dos aspectos jurídicos que norteiam esta separação de papeis entre emissor e mantenedor de aplicações, que garantem higidez legal ao sistema – base essencial sobre as quais se constroem regras de segurança técnicas e operacionais, é estratégico ao interesse nacional a existência de um segmento específico que cuide da identificação de indivíduos e empresas no ambiente da internet.

A longevidade do ramo dos cartórios, instituições seculares que justamente se responsabilizam pelo cumprimento desta e de outras missões análogas no mundo físico, é a comprovação de que é fundamental nas relações humanas a manutenção do conceito da **terceira parte confiável**.

O desaparecimento deste segmento na realidade (ainda que não formalmente), cujas atividades serão assumidas inteiramente por instituições do ramo bancário, em nossa opinião colocam em risco a consistência legal da certificação digital no país.

Riscos operacionais e de segurança

Verificamos também riscos operacionais e de segurança, alguns que inevitavelmente deverão ser enfrentados pela própria ampliação do uso em aplicações financeiras e outro causado especificamente por um aspecto da mudança proposta, a transformação da operação de dupla checagem (validação e posterior verificação).

Rua Cayowaa, 233 - Perdizes
São Paulo - SP - CEP: 05018-000

Tel: (+55 11) 3675-2230

www.aarb.org.br

O crescimento da virtualização das operações bancárias tem causado um incremento das fraudes em todo o mundo. Em nosso país temos um importante histórico de fraudes bancárias, com prejuízo para a sociedade na casa de bilhões de reais anualmente. Uma parcela considerável destas fraudes tem origem interna, ou seja, são realizados por funcionários dos bancos.

Especialistas dão conta de que o fenômeno ainda não está sendo devidamente tratado pelas instituições bancárias. Carlos Sevegni, especialista em prevenção de fraudes bancárias do SAS América Latina comenta, segundo matéria do site especializado DCI, que "Ou existe um processo fraudado dentro do banco que não se sabe nem de onde vem ou a instituição sequer descobriu que tem uma perda. Quanto maior uma organização, mais difícil fica ter controle". Fábio Cegali, especialista em desenvolvimento de soluções antifraude da FICO América Latina, segundo a mesma fonte diz que as instituições ainda "não prestaram a devida atenção" a fraudes em sistemas internos. Segundo ele, "É costume esperar o problema acontecer para o gasto vir na remediação de perdas e isto atrapalha muito".

No caso presente, em que existe a possibilidade da substituição da atual cadeia produtiva de certificação digital por outra formada no interior do segmento bancário, a adoção de novos processos de identificação formal imbricados aos processos internos dos bancos oferece riscos que vão muito além dos aspectos financeiros. O risco essencial é a credibilidade de todo o sistema, baseado em uma cadeia de confiança formada por componentes autônomos e isentos.

Ou seja, os riscos são incrementados pela ampliação do uso pelos bancos são potencializados pela concessão da função da identificação formal e de "Estado" ao ambiente mais exposto as fraudes bancárias.

Soma-se a isto um aspecto operacional importante: atualmente a dupla checagem realizada entre a validação e a verificação abrange todos os aspectos da identificação, desde a presença física do titular, a validade e veracidade dos documentos apresentados, a identificação "cara x crachá" e a execução fidedigna da identificação biométrica. Com o isolamento das duas atividades - esta dupla checagem é substituída por outra mais frágil - cresce o risco de contaminação de nosso sistema por falhas oriundas do sistema bancário.

É inevitável a extensão da certificação digital ao sistema bancário. Isto irá exercer importante pressão por mais segurança em nosso sistema. Para isto, devemos intensificar os esforços antifraude, com mais controle e monitoramento. Infelizmente não identificamos na proposta direcionamento neste sentido.

Conclusões

Rua Cayowaa, 233 - Perdizes
São Paulo - SP - CEP: 05018-000

Tel: (+55 11) 3675-2230

www.aarb.org.br

Como mencionado no início deste documento, consideramos que a adoção da proposição, da maneira como então apresentada, causarão grande transformação no cenário da certificação digital. Tal mudança não tem origem em transformações tecnológicas “disrruptivas” mas na criação de vantagem competitiva a players com grande poder econômico e interesses específicos na disseminação da certificação digital em seus clientes.

Não verificamos a criação de novas vantagens para os titulares de certificados digitais ou para a sociedade. Teremos apenas o crescimento do grau de concentração e a passagem da responsabilidade de identificação de pessoas na internet ao segmento bancário.

Pela relevância destas definições e por seu impacto na estrutura econômica e social, assim como pelas questões de segurança apontadas, não consideramos que haja amadurecimento suficiente para que seja tomada nessa reunião de 10 de novembro, na reunião do Comitê Gestor.

Acreditamos que é essencial ampliar a discussão, envolvendo mais profundamente a sociedade, inclusive através de mecanismos formais de consulta, de maneira que tenhamos definições alinhadas aos interesses nacionais e à maioria dos que participam do mercado.

Neste sentido apelamos à Direção do ITI que retire de pauta o presente ponto, redirecionando-o à discussão e ao debate.

Caso o nosso pleito não seja atendido, nossa manifestação é contra à aprovação da Proposta de Resolução de Emissão de Cerificados pelo Sistema Financeiro Nacional (Bancos), DOC ICP enviada no último dia 07/11/2017.

Atenciosamente

Nivaldo Cleto

Presidente da AARB

Rua Cayowaa, 233 - Perdizes
São Paulo - SP - CEP: 05018-000

Tel: (+55 11) 3675-2230

www.aarb.org.br

REUNIÃO DO CG DA ICP-BRASIL

Voto nº 02, de 10 de novembro de 2017.

Delibera sobre a criação do Prestador de Serviço de Confiança para custodiar chaves privativas de titulares finais emitidas em hardware criptográfico - HSM.

CONSIDERANDO que o tema em questão deve atender a integralidade do que dispõe a Medida Provisória nº 2.200-2/2001, especialmente o que preconiza o parágrafo único do artigo 6º ("*o par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento*");

CONSIDERANDO que a proposta apresentada possui 3 escopos distintos que não são, necessariamente, conectados entre si para justificar sua apreciação em conjunto, quais sejam: (a) a criação de Prestador de Serviço de Confiança; (b) o armazenamento de chaves privativas em HSM; e (c) a exportação das chaves privativas de usuários finais;

CONSIDERNADO que a possibilidade de armazenamento de chaves privativas em ambiente de PSC, mediante rigorosos requisitos, resultaria em potencial aumento do grau de eficiência das atividades desempenhadas pela Administração Pública, destacadamente no bojo dos trabalhos do Conselho Nacional para a Desburocratização - 'Brasil Eficiente';

CONSIDERANDO o entendimento deste membro do Comitê Gestor de que a possibilidade de realização de portabilidade, importação, exportação, clone, cópia e/ou transferência única de chaves privativas fere uma das principais cláusulas pétreas de uma infraestrutura de chaves públicas;

CONSIDERANDO, ainda no entendimento deste membro do Comitê Gestor, que a possibilidade de se replicar as chaves privativas de usuários finais de certificados digitais, responsáveis por atribuir validade jurídica e presunção de autoria às transações eletrônicas dos mesmos, potencializa eventuais ataques e fragilização/comprometimento das chaves privativas em prejuízo de toda a ICP-Brasil e, sobretudo, dos titulares finais dos certificados digitais;

Ante o exposto, **PROPÕE**:

a) Que para a apreciação da pauta, sejam desmembrados 2 dos escopos mencionados (a criação de prestador de serviço de confiança; e o armazenamento de chaves privativas em HSM), sendo excluído o terceiro escopo (exportação das chaves privativas de usuários finais), pelas motivações apresentadas;

b) A aprovação do armazenamento de chaves privativas em HSM custodiado em ambiente de segurança de PSC **absolutamente condicionada** à imposição de vedação da possibilidade de realização de portabilidade, cópia, transferência única, clone, importação e exportação das chaves privativas de usuários finais de certificados digitais, ou qualquer forma que permita a extração da chave privativa do titular do certificado digital ICP-Brasil do ambiente em que foi originalmente gerada, para quaisquer fins.

Por fim, solicita que esta manifestação seja lida e anexada em sua integralidade à ata da presente reunião do Comitê Gestor da ICP-Brasil.

MANUEL DANTAS MATOS
Câmara Brasileira de Comércio Eletrônico

INCIDENTE NORMATIVO – VOTO Nº 02 DE 10 DE NOVEMBRO DE 2017

Complementa a deliberação sobre a criação do Prestador de Serviço de Confiança para custodiar chaves privativas de titulares finais emitidas em hardware criptográfico - HSM.

CONSIDERANDO que o artigo 3º da MP nº 2.200-2/2001 atribui competências normativas exclusivas ao Comitê Gestor da ICP-Brasil e que, ainda, o artigo 13 da Lei nº 9.784, de 29 de janeiro de 1999, determina ser indelegável a edição de atos de caráter normativo e de competência exclusiva atribuída a um órgão ou entidade;

PROPÕE os seguintes ajustes:

a) A supressão do item 'vi' ("Outras autenticações semânticas em acordo com esse documento e previamente aprovadas pela AC Raiz"), do item 6.1, alínea 'c' do DOC-ICP-17.01, o qual transfere atribuições exclusivas do Comitê Gestor para a AC Raiz; e

b) A supressão da NOTA 1 da proposta de resolução que altera o item 2.1.6 do DOC-ICP-03, a qual transfere atribuições exclusivas do Comitê Gestor para a AC Raiz para, por meio de Instrução Normativa, determinar os procedimentos técnicos para operação dos PSC.

Por fim, solicita que esta manifestação seja lida e anexada em sua integralidade à ata da presente reunião do Comitê Gestor da ICP-Brasil.

MANUEL DANTAS MATOS
Câmara Brasileira de Comércio Eletrônico

LabSEC
Laboratório de Segurança em Computação

Florianópolis, 09 de Novembro de 2017

Prezado Manuel Dantas Matos,

É sempre uma grande satisfação poder contribuir com a ICP-Brasil e a sociedade Brasileira. O LabSEC é o Laboratório de Pesquisa e Desenvolvimento em Segurança Computacional da Universidade Federal de Santa Catarina (UFSC), e não poderíamos deixar de responder à sua demanda. Seguem respostas às suas perguntas:

1 - "O LABSEC-UFSC considera que os testes realizados foram suficientes para a aprovação da pauta colocada em debate no âmbito do Comitê Gestor da ICP-Brasil?"

Não temos como afirmar se os testes realizados foram ou não suficientes para atender a **todas** as demandas apostas nos normativos em referência. Tenho dúvidas quanto a, por exemplo, como será tratado a questão da cópia de segurança dos HSMs dos prestadores de serviços de confiança (PSC). Vejamos: um PSC-1 tem um HSM operacional e respectivos backups. Ao realizar o transporte de uma chave privada de um titular de certificado para o HSM do PSC-2, não está claro como será tratado os backups já realizados pelo PSC-1. Neste caso, o PSC-1 ainda terá cópias da chave privada do titular do certificado.

O que podemos afirmar é que os testes com o excelente protocolo de gerenciamento de chaves KMIP foram feitos com sucesso e este protocolo trabalha muito bem.

2 - "A Instituição considera pertinente que seja realizada a votação em apartado de normas e procedimentos para portabilidade de chaves privativas de titulares de certificados digitais armazenados em HSM? Em caso positivo e acaso tal fato venha a ocorrer, a Instituição entende que este tema poderá voltar a ser debatido pelo Comitê Gestor da ICP- Brasil depois de realizados exaustivos testes de hardwares criptográficos de fornecedores diversos e edição de laudo conclusivo devidamente publicado por parte desta prestigiosa Instituição?"

Entendemos que seja prudente realizarmos um piloto, não somente para avaliar de forma mais ampla o processo de portabilidade, mas também para tratar de questões

importantes como a auditoria dos PSCs no tangente a portabilidade. É fato que a possibilidade de permitir a salvaguarda e uso de certificados e respectivas chaves privadas na nuvem é um grande avanço na ICP-Brasil e enorme benefício para os usuários e permitirá, não somente o barateamento do certificado digital, mas também abrirá muitas oportunidades de novos modelos de negócios relacionados ao mercado de certificação digital no Brasil. Isso, certamente levará a um modelo mais racional e justo quanto aos custos de gerenciamento do ciclo de vida dos certificados digitais. Outro ponto que precisa ser tratado é o monitoramento dos PSCs quanto ao correto uso da portabilidade. Por exemplo, o que ocorre com a chave privada se o titular de um certificado digital perder o seu smartphone?

Colocamo-nos à disposição da ICP-Brasil para avaliar todos os aspectos técnicos relacionados a portabilidade e também, se necessário, avaliar os HSMs que implementem o KMIP.

3 - "Por fim, qual a recomendação técnica exarada por parte do LABSEC- UFSC acerca dos graves incidentes de segurança que ocorreram em países da Europa, que se valem de identidades digitais em parâmetros semelhantes ao proposto?"

Os recentes incidentes de segurança relacionados ao uso de smartcards com problemas na geração de chaves privadas têm assustado várias nações. Países como a Estônia há alguns dias e mais recente ainda, a Espanha estão revogando seus certificados em escala até agora inimagináveis. Seria imperativo que a ICP-Brasil se preocupasse com isso e tivesse um levantamento preciso de quais Autoridades Certificadoras utilizam os mesmos dispositivos criptográficos com falhas reportados e defina o que será feito, caso existam, com os certificados já emitidos.

Prof. Ricardo Custódio
Supervisor do LabSEC

PROCURAÇÃO

Eu, Manuel Dantas Matos, inscrito no CPF/MF sob o nº 338.584.897-00, membro titular do CG ICP-Brasil, venho, por meio da presente procuração, e nos expressos termos em que facultado pelo art. 15 do Regimento Interno deste e. Comitê[1], nomear, *ah hoc*, para a representação institucional da CAMARA E-NET, em face da impossibilidade de meu comparecimento/permanência, bem como de meu suplente, André Pinto Garcia, na reunião ordinária que se realizará no dia 10/11/2017, a Dra. Ledi Priscila Figueiredo, inscrita no CPF/MF sob o nº 392.914.818-82.

Os votos a serem proferidos relacionados à pauta de convocação seguem no anexo do presente instrumento, que serão lidos pela mandatária e anexados à ata da reunião do colegiado.

Brasília-DF, 10 de novembro de 2017.

MANUEL DANTAS MATOS

[1] Art. 15. Terão direito a voto no Comitê Gestor os membros designados pelo Presidente da República, ou seus suplentes, em caso de ausência ou impedimento do titular. Parágrafo único. Caso haja a impossibilidade de participação do titular e seu suplente, poderá ser indicado representante com direito a voto, desde que outorgada procuração que contenha o assunto referente da pauta e o teor do voto, que constará na ata da reunião.