COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA

ATA DE REUNIÃO

Aos 3 dias do mês de julho do ano de 2018, às 9 horas, nas dependências do Instituto Nacional de Tecnologia da Informação – ITI, situado no endereço SCN Qd. 02 Bl. E, na cidade de Brasília/DF, reuniram-se 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: Antonio José Barreto de Araújo Junior (Coordenador titular do CG ICP-Brasil); Gastão José de Oliveira Ramos (Secretário-Executivo do CG ICP-Brasil); Fernando Nascimento Barbosa (Titular do Ministério da Fazenda); Rafael Cunha Alves Moreira (Titular do Ministério da Indústria, Comércio Exterior e Serviços); Luis Felipe Salin Monteiro (Titular do Ministério do Planejamento, Desenvolvimento e Gestão); Tiago Oliveira Loup (Suplente do Ministério da Justiça e Segurança Pública); Otávio Viegas Caixeta (Titular do Ministério da Ciência, Tecnologia, Inovação e Comunicações); José Garcia da Luz (Titular do Gabinete de Segurança Institucional da Presidência da República); Márcio Nunes da Silva (Suplente da ANCD); Ubiratan Pereira Guimarães (Titular da Camara-e.net); Marcelo Lemgruber (Titular da AARB); Gianni Moreira Leitão (Titular da CNC/Fenacor); Salvador Medeiros Ferrer (Titular da Febraban); Waldeck Pinto de Araújo Júnior (Diretor de Infraestrutura de Chaves Públicas do ITI); Wilson Roberto Hirata (Diretor Substituto de Auditoria, Fiscalização e Normalização); Alexandre Munia Machado (Procurador Federal Chefe); Eduardo Magalhães de Lacerda Filho (Assessor do Diretor-Presidente do ITI); Ruy Cesar Ramos Filho (Assessor do Diretor-Presidente do ITI); José Rodrigues Gonçalves Júnior (Coordenador-Geral de Segurança da Informação do ITI); André Machado Caricatti (Coordenador-Geral de Operações do ITI); Noara Gouvêa Conceição (Coordenador-Geral de Auditoria e Fiscalização); Marlene Isidro da Silva (Coordenadora de Auditoria e Fiscalização); Os demais, a seguir, participaram na qualidade de ouvintes: Maurício Balassiano, Egon Schaden, Vinícius Vieira de Sousa, Vinicius Ghibu, Renan Correia Martino, Priscila Figueiredo, Leonardo Elias, Sara Coraini, Gabriell Campos de Assunção, José Camilo de Oliveira Nagano e Rafael Piacentini Caporali.

Registra-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=OEcogiDC0Lo

Após os cumprimentos protocolares, as senhoras e senhores acima identificados como membros do CG ICP-Brasil deliberaram sobre os seguintes temas:

1. PORTABILIDADE DE CHAVES - PSC

Ao assessor técnico da presidência do ITI, Eduardo Magalhães de Lacerda Filho, foi concedida a palavra para que apresentasse o parecer técnico sobre a portabilidade de chaves criptográficas no âmbito dos Prestadores de Serviço de Confiança - PSC da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil. Tal documento havia sido encaminhado a todos os membros do Comitê Gestor em 14 de Junho de 2018. Prosseguiu Lacerda sobre a autoria do referido parecer, esta do ITI, e que os testes em questão foram realizados com o apoio da equipe técnica do Labsec/UFSC e das equipes técnicas das empresas Dinamo e Kryptus, ambas provedoras de hardware e software de Host Security Modules (HSM). Após suas explicações técnicas, o coordenador do Comitê abriu a palavra aos presentes. O representante da ANCD, Márcio Nunes, pediu ao Coordenador que retirasse o item da pauta a ser deliberado face ao tempo exíguo para análise e amadurecimento da proposta no âmbito de sua entidade, além de propor o encaminhamento do tema à Comissão Técnica Executiva do CG ICP-Brasil (COTEC). Em seguida, o assessor técnico do ITI esclareceu que os processos de emissão de certificados digitais ICP-Brasil não mudam, mas apenas o armazenamento que deixa de ser em cartão e em token e passa a ser em HSM, mais seguro e com requisitos de segurança adicionais, como a dupla autenticação. Concedida a palavra à representante da CNC/FENACOR, Gianni Moreira Leitão, esta explicou aos presentes que não se sentia segura para deliberar sobre o tema, reforçou as colocações do senhor representante da ANCD, e solicitou que o item fosse retirado de pauta para que houvesse mais tempo para análises e estudos. Ainda afirmou que havia questionamentos técnicos a serem apresentados aos demais colegas do Comitê Gestor. O coordenador do CG ICP-Brasil concedeu a palavra ao diretor de Infraestrutura de Chaves Públicas do ITI Waldeck de Araújo Júnior, tendo este destacado que a portabilidade amplia a competição no âmbito da ICP-Brasil, favorece as próprias autoridades certificadoras já que estas, ao terem algum problema com determinados fabricantes ou fornecedores, poderiam exportar suas chaves em vez de revoga-las, como atualmente ocorre. O secretário-executivo do CG ICP-Brasil, depois que lhe foi concedida a palavra, ratificou os dizeres do diretor de Infraestrutura do ITI e, ainda, expôs que entendia que o tema fora objeto de deliberação na reunião do colegiado ocorrida em 10 de novembro de 2017 (ata disponível em http://www.iti.gov.br/images/repositorio/comite/atacgicpbrasil_10112017.pdf). Na sequência, o representante da AARB, Marcelo Lemgruber, ponderou que também se sentia inseguro com relação aos testes apresentados, muito embora a AARB compreendesse a relevância do tema e fosse favorável ao mesmo, concordando com os membros do Comitê que o antecederam pelo adiamento do item na pauta do colegiado. Neste momento, o coordenador do CG ICP-Brasil recordou que o tema da portabilidade não estava em pauta, mas sim o parecer técnico produzido e encaminhado aos membros do colegiado. Após, concedeu a palavra ao representante da Camara.e-net, Ubiratan Pereira Guimarães, que destacou que o tema não estava amadurecido o suficiente para deliberação, sendo também favorável à retirada do item da pauta, além de comentar que o assessor técnico do ITI tinha deixado a entender que ainda havia evoluções a se realizar. Então, após ter a palavra concedida, o representante da FEBRABAN, Salvador Medeiros, ponderou que igualmente concordava que o tema carecia de amadurecimento, muito embora compreendesse a importância da portabilidade. Concedida a palavra, Eduardo Lacerda, o assessor técnico do ITI, expôs sua opinião de que evoluções desta natureza são factíveis face a condição da própria tecnologia, sempre renovada pela quantidade de possibilidades de aprimoramento. Ratificou, ainda, que os testes, em seu entendimento, foram conclusivos e que havia viabilidade e segurança para a portabilidade. Ato contínuo, o representante da Camara.e-net apresentou duas questões de um conjunto maior de

perguntas ainda em aberto, que geram desconfortos e insegurança, sem prejuízo de outras questões que permeiam o tema, a saber, 1) como o usuário saberá se sua chave privada foi excluída; e 2) como o usuário poderia auditar os processos de portabilidade de chaves. Neste momento, o coordenador do CG ICP-Brasil pediu que Lacerda explicasse as questões lidas pelo representante da Camara.e-net. À primeira, tratou de esclarecer que era procedimento simples por meio de envelopamento de chave e verificado a partir de *dubbing loop*, quando se é possível identificar o log de extinção daquela chave; À segunda, esclareceu que o usuário tem diversas formas de contato com o PSC para saber sobre as atividades de sua chave privada. O PSC, como já consta em norma, tem que enviar ao titular da chave informações sobre quaisquer usos do certificado. Em seguida, o representante da ANCD manifestou-se que a discussão não era sobre a capacidade criptográfica, enfim, sobre transferência, mas sim todo o processo envolvido. Explicou que a sugestão de exercitar mais o próprio relatório era em detrimento das próprias experiências que as ACs têm, pois são infraestruturas diferentes, cada qual respeitando padrões, mas diferentes. Destacou a necessidade de exercitar sobre como ter o controle sobre essas evidências todas e como disponibilizá-las para os usuários, e que quando se fala de portabilidade, já está se falando de portabilidade de chave privada, sobre portabilidade do usuário. Continuou Márcio Nunes que ao emitir o certificado digital e gerar um par de chaves, vincula-se a titularidade daquele par de chaves, não havendo necessidade de transportar a chave para gerar novo certificado digital. Então, segundo o representante da ANCD, a portabilidade de um usuário titular não está intrínseca à transferência da chave, sendo possível gerar o certificado para outro usuário em outra chave. Márcio Nunes ponderou que a preocupação tratava-se da possibilidade de criar mais processos digitais ou mais processos dentro de uma mesma operação, o que segundo ele aumentaria as vulnerabilidades ou os itens de controle. A preocupação da ANCD não teria a ver com segurança sobre a operação como um todo, pois não há dúvida sobre o protocolo KMIP em si, mas sim como implementar adequadamente, levando em consideração que há um PSC operando e que não haveria experiências e cenários de uso suficientes para mensurar os efeitos. Por fim, Márcio Nunes disse não ser contrário ao tema, mas entendia ser necessário tempo para poder exercitar o tema e tirar dúvidas e outras questões de sua entidade. Face às manifestações pela retirada do item da pauta, o coordenador do CG ICP-Brasil recordou aos presentes que o Regimento Interno do próprio CG prevê a possibilidade de retirada de pauta desde que houvesse a concordância pela maioria dos presentes (Art 21° da Resolução n° 137, de 8 de Março de 2018 - http://www.iti.gov.br/comite-gestor/2-uncategorised/97-regimento-interno). O representante do Gabinete de Segurança Institucional da Presidência da República, José Garcia, ao ter a palavra, ponderou que havia entendido não haver contestações acerca do relatório técnico, mas que a iniciativa privada desejava regras de migração e regras de segurança explícitas para a portabilidade. Questionou aos presentes se seu entendimento estava correto. O representante da ANCD, Márcio Nunes, após a concessão da palavra, ponderou que a preocupação da entidade versava sobre dois aspectos: o primeiro tem a ver com o relatório técnico que explicita o resultado de dois fabricantes. Cada um dos PSCs utilizarão fabricantes distintos, aqueles que estiverem homologados, que também farão os seus testes, e que não estivam confortáveis por estarem, ainda, decidindo quais serão os HSMs. Reiterou não haver dúvida sobre a capacidade técnica envolvida, mas sobre o corpo dos PSS que se enquadram em ACs e que pretendem se qualificar como PSC. Que haverá uma óbvia seleção de equipamentos no mercado, havendo dois disponíveis no momento, que já tem suas baterias de testes, seus controles de qualidade sobre os HSMs, sobre os equipamentos em si dentro de uma Infraestrutura, não sendo suficiente apenas suportar o KMIP, mas que há outro contexto de uma infraestrutura. O outro aspecto teria a ver com a junção dessa análise, cada qual nas suas experiências e necessidades, posto que há apenas um PSC operando atualmente, então ainda não

existe uma massa crítica de PSCs rodando com interações de usuários diferentes, para justamente ser possível entender como isso funcionaria. Na sequência, o Coordenador do Comitê Gestor da ICP-Brasil colocou em deliberação a retirada do item 1 da pauta, tendo resultado no seguinte: cinco votos favoráveis à retirada do item da pauta (AARB, FEBRABAN, ANCD, CNC/FENACOR e Camara-e.net) e sete votos contrários a retirada do item de pauta (Ministério da Justiça, MCTIC, Ministério da Fazenda, Casa Civil, Ministério do Planejamento, MDIC, Gabinete de Segurança Institucional da Presidência da República). Posto isso, o coordenador reiterou que o debate era acerca do parecer técnico e não de novo regramento no âmbito da ICP-Brasil.

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/PRGabinete 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.

Apuração: 12 a 0 (aprovado por unanimidade)

2. CERTIFICADO DIGITAL PARA OBJETOS METROLÓGICOS

Ao assessor técnico da presidência do ITI, Ruy Cesar Ramos Filho, foi concedida a palavra quando explicou em linhas gerais sobre a criação de um certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil para objetos metrológicos acreditados pelo Inmetro. Recordou que a Portaria nº 294, de 29 de Junho de 2018, determina que o certificado ICP-Brasil deverá ser observado no que concerne à assinatura digital e algoritmos criptográficos para emissão de certificado digital aplicável aos instrumentos pertinentes ao normativo, tendo seu primeiro uso nas bombas de gasolina, mas poderá ser aplicado em outros equipamentos, como balanças e relógios medidores de energia elétrica. Advindo de parceria entre as duas entidades, o principal objetivo desse novo certificado é coibir fraudes ocorridas na venda de combustíveis. O secretário-executivo do CG ICP-Brasil explicou que inicialmente pensava-se no nome "IOT-BR" para este certificado, alterado face a iminente publicação de regramento pelo Ministério da Ciência, Tecnologia, Inovação e Comunicações sobre Internet das coisas que, coincidentemente, escolhera o mesmo nome. Explicou, também que tal item vai ao encontro de demanda apresentada pelo Inmetro e MDIC ao ITI, inclusive por meio de reuniões com o próprio ministro do MDIC. Concedida a palavra, o membro titular do MCTIC Otávio Viegas destacou que a aprovação do certificado para objetos metrológicos ocorre em bom momento. Sobre o programa para internet das coisas, explicou que desde 2014 há uma câmara setorial para traçar estratégias de desenvolvimento da internet das coisas coordenada pela pasta. Buscou-se as áreas de oportunidade para o desenvolvimento da internet das coisas, chamadas de verticais, elegendo-se as verticais "Cidades", "Saúde", "Rural" e "Indústria". Márcio Nunes, representante da ANCD, ao proferir seu voto favorável, sugeriu que o tema fosse encaminhado à COTEC para que fosse possível discutir a aplicabilidade do item para outros objetos, bem como os desdobramentos e regras do processo de emissão destes certificados.

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/PRGabinete 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.

Apuração: 12 a 0 (aprovado por unanimidade)

3. ALTERA A CONCEITUAÇÃO DE LABORATÓRIOS DE ENSAIOS E AUDITORIA - LEA

Ao coordenador-geral de operações do ITI André Machado Caricatti foi concedida a palavra para que explanasse sobre o item em deliberação. A proposta tem por objetivo autorizar que os laboratórios acreditados ou designados no âmbito do SBAC/INMETRO possam realizar as atividades de avaliação e homologação de equipamentos, atualmente deferidas apenas aos LEA que tenham sido previamente credenciados. A aprovação deverá atender demanda hoje existente, bem como conferir maior segurança ao processo de avaliação de conformidade dos produtos da ICP-Brasil, haja vista que tais laboratórios estão sujeitos a prévio credenciado no âmbito do SBAC/INMETRO, bem como devem observar os Requisitos Gerais de Certificação de Produtos - RGCP, aproximando, com isso, o modelo de acreditação dos produtos da ICP-Brasil com aqueles que constam do SBAC/INMETRO.

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/PRGabinete 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.

Apuração: 12 a 0 (aprovado por unanimidade)

4. PROCEDIMENTOS PARA A EMISSÃO DE CERTIFICADOS DIGITAIS PARA SERVIDORES PÚBLICOS DA ATIVA DOS ESTADOS

Ao diretor Substituto de Auditoria, Fiscalização e Normalização do ITI Wilson Hirata, foi concedida a palavra, quando este explanou sobre o item em deliberação. Explicou que a Imprensa Oficial do Estado de São Paulo (IMESP), face a demanda em curso, propôs que a atual norma que possibilita a emissão de certificados digitais para servidores públicos da ativa e militares da união (Resolução nº 121, de 6 de Julho de 2017 – http://www.iti.gov.br/images/repositorio/legislacao/resolucoes/emvigor/Resolucao_121_-_CERTIFICADO_PARA_SERVIDORES_PUBLICOS_DA_ATIVA_E_MILITARES_DA_UNIAO_Assinada.pdf) seja estendida aos servidores públicos da ativa dos estados. O secretário-executivo do Comitê Gestor, após concessão da palavra, complementou que não apenas o estado de São Paulo, mas outros, como o Paraná, também já manifestaram interesse na proposta. Explicou ainda que a norma aprovada pelo Comitê evitará a criação de muitos modelos estaduais, o que é prejudicial para a toda a cadeia hierárquica. Concedida a palavra, o representante titular do

Ministério do Planejamento Luis Felipe Salin Monteiro defendeu a proposta ao afirmar que o governo tem estudado as melhores formas de emissão de certificados para servidores públicos federais, além de que os certificados emitidos estarão devidamente vinculados às necessidades de uso do certificado, finalizando que a extensão do texto é algo vantajoso e deveria ser aprovada pelo Comitê Gestor. O coordenador do CG ICP-Brasil explicou que trata-se de uma demanda importante e que a aprovação evita expansões desordenadas e que a omissão do CG traria uma série de inconvenientes. Neste instante, o representante da ANCD recordou que a proposta para emissão de certificados digitais para servidores públicos da ativa e militares da união foi rejeitada por sua entidade. Disse também que o processo de identificação e validação deveria ser idêntico para servidores públicos como é para o cidadão comum e que, em tese, o texto proposto feriria a Medida Provisória 2.200-2, de 24 de agosto de 2001. Posto isso, o coordenador concedeu a palavra ao Procurador Federal Chefe do ITI Alexandre Munia, que explicou que a questão de afronta ao diploma legal estaria superada desde outras propostas. Explicou o procurador, também, que todas as etapas de identificação bem como os entes que emitiriam estes certificados para servidores públicos serão, respectivamente, idênticos ao ocorrido no âmbito das AR, e credenciados à luz de todos os normativos em voga da ICP-Brasil. A particularidade no âmbito do serviço público é a fé pública envolvida, além da utilização de cadastros prévios, como o biométrico do TSE. Concedida a palavra, o membro titular Marcelo Lemgruber demonstrou preocupação com as possibilidades de controle face aos inúmeros níveis de serviço público existentes no Brasil, o que em tese dificultaria a uniformização e padronização dos procedimentos para emissão de certificados digitais. O diretor de Infraestrutura de Chaves Públicas do ITI Waldeck de Araújo Jr. explicou que há condições sine qua non para que os estados possam emitir certificados digitais aos seus servidores, como um sistema confiável de gestão de pessoal análogo ao Sistema de Gestão de Pessoas (SIGEPE). Após, o secretário-executivo do CG ICP-Brasil Gastão José de Oliveira Ramos deixou claro que não haverá flexibilização das normas de credenciamento às AR dos governos federal e estadual. O ITI, prosseguiu Gastão, dará o mesmo tratamento e utilizará os mesmos critérios independentemente de quem deseje ser ente credenciado da ICP-Brasil.

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/PRGabinete de Segurança Institucional; e Febraban – Federação Brasileira de Bancos.

Contrário: ANCD – Associação Nacional de Certificação Digital; Camara-e.net – Câmara Brasileira de Comércio Eletrônico, Fenacor/CNC e AARB –Associação das Autoridades de Registro do Brasil.

Apuração: 8 a 4 (aprovado)

Após as deliberações, o representante da Camara-e.net solicitou que seus votos constassem por escrito nesta ata em sua totalidade.

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 7° da Resolução 137, de 8 de março de 2018, que aprova o regimento interno do Comitê Gestor, lavrei

a presente Ata, que, lida e aprovada, encaminha-se assinada digitalmente para aquiescência do secretário-executivo do Comitê Gestor da ICP-Brasil, e posterior publicação no site do ITI www.iti.gov.br

EDMAR DA SILVA ARAUJO:98643622168

Assinado de forma digital por EDMAR DA SILVA ARAUJO:98643622168
Dados: 2018.07.31 17:08:44 -03'00'

Aprovo a lavratura da presente Ata de Reunião. Publique-se.

GASTAO JOSE DE OLIVEIRA RAMOS:15016609187

Assinado de forma digital por GASTAO JOSE DE OLIVEIRA RAMOS:15016609187
Dados: 2018.07.31 17:54:18 -03'00'

GASTÃO JOSÉ DE OLIVEIRA RAMOS

Secretário-Executivo do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil