

REUNIÃO DO CG DA ICP-BRASIL
Voto nº 01, de 03 de julho de 2018.

Delibera sobre a portabilidade de chaves privadas de usuários finais

A CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO – CAMARA-E.NET, por seu representante designado nos moldes do disposto no artigo 3º da Medida Provisória nº 2.200-2/2001, quanto ao item em questão, manifesta-se no seguinte sentido:

- I. **CONSIDERANDO** que Medida Provisória nº 2.200-2/2001 dispõe que a chave privada do titular deve permanecer sob seu exclusivo controle, uso e conhecimento (parágrafo único do artigo 6º);
- II. **CONSIDERANDO** que a geração e armazenamento das chaves privadas em HSM de terceiros, por si só, já relativizam a exclusividade do controle das mesmas por seu titular;
- III. **CONSIDERANDO** que a portabilidade de chaves privadas expõe os usuários de certificados à múltiplos riscos conforme menciona a descrição expressa no detalhamento da pauta encaminhada para deliberação deste colegiado (item 6 – *“Não foram identificados impactos ou riscos associados à medida proposta, além dos já mapeados no manuseio de uma chave privada”*);
- IV. **CONSIDERANDO** que a portabilidade das chaves privadas infringe o disposto no parágrafo único do artigo 6º da MP nº 2.200-2/2001, dada a perda de controle e rastreabilidade das chaves privadas por seu titular, comprometendo a chave privada e expondo os usuários à múltiplos riscos, inclusive de responsabilidades civis decorrentes do uso indevido das chaves;
- V. **CONSIDERANDO**, que esta entidade apresentou inúmeros questionamentos ao Instituto Nacional de Tecnologia da Informação mediante ofício nº 05/2017, protocolado aos 08/11/2017, sem que tenha recebido respostas até o presente momento;
- VI. **CONSIDERANDO**, ainda, que esta entidade já se posicionou contrária a qualquer forma de manipulação das chaves privadas do local onde originalmente tenha sido gerada, conforme voto apresentado perante o Colegiado em 10/11/2017, inclusive mediante fundamentação em parecer apresentado pelo Laboratório de Segurança em Computação – LABSEC da Universidade Federal de Santa Catarina;
- VII. **CONSIDERANDO** que a Resolução CG ICP Brasil nº 132/2017 instituiu os Prestadores de Serviços de Confiança, mas vinculou expressamente a vigência dos dispositivos relacionados à portabilidade de chaves privadas de usuários finais à uma nova deliberação do Comitê Gestor especificamente sobre os itens suspensos, desde que respaldada por laudos técnicos, exaustivos testes, inclusive com diversos fornecedores e amplos debates na academia, junto aos Poderes da República e junto à sociedade civil, conforme disposto na ata da referida reunião – disponível em http://www.iti.gov.br/images/repositorio/comite/atacgicpbrasil_10112017.pdf;
- VIII. **CONSIDERANDO** que a presente deliberação visa meramente apreciar o parecer

técnico de autoria do Instituto Nacional de Tecnologia da Informação – ITI, que aponta pela realizabilidade técnica do procedimento de portabilidade de chaves privadas de usuários finais entre HSMs;

ANTE O EXPOSTO,

Vota pela aprovação do parecer técnico de autoria do Instituto Nacional de Tecnologia da Informação – ITI.

Contudo, reitera o entendimento de que a portabilidade de chaves privadas de usuários finais viola as disposições da Medida Provisória nº 2.200-2/2001 e que expõe os cidadãos à riscos de uso e acesso indevido das chaves, com perda de rastreabilidade e perda do controle das manifestações de vontade do signatário em meio eletrônico.

Destarte, roga para que eventuais novos debates relacionados a vigência dos dispositivos relacionados à portabilidade de chaves somente seja encaminhado ao Comitê Gestor da ICP-Brasil para nova apreciação com base no artigo 22 da Resolução nº 132/2017, desde que exauridos os testes e debates no âmbito da COTEC, inclusive nos aspectos jurídicos e que os debates no âmbito da sociedade civil e demais poderes, mediante realização de audiências públicas, sejam evidenciados e amplamente divulgados.

Por fim, pugna pela leitura e inclusão integral deste voto na ata da presente reunião do Comitê Gestor da ICP-Brasil.

UBIRATAN PEREIRA GUIMARÃES

CAMARA-E.NET

REUNIÃO DO CG DA ICP-BRASIL
Voto nº 02, de 03 de julho de 2018.

Delibera sobre a criação de política de certificados IOT-BR, exclusiva para objetos metrológicos no âmbito do INMETRO

A CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO – CAMARA-E.NET, por seu representante designado nos moldes do disposto no artigo 3º da Medida Provisória nº 2.200-2/2001, quanto ao item em questão, manifesta-se no seguinte sentido:

- I. **CONSIDERANDO** que a proposta em questão visa criar uma política específica de certificados para objetos metrológicos no âmbito do INMETRO;
- II. **CONSIDERANDO** que o INMETRO é uma autarquia federal vinculada ao Ministério da Indústria, Comércio Exterior e Serviços – MDIC e que, nesta condição, à luz do Decreto nº 3.996, de 31 de outubro de 2001, a autarquia somente poderia utilizar ou expedir certificados (e neste último caso, se credenciado no âmbito da ICP-Brasil como entidade integrante da Infraestrutura) se forem providos no âmbito da ICP-Brasil;
- III. **CONSIDERANDO** que os debates sobre a presente pauta se iniciaram a partir da edição da Portaria INMETRO nº 559/2016, que estabelece *“condições técnicas e metrológicas mínimas e de segurança de software e hardware a que devem atender as bombas medidoras de combustíveis líquidos utilizadas nas medições de volume”*;
- IV. **CONSIDERANDO** que a referida Portaria menciona que o estabelecimento dos critérios nela contidos, inclusive da aposição de assinaturas digitais, servem-se para *“melhorar a confiabilidade das bombas medidoras de combustíveis líquidos em relação à possibilidade de fraudes”*;
- V. **CONSIDERANDO** que os certificados digitais da ICP-Brasil atribuem autenticidade, integridade e validade jurídica às transações e registros realizados por meio de sua aposição em relação ao seu signatário;
- VI. **CONSIDERANDO** que, no caso em tela, o titular do certificado digital seria o fabricante do objeto metrológico (bomba de combustível, no caso da Portaria em comento) e que não prevê os procedimentos necessários ou decorrentes de manipulação indevida, manutenção, quebra ou substituição dos equipamentos metrológicos, como também não trata da delimitação das responsabilidades entre o titular do certificado digital que estaria contido no objeto metrológico, do proprietário/possuidor do objeto e do próprio INMETRO (que seria, na pauta em deliberação, um dos responsáveis pela revogação do certificado digital do objeto metrológico);
- VII. **CONSIDERANDO**, portanto, que a política em tela ainda carece de maior detalhamento em relação aos objetos metrológicos

ANTE O EXPOSTO

Vota pela aprovação da pauta com o encaminhamento do tema para

análise e refinamento da COTEC, com participação do INMETRO, CONMETRO e MDIC, para que a política destes certificados digitais para objetos metrológicos seja melhor detalhada e que os certificados digitais apostos nos objetos contribuam de fato com a segurança do mercado e do consumidor, garantida a segurança dos certificados ali armazenados contra qualquer forma de comprometimento das chaves privadas neles contidas.

Por fim, pugna pela leitura e inclusão integral deste voto na ata da presente reunião do Comitê Gestor da ICP-Brasil.

UBIRATAN PEREIRA GUIMARÃES

CAMARA-E.NET

REUNIÃO DO CG DA ICP-BRASIL
Voto nº 03, de 03 de julho de 2018.

Delibera sobre a ampliação do rol de entidades consideradas como Laboratórios de Ensaios e Auditoria – LEA

A **CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO – CAMARA-E.NET**, por seu representante designado nos moldes do disposto no artigo 3º da Medida Provisória nº 2.200-2/2001, quanto ao item em questão, manifesta-se no seguinte sentido:

- I. **CONSIDERANDO** que compete ao Comitê Gestor da ICP-Brasil “*aprovar as normas para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil*” (art. 5º do Regimento Interno do Comitê Gestor);
- II. **CONSIDERANDO** que o encaminhamento de pauta que pretende ampliar o rol de entidades consideradas como Laboratórios de Ensaios e Auditoria - LEAs indica uma eventual necessidade de revisão das normas da ICP-Brasil sobre o processo de credenciamento destas entidades da ICP-Brasil;
- III. **CONSIDERANDO** a importância de que todas as entidades que atuem sob a égide da ICP-Brasil, na condição de AC, ARs e prestadores de serviços (nos moldes da MP nº 2.200-2/2001) devam ser devidamente credenciados perante a ICP-Brasil, com a devida publicidade do procedimento de credenciamento;
- IV. **CONSIDERANDO** que a ampliação do rol de entidades acreditadas pelo INMETRO deve manter o controle da AC RAIZ sobre os prestadores de serviços credenciados/autorizados a realizar os procedimentos de avaliação da qualidade dos produtos de certificação digital nos moldes das normas editadas por este Comitê Gestor;
- V. **CONSIDERANDO** que, neste contexto, é imprescindível que o A AC RAIZ/ITI mantenha o controle e, no mínimo, o cadastro e autorização destas entidades que realizarão ensaios e auditorias no âmbito da ICP-Brasil se aprovada a proposta

ANTE O EXPOSTO

Vota pela aprovação do item da pauta e registra a importância da revisão dos atos normativos de credenciamento de LEAs na ICP-Brasil.

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

UBIRATAN PEREIRA GUIMARÃES

CAMARA-E.NET

REUNIÃO DO CG DA ICP-BRASIL
Voto nº 04, de 03 de julho de 2018.

Delibera sobre a emissão de certificados digitais para Servidores Públicos da Ativa e Militares da União

A **CÂMARA BRASILEIRA DE COMÉRCIO ELETRÔNICO – CAMARA-E.NET**, por seu representante designado nos moldes do disposto no artigo 3º da Medida Provisória nº 2.200-2/2001, quanto ao item em questão, manifesta-se no seguinte sentido:

- I. **CONSIDERANDO** que o tema desta pauta já foi objeto de deliberação do Comitê Gestor em 06/07/2017, especificamente para o âmbito federal, e que, naquela oportunidade, esta entidade manifestou-se contrária a aprovação da Resolução, mas que culminou na edição da Resolução nº 121/2017;
- II. **CONSIDERANDO** que a referida Resolução e o item da pauta em debate criam situações de desigualdades em relação aos requerentes de certificados digitais sejam servidores públicos ou não, em violação ao *caput* do artigo 5º Constituição Federal;
- III. **CONSIDERANDO** que, inclusive, a criação de procedimento diferenciado de emissão de certificados para servidores federais ou estaduais sem exigir a presença física dos mesmos nas etapas do processo de geração do par de chaves criptográficas, emissão do certificado digital, recepção do certificado e assinatura do termo de titularidade, fere a disposição do artigo 7º da Medida provisória nº 2.200-2/2001, que exige identificação presencial dos usuários de certificados digitais, e também viola a determinação de que a geração das chaves privadas seja efetuada exclusivamente pelo titular, que passa a ter o controle, conhecimento e uso exclusivo da mesma (parágrafo único do artigo 6º da MP nº 2.200-2/2001);
- IV. **CONSIDERANDO** que, inclusive, a possibilidade de que o superior hierárquico do servidor público possa assinar o termo de titularidade em sua representação macula, na origem, a eventual instauração de sindicância para apuração de responsabilidades decorrentes do uso do certificado digital emitido;
- V. **CONSIDERANDO** que, em decorrência disto, o certificado digital dos servidores públicos federais e estaduais tende a perder os atributos de autenticidade, uma vez que o processo de emissão viola a norma básica da emissão de certificados na ICP-Brasil (a MP nº 2.200-2/2001) como também fragiliza a comprovação da manifestação de vontade da expedição do documento e, no mesmo sentido, do uso do certificado digital depois de sua emissão;
- VI. **CONSIDERANDO** que o certificado digital ICP-Brasil de titularidade de pessoa física, seja servidor público ou não, tem as mesmas funcionalidades e aplicabilidades, sendo possível que, em decorrência do processo diferenciado de emissão sem a presença física do titular e que a geração da chave privada tenha sido realizada por ele, possa se permitir que terceiros tenham acesso à informações sigilosas, dados pessoais e sensíveis, sem autorização do seu titular.

ANTE O EXPOSTO

Vota pela rejeição da pauta tela, reiterando a discordância já manifestada quando da edição da Resolução 121/2017, por todas as razões aqui registradas.

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

UBIRATAN PEREIRA GUIMARÃES

CAMARA-E.NET