RESOLUÇÃO Nº 109, DE 25 DE AGOSTO DE 2015.

APROVA A VERSÃO 3.0 DO DOCUMENTO VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL (DOC-ICP-15), QUE REGULAMENTA O PADRÃO DE ASSINATURA DIGITAL PADES ICP-BRASIL.

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA, no exercício do cargo de Coordenador do referido Comitê, no uso das atribuições legais previstas nos incisos I, III, V e VI do art. 4° da Medida Provisória n° 2.200-2, de 24 de agosto de 2001,

CONSIDERANDO o Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira – CG ICP-Brasil e fixa a competência, prevista no § 6º art. 2º, do Secretário Executivo para coordená-lo na hipótese de ausência do Coordenador titular e suplente;

CONSIDERANDO que compete ao Comitê Gestor normatizar acerca de padrões de assinatura digital no âmbito da ICP-Brasil;

CONSIDERANDO a necessidade de regulamentação do padrão de assinatura digital PAdES na ICP-Brasil.

RESOLVE:

Art. 1º Renumeram-se as Figuras e Tabelas do DOC-ICP-15, versão 2.1, em ordem sequencial crescente, sem vínculo ao item a que se refere. Acrescentam-se as figuras relacionadas abaixo:

Figura 5: Assinatura simples em um documento
Figura 6: Coassinaturas em um documento
Figura 7: Contra-assinatura em um documento
Figura 8: Assinatura Serial em PDF

Art. 2º Incluir a alínea “c” no item 6.4.1 do DOC-ICP-15, versão 2.1, com a seguinte redação:

c) assinatura eletrônica avançada sobre o PDF.

Art. 3º Acrescentar o item 6.4.4 no DOC-ICP-15, versão 2.1, incluindo seus subitens, com a seguinte redação:

6.4.4 PDF *Advanced Electronic Signature*

6.4.4.1 O padrão PDF – *Portable Document Forma*t - é um formato de arquivo definido nas especificações da PDF ISO 32000-1 [20] para codificação de documentos eletrônicos que apresenta aparência exata que os documentos terão se forem

impressos.

6.4.4.2 O PDF *Advanced Electronic Signature* (PAdES) é um formato específico para assinaturas eletrônicas avançadas construídas sobre o padrão PDF ISO 32000-1 [20] e descrita nos documentos ETSI TS 102 778 partes 1 à 6, criado com vistas a prover as assinaturas digitais de informações que permitam sua validação por longo prazo.

6.4.4.3 O PDF possui uma estrutura para suportar e incluir informações relevantes às assinaturas digitais. Nessa estrutura, um CMS é o padrão de assinatura digital usado para proteger os dados assinados.

6.4.4.4 O PAdES deve ser usado sempre em documentos no padrão PDF. Um CMS *detached* é inserido dentro da estrutura de dados do PDF. O conteúdo assinado pelo CMS deve ser todos os *bytes* do PDF, menos o bloco de *bytes* do próprio CMS.

6.4.4.5 Pelo fato de existir uma estrutura no PDF para armazenar algumas informações sobre a assinatura, há algumas restrições quanto ao uso dos atributos no CMS. Essas restrições estão descritas no documento DOC-ICP-15.02 [4] na Tabela 7. Um exemplo disso é a hora que o assinante declara que assinou, pois no PDF há uma entrada no dicionário de assinatura, chamada de "M", e no CMS há um atributo assinado, chamado de "*signing-time*". Como os dois possuem a mesma informação, quando for de interesse do desenvolvedor incluir tal informação na assinatura, então, a entrada "M" deve ser codificada e o atributo "*signing-time*" não deve ser codificado.

6.4.4.6 PAdES-ICP-Brasil é toda assinatura no formato PAdES que, além de seguir os requisitos de Assinatura Digital ICP-Brasil, descritas na Seção 4.1, possui um identificador de política de assinatura pertencente ao conjunto de políticas de assinatura divulgadas e aprovadas conforme o DOC-ICP 15.03 [5].

6.4.4.7 A validação de uma assinatura digital de acordo com o padrão PAdES-ICP-Brasil deve exigir que essa assinatura esteja de acordo com uma das políticas de assinatura aprovadas pela ICP-Brasil (ver Seção 6.6).

6.4.4.8 Como uma assinatura PAdES é diretamente relacionada com um arquivo PDF, é necessário que o arquivo PDF esteja na versão 1.7 para que todas as características do PAdES funcionem corretamente em um leitor PDF aderente ao padrão PDF ISO 32000-1 [20]. Adicionalmente, no documento ETSI TS 102 778-4 [16], em sua seção 4.4, é descrito o uso de extensões de dicionário, que são estruturas usadas para informar ao leitor PDF aderente que aquele PDF possui determinadas características.

6.4.4.9 O PAdES também admite que se incorporem às assinaturas digitais dados adicionais, que levam à criação de diferentes formatos de assinaturas. Para cada formato, existe um

conjunto de atributos de caráter obrigatório, sendo permitida a incorporação de atributos não obrigatórios à assinatura, conforme a necessidade de cada signatário, organização, aplicação ou negócio.

6.4.4.10 O PAdES permite que as assinaturas fiquem visíveis aos usuários que estão “lendo” o documento assinado. No entanto, essa visualização não substitui a validação da assinatura nem acrescenta segurança ao processo. Nesta representação visual podem ser incluídas imagens sem vínculo com o assinante.

Art. 4º Alterar o item 6.5.1 do DOC-ICP-15, versão 2.1, que passa a vigorar com a seguinte redação:

6.5.1 Os padrões CAdES, XAdES e PAdES disponibilizam uma diversificada gama de atributos, propriedades ou entradas de dicionários, que permitem às entidades envolvidas incorporar às assinaturas digitais informações com os mais diferentes objetivos.

Art. 5º Alterar o item 6.5.4 do DOC-ICP-15, versão 2.1, que passa a vigorar com a seguinte redação:

6.5.4 Para a ICP-Brasil, foi definido um perfil de assinatura para uso geral, baseado nos padrões CAdES, XAdES e PAdES, que sintetiza os principais atributos e propriedades a serem utilizados nas assinaturas digitais. Podem ser criados outros perfis, para uso em segmentos específicos de atividade, como Governo Eletrônico, se julgado necessário.

Art. 6º Alterar o item 6.7.1 do DOC-ICP-15, versão 2.1, incluindo o padrão PAdES na figura que ilustra a relação existente entre os padrões internacionais que tratam de assinatura digital e os documentos da ICP-Brasil.

Art. 7º Alterar o item 6.8.1 do DOC-ICP-15, versão 2.1, que passa a vigorar com a seguinte redação:

6.8.1 Com relação ao processo de geração de assinatura digital, podemos ter contextos diferentes:

a) assinaturas digitais simples, coassinaturas digitais e contra-assinaturas digitais, para assinaturas baseadas no padrão CAdES e XAdES; e

b) assinaturas digitais simples e assinaturas digitais seriais, para assinaturas baseadas no padrão PAdES.

6.8.1.1 Assinatura Simples - A geração de assinatura digital simples ocorre quando uma única assinatura digital é gerada sobre um conteúdo digital disponível. Esta propriedade pode ocorrer para os padrões CAdES, XAdES e PAdES. A Figura 5 apresenta a implementação de uma assinatura simples.

6.8.1.2 Coassinatura - A geração de coassinaturas digitais ou assinatura paralela ocorre quando duas ou mais assinaturas digitais são geradas de forma paralela e independente pelos signatários, utilizando conteúdos digitais idênticos. Cada coassinatura gerada

pode conter atributos assinados e não assinados próprios. Esta propriedade ocorre somente para os padrões CAdES e XAdES. A Figura 6 apresenta a implementação de coassinaturas.

6.8.1.3 Contra-assinatura - A geração de contra-assinaturas digitais ocorre quando uma ou mais assinaturas digitais são realizadas sobre a sequência de bytes (bloco) que representa uma assinatura digital já existente. Uma contra-assinatura pode conter outros atributos assinados próprios. Esta propriedade ocorre somente para os padrões CAdES e XAdES. A Figura 7 apresenta a implementação de contra-assinatura.

6.8.1.4 Assinatura Serial - A geração de assinaturas digitais seriais, conforme definido no ETSI TS 102 778.1-2009 [16], ocorre quando uma assinatura digital é realizada sobre toda a estrutura do documento assinado, inclusive assinaturas anteriores, quando houver. Esta propriedade pode ocorrer somente no padrão PAdES. A Figura 8 apresenta a implementação de assinaturas seriais em PDF.

Art. 8º Alterar o item 6.11.1 do DOC-ICP-15, versão 2.1, que passa a vigorar com a seguinte redação:

6.11.1 É RECOMENDADO que os arquivos com assinaturas digitais ICP-Brasil sejam gerados com as extensões p7s [18], xml [9] e pdf [20].

Art. 9º Alterar o item 6.12.3 do DOC-ICP-15, versão 2.1, que passa a vigorar com a seguinte redação:

6.12.3 O instante referente a geração de uma assinatura digital a ser utilizado é o Tdec. O instante Tdec é comumente representado no CMS/CAdES pelo atributo *id-signingTime*, em XML-DSIG/XAdES pela propriedade *SigningTime* e em PDF/PAdES pela chave de entrada M do dicionário de assinatura.

Art. 10 Acrescentar o item 6.14.5 no DOC-ICP-15, versão 2.1, com a seguinte redação:

6.14.5 Importante destacar que no padrão PAdES um conteúdo assinado digitalmente acrescenta conteúdo digital ao arquivo PDF, embora preserve dentro do arquivo PDF o conteúdo original.

Art. 11 Fica aprovada a versão 3.0 do Documento VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL (DOC-ICP-15).

§ 1º Todas as demais cláusulas do DOC-ICP-15, na sua versão 2.1, em sua ordem originária, integram a presente versão 3.0 e mantêm-se válidas.

§ 2º O documento referido no caput encontra-se disponibilizado, em sua totalidade, no sítio http://www.iti.gov.br.

Art. 12 Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI