

INSTRUÇÃO NORMATIVA Nº 05 , DE 25 DE AGOSTO DE 2015.

APROVA A VERSÃO 3.0 DO DOCUMENTO REQUISITOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL (DOC-ICP-15.01).

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – CG ICP-BRASIL, no exercício do cargo de Coordenador do referido Comitê, conforme previsão constante no art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, no uso das atribuições legais previstas nos incisos I, III, V e VI do art. 4º da Medida Provisória nº 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; e

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

RESOLVE:

Art. 1º Renumeram-se as Figuras do DOC-ICP-15.01, versão 2.1, em ordem sequencial crescente, sem vínculo ao item a que se refere.

Art. 2º Alterar o item 1.4 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

1.4 A seguir o capítulo 2 apresenta os requisitos técnicos para geração e validação de assinaturas digitais na ICP-Brasil, está organizado da seguinte forma: a seção 2.1 apresenta os formatos de assinatura digital admitidos na ICP-Brasil; a seção 2.2 descreve os requisitos técnicos para geração e validação dessas assinaturas; a seção 2.3 apresenta as políticas de assinatura digital; a seção 2.4 faz referência aos perfis de assinatura digital; a seção 2.5 referencia os algoritmos admitidos para assinaturas digitais; e a seção 2.6 referencia os formatos do documento eletrônico assinado.

Art. 3º Alterar o item 2.1.1 do DOC-ICP-15.01, versão 2.1, alíneas a e b, que passam a vigorar com as seguintes redações:

- a) assinatura digital com Referência Básica (AD-RB), ilustrada na Figura 1;
- b) assinatura digital com Referência de Tempo (AD-RT), ilustrada na Figura 2;

Art. 4º Alterar o item 2.1.1 do DOC-ICP-15.01, versão 2.1, alínea c, bem como a respectiva ilustração, que passa a vigorar com a seguinte redação:

c) assinatura digital com Referências para Validação (AD-RV), ilustrada na Figura 3, este formato é suportado apenas nos padrões CADES e XAdES, inexistindo representação no PAdES;

Art. 5º Alterar a ilustração do item 2.1.1 do DOC-ICP-15.01, versão 2.1, alínea d, referente a assinatura digital com Referências Completas (AD-RC), ilustrada na Figura 4, que passa a apresentar também a possibilidade de Carimbo do Tempo sobre todo o documento, somente para PAdES.

Art. 6º Alterar a ilustração do item 2.1.1 do DOC-ICP-15.01, versão 2.1, alínea e, referente a assinatura digital com Referências para Arquivamento (AD-RA), ilustrada na Figura 5, que passa a apresentar também a necessidade de inclusão da PA e da LPA para validação da assinatura, somente para PAdES.

Art. 7º Alterar o item 2.1.4 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.1.4 Uma assinatura digital ICP-Brasil com Referências para Validação é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT) na qual foram acrescentadas referências sobre todos os certificados de chave pública e sobre todas as Listas de Certificados Revogados (LCR) ou respostas de Online Certificate Status Protocol (OCSP) que são necessários para a validação daquela assinatura. Sobre esses dados é acrescentado ou logicamente conectado outro carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil. A política AD-RV é suportada apenas nos padrões de assinatura CADES e XAdES, inexistindo representação no padrão PAdES.

Art. 8º Alterar o item 2.1.5 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.1.5 Uma assinatura digital ICP-Brasil com Referências Completas:

a) representada nos padrões *CADES* e *XAdES* é formada por uma assinatura digital ICP-Brasil com Referências para Validação (AD-RV) à qual foram acrescentados todos os dados necessários para validação da assinatura, de acordo com o item 2.2.3.1 deste documento;

b) representada no padrão *PAdES* é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT), à qual foram acrescentados todos os dados necessários para validação da assinatura, de acordo com o item 2.2.3.1 deste documento. Além disso, será acrescentado ou logicamente conectado, sobre todo o conjunto de dados, um carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil. Este carimbo marca a data de inserção dos valores de validação e revogação da assinatura. Na Figura 4, este carimbo é representado com uma linha tracejada, representando sua aplicação específica para o formato *PAdES*.

Art. 9º Alterar o item 2.1.6 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.1.6 Uma assinatura digital ICP-Brasil com Referências para Arquivamento:

a) representada nos padrões CADES e XAdES é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT) à qual foram acrescentadas referências de

validação e todos os dados necessários para validação da assinatura, de acordo com o item 2.2.3.1 deste documento. Um carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil é criado sobre todo esse conjunto de dados, ficando anexado ou logicamente conectado ao conjunto.

b) representada no padrão PAdES é formada por uma assinatura digital ICP-Brasil com Referência de Tempo (AD-RT) à qual foram acrescentados todos os dados necessários para validação da assinatura, de acordo com o item 2.2.3.1 deste documento. Inclui-se à assinatura, ainda, a Política de Assinatura (PA) em linguagem de máquina, a Lista de Políticas de Assinatura Aprovadas (LPA) e a assinatura da LPA. Na Figura 5, esta informação é representada com uma linha tracejada, representando sua aplicação específica para o formato PAdES. Somam-se às características da política AD-RA um carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil criado sobre todo esse conjunto de dados, ficando anexado ou logicamente conectado ao conjunto.

Art. 10 Acrescentar ao item 2.2.1.3 do DOC-ICP-15.01, versão 2.1, a alínea c, com a seguinte redação:

- c) Assinaturas com base no padrão PDF Advanced Electronic Signature (PAdES)
 - i. id-contentType
 - ii. id-messageDigest
 - iii. id-aa-signingCertificateV2
 - iv. id-aa-ets-sigPolicyId

Art. 11 Acrescentar o item 2.2.1.4 no DOC-ICP-15.01, versão 2.1, com a seguinte redação:

2.2.1.4 Presença de Scripts em Documentos PDF

O PDF possui suporte para scripts que fornecem uma gama de funcionalidades ao documento. Entretanto esses scripts podem ser utilizados para alterar o conteúdo visualizado pelo usuário de forma transparente, ou seja, sem que o usuário perceba. Como não é evidente que o documento faz uso de scripts, estes podem causar problemas em determinados contextos. Portanto o usuário deve ser alertado sobre a presença de scripts que podem alterar ou não o conteúdo do documento tanto no momento em que assina quanto no que verifica uma assinatura PAdES-ICP-Brasil.

Art. 12 Alterar o item 2.2.2.6 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.2.2.6 A menos que explicitamente mencionado, as regras, definidas nesta seção, referentes ao processo de geração de assinatura digital aplicam-se à geração de assinaturas digitais:

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

Art. 13 Alterar o item 2.2.2.12 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.2.2.12 Uma assinatura digital ICP-Brasil com referências para validação é criada com base numa assinatura digital ICP-Brasil com referência de tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com o item 2.2.3.1 deste documento, bem como um carimbo do tempo sobre o conjunto

de dados, emitido por uma ACT credenciada na ICP-Brasil. As referências e o segundo carimbo do tempo DEVEM ser incorporados pelo signatário ou pelo verificador da assinatura. Este formato de assinatura é suportado apenas em assinaturas baseadas nos padrões CAdES ou XAdES, inexistindo representação no padrão PAdES.

Art. 14 Alterar o item 2.2.2.13 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.2.2.13 Uma assinatura digital ICP-Brasil com referências completas:

- a) representada nos padrões CAdES e XAdES é criada com base numa assinatura digital ICP-Brasil com referência de tempo, adicionando-lhe referências para todos os dados necessários à verificação daquela assinatura, de acordo com o item 2.2.3.1 deste documento, bem como todos os dados necessários para a verificação dessa assinatura digital ICP-Brasil. As referências e os dados de validação DEVEM ser incorporados pelo signatário ou pelo verificador da assinatura.
- b) representada no padrão PAdES é criada com base numa assinatura digital ICP-Brasil com referência de tempo, adicionando-lhe todos os dados necessários para a verificação dessa assinatura digital ICP-Brasil, de acordo com o item 2.2.3.1 deste documento. Do mesmo modo, será acrescentado ou logicamente conectado, sobre o conjunto de dados, um carimbo do tempo, emitido por uma ACT credenciada na ICP-Brasil. O signatário ou o verificador da assinatura DEVE incorporar os dados de validação e o carimbo do tempo.

Art. 15 Acrescentar os itens 2.2.2.15 e 2.2.2.16 no DOC-ICP-15.01, versão 2.1, com a seguinte redação:

2.2.2.15 Se um documento PDF possuir conteúdo XML embarcado e a intenção for assinar o PDF, então deve-se usar uma assinatura PAdES-ICP-Brasil. Caso necessite assinar apenas o conteúdo XML, então é possível assinar com XAdES-ICP-Brasil, no entanto, esse procedimento pode não proteger o PDF como um todo.

2.2.2.16 Recomenda-se que ao adicionar os objetos de validação de uma assinatura no DSS, mantenha-se todos os objetos presentes de possíveis assinaturas anteriores. Dessa forma, a última revisão do DSS sempre terá todos os objetos de validação referenciados de forma correta. Os VRIs devem ser gerados para as assinaturas e carimbos do tempo.

Art. 16 Alterar o item 2.2.3.2 do DOC-ICP-15.01, versão 2.1, alínea b, que passa a vigorar com a seguinte redação:

- b) o caminho de certificação do signatário seja válido na referência temporal adotada para a verificação da assinatura, o que envolve a verificação de:
 - i. observância aos requisitos definidos nos itens 2.2.2.2 e 2.2.2.3;
 - ii. validade da assinatura digital da entidade que emitiu o certificado do signatário.

Art. 17 Alterar o item 2.2.3.8 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.2.3.8 Os processos de validação de assinatura digital e seus requisitos aplicam-se para os contextos de geração:

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

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

Cada assinatura gerada DEVE ser verificada e DEVE atender aos requisitos do processo de validação.

Art. 18 Alterar o item 2.2.3.9 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.2.3.9 Com exceção do padrão PAdES, um conteúdo digital PODE estar armazenado de forma particionada em um repositório interno de um ambiente computacional. Por exemplo, um conteúdo digital PODERIA ser composto de várias partes que estejam armazenadas em tabelas diferentes de um mesmo servidor de banco de dados. Neste caso específico, o processo de geração DEVE primeiro juntar as partes para formar o conteúdo digital e depois gerar a assinatura digital propriamente dita. Como consequência, o processo de verificação de assinatura digital DEVE requerer, quando necessário, a reconstrução, de forma confiável, de um conteúdo digital já assinado anteriormente para a verificação das assinaturas. Este requisito não se aplica para o padrão PAdES porque a assinatura deve estar inserida em um documento PDF.

Art. 19 Acrescentar o item 2.2.3.12 no DOC-ICP-15.01, versão 2.1, com a seguinte redação:

2.2.3.12 Verificação de Longo Prazo no PAdES

A validação do carimbo do tempo do PAdES, o Document Timestamp, deve ser feita de acordo com o descrito no capítulo 7, DOC-ICP 12, e no documento que descreve o PAdES-LTV, ETSI TS 102 778-4. No primeiro documento são referenciadas as normas para validar o carimbo do tempo na ICP-Brasil e no segundo é descrito como usar o DSS na validação do PAdES e carimbos do tempo. Nota-se, ainda, que foram adicionadas a PA, a LPA e a assinatura da LPA ao DSS, de forma obrigatória na PA_AD_RA e opcional nas demais PAs. Dessa maneira, quando o verificador encontrar tais artefatos no DSS eles devem ser usados, após a validação dos Document Timestamps, no processo de validação da assinatura. Esse processo poderia seguir o fluxo descrito a seguir, no entanto fica a critério do verificador implementar dessa forma, o importante é que o resultado da verificação deve ser o mesmo.

- 1 - Buscar os objetos (PA, LPA e assinatura da LPA) referenciados pelo VRI dentro do DSS;
- 2 - Validar a LPA através da verificação da assinatura da LPA;
- 3 - Verificar se a PA está ou estava válida na data de verificação de acordo com a LPA validada no passo anterior;
- 4 - Verificar se a PA referenciada no VRI possui o mesmo OID e hash presentes no atributo identificador da política de assinatura.

Caso o processo falhe em algum desses passos a assinatura deverá ser considerada inválida e o verificador pode apontar que existe inconsistências entre a assinatura aposta e os artefatos PA e/ou LPA arquivados no documento.

Art. 20 Acrescentar o item 2.2.3.13 no DOC-ICP-15.01, versão 2.1, com a seguinte redação:

2.2.3.13 Verificação de Revisões PAdES

Uma característica do PDF é o uso de revisões de documento a cada assinatura. Essa característica pode trazer problemas para a validação da assinatura digital. Ao adicionar uma nova assinatura o DSS anterior pode perder ou ter algum objeto sobreposto se for mal manipulado. Assim, recomenda-se, antes de iniciar o processo de verificação das

assinaturas, verificar os objetos presentes no DSS e garantir que durante o processo de inserção de novas assinaturas não tenha ocorrido nenhuma perda ou substituição de objetos de validação.

Para a validação das assinaturas recomenda-se que sejam considerados apenas dados de validação referentes a revisão do DSS ou anteriores, de modo que a substituição de dados de validação seja inibida.

Art. 21 Alterar o item 2.4.1 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.4.1 Com o objetivo de orientar os desenvolvedores de aplicações, foi definido um perfil de uso geral para assinaturas digitais que incorpora as principais informações julgadas relevantes para o contexto brasileiro. Tal perfil encontra-se detalhado no documento “Perfil de uso Geral para Assinaturas Digitais na ICP-Brasil” (DOC-ICP-15.02) [4] para CAdES, XAdES e PAdES.

Art. 22 Alterar o item 2.5 do DOC-ICP-15.01, versão 2.1, que passa a vigorar com a seguinte redação:

2.5 ALGORITMOS ADMITIDOS PARA ASSINATURAS DIGITAIS NA ICP- BRASIL
A lista dos algoritmos aprovados e parâmetros para algoritmos para criação de assinatura digital ICP-Brasil é dada no documento “Padrões e Algoritmos Criptográfico da ICP-Brasil” (DOC-ICP-01.01) [2], em sua versão mais atual.

Art. 23 Acrescentar as referências [11] e [12] na Bibliografia do DOC-ICP-15.01, versão 2.1, com a seguinte redação:

[11] INSTITUTE, E. T. S. Technical Specification, ETSI TS 102 778-1 V1.1.1 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES. Julho 2009.

[12] ITI. Visão Geral sobre Assinaturas Digitais na ICP-Brasil. v.2.2. Brasília. DOC-ICP-15.

Art. 24 Aprovar a versão 3.0 do DOC-ICP-15.01 - REQUISITOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL.

§ 1º Todas as demais cláusulas do DOC-ICP-15.01, 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. 25 Esta Instrução Normativa entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI