INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

INSTRUÇÃO NORMATIVA Nº 10, DE 05 DE JULHO DE 2012

APROVA A VERSÃO 6.0 DO DOCUMENTO REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL (DOC-ICP-15.03).

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso I, do art. 1º, do anexo I, do Decreto nº 4.689, de 7 de maio de 2003, e pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004;

CONSIDERANDO a necessidade de melhoria do conjunto normativo de assinaturas digitais da ICP-Brasil; e

CONSIDERANDO a deliberação da reunião do Comitê Gestor da ICP-Brasil, ocorrida em 05.07.2012;

RESOLVE:

Art. 1º Altera-se a Nota (4) do item 1, do Anexo 1, do DOC-ICP-15.03, versão 5.0, que passa a vigorar com a seguinte redação:

Nota 4: Para o atributo ESSCertIDv2, utilizada nas versões 2.1 das políticas de assinatura baseadas em CAdES, as aplicações NÃO DEVEM codificar o campo "hashAlgorithm" caso utilize o mesmo algoritmo definido como valor *default* (SHA-256), conforme ISO 8825-1.

Art. 2º Acrescentam-se as Notas ao item 1, do Anexo 1, do DOC-ICP-15.03, versão 5.0, com as seguintes redações:

Nota 5: Quando do uso da codificação *MIME* no campo *eContent*, alerta-se para a necessidade de cuidado com a conversão do arquivo (*attached/detached*), pois esta conversão poderá invalidar a assinatura digital.

Nota 6: Recomenda-se o uso do *MimeType* caso seja codificado a propriedade *DataObjectFormat*, para as políticas XAdES.

Art. 3º Alteram-se nas Tabelas A.3 e A.5, do item 1, do Anexo 1, do DOC-ICP-15.03, versão 5.0, o contido nos campos Carimbo do Tempo de Assinatura e Carimbo do Tempo das Referências, relacionados na coluna RA, que passam a vigorar com o conteúdo "ND".

Art. 4º Alteram-se nas Tabelas A.7, A.9 e A.11, do item 1, do Anexo 1, do DOC-ICP-15.03, versão

5.0, o contido no campo Carimbo do Tempo das Referências relacionado em todas as colunas do Perfil AD, que passam a vigorar com o conteúdo “ND”.

Art. 5º Altera-se na Tabela A.13, do item 1, do Anexo 1, do DOC-ICP-15.03, versão 5.0, o contido no campo Carimbo do Tempo das Referências relacionado nas colunas do identificador Carimbo, que passam a vigorar com o conteúdo “ND”.

Art. 6º Altera-se o item 5.2.1.1.3, do capítulo 5-POLÍTICA-PADRÃO AD-RA BASEADA EM CADES, do DOC-ICP-15.03, versão 5.0, que passa a vigorar com a seguinte redação:

5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórios os seguintes atributos não- assinados:

Para as versões 1.0, 1.1, 2.0 e 2.1:
a) id-aa-signatureTimeStampToken;
b) id-aa-ets-certificateRefs;
c) id-aa-ets-revocationRefs;
d) id-aa-ets-certValues;
e) id-aa-ets-revocationValues;
f) id-aa-ets-archiveTimestampV2.

Para as versões posteriores a 2.1:
a) id-aa-ets-certificateRefs;
b) id-aa-ets-revocationRefs;
c) id-aa-ets-certValues;
d) id-aa-ets-revocationValues;
e) id-aa-ets-archiveTimestampV2.

Art. 7º Altera-se o item 5.2.1.2.1, do capítulo 5-POLÍTICA-PADRÃO AD-RA BASEADA EM CADES, do DOC-ICP-15.03, versão 5.0, que passa a vigorar com a seguinte redação:

5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídos pelo signatário, os seguintes atributos DEVEM ser incluídos pelo verificador:

Para as versões 1.0, 1.1, 2.0 e 2.1:
a) id-aa-signatureTimeStampToken;
b) id-aa-ets-certificateRefs;
c) id-aa-ets-revocationRefs;
d) id-aa-ets-certValues;
e) id-aa-ets-revocationValues;
f) id-aa-ets-archiveTimestampV2.

Para as versões posteriores a 2.1:
a) id-aa-ets-certificateRefs;
b) id-aa-ets-revocationRefs;
c) id-aa-ets-certValues;
d) id-aa-ets-revocationValues;
e) id-aa-ets-archiveTimestampV2.

Art. 8º Alteram-se os itens 5.2.1.1.2, dos capítulos 6-POLÍTICA-PADRÃO AD-RB BASEADA EM XADES, 7-POLÍTICA-PADRÃO AD-RT BASEADA EM XADES, 8-POLÍTICA-PADRÃO AD-RV BASEADA EM XADES, 9-POLÍTICA-PADRÃO AD-RC BASEADA EM XADES, 10-POLÍTICA-PADRÃO AD-RA BASEADA EM XADES, do DOC-ICP-15.03, versão 5.0, que passam a vigorar com a seguinte redação:

5.2.1.1.2 Atributos ou Propriedades Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:
a) DataObjectFormat (em assinaturas do tipo *detached*);
b)SigningCertificate;
c) SignaturePolicyIdentifier.

Para as versões posteriores a 2.1:
a) SigningCertificate;
b) SignaturePolicyIdentifier.

Art. 9º Altera-se o item 5.2.1.1.3, do capítulo 10-POLÍTICA-PADRÃO AD-RA BASEADA EM XADES, do DOC-ICP-15.03, versão 5.0, que passa a vigorar com a seguinte redação:

5.2.1.1.3 Atributos ou Propriedades Não-Assinados Obrigatórios

As assinaturas feitas segundo esta PA definem como obrigatórias as seguintes propriedades não assinadas:

Para as versões 1.0, 1.1, 2.0 e 2.1:
a) SignatureTimeStamp;
b) CompleteCertificateRefs;
c) CompleteRevocationRefs;
d) CertificateValues;
e) RevocationValues;
f) ArchiveTimeStamp.

Para as versões posteriores a 2.1:
a) CompleteCertificateRefs;
b) CompleteRevocationRefs;
c) CertificateValues;
d) RevocationValues;
e) ArchiveTimeStamp.

Art. 10. Altera-se o item 5.2.1.2.1, do capítulo 10-POLÍTICA-PADRÃO AD-RA BASEADA EM XADES, do DOC-ICP-15.03, versão 5.0, que passa a vigorar com a seguinte redação:

5.2.1.2.1 Atributos ou Propriedades Não-Assinados Obrigatórios

Caso não tenham sido incluídas pelo signatário, as seguintes propriedades DEVEM ser incluídas pelo verificador:

Para as versões 1.0, 1.1, 2.0 e 2.1:
a) SignatureTimeStamp;
b) CompleteCertificateRefs;
c) CompleteRevocationRefs;
d) CertificateValues;
e) RevocationValues;
f) ArchiveTimeStamp.

Para as versões posteriores a 2.1:
a) CompleteCertificateRefs;
b) CompleteRevocationRefs;
c) CertificateValues;
d) RevocationValues;
e) ArchiveTimeStamp.

Art. 11. Alteram-se os subitens 4.2 a 4.5, do item 4, do DOC-ICP-15.03, versão 5.0, que passam a vigorar com as seguintes redações:

4.2 As LPAs são assinadas e publicadas pela AC Raiz da ICP-Brasil, de forma segura, no seu repositório no endereço web http://www.iti.gov.br/twiki/bin/view/Certificacao/artefatos .

4.3 As LPAs são atualizadas pela AC Raiz **a cada 90 dias** e contêm em seus corpos a data da sua próxima atualização.

4.4 As LPAs são assinadas com Assinaturas Digitais ICP-Brasil, utilizando PKCS #7 para CAdES e XMLdSIG para XAdES, ambos assinados por um certificado de pessoa jurídica do ITI, emitido por uma das autoridades certificadoras credenciadas na ICP-Brasil.

4.5 As LPAs são codificadas em linguagem de máquina (ASN.1 e XML) e trazem, para cada PA aprovada, os seguintes dados:

a) nome;
b) uma breve descrição da política: os aplicativos assinadores poderão exibir essa informação para que o usuário decida qual PA empregar;
c) período de validade da Política;
d) data de revogação, se for o caso;
e) URLs da PA em formato textual e processável por máquina (XML/DER);
f) resumos criptográficos dos arquivos da PA, no formato textual e processável por máquina (XML/DER);
g) assinatura digital PKCS #7 para o formato ASN.1 e XMLdSIG para o formato XML.

Art. 12. Acrescenta-se a alínea “i” do subitem 7.1, do DOC-ICP-15.03, versão 5.0, com a seguinte redação:

i) assinatura digital PKCS #7 para o formato ASN.1 e XMLdSIG para o formato XML.

Art. 13. Acrescenta-se ao item 7.4.1 do DOC-ICP-15.03, versão 5.0, nova estrutura da LPA em ASN.1 com o seguinte conteúdo:

ListaDePAsAprovadasV2

```
        { joint(2) country(16) br(76) iti(1) lpa(9) v2(1) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

        IMPORTS
                -- Electronic Signature Formats for long term electronic signatures: RFC
3126
                OtherHashAlgAndValue
                FROM ETS-ElectronicSignatureFormats-88syntax { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-mod(0) 5}
                -- Electronic Signature Policies: RFC 3125
                SigningPeriod
                FROM ETS-ElectronicSignaturePolicies-88syntax { iso(1) member-body(2)
us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) id-mod(0) 7};


-- Estrutura principal
LPA ::= SEQUENCE {
        version         Version DEFAULT v2,
        policyInfos     PolicyInfos,
        nextUpdate      GenerelizedTime }

Version  ::=  INTEGER  {  v2(0) }

PolicyInfos ::= SEQUENCE OF PolicyInfo

PolicyInfo ::= SEQUENCE {
    signingPeriod      SigningPeriod,
    revocationDate     GeneralizedTime OPTIONAL,
    policyOID                  OBJECT IDENTIFIER,
    policyURI          IA5String,
    policyDigest       OtherHashAlgAndValue }

END
```

Art. 14. Acrescenta-se ao item 7.4.2 do DOC-ICP-15.03, versão 5.0, nova estrutura da LPA em XML com o seguinte conteúdo:

```
<xsd:schema                              targetNamespace="http://www.iti.gov.br/LPA/v2#"
elementFormDefault="qualified">
        <xsd:import              namespace="http://www.w3.org/2000/09/xmldsig#"
        schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
        <!-- Lista de Politicas de Assinatura Aprovadas →
        <xsd:element                    name="ApprovedSignaturePoliciesList"
        type="ApprovedSignaturePoliciesListType"/>
        <xsd:complexType name="ApprovedSignaturePoliciesListType">
                <xsd:sequence>
                <xsd:element name="Version" type="xsd:integer" default="0"/>
                <xsd:element name="NextUpdate" type="xsd:dateTime"/>
                <xsd:element name="PolicyInfo" type="PolicyInfoType"
```

```
                maxOccurs="unbounded"/>
                </xsd:sequence>
        </xsd:complexType>
        <!-- Informacoes da Politica →
        <xsd:complexType name="PolicyInfoType">
                <xsd:sequence><xsd:element name="SigningPeriod"
                type="SigningPeriodType"/>
                <xsd:element minOccurs="0" name="RevocationDate"
type="xsd:dateTime"/>
                <xsd:element name="policyOID" type="XAdES:ObjectIdentiferType"/>
                <xsd:element name="PolicyDigestAndURI"
                type="PolicyDigestAndURIType"/>
                </xsd:sequence></xsd:complexType>
        <!-- Periodo para Assinatura →
        <xsd:complexType name="SigningPeriodType">
                <xsd:sequence>
                <xsd:element name="NotBefore" type="xsd:dateTime"/>
                <xsd:element minOccurs="0" name="NotAfter" type="xsd:dateTime"/>
                </xsd:sequence></xsd:complexType>
        <!-- Resumos Criptograficos e URLs da PA →
        <xsd:complexType name="PolicyDigestAndURIType">
                <xsd:sequence>
                <xsd:element name="PolicyURI" type="xsd:anyURI"/>
                <xsd:element name="PolicyDigest" type="DigestType"/>
                </xsd:sequence>
        </xsd:complexType>
        <xsd:complexType name="DigestType">
                <xsd:sequence><xsd:element name="DigestMethod"
                type="ds:DigestMethodType"/>
                <xsd:element name="DigestValue" type="ds:DigestValueType"/>
                </xsd:sequence>
        </xsd:complexType>
</xsd:schema>
```

Art. 15. Fica aprovada a versão 6.0 do Documento REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL (DOC-ICP-15.03).

§ 1º Todas as demais cláusulas do DOC-ICP-15.03, na sua versão 5.0, em sua ordem originária, integram a presente versão 6.0 e mantêm-se válidas.

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

Art. 16. Esta Instrução Normativa entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI