

**PERFIL DE USO GERAL PARA ASSINATURAS
DIGITAIS NA ICP-BRASIL**

DOC-ICP-15.02

Versão 3.1

01 de junho de 2016

SUMÁRIO

CONTROLE DE ALTERAÇÕES.....	3
LISTA DE SIGLAS E ACRÔNIMOS.....	5
LISTA DE TABELAS.....	6
1 INTRODUÇÃO.....	7
2 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES CMS/CADES.....	1
2.1 ATRIBUTOS ASSINADOS.....	1
2.2 ATRIBUTOS NÃO ASSINADOS.....	1
3 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES XMLDSIG/XAdES.....	3
3.1 PROPRIEDADES ASSINADAS.....	3
3.2 PROPRIEDADES NÃO ASSINADAS.....	3
4 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES PDF/PAdES.....	6
4.1 ATRIBUTOS ASSINADOS.....	6
4.2 ATRIBUTOS NÃO ASSINADOS.....	7
4.3 ENTRADAS DO DICIONÁRIO DE ASSINATURAS.....	8
4.4 DICIONÁRIOS DE VALIDAÇÃO.....	9
4.4.1 Document Security Store (DSS).....	9
4.4.2 Validation Related Information (VRI).....	9
4.4.3 Document Time-stamp.....	10
4.4.4 Versões e Extensões do PDF.....	11
BIBLIOGRAFIA.....	12



CONTROLE DE ALTERAÇÕES

<i>Ato que aprovou a alteração</i>	<i>Item alterado</i>	<i>Descrição da alteração</i>
IN nº 03, de 01.01.2016 Versão 3.1		Ajustes na nomenclatura utilizada no PAdES.
IN nº 06, de 25.08.2015 Versão 3.0	Alteração itens 1 e 1.4. Inclusão item 4 e subitens.	Regulamentação do PAdES.
IN nº 09-2012, de 05.07.2012. Versão 2.1	Tabela 3.1, referência 7.2.5 Tabela 2.2 e 3.2, referências 5.9.2 e 7.2.4	Acrescenta a coluna “Requisitos adicionais /Observações”. Inclui o texto “Caso seja codificado, recomenda-se a identificação do conteúdo com o preenchimento do campo MimeType”. Inclui o texto “Contra-assinaturas NÃO DEVEM ser empregadas após a aposição de qualquer carimbo do tempo de arquivamento, devido à interferência no processo de validação”.
IN nº 02-2010, de 31.03.2010 Versão 2.0	Estrutura do documento Tabela 2.1 Tabela 3.1	O documento foi remodelado. O item “terminologia” foi suprimido. O atributo id-aassigningCertificateV2 foi removido da tabela de atributos assinados. A propriedade CommitmentTypeIndication foi removida da tabela de propriedades assinadas.
IN nº 02-2009, 09.01.2009	Versão inicial	Aprovação da versão 1.0 do DOC-ICP-15.02

<i>Ato que aprovou a alteração</i>	<i>Item alterado</i>	<i>Descrição da alteração</i>
Versão 1.0		



Infraestrutura de Chaves Públicas Brasileira

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
CAAdES	<i>CMS Advanced Electronic Signatures</i>
CMS	<i>Cryptographic Message Syntax</i>
DSS	<i>Document Security Store</i>
e-PING	<i>Padrões de Interoperabilidade de Governo Eletrônico</i>
ETSI	<i>European Telecommunication Standard Institute</i>
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
OCSP	<i>Online Certificate Status Protocol</i>
PAdES	<i>PDF Advanced Electronic Signatures</i>
PDF	<i>Portable Document Format</i>
RFC	<i>Request For Comments</i>
VRI	<i>Validation Related Information</i>
XAdES	<i>XML Advanced Electronic Signatures</i>
XML	<i>EXtensible Markup Language</i>

LISTA DE TABELAS

Tabela 1: Atributos assinados para assinaturas no formato CAAdES.....	1
Tabela 2: Atributos não assinados para assinaturas no formato CAAdES.....	2
Tabela 3: Propriedades assinadas para assinaturas em formato XAdES.....	3
Tabela 4: Propriedades não assinadas para assinaturas no formato XAdES.....	5
Tabela 5: Atributos assinados para assinaturas no formato PAdES.....	6
Tabela 6: Atributos não assinados para assinaturas no formato PAdES.....	7
Tabela 7: Relação de entradas do dicionário de assinatura e atributos com conteúdos similares...7	7
Tabela 8: Entradas do dicionário de assinatura.....	8
Tabela 9: Entradas do dicionário DSS.....	9
Tabela 10: Entradas do dicionário VRI.....	10
Tabela 11: Entradas do dicionário Document Time-stamp.....	10

1 INTRODUÇÃO

1.1 Este documento define um perfil para assinatura digital na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) que contém um sub-conjunto dos atributos, propriedades ou entrada de dicionários definidos respectivamente nos padrões CMS *Advanced Electronic Signatures* (CADES) [1], XML *Advanced Electronic Signatures* (XADES) [2] e PDF *Advanced Electronic Signatures* (PADES) [9]. Tal perfil foi criado com o objetivo de minimizar as diferenças entre implementações e maximizar a interoperabilidade das aplicações para geração e verificação de assinaturas digitais.

1.2 Este documento está associado a um conjunto de normativos criados para regulamentar a geração e verificação de assinaturas digitais no âmbito da ICP-Brasil. Tal conjunto se compõe de:

- a) Visão Geral sobre Assinaturas Digitais na ICP-Brasil (DOC-ICP-15) [3];
- b) Requisitos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil (DOC-ICP-15.01) [4];
- c) Perfil de Uso Geral para Assinaturas Digitais na ICP-Brasil (DOC-ICP-15.02) (este documento);
- d) Requisitos das Políticas de Assinatura na ICP-Brasil (DOC-ICP-15.03) [5].

1.3 As diretrizes aqui constantes DEVEM ser observadas por todas as entidades da ICP-Brasil, em especial pelos desenvolvedores de aplicações para geração/verificação de assinatura digital.

1.4 O restante deste documento está organizado da seguinte forma. O capítulo 2 apresenta o perfil de assinatura digital com base no CADES; o capítulo 3 apresenta o perfil de assinatura digital com base no XADES e o capítulo 4 o perfil de assinatura digital com base no PADES.

2 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES CMS/CADES

2.1 ATRIBUTOS ASSINADOS

A Tabela 1 apresenta os atributos assinados para assinaturas no formato CADES. A coluna **Ref** aponta a seção no documento ETSI TS 101 733 [1] em que o atributo está especificado.

Atributo	Ref [1]	Requisitos adicionais / Observações
id-aa-ets-contentTimestamp	5.11.4	Os carimbos do tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [6].
id-aa-ets-signerAttr	5.11.3	
id-aa-ets-signerLocation	5.11.2	Nos processos de assinatura digital, caso o signatário deseje informar o local físico onde a assinatura digital foi gerada, esse DEVE ser expresso, no mínimo, pela combinação de dois elementos: <ul style="list-style-type: none"> a) Identificador do país, como especificado no padrão internacional ISO 3166 [10]. No caso do Brasil, esse valor é 76 (setenta e seis) b) Localidade: Nome do Município-UF.
id-signingTime	5.9.1	
id-contentType	5.7.1	
id-messageDigest	5.7.2	
id-aa-signingCertificate	5.7.3	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
id-aa-ets-sigPolicyId	5.7.3	

Tabela 1: Atributos assinados para assinaturas no formato CADES

2.2 ATRIBUTOS NÃO ASSINADOS

A Tabela 2 apresenta os atributos não assinados para assinaturas no formato CADES. A coluna **Ref** aponta a seção no documento ETSI TS 101 733 [1] em que o atributo está especificado.

Atributo	Ref [1]	Requisitos adicionais / Observações
id-countersignature	5.9.2	Contra-assinaturas são empregadas quando a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no

		<p>mínimo, atestar o recebimento do documento com a primeira assinatura já presente.</p> <p>O uso de contra-assinaturas DEVE ser previamente acordado entre as partes geradora e verificadora, de modo que o verificador esteja ciente da presença, número, e significado da contra-assinatura.</p> <p>Contra-assinaturas NÃO DEVEM ser empregadas após a aposição de qualquer carimbo do tempo de arquivamento, devido à interferência no processo de validação.</p>
id-aa-signatureTimeStampToken	6.1.1	Os carimbos de tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [6].
id-aa-ets-certificateRefs	6.2.1	Certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
id-aa-ets-revocationRefs	6.2.2	Listas de Certificados Revogados empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
id-aa-ets-attrCertificateRefs	6.2.3	
id-aa-ets-attrRevocationRefs	6.2.4	
id-aa-ets-escTimeStamp	6.3.5	Os carimbos de tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [6].
id-aa-ets-certValues	6.3.3	Certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7]. Conforme especificado no documento DOC-ICP-05 [8], cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas Autoridades Certificadoras (ACs) da ICP-Brasil para fins de consulta histórica.
id-aa-ets-revocationValues	6.3.4	Conforme especificado no documento DOC-ICP-05 [8], cláusula 4.6.2, as LCRs são retidas permanentemente pelas ACs da ICP-Brasil para fins de consulta histórica.
id-aa-ets-archiveTimestamp	6.4.1	Carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [6].

Tabela 2: Atributos não assinados para assinaturas no formato CADES

3 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES XMLDSIG/XAdES

3.1 PROPRIEDADES ASSINADAS

A Tabela 3 apresenta as propriedades assinadas para assinaturas em formato XAdES. A coluna **Ref** aponta a seção no documento ETSI TS 101 903 [2] em que a propriedade está especificada.

Propriedade	Ref[2]	Requisitos adicionais / Observações
SignatureProductionPlace	7.2.7	Nos processos de assinatura digital, caso o signatário deseje informar o local físico onde a assinatura digital foi gerada, esse DEVE ser expresso, no mínimo, pela combinação de dois elementos: a) Identificador do país, como especificado no padrão internacional ISO 3166 [10]. No caso do Brasil, esse valor é 76 (setenta e seis); b) Localidade: Nome do Município-UF
SignerRole	7.2.8	
SigningTime	7.2.1	
AllDataObjectsTimeStamp	7.2.9	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [6].
IndividualDataObjectsTimeS tamp	7.2.10	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [6].
DataObjectFormat	7.2.5	Caso seja codificado, recomenda-se a identificação do conteúdo com o preenchimento do campo <code>MimeType</code> .
SigningCertificate	7.2.2	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
SignaturePolicyIdentifier	7.2.3	

Tabela 3: Propriedades assinadas para assinaturas em formato XAdES.

3.2 PROPRIEDADES NÃO ASSINADAS

A Tabela 4 apresenta as propriedades não assinadas para assinaturas no formato XAdES. A coluna **Ref** aponta a seção no documento ETSI TS 101 903 [2] em que a propriedade está especificada.

Propriedade	Ref [2]	Requisitos adicionais / Observações
CounterSignature	7.2.4	Contra-assinaturas são empregadas quando a ordem de aplicação das assinaturas é relevante, ou seja, quando a função da segunda assinatura é, no mínimo, atestar o recebimento do documento com a primeira assinatura presente. O uso de contra-assinaturas DEVE ser

Propriedade	Ref [2]	Requisitos adicionais / Observações
		<p>previamente acordado entre as partes geradora e verificadora, de modo que o verificador esteja ciente da presença, número e significado da assinatura paralela.</p> <p>Contra-assinaturas NÃO DEVEM ser empregadas após a aposição de qualquer carimbo do tempo de arquivamento, devido à interferência no processo de validação.</p>
SignatureTimeStamp	7.3	Os carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [6].
CompleteCertificateRefs	7.4.1	Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
CompleteRevocationRefs	7.4.2	As Listas de Certificados Revogados (LCR) e respostas de <i>Online Certificate Status Protocol</i> (OCSP) empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
AttributeCertificateRefs	7.4.3	
AttributeRevocationRefs	7.4.4	
SigAndRefsTimeStamp	7.5.1	Os carimbos do tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [6].
CertificateValues	7.6.1	<p>Conforme especificado no documento DOC-ICP-05 [8], cláusula 4.6.2, os certificados de assinatura digital são retidos permanentemente pelas Autoridades Certificadoras da ICP-Brasil para fins de consulta histórica.</p> <p>Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].</p>
RevocationValues	7.6.2	<p>Conforme especificado no documento DOC-ICP-05 [8], cláusula 4.6.2, as LCRs são retidas permanentemente pelas ACs da ICP-Brasil para fins de consulta histórica.</p> <p>As LCRs empregadas DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].</p>
AttrAuthoritiesCertValues	7.6.3	
AttributeRevocationValues	7.6.4	
ArchiveTimeStamp	7.7	Os carimbos de tempo empregados DEVEM atender ao perfil definido no documento DOC-ICP-12 [6].

Tabela 4: Propriedades não assinadas para assinaturas no formato XAdES.

4 PERFIL DE ASSINATURA DIGITAL COM BASE NOS PADRÕES PDF/PAdES

4.1 ATRIBUTOS ASSINADOS

A Tabela 5 apresenta os atributos assinados para assinaturas no formato PAdES, em conformidade com o documento ETSI TS 102 778-3 [11] e ETSI TS 102 778-4 [12]. A coluna Ref aponta a seção no documento ETSI TS 101 733 [1] em que o atributo está especificado.

Atributo	Ref [1]	Requisitos adicionais / Observações
id-contentType	5.7.1	
id-messageDigest	5.7.2	
id-aa-signingCertificate	5.7.3	Uso proibido no padrão PAdES.
id-aa-signingCertificate V2		Os certificados digitais empregados DEVEM atender ao perfil definido no documento DOC-ICP-04 [7].
id-aa-ets-sigPolicyId	5.8	
id-aa-ets-signerAttr	5.11.3	
id-aa-ets-signerLocation	5.11.2	Uso proibido no padrão PAdES. A entrada <i>Location</i> do dicionário de assinatura deve ser utilizada para este propósito. Ver Tabela 7 para mais detalhes.
id-signingTime	5.9.1	Uso proibido no padrão PAdES. O instante da geração da assinatura digital declarado pelo assinante deve estar na entrada M do dicionário de assinatura. Ver Tabela 7 para mais detalhes.
id-aa-ets-contentTimestamp	5.11.4	Os carimbos do tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [6].
adbe-revocationInfoArchival		Uso proibido no padrão PAdES. O atributo está descrito no item 12.8.3.3.2 Revocation Information da ISO 32000-1 [13].

Tabela 5: Atributos assinados para assinaturas no formato PAdES

4.2 ATRIBUTOS NÃO ASSINADOS

A Tabela 6 apresenta os atributos não assinados para assinaturas no formato PAdES, em conformidade com o documento ETSI TS 102 778-3 [11] e ETSI TS 102 778-4 [12]. A coluna **Ref** aponta a seção no documento ETSI TS 101 733 [1] em que o atributo está especificado.

Atributo	Ref [1]	Requisitos adicionais / Observações
id-countersignature	5.9.2	Uso proibido no padrão PAdES.
id-aa-signatureTimeStampToken	6.1.1	Os carimbos de tempo utilizados DEVEM seguir o perfil definido no documento DOC-ICP-12 [6].
id-aa-ets-certificateRefs	6.2.1	Uso proibido no padrão PAdES.
id-aa-ets-revocationRefs	6.2.2	Uso proibido no padrão PAdES.
id-aa-ets-attrCertificateRefs	6.2.3	Uso proibido no padrão PAdES.
id-aa-ets-attrRevocationRefs	6.2.4	Uso proibido no padrão PAdES.
id-aa-ets-certValues	6.3.3	Uso proibido no padrão PAdES.
id-aa-ets-revocationValues	6.3.4	Uso proibido no padrão PAdES.
id-aa-ets-escTimeStamp	6.3.5	Uso proibido no padrão PAdES.
id-aa-ets-archiveTimestamp	6.4.1	Uso proibido no padrão PAdES.

Tabela 6: Atributos não assinados para assinaturas no formato PAdES

A Tabela 7 apresenta a relação entre atributos e entradas do dicionário de assinaturas com conflito de conteúdo e que devem ser atendidos no PAdES.

Informação	Uso Recomendado	Uso Proibido
Instante de geração da assinatura declarado pelo assinante	Entrada M	Atributo id-signingTime
Localização do assinante	Entrada Location	Atributo id-aa-ets-signerLocation
Certificado do assinante	Campo “certificates” do SignedData	Entrada Cert
Certificados do caminho de certificação	DSS e VRI	Atributo id-aa-ets-certValues
LCRs ou OCSPs do caminho de certificação	DSS e VRI	Atributo id-aa-ets-revocationValues

Tabela 7: Relação de entradas do dicionário de assinatura e atributos com conteúdos similares

4.3 ENTRADAS DO DICIONÁRIO DE ASSINATURAS

Entrada	Requisitos adicionais / Observação
Type	Indica o tipo de Objeto PDF que esse dicionário representa. Conforme a Tabela A.18, do DOC-ICP 15.03, o valor padrão é Sig.
Filter	Define o nome do plugin adequado para executar a verificação da assinatura. Conforme a Tabela A.18, do DOC-ICP 15.03, o valor padrão é PBAD_PADES.
SubFilter	Identifica o padrão de assinatura utilizado. Um leitor PDF aderente deve utilizar um <i>plugin</i> que saiba verificar esse tipo de padrão de assinatura. Conforme a Tabela A.18, do DOC-ICP 15.03, o valor padrão é PBAD.PAdES.
Contents	
Cert	Uso proibido no padrão PAdES. O campo “certificates” do SignedData deve ser utilizado para este propósito. Ver Tabela 7 para mais detalhes.
ByteRange	
Reference	
Changes	
Name	
M	Entrada com função similar ao atributo “id-signingTime”. Ver Tabela 7 para mais detalhes sobre o uso dessa entrada.
Location	Entrada com função similar ao atributo “id-aa-ets-signerLocation”. Ver Tabela 7 para mais detalhes sobre o uso dessa entrada.
Reason	
ContactInfo	
R	
V	
Prop_Build	
Prop_AuthTime	
Prop_AuthType	

Tabela 8: Entradas do dicionário de assinatura

4.4 DICIONÁRIOS DE VALIDAÇÃO

4.4.1 Document Security Store (DSS)

A Tabela 9 apresenta as entradas do dicionário DSS, em conformidade com o documento ETSI TS 102 778-4. Todas as entradas descritas estão definidas na Tabela “*Entries in a DSS Dictionary*”, Anexo A.1 do documento ETSI 102 778-4.

Entrada	Requisitos adicionais / Observação
Type	Indica o tipo do dicionário.. Conforme a Tabela A.19, do DOC-ICP 15.03, o valor padrão é DSS.
VRI	
Certs	Entrada com função similar ao atributo “id-aa-ets-certValues”. Ver Tabela 7 para mais detalhes sobre o uso dessa entrada.
OCSPs	Entrada com função similar ao atributo “id-aa-ets-revocationValues”. Ver Tabela 7 para mais detalhes sobre o uso dessa entrada.
CRLs	Entrada com função similar ao atributo “id-aa-ets-revocationValues”. Ver Tabela 7 para mais detalhes sobre o uso dessa entrada.
PBAD_PolicyArtifacts	Descrição na Tabela A.4.1, do DOC-ICP 15.03.
PBAD_LpaArtifacts	Descrição na Tabela A.4.1, do DOC-ICP 15.03.
PBAD_LpaSignatures	Descrição na Tabela A.4.1, do DOC-ICP 15.03.

Tabela 9: Entradas do dicionário DSS

4.4.2 Validation Related Information (VRI)

A Tabela 10 apresenta as entradas do dicionário VRI, em conformidade com o documento ETSI TS 102 778-4. Todas as entradas descritas estão definidas na Tabela “*Entries in a Signature VRI Dictionary*”, Anexo A.1 do documento ETSI 102 778-4.

Entrada	Requisitos adicionais / Observação
Type	Indica o tipo do dicionário. Conforme a Tabela A.20, do DOC-ICP 15.03, o valor padrão é VRI.
Cert	
OCSP	
CRL	

Entrada	Requisitos adicionais / Observação
TU	A presença deste campo não invalida a assinatura, porém não será considerado no processo de validação.
TS	A presença deste campo não invalida a assinatura, porém não será considerado no processo de validação.
PBAD_PolicyArtifacts	Descrição na Tabela A.4.2, do DOC-ICP 15.03.
PBAD_LpaArtifacts	Descrição na Tabela A.4.2, do DOC-ICP 15.03.
PBAD_LpaSignatures	Descrição na Tabela A.4.2, do DOC-ICP 15.03.

Tabela 10: Entradas do dicionário VRI

4.4.3 Document Time-stamp

A Tabela 11 apresenta as entradas do dicionário *Document Time-stamp*, em conformidade com o documento ETSI TS 102 778-4. Todas as entradas descritas estão definidas na Tabela “*Modifications to table 252 for a Document Time-stamp Dictionary*”, Anexo A.2 do documento ETSI 102 778-4.

Entrada	Requisitos adicionais / Observação
Type	Indica o tipo do dicionário. Conforme a Tabela A.21, do DOC-ICP 15.03, o valor padrão é DocTimeStamp.
SubFilter	Identifica o padrão de assinatura utilizado. Conforme a Tabela A.21, do DOC-ICP 15.03, o valor padrão é ETSI.RFC3161.
Contents	
V	

Tabela 11: Entradas do dicionário Document Time-stamp

4.4.4 Versões e Extensões do PDF

4.4.4.1 Versões

Para garantir que todos os recursos necessários na validação de uma assinatura PAdES sejam interpretados corretamente pelo leitor aderente, deve-se usar no mínimo a versão 1.7 do PDF. Esta versão é a mais atual, mantida pelo documento ISO 32000-1 [13], e possibilita a utilização das extensões necessárias para a inclusão do DSS e VRI. Os detalhes sobre as versões do PDF estão descritos no Anexo I, do documento ISO 32000-1. Caso seja necessário usar PDF/A deve-se usar a versão PDF/A-2 ou superior, pois a versão PDF/A-1 não possui suporte para assinaturas CA-dES, que é um requisito para o PAdES-ICP-Brasil.

4.4.4.2 Extensões

Nos documentos de referência, ETSI TS 102 778-3 e ETSI 102 778-4, há a indicação do uso de extensões de dicionário para indicar o uso de características específicas do PDF, que no caso de assinaturas Padrão ICP-Brasil serão identificadas com o prefixo PBAD. Assim, para indicar que a assinatura PAdES possui política de assinatura, deve-se utilizar a seguinte extensão:

```
<</ESIC
  <</BaseVersion /1.7
    /ExtensionLevel 2
  >>
>>
```

E para assinaturas que possuam DSS e VRI, deve-se usar a seguinte extensão:

```
<</PBAD
  <</BaseVersion /1.7
    /ExtensionLevel 1
  >>
>>
```

BIBLIOGRAFIA

- [1] ETSI. *CMS Advanced Electronic Signatures (CAAdES). V.1.7.4.* ed. [S.l.], 2009. Acesso em 23/02/2009.
- [2] ETSI. *XML Advanced Electronic Signatures (XAdES). 1.3.2.* ed. [S.l.], 2006. Acesso em: 23/02/2009.
- [3] ITI. *Visão Geral Sobre Assinaturas Digitais na ICP-Brasil.* v.1.0. Brasília. DOC-ICP-15.
- [4] ITI. *Requisitos Mínimos para Geração e Verificação de Assinaturas Digitais na ICP-Brasil.* v.1.0. Brasília. DOC-ICP-15.01.
- [5] ITI. *Requisitos Mínimos para Políticas de Assinatura Digital na ICP-Brasil.* v.1.0. Brasília. DOC-ICP-15.03.
- [6] ITI. *Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil.* v.1.0. Brasília, Dezembro 2008. DOC-ICP-12.
- [7] ITI. *Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil.* v.3.0. Brasília, Dezembro 2008. DOC-ICP-04.
- [8] ITI. *Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.* v.3.1. Brasília, Junho 2009. DOC-ICP-05.
- [9] ETSI. *PDF Advanced Electronic Signatures Profiles. Part 1 PAdES Overview – a framework document for PAdES: TS 102 778-1 V1.1.1.* ed. [S.l.], 2009. Acesso em: 23/01/2015.
- [10] ISO. ISO 3166 – *Country Codes.* <https://www.iso.org/obp/ui/#search>. Acesso em 20/01/2015.
- [11] ETSI. *PDF Advanced Electronic Signatures Profiles. Part 3: PAdES Enhanced – PAdES BES and PAdES EPES Profiles. TS 102 778-3 V1.2.1.* ed. [S.l.], 2010. Acesso em: 23/01/2015.
- [12] ETSI. *PDF Advanced Electronic Signatures Profiles. Part 4: PAdES Long Term – PAdES LTV Profile. TS 102 778-4 V1.1.2.* ed. [S.l.], 2009. Acesso em: 23/01/2015.
- [13] ISO. ISO 32000-1 - Document management - Portable document format - Part 1: PDF 1.7. <https://www.iso.org/obp/ui/#iso:std:iso:32000:-1:ed-1:v1:en>. Acesso em 28/04/2015