INSTRUÇÃO NORMATIVA ITI Nº 04, DE 12 DE FEVEREIRO DE 2021

Aprova a versão revisada e consolidada do documento Perfil de Uso Geral de Requisitos para Geração e Verificação de Certificados de Atributos na ICP-Brasil DOC-ICP-16.01.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso das atribuições que lhe foram conferidas pelo inciso VI do art. 9º do anexo I do Decreto nº 8.985, de 8 de fevereiro de 2017, pelo art. 1º da Resolução nº 33 do Comitê Gestor da ICP-Brasil, de 21 de outubro de 2004, e pelo art. 2º da Resolução nº 163 do Comitê Gestor da ICP-Brasil, de 17 de abril de 2020,

CONSIDERANDO a determinação estabelecida pelo Decreto nº 10.139, de 28 de novembro de 2019, para revisão e consolidação dos atos normativos inferiores a decreto, editados por órgãos e entidades da administração pública federal direta, autárquica e fundacional,

RESOLVE:

Art. 1º Esta Instrução Normativa aprova a versão revisada e consolidada do documento Perfil de Uso Geral de Requisitos para a Geração e Verificação de Certificados de Atributos na ICP-Brasil (DOC-ICP-16.01).

Art. 2º Fica aprovada a versão 2.0 do documento DOC-ICP-16.01 – Perfil de Uso Geral de Requisitos para a Geração e Verificação de Certificados de Atributos na ICP-Brasil, anexa a esta Instrução Normativa.

Art. 3º Ficam revogadas:

I – a Instrução Normativa nº 15, de 27 de dezembro de 2012; e

II – a Instrução Normativa nº 11, de 13 de outubro de 2016.

Art. 4º Esta Instrução Normativa entra em vigor em 1º de março de 2021.

CARLOS ROBERTO FORTNER

Assinado de forma digital por CARLOS ROBERTO FORTNER
Dados: 2021.02.12 18:19:37 -03'00'

CARLOS ROBERTO FORTNER

Infraestrutura de Chaves Públicas Brasileira

PERFIL DE USO GERAL E REQUISITOS PARA GERAÇÃO E VERIFICAÇÃO DE CERTIFICADOS DE ATRIBUTO NA ICP-BRASIL

DOC-ICP-16.01

Versão 2.0

12 de fevereiro de 2021

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Ato que aprovou alteração	Item Alterado	Descrição da Alteração
IN ITI nº 04, de 12/02/2021 Versão 2.0		Revisão e consolidação conforme o Decreto nº 10.139, de 28 de novembro de 2019.
IN nº 11, de 13/10/2016 Versão 1.1	3.5	Exclusão do termo “sequencial”.
IN nº 15, de 27/12/2012 Versão 1.0		Estabelece os procedimentos para regulamentar o perfil de uso geral e requisitos para geração e verificação de certificados de atributo na ICP-Brasil.

LISTA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ANS.1	*Abstract Sintax Notation One*
CA	Certificado de Atributo
CAA	Certificado de Atributo Autônomo
CAV	Certificado de Atributo Vinculado ao Certificado Digital
CD	Certificado de Atributo
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
DER	*Distinguished Encoding Initiative*
DNS	*Domain Name System*
EEA	Entidade Emissora de Certificado de Atributo
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IEC	*International Electotechinical Comission*
ISO	*International Organization for Standerdization*
ITU	*International Telecommunication Union*
LCAR	Lista de Certificados de Atributo Revogados
LDAP	*Lightweigtht Directory Access Protocol*
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
RFC	*Request For Comments*
URI	*Uniforn Resource identifier*
URL	*Uniforn Resource Locator*

1 INTRODUÇÃO

1.1 Este documento está associado ao normativo criado para regulamentar a emissão de certificados de atributos no âmbito da ICP-Brasil:

a) VISÃO GERAL SOBRE CERTIFICADO DE ATRIBUTO PARA A ICP-BRASIL – DOC-ICP-16 **[1].**

1.2 Ele regulamenta os requisitos a serem observados nos processos que tratam da geração e verificação de certificados de atributo no âmbito da ICP-Brasil, quanto a:

a) algoritmos e parâmetros para criação de certificados de atributo;
b) formato e maneira de criar um certificado de atributo;
c) procedimento para verificação e condições para validação de um certificado de atributo.

1.3 Na ICP-Brasil, o formato e a estrutura a serem usados para a criação do certificado de atributo DEVEM seguir as especificações contidas na RFC 5755 [2].

1.4 As diretrizes aqui constantes DEVEM ser observadas por todas as entidades da ICP-Brasil, em especial pelos desenvolvedores de aplicações para emissão, guarda e verificação de certificado de atributo emitido por uma Entidade Emissora de Atributos - EEA, conforme estabelecido no DOC-ICP-16 **[1]**.

1.5 O restante deste documento está organizado da seguinte forma. O capítulo 2 apresenta o perfil do Certificado de Atributo considerando a estrutura lógica e a estrutura de implementação; e o capítulo 3 apresenta as recomendações para emissão, guarda e verificação do Certificado de Atributo.

2 CERTIFICADO DE ATRIBUTO

2.1 Todo Certificado de Atributo - CA é emitido por uma instituição, caracterizada no âmbito da ICP-Brasil, como Entidade Emissora de Certificado de Atributo - EEA.

2.3 Quaisquer informações sob gestão de uma EEA, a respeito de um cidadão ou de uma empresa são passíveis de serem incluídas num certificado de atributo, desde que a EEA seja a gestora e responsável legal pela informação a estar contida no CA.

2.4 Um CA é um documento eletrônico no formato X.509 assinado por um certificado digital ICP-Brasil. Este documento eletrônico trata-se de uma declaração oficial e legal de uma EEA sobre determinada situação ou qualificação de um cidadão ou de uma empresa.

2.5 O conteúdo de um CA é sempre assinado por um Certificado Digital padrão ICP-Brasil, o que confere garantias técnicas e legais quanto ao uso e aplicação pela sociedade em geral.

2.6 Tipos de Certificados

2.6.1 Conforme estabelecido no DOC-ICP-16 **[1]**, o certificado de atributos emitido seguindo as recomendações e padrões da ICP-Brasil pode ser de dois tipos: Certificado de Atributo Autônomo - CAA e Certificado de Atributo Vinculado - CAV.

2.6.1.1 Certificado de Atributo Autônomo - CAA_- este certificado tem como característica principal a possibilidade de ser emitido de forma independente da presença do titular. É necessário que o CA emitido nesta modalidade tenha relação direta ou faça referência a alguma informação que permita inequívoca identificação e qualificação do cidadão ou da empresa, que passa a ser titular do Certificado de Atributo - CA emitido. O CAA quando submetido a uma terceira parte deve ter efeito de correspondência ao que se pretende validar em relação ao titular do mesmo CAA. O uso deste tipo de certificado é recomendado quando há necessidade de validar uma informação ou uma consulta eletrônica, cuja a fonte primária de origem é exclusiva de uma determinada EEA, e portanto responsável pelo fornecimento do atributo em questão.

2.6.1.2 Certificado de Atributos Vinculado ao Certificado Digital - CAV – este certificado se caracteriza por ter um vínculo direto com o certificado digital - CD ICP-Brasil previamente emitido ao mesmo titular do CA. Isso garante maior segurança ao processo de autenticação e autorização associado ao uso da certificação digital. Enquanto o CD permite a identificação e autenticação de seu titular, o CA qualifica este mesmo titular para uma determinada ação qualificada. Para a emissão de um CAV, a EEA tem que necessariamente requerer a autenticação via CD do titular para assim associar as informações constantes do certificado digital ao CAV emitido.

2.7 Estrutura lógica do Certificado de Atributos:

2.7.1 Certificados de Atributo podem ser utilizados numa vasta gama de aplicações e ambientes cobrindo amplo espectro de objetivos de interoperabilidade e de requisitos operacionais e de segurança. O objetivo deste documento é estabelecer uma linha base comum para aplicações genéricas que exigem uma extensa interoperabilidade.

2.7.2 A seguir são descritos os principais campos de dados/informações constantes de um Certificado de Atributo de maneira a prover adequada orientação para emissão de um CA por uma EEA no âmbito deste regulamento.

EMISSOR: é toda entidade gestora de determinada informação passível de ser tratada no formato de CA conforme este regulamento, ou seja, a EEA. Deve utilizar o nome da EEA e o CNPJ associado para inequívoca identificação.

TITULAR DO CERTIFICADO DE ATRIBUTO: é a pessoa ou instituição titular do certificado de atributo. Deve ser utilizado o nome precedido de uma identificação única que permita a plena caracterização do titular. Admite-se como identificação única alguns atributos públicos, entre os quais: CPF, CNPJ; ou a identificação única utilizada pela EEA para gestão da informação sobre o titular do CA, entre os quais: matrícula ou registro ou outra informação de qualificação e identificação junto a EEA sobre o titular do Certificado de Atributo.

PERÍODO DE VALIDADE: todo certificado deve necessariamente ter uma validade

compreendida entre um período de tempo. Deve ser considerado a data e hora de início e a data e hora de término da validade do CA.

NÚMERO DE SÉRIE: todo CA deve ter um número único correspondente a sua emissão de modo a permitir controle e gestão de certificados emitidos pela EEA e ainda facilitar processo de VALIDAÇÃO sem necessidade de explicitar outras informações contidas num CA.
TIPO DE CERTIFICADO DE ATRIBUTO: a EEA deve explicitar o tipo de CA que está sendo emitido, se do tipo CAA ou CAV.

ATRIBUTOS: neste campo a EEA estabelece a principal finalidade do Certificado de Atributo. Este conteúdo explicita a qualificação do TITULAR DO CERTIFICADO DE ATRIBUTO. As informações constantes neste campo permitirão o adequado uso e tratamento do CA pela EEA e também quando apresentado para uma terceira parte para a qualificação do titular do CA. Os atributos admissíveis para este campo são: Informações de Serviço de Autentificação, Identificação de Acesso, Identificação de Incumbência, Grupo, Função e Nível de Acesso.

ASSINATURA DIGITAL DA EEA: trata-se de informação fundamental que deverá conferir a autenticidade e validade jurídica do Certificado de Atributo emitido.

EXTENSÃO: este campo descreve as informações necessárias para o qual o CA deve ser verificado, no caso da EEA estabelecer condições de revogação do CA antes do término da VALIDADE. Toda a aplicação deve considerar este campo, conjuntamente com as outras formas de verificação do CA quanto a autenticidade, integridade e validade técnica e legal. Este campo deverá conter a Lista de Certificados de Atributo Revogados - LCAR, quando definido pela EEA.

VERSÃO: este campo deve ser preenchido com a versão V2, conforme a RFC 5755 [2].

3 PERFIL DO CERTIFICADO DE ATRIBUTO

3.1 Este capítulo apresenta o perfil para Certificado de Atributos que promovam a interoperabilidade e a adequada aplicação no âmbito da ICP-Brasil pela sociedade em geral. Este documento também define algumas extensões privadas para a comunidade da Internet.

3.2 Enquanto os documentos ISO / IEC / ITU usam a versão de 1993 (ou posterior) do ASN.1, este documento utiliza a sintaxe ASN.1 de 1988, como tem sido feito para Certificados de Chave Pública [PKIXPROF].

3.3 Onde os comprimentos máximos de campos são especificados, estes referem-se aos tamanhos para codificação DER e não incluem o rótulo nem o tamanho do campo da sintaxe ASN.1.

3.4 Os certificados de atributos deverão estar em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, que contém os seguintes campos:

```
AttributeCertificate ::= SEQUENCE {
        acinfo              AttributeCertificateInfo,
```

```
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
        version              AttCertVersion, -- version is v2
        holder               Holder,
        issuer               AttCertIssuer,
        signature            AlgorithmIdentifier,
        serialNumber         CertificateSerialNumber,
        attrCertValidityPeriod  AttCertValidityPeriod,
        attributes           SEQUENCE OF Attribute,
       extensions            Extensions OPTIONAL
}

AttCertVersion ::= INTEGER { v2(1) }

Holder ::= SEQUENCE {
        baseCertificateID   [0] IssuerSerial OPTIONAL,
           -- the issuer and serial number of
           -- the holder's Public Key Certificate
        entityName          [1] GeneralNames OPTIONAL,
           -- the name of the claimant or role
        objectDigestInfo    [2] ObjectDigestInfo OPTIONAL
           -- used to directly authenticate the holder,
           -- for example, an executable
}

ObjectDigestInfo ::= SEQUENCE {
        digestedObjectType  ENUMERATED {
          publicKey            (0),
          publicKeyCert        (1),
          otherObjectTypes     (2) },
        -- otherObjectTypes MUST NOT
        -- be used in this profile
        otherObjectTypeID   OBJECT IDENTIFIER OPTIONAL,
        digestAlgorithm     AlgorithmIdentifier,
        objectDigest        BIT STRING
}
AttCertIssuer ::= CHOICE {
        v2Form   [0] V2Form     -- v2 only
}

V2Form ::= SEQUENCE {
        issuerName            GeneralNames  OPTIONAL,
        baseCertificateID     [0] IssuerSerial  OPTIONAL,
        objectDigestInfo      [1] ObjectDigestInfo  OPTIONAL
```

```
        -- issuerName MUST be present in this profile
        -- baseCertificateID and objectDigestInfo MUST NOT
        -- be present in this profile
}
IssuerSerial  ::=  SEQUENCE {
        issuer         GeneralNames,
        serial         CertificateSerialNumber,
        issuerUID      UniqueIdentifier OPTIONAL
}
AttCertValidityPeriod  ::= SEQUENCE {
        notBeforeTime  GeneralizedTime,
        notAfterTime   GeneralizedTime
}

Attribute ::= SEQUENCE {
        type      AttributeType,
        values    SET OF AttributeValue
          -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

3.5 No âmbito deste documento, no mínimo os seguintes campos devem estar contidos num certificado de atributo, padrão ICP-Brasil:

1	Versão	*version*
2	Titular do Certificado de Atributo	*holder*
3	Emissor	*issuer*
4	Algoritmo de Assinatura	*signature*
5	Número de Série	*serialNumber*
6	Período de Validade	*attCertValidityPeriod*
7	Atributos	*attributes*
8	Extensões	*extensions*
9	Assinatura Digital	*SignatureValue*

3.5.1 Versão - *version*

Este campo DEVE conter o valor da versão v2, o valor inteiro um (1).

3.5.2 Titular do Certificado de Atributo- *holder*

3.5.2.1. O campo *holder* contém a informação de identificação do titular. Pode ser representado de três formas: *baseCertificateID, entityName,* ou *objectDigestInfo*, ou seja, respectivamente

baseado na identificação de um certificado, baseado em um nome de entidade ou baseado em informação de resumo de um objeto.
Recomenda-se que somente uma das formas seja usada para evitar ambiguidades.

3.5.2.2 Para o CAV, a forma vinculada ao certificado digital é definida pelo uso do campo *baseCertificateID*. O campo *issuer* do Certificado Digital - CD NÃO DEVE ser vazio e DEVE ser único. Os campos *serialNumber* e *issuer* do CD devem ser iguais ao campo *holder* do CA.
3.5.2.3. Para o CAV, a forma baseada em um nome de entidade é definida pelo uso do campo *entityName*. O campo *entityName* DEVE ser igual ao campo *subject* do CD do titular do atributo ou um dos valores da extensão *subjectAltName* (se houver a extensão).

3.5.2.4 Possível também para o CAV a forma baseada em informação de resumo de um objeto que é definida pelo uso do campo *objectDigestInfo*. Essa forma é usada nos casos em que o CA não é ligado nem pelo nome de identificação (via *entityName*) e nem pela identificação por um CD (via *baseCertificateID*). Neste caso é realizado uma ligação do objeto e o CA, através da adição do resumo criptográfico (*hash*) do objeto no campo *holder* do CA.

3.5.2.5. Para realizar a ligação do CA com um CD via resumo criptográfico, este DEVE ser calculado sobre a codificação DER de todo o CD, incluindo o *signatureValue*. Neste caso, o *digestedObjectType* DEVE ser "*publicKeyCert*". Para ligação do resumo criptográfico somente da chave pública do titular do CD, o *digestedObjectType* DEVE ser "*publicKey*" e o resumo DEVE ser calculado somente sobre a chave pública do titular do CD. Em qualquer caso, para conformidade com este documento, o campo otherObjectTypeID NÃO DEVE estar presente.

3.5.3 Emissor - *issuer*

O campo *issuer* deve conter nome único (*distinguished name-DN*) do emissor e não vazio. CAs de acordo com este documento DEVEM omitir os campos *baseCertificateID* e *objectDigestInfo*.

3.5.4 Algoritmo de Assinatura - *signature*

Contém o identificador do algoritmo utilizado para validar a assinatura do CA. Este algoritmo DEVE ser um dos algoritmos definido no DOC-ICP-01.01 [3].

3.5.5 Número de Serie - *serialNumber*

Todos CAs devem possuir o par *issuer/serialNumber* ÚNICO, mesmo que o CA tenha curta validade. O *serialNumber* deve ser um número inteiro e positivo com um limite máximo de até 20 octetos.

3.5.6 Período de Vigência - *attCertValidityPeriod*

Este campo define o período o qual o emissor do CA certifica que as ligações entre o titular e o campo atributo serão válidos. Este período é dado pelo intervalo *nãoAntes* e *nãoApós*. Deve possuir o formato *GeneralizedTime*, padrão ASN.1 e expresso em UTC (*Universal Time Coordinated*) AAAAMMDDHHMMSSZ.

3.5.7 Atributos - *attributes*

O campo fornece os atributos, informações concedidas ao titular do CA. Se utilizado para autorização, contém um conjunto de privilégios.

Um CA DEVE conter pelo menos um atributo. Cada atributo contém o tipo do atributo e um conjunto de valores.

3.5.7.1 Tipos de Atributo

Alguns dos tipos de atributos definidos abaixo fazem uso do tipo *IetfAttrSyntax*, também definido a seguir. As razões para a utilização deste tipo são:

1. Ele permite uma separação entre o emissor do atributo e a Autoridade da Política de Atributo. Isso é útil para situações em que uma única autoridade de política (ex: uma organização) aloca valores de atributo, mas onde múltiplos EEA são implantados para melhor desempenho ou outras razões.
2. As sintaxes permitidas para valores estão restritas a *OCTET STRING, OBJECT IDENTIFIER*, UTF8String, que significativamente reduzem a complexidade associada com as correspondentes sintaxes mais gerais. Todos os atributos de valores múltiplos usando a sintaxe restrita para cada valor DEVEM usar a mesma opção de sintaxe do valor. Por exemplo, os emitentes de CA não devem usar um valor com um OID e um segundo valor com uma string.

```
IetfAttrSyntax :: =     SEQUENCE {
        policyAuthority [0]   GeneralNames          FACULTATIVO,
        values                SEQUENCE OF CHOICE {
                                    octets          OCTET STRING,
                                    oid             OBJECT IDENTIFIER,
                                    string          UTF8String
                                    }
        }
```

Nas descrições abaixo, cada tipo de atributo é marcado como "Múltiplo Permitido" ou "Somente um valor de Atributo; múltiplos valores dentro do IetfAttrSyntax". Isto se refere ao conjunto de *AttributeValues*; o *AttributeType* ainda ocorre apenas uma vez, conforme especificado na RFC 5755 [2].

3.5.7.1.1 Informações do Serviço de Autenticação

O atributo *SvceAuthInfo* identifica o titular do CA para o servidor/serviço por um nome, e o atributo PODE incluir serviço opcional específico de autenticação de informação. Normalmente, este conterá um par de nome de usuário/senha para uma aplicação “legado”.

Este atributo fornece informação que pode ser apresentada por um verificador de CA para ser interpretado e autenticado por um aplicativo separado dentro do sistema alvo. Note-se que esta é uma utilização diferente da destinada ao atributo *accessIdentity* descrito abaixo.

Este tipo de atributo será tipicamente encriptado quando o campo *authInfo* contiver informação sensível, como uma senha.

name	id-aca-authenticationInfo
OID	{id-aca 1}
syntax	SvceAuthInfo
values	Múltiplos permitidos

```
SvceAuthInfo ::= SEQUENCE {
        service GeneralName,
        ident           GeneralName,
        authInfo        OCTET STRING OPCIONAL
}
```

3.5.7.1.2. Identificação de Acesso

O atributo *accessIdentity* identifica o titular do CA para o servidor/serviço. Para este atributo, o campo *authInfo* NÃO DEVE estar presente.

Este atributo é utilizado para fornecer informação acerca do titular do CA, que pode ser usada pelo verificador do CA (ou um sistema maior o qual o verificador do CA é um componente) para autorizar as ações do titular do CA dentro de um sistema de verificação de AC. Note que isto é uma utilização diferente da destinada ao atributo *svceAuthInfo* descrito acima.

name	*id-aca-accessIdentity*
OID	*{id-aca 2}*
syntax	*SvceAuthInfo*
values	Vários permitidos

3.5.7.1.3. Identificação de Incumbência

O atributo *chargingIdentity* identifica o titular do CA para finalidade de delegação. Em geral, a identidade de incumbência será diferente de outras identidades do titular. Por exemplo, a empresa do titular pode ser encarregada para o serviço.

name	*id-aca-chargingIdentity*
OID	*{id-aca 3}*
syntax	*IetfAttrSyntax*
values	somente um valor de atributo; vários valores dentro da IetfAttrSyntax

3.5.7.1.4. Grupo

O atributo *group* traz informações sobre a adesão ao grupo do titular do CA.

name	*id-aca-grupo*
OID	*{id-aca 4}*
syntax	*IetfAttrSyntax*
values	somente um valor de atributo; vários valores dentro da *IetfAttrSyntax*

3.5.7.1.5. Função

O atributo *role*, especificado no X.509-2000[4], traz informações sobre a função atribuída ao titular do CA.

A sintaxe utilizada para este atributo é:

```
RoleSyntax :: = SEQUENCE {
        roleAuthority          [0] GeneralNames OPCIONAL,
        roleName               [1] GeneralName
}
```

O campo *roleAuthority* PODE ser utilizado para especificar a autoridade que emitiu o certificado do tipo da função. Não há exigência que a função especificada no certificado necessariamente exista para o *roleAuthority*. Isto difere da [X.500-2000], onde o campo *roleAuthority* assume o nome do emissor de um certificado de especificação de função. Por exemplo, para distinguir o função de administrador, conforme definido pela "Empresa A" do definido pela "Empresa B", uma poderia colocar o valor "*urn:administrador*" no campo *roleName* e o valor "Empresa A" ou "empresa B" no campo *roleAuthority*.

O campo *roleName* DEVE estar presente, e *roleName* DEVE usar a opção *uniformResourceIdentifier* do *GeneralName*.

name	*id-at-role*
OID	*{id-at 72}*
syntax	*RoleSyntax*
values	Várias valores permitidos

3.5.7.1.6. Nível de Acesso

O atributo *clearance*, especificado no [X.501-1993], traz informação de nível de acesso (associada à classificação de segurança) do titular do CA.

O campo *policyId* é utilizado para identificar a política de segurança o qual o nível de acesso se refere. O *policyId* indica a semântica dos campos *classList* e *securityCategories*.

Esta especificação inclui o campo *classList* exatamente como está especificado na X.501-1993[5]. Valores adicionais na classificação de segurança e sua posição na hierarquia de classificação podem ser definidos por uma política de segurança como uma questão local ou por acordo bilateral. A hierarquia de classificação de segurança básica é, em ordem crescente: desmarcado, não classificado, restrito, confidencial, secreto, e ultrassecreto.

Uma organização pode desenvolver a sua própria política de segurança que define os valores de classificação de segurança e seus significados. No entanto, a posição do BIT STRING de 0 a 5 é reservada para a hierarquia básica de classificação de segurança.

Se presente, o campo *SecurityCategory* fornece informação de autorização adicional. A política de segurança identificada pelo campo *policyId* indica os sintaxes que têm permissão para estar presente no SET *securityCategories*. Um *OBJECT IDENTIFIER* identifica cada uma das sintaxes permitidas. Quando uma dessas sintaxes estiver presente no SET *securityCategories*, o *OBJECT IDENTIFIER* associado à sintaxe será carregado no campo *SecurityCategory.type*.

O identificador de objeto para o atributo clearance da X.509-1997[6] é:

```
id-at-clearance          OBJECT IDENTIFIER :: = {
joint-iso-ccitt (2) ds (5) attributeType (4) clearance (55) }
```

A sintaxe associada é a seguinte:

```
Clearance ::= SEQUENCE {
        policyId          OBJECT IDENTIFIER,
        classList                 ClassList DEFAULT {não-classificada},
        securityCategories        SET OF SecurityCategory OPCIONAL
}
```

Implementações DEVEM suportar o atributo Permissão (*clearance*) como definido no X.501-1997[5]. Implementações NÃO DEVEM codificar o atributo Clearance como definido na RFC3281 [7].

```
ClassList ::=             BIT STRING {
não-marcado               (0),
não-classificado  (1),
restrito          (2),
confidencial              (3),
secreto           (4),
ultra-secreto             (5)
}
SecurityCategory ::= SEQUENCE {
        type              [0] OBJECT IDENTIFIER,
        value             [1] EXPLICITO DEFINIDO POR QUALQUER type
}
```

3.5.8 Extensões - *extensions*

As extensões presentes nos CAs provêm métodos adicionais de associação entre os titulares dos CA e seus atributos.

Um CA sem extensões está de acordo com a RFC 5755 [2], no entanto, a relação abaixo define as extensões que PODEM ser utilizadas com este perfil, podendo ser marcadas como críticas. Se qualquer outra extensão crítica for utilizada, o CA não estará em conformidade com este perfil. No entanto, se qualquer outra extensão não-crítica for utilizada, o CA estará em conformidade com este perfil.l.

As extensões definidas pela RFC 5755:

- *Audit Identity*
- *AC Targeting*
- *Authority Key Identifier*
- *Authority Information Access*
- *CRL Distribution Points*
- *No Revocation Available*

Este perfil permite também que as comunidades definam extensões privadas para levar informações exclusivas para elas. Cada extensão em um CA pode ser designada como crítica ou

não-crítica. Um sistema que usa CA DEVE rejeitar um CA se encontrar uma extensão crítica que não reconhece. No entanto, uma extensão não-crítica pode ser ignorada se ela não for reconhecida.

3.5.8.1 Identidade de auditoria

Em algumas situações, há necessidade de que trilhas de auditoria não contenham registros que identifiquem diretamente indivíduos (por exemplo: proteção de dados / legislação de privacidade de dados). Esta circunstância pode tornar o uso do campo Titular do CA inadequado para uso em trilhas de auditoria.

Para permitir tais casos, um CA pode conter uma extensão de identidade de auditoria. Idealmente, DEVERIA ser inviável a obtenção da identidade do titular do CA de uma identidade de auditoria sem a cooperação do emissor do CA. O valor de uma identidade de auditoria DEVE ser maior que zeros octetos.
O valor de uma identidade de auditoria não deve ter mais de 20 octetos.

name	*id-pe-ac-auditIdentity*
OID	*{id-pe 4}*
syntax	*OCTET STRING*
CRITICALITY	*must be TRUE*

3.5.8.2 Certificado de Atributo Direcionado

Para direcionar um CA, o alvo das informações, importado da X.509-2000[4], PODE ser utilizado para especificar um número de servidores / serviços. A intenção é que o CA só DEVERIA ser usado em servidores/serviços específicos. Um verificador de CA que não está entre os servidores / serviços especificados DEVE rejeitar o CA.
Se essa extensão não estiver presente, o CA não é direcionado e pode ser aceito por qualquer servidor.

Neste perfil, a informação dirigida consiste simplesmente de uma lista de nomeados alvos ou grupos.

A seguinte sintaxe é usada para representar a informação de direcionamento:

```
Targets :: = SEQUENCE OF Target
        Target   :: = CHOICE {
                targetName    [0] GeneralName,
                targetGroup   [1] GeneralName
        }
```

A checagem de direcionamento verifica se o atual servidor (receptor) é um dos campos no *TargetName* na *SEQUENCE Targets*, ou se o servidor atual é um membro do campo *targetGroup* na *SEQUENCE Targets*. Neste caso, diz-se do servidor atual que "combina" com a extensão *Targets*.

Como a adesão de um *Target* dentro de um *targetGroup* não é determinada aqui, supõe-se que qualquer dado alvo "conhece" os nomes dos *targetGroups* a que pertence ou, caso contrário

determina sua adesão. Para exemplo, o *targetGroup* especifica um domínio DNS, e o verificador do CA conhece o Domínio DNS ao qual ele pertence. Em outro exemplo, o *targetGroup* especifica "Impressoras", e ao verificador do AC sabe se é ou não uma impressora ou servidor de impressão.

name	*id-ce-targetInformation*
OID	*{id-ce 55}*
Syntax	*SEQUENCE OF Targets*
criticality	DEVE ser *TRUE*

3.5.8.3 *Authority Key Identifier*

A extensão *AuthorityKeyIdentifier*, como perfilado em [PKIXPROF], PODE ser utilizada para auxiliar o verificador do CA na verificação da assinatura do CA. A descrição [PKIXPROF] deveria ser lida como se "CA" significasse o "emitente do CA". Tal como acontece com certificados digitais, esta extensão DEVERIA ser incluída nos CAs.

Nota: Em um CA, onde o campo emissor implementa a opção *baseCertificateID*, não seria necessária a extensão *AuthorityKeyIdentifier*, visto que está explicitamente ligada à chave do referido certificado. No entanto, CAs DEVEM utilizar o *v2Form* com a opção *issuerName*, onde esta duplicação não acontece.

name	*id-ce-AuthorityKeyIdentifier*
OID	*{id-ce 35}*
syntax	*AuthorityKeyIdentifier*
criticality	DEVE ser *FALSE*

3.5.8.4 Acesso a Informações da Autoridade

A extensão *authorityInfoAccess*, tal como definido em [PKIXPROF], PODE ser utilizada para auxiliar o verificador do CA quanto ao status de revogação do CA. Suporte para o *accessMethod id-ad-caIssuers* é OPCIONAL para este perfil desde que cadeias de CA não são esperadas.

O *accessMethod* a seguir é usado para indicar que a verificação do status de revogação é fornecida para este CA, usando o *Online Certificate Status Protocol* (OCSP) definida na [OCSP]:

id-ad-ocsp	OBJECT IDENTIFIER :: = {id-ad 1}

O *accessLocation* DEVE conter uma URI, e a URI DEVE conter uma URL HTTP [HTTP URL] que especifica a localização de um respondedor OCSP. O emissor do CA DEVE, evidentemente, manter um respondedor OCSP neste local.

name	id-ce-authorityInfoAccess
OID	{id-pe 1}
syntax	AuthorityInfoAccessSyntax
criticality	DEVE ser FALSE

3.5.8.5 Pontos de Distribuição de LCR

A extensão *cRLDistributionPoints*, como definido em [PKIXPROF], PODE ser utilizada para ajudar o verificador do CA quanto ao estado de revogação do CA.

Se a extensão *cRLDistributionPoints* estiver presente, então exatamente um ponto de distribuição DEVE estar presente. A extensão *cRLDistributionPoints* DEVE usar a opção *DistributionPointName*, a qual DEVE conter um *fullName*, que DEVE conter um formato de nome único. Esse nome DEVE conter um DN ou uma URI. A URI DEVE ser uma URL HTTP [HTTP URL] ou uma URL LDAP (*Lightweight Directory Access Protocol*) [LDAP-URL].

Name	*ID-ce-cRLDistributionPoints*
OID	*{id-ce 31}*
syntax	*cRLDistributionPoints*
criticality	DEVE ser *FALSE*

3.5.8.6 Revogação não Disponibilizada

A extensão *noRevAvail*, definida em X.509-2000[4], permite que um emissor de CA indique que nenhuma informação de revogação será disponibilizada para este CA.

Esta extensão DEVE ser não-crítica. Um verificador de CA que não entende essa extensão pode ser capaz de encontrar uma lista de revogação do emissor do CA, mas a lista de revogação nunca vai incluir uma entrada para o CA.

name	*id-ce-noRevAvail*
OID	*{id-ce 56}*
syntax	*NULL (isto é, '0500'H é a codificação DER)*
criticality	DEVE ser *FALSE*

3.5.9 Assinatura Digital da EEA

a) o período de validade do atributo;

b) o período de validade dos CAs contendo o atributo: o período de validade do CA pode ser igual ou menor que o período de validade do atributo, desde que seja feito um controle do estado de revogação. É possível que a validade do CA seja questão de minutos ou horas e não necessitaria do controle do estado de revogação;

c) o suporte ou não suporte de revogação de atributo: quando a revogação é suportada, as condições de revogação e regras de revogação;

d) a possibilidade de obter um atributo em conjunto com outros através de um subconjunto de atributos. Quando isso ocorre, é necessário especificar como esse subconjunto pode ser obtido;

e) a possibilidade de delegação de um atributo: o nome da pessoa que delega DEVE ser rastreável e os métodos para rastreá-la DEVEM ser indicados. DEVE ser indicado se há alguma restrição, tal como a aplicabilidade das políticas de

assinatura, na aplicação da delegação.A – Aasignature Contém a assinatura digital da EEA.

4 REQUISITOS PARA GERAÇÃO E VALIDAÇÃO DE CERTIFICADO DE ATRIBUTO

4.1 Requisitos Gerais

4.1.1 Os processos relacionados ao ciclo de vida de um certificado de atributo DEVEM ser capazes de identificar e manipular certificados de atributos emitidos no âmbito da ICP-Brasil, bem como suas extensões, campos e "campos específicos ICP-Brasil".

4.1.2 Nos processos relacionados ao ciclo de vida do certificado de atributo, por meios técnicos e procedimentais, os seguintes requisitos DEVEM ser atendidos:

a) a assinatura digital DEVE estar protegida contra falsificação;
b) os conteúdos digitais assinados DEVEM ser protegidos contra alterações;
c) qualquer componente de *software* ou *hardware* utilizado não DEVE provocar alterações no conteúdo digital;
d) qualquer componente de *software* ou *hardware* utilizado NÃO DEVE impedir que o conteúdo digital seja apresentado e visualizado antes e depois de cada um dos processos relacionados ao ciclo de vida da assinatura digital.

4.2 Requisitos para Entidade Emissora de Certificado de Atributo (EEA)

4.2.1 A EEA DEVE indicar para todo CA emitido qual das alternativas ela segue:

a) verificação do atributo somente no registro inicial, sem suporte à revogação;
b) verificação do atributo somente no registro inicial, com suporte à revogação;
c) verificações subsequentes de atributo, com suporte à revogação, e onde aplicável, um período de tempo para verificação.

4.2.2 Para qualquer atributo, quando suportado pela EEA, esta DEVE especificar na sua política, quando aplicável:

a) o período de validade do atributo;
b) o período de validade dos CAs contendo o atributo: o período de validade do CA pode ser igual ou menor ao período de validade do atributo, desde que seja feito um controle do estado de revogação. É possível que a validade do CA seja questão de minutos ou horas e não necessitaria do controle do estado de revogação;
c) o suporte ou não suporte de revogação de atributo: quando a revogação é suportada, as condições de revogação e regras de revogação;
d) a possibilidade de obter um atributo em conjunto com outros através de um subconjunto de atributos. Quando isso ocorre, é necessário especificar como esse subconjunto pode ser obtido.
e) a possibilidade de delegação de um atributo: o nome da pessoa que delega DEVE ser rastreável e os métodos para rastreá-la DEVEM ser indicados. DEVE ser indicado se há alguma restrição, tal como a aplicabilidade das políticas de assinatura, na aplicação da delegação.

4.3. Perfil do Certificado Digital da EEA

O certificado digital - CD da EEA do Certificado de Atributo - CA DEVE obedecer a [PKIXPROF] e a extensão *keyUsage* do CD NÃO DEVE indicar explicitamente que a chave pública da EEA não pode ser usada para validar uma assinatura digital. A fim de evitar confusão quanto a números de série e revogações, uma EEA NÃO DEVE ser também um emissor de certificado digital - CD. Isto é, um emissor de CA não pode ser uma Autoridade Certificadora - AC também. Então, o certificado digital - CD do emissor do certificado de Atributo - CA não deve ter uma extensão *BasicConstraints* com o conjunto da EEA *cA boolean* indicando TRUE.

5 DOCUMENTOS ICP-BRASIL REFERENCIADOS

5.1. Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref	Nome do documento	Código
[1]	**VISÃO GERAL SOBRE CERTIFICADO DE ATRIBUTO PARA A ICP-BRASIL** Aprovado pela Resolução nº 93, de 05 de julho de 2012	DOC-ICP-16

5.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref	Nome do documento	Código
[3]	**PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL** Aprovado pela Instrução Normativa nº 04, de 18 de maio de 2006	DOC-ICP-01.01

6 REFERÊNCIAS

[2] RFC 5755, IETF - AC *Profile for Authorization, january*, 2010.

[4] ITU-T *Recommendation X.509: The Directory – Public-Key and Attribute Certificate Frameworks*, 2000.

[5] ITU-T R*ecommendation X.501: The Directory – Authentication Framework*. 1993.

[6] ITU-T R*ecommendation X.509: The Directory – Authentication Framework*. 1997.

[7] RFC 3281, IETF – *An Internet Attribute Certificate Profile for Authorization, april*, 2002.

[8] RFC 5280, IETF - *Internet X.509 Public Key Infraestructure Certificate and Certificate Revocation List (CRL) Profile, may* 2008.