Receita Federal

Leiaute dos Certificados Digitais da Secretaria da Receita Federal do Brasil

Versão 4.1

Receita Federal

Sumário

1. Leiaute do Certificado de Autoridade Certificadora

1.1. Requisitos de Certificado

Os certificados emitidos pela Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) obedecem as Resoluções do Comitê Gestor da ICP-Brasil.

Os certificados de Autoridade Certificadora da Receita Federal do Brasil são destinados a Autoridades Certificadoras credenciadas pelo ICP-Brasil e habilitadas pela AC-RFB a emitir certificados para pessoas físicas e jurídicas.

Os certificados para Autoridade Certificadora subseqüente a AC-RFB atende aos seguintes requisitos;

1.1.1. Número de Versão

Os certificados digitais implementam a versão 3 de certificados definida no padrão ITU-T X.509 de acordo com o perfil estabelecido na RFC 3280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

1.1.2. Campo Issuer

Todo certificado possui neste campo o nome X.500 da Autoridade Certificadora da Secretaria da Receita Federal do Brasil.

1.1.3. Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave

O algoritmo utilizado para a geração das chaves dos certificados de Autoridade Certificadora é o RSA.

Tamanho de Chave	Processo de Geração de Chave Criptográfica
2048	Hardware

1.1.4. Algoritmo de Assinatura Digital

Os certificados deverão ser assinados com uso do algoritmo conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

1.1.5. Limite de Tamanho

O tamanho máximo de cada componente do DN (CN, OU, O e C) é de 64 caracteres.

1.1.6. Chave Pública do Titular do Certificado

Conforme definido na RFC 3280.

1.1.7. Identificação do Sistema Criptográfico Utilizado

Conforme definido na RFC 3280.

1.1.8. Conjunto de Caracteres

Todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Name*) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere 'c'.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27

(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

1.1.9. Identificação e Assinatura Digital da Autoridade Certificadora da RFB

Conforme definido na RFC 3280.

1.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 3280.

1.1.11. Validade do Certificado Digital

Conforme definido na RFC 3280.

1.1.12. Composição do *Distinguished Name* (DN) do certificado

CN=<Nome da Autoridade Certificadora Habilitada>
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C = BR

Onde

O *Common Name* (CN) é o nome da Autoridade Certificadora definido na Declaração de Praticas da Certificação (DPC) aprovada pelo ITI.

O campo *Organizational Unit* (OU) com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

O campo Or*ganization Name* (O) com conteúdo fixo igual a “ICP-Brasil”.

O campo *Country Name* (C) com conteúdo fixo igual a “BR”.

No formato os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

Exemplo:

CN= AUTORIDADE CERTIFICADORA
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

1.2. Extensões Obrigatórias.

1.2.1. AuthorityKeyIdentifier

Não crítica

O campo *keyIdentifier* deve conter o hash SHA-1 da chave pública da AC-RFB.

1.2.2. SubjectKeyIdentifier

Não critica

O campo *SubjectKeyIdentifier* deve conter o hash SHA-1 da chave pública da AC titular do certificado.

1.2.3. KeyUsage

Crítica

Somente os seguintes bits devem estar ativados:

- *KeyCertSign;* e
- *CRLSign*.

1.2.4. Certificate Policies

Não crítica

- o campo *policyIdentifier* contém o OID da Política de Certificação (PC) que a AC titular do certificado implementa;
- o campo *policyQualifiers* contém o endereço URL da página *Web* da AC-RFB onde se obtém a Declaração de Práticas de Certificação (DPF) da AC-RFB.

1.2.5. CRL Distribution Points

Não crítica

Deve conter o endereço na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC-RFB que gerou este certificado.

Deverão conter dois (2) endereços *web* diferentes para busca da LCR.

1.2.6. Basic Constraints

Crítica

Opcional, deve conter;

- Subject Type=CA; e
- Path Lenght Constraint=0 (zero).

2. Leiaute do Certificado e-CPF

2.1. Requisitos de Certificado

Os certificados e-CPF emitidos pelas Autoridades Certificadoras subordinadas à Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) obedecem as Resoluções do Comitê Gestor da ICP-Brasil.

Os certificados e-CPF são destinados a todas as pessoas físicas que possuem registro no Cadastro de Pessoa Física da Receita Federal do Brasil (CPF).

Os certificados e-CPF são utilizados para assinatura digital e autenticação do seu titular em sistemas e aplicações.

Não poderão ser emitidos certificados e-CPF para pessoas físicas cuja situação cadastral, perante o CPF, esteja enquadrada na condição de cancelada ou nula. A validação desta situação é realizada por intermédio do sistema Consulta Prévia, disponibilizado pela RFB às Autoridades Certificadoras Habilitadas.

O nome do titular do certificado é obtido do Cadastro de Pessoa Física da RFB, utilizando o sistema Consulta Prévia.

Os certificados e-CPF atendem os seguintes requisitos:

2.1.1. Número de Versão

Os certificados digitais e-CPF implementam a versão 3 de certificados definida no padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 3280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

2.1.2. Campo *Issuer*

Todo certificado e-CPF possui neste campo o nome X.500 da Autoridade Certificadora habitada pela AC-RFB.

2.1.3. Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave

O algoritmo utilizado para a geração das chaves dos certificados e-CPF é o RSA.

São quatro os tipos de certificados admitidos:

Tipo	Tamanho de Chave	Processo de Geração de Chave Criptográfica
A1	1024	Software

A2	1024	Software
A3	1024	Hardware
A4	2048	Hardware

2.1.4. Algoritmo de Assinatura Digital

Os certificados e-CPF deverão ser assinados conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

2.1.5. Limite de Tamanho

O tamanho máximo de cada componente do *Distinguished Name* (DN), CN, OU, O e C, é de 64 caracteres.

2.1.6. Chave Pública do Titular do Certificado

Conforme definido na RFC 3280.

2.1.7. Identificação do Sistema Criptográfico Utilizado

Conforme definido na RFC 3280.

2.1.8. Conjunto de Caracteres

Salvo o previsto no item 2.2.5, todas as seqüências de caracteres nos certificados, inclusive as dos *Distinguished Name* (DN) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere ‘c’.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
"	22

#	23
$	24
%	25
&	26
‘	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40

\	5C

2.1.9. Identificação e Assinatura Digital da Autoridade Certificadora Emitente

Conforme definido na RFC 3280.

2.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 3280.

2.1.11. Validade do Certificado Digital

Conforme definido na RFC 3280.

2.1.12. Composição do *Distinguished Name* (DN) do certificado e-CPF

CN=<Nome da Pessoa Física> <:> <número de inscrição no CPF>
OU= <Identificação da AR >
OU=<Domínio do certificado>
OU=<RFB e-CPF ** >
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

Onde

O *Common Name* (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com cumprimento máximo de 52 (cinqüenta e dois) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro composto por 11 (onze) caracteres.

São quatro os campos *Organizational Unit* (OU) definidos no certificado, assim constituídos:

Primeiro “OU” com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

Segundo “OU” com conteúdo variável, informando no campo domínio a identificação da empresa ou órgão fornecedor do certificado, quando o titular do certificado for seu empregado, funcionário ou servidor. Caso esse OU não seja utilizado, o mesmo deverá ser grafado com o texto “(EM BRANCO)”.

Terceiro “OU” com conteúdo variável conforme o tipo de certificado:

- Tipo A1 = “RFB e-CPF A1”;
- Tipo A2 = “RFB e-CPF A2”;
- Tipo A3 = “RFB e-CPF A3”;
- Tipo A4 = “RFB e-CPF A4”.

Quarto “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

O campo *Organization Name* (O) com conteúdo fixo igual a “ICP-Brasil”.

O campo *Country Name* (C) com conteúdo fixo igual a “BR”.

No formato os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

Exemplo:

CN=JOAO DA SILVA:01672780838
OU= Autoridade de Registro
OU= DOMINIO RFB
OU=RFB e-CPF A3
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

2.2. Extensões Obrigatórias.

2.2.1. Authority Key Identifier

Não crítica

O campo *key Identifier* deve conter o hash SHA-1 da chave pública da AC Habilitada que emitiu o certificado.

2.2.2. Key Usage

Crítica

Somente os seguintes bits devem estar ativados:

- *DigitalSignature* ;
- *NonRepudiation; e*
- *keyEncipherment*.

2.2.3. Certificate Policies

Não crítica

- o campo *policyIdentifier* contém o OID da Política de Certificação (PC) correspondente;
- o campo *policyQualifiers* contém o endereço URL da página *Web* onde se obtém a Declaração de Praticas de Certificação (DPC) da AC Habilitada que emitiu o certificado.

2.2.4. CRL Distribution Points

Não crítica

Contém os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC Habilitada que assinou o certificado.

Deverão conter três (3) endereços *web* diferentes para busca da LCR.

2.2.5. Subject Alternative Name

Não crítica

Contendo três campos O*therName* obrigatórios e dois campos opcionais com os seguintes conteúdos:

Campos Obrigatórios

OID = 2.16.76.1.3.1 com o seguinte conteúdo:

Nas primeiras 8 (oito) posições, a data de nascimento da pessoa física titular do certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoa Física (CPF) da pessoa física titular do certificado; nas

11 (onze) posições subseqüentes, o número de Identificação Social da pessoa física titular do certificado - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subseqüentes, o número do Registro Geral - RG da pessoa física titular do certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.

OID = 2.16.76.1.3.5 com o seguinte conteúdo:

Nas primeiras 12 (onze) posições, o número de inscrição do Título de Eleitor da pessoa física titular do certificado; nas 3 (três) posições subseqüentes, o número correspondente a Zona Eleitoral; nas 4 (quatro) posições seguintes, o número correspondente a Seção; nas 22 (vinte e duas) posições subseqüentes, o nome do município e a UF do Título de Eleitor.

OID = 2.16.76.1.3.6 com o seguinte conteúdo:

Nas 12 (doze) posições, o número do Cadastro Especifico do INSS (CEI) da pessoa física titular do certificado.

Campos Opcionais

OID = 2.16.76.1.4.x.y.z com o seguinte conteúdo;

Tamanho variável correspondente ao número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

A AC Raiz, por meio do documento ATRIBUIÇÃO DE OID DA ICP-BRASIL (DOC ICP-04-01) regulamentará a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.

OID = 1.3.6.1.4.1.311.20.2.3 com o seguinte conteúdo:

Este campo *Principal Name* contém a Identificação do endereço de *login* do titular do certificado no diretório *Active Direct* (AD) Microsoft.

O conjunto de informações definido em cada campo *OtherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, com exceção do campo *Principal Name* cuja cadeia de caracteres é do tipo UTF-8 String.

Os seguintes campos são de preenchimento obrigatório:

- Nome;
- CPF;
- Data de nascimento; e
- Email.

Quando os números de NIS (PIS/PASEP/CI) RG, CEI, ou Titulo de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.

Se o número do RG ou o número de inscrição do Titulo de Eleitor não estiver disponível, não se deve preencher os campos de órgão expedidor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente.

Todas informações de tamanho variável, referentes a números, tais como RG ou Titulo de Eleitor, devem ser preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível.

As 6 (seis) posições das informações sobre órgão expedidor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor.

Para todos os campos *OtherName*, com exceção do campo *Principal Name,* apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

Para o preenchimento do campo *Principal Name* serão permitidos os caracteres de “A” a “Z”, de “0” a “9” além dos caracteres “.” (ponto), “-“ (hífen) e “@” (arroba), necessários à formação do endereço de *login* do titular do certificado. Outros caracteres especiais, símbolos, espaços ou acentuação não são permitidos.

O campo *rfc822Name*, parte da extensão obrigatória *Subject Alternative Name*, contendo o endereço e-mail do titular do certificado também deverá estar presente.

2.2.6. Basic Constraints

Não crítica

Opcional,

- Subject Type= End Entity; e
- Path Length Constraint-None.

2.2.7. Extended-Key-Usage

Não crítica

Deve conter os seguintes valores representados por seus respectivos OID:

- **Obrigatório**

OID	**Propósito**
1.3.6.1.5.5.7.3.2	Autenticação de Cliente
1.3.6.1.5.5.7.3.4	Proteção de E-mail

- **Opcional**

OID	**Propósito**
1.3.6.1.4.1.311.20.2.2	Logon com certificado em estações Windows

2.2.8. Authority Information Access (opcional)

Não crítica

Com os seguintes campos:

- Endereço de acesso ao protocolo de OCSP (On-line Certificate Status Protocol), conforme definido na RFC 3280;
- Endereço na *web* onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.

3. Leiaute do Certificado e-CNPJ

3.1. Requisitos de Certificado

Os certificados emitidos pelas Autoridades Certificadoras subordinadas à Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) obedecem as Resoluções do Comitê Gestor da ICP-Brasil.

Os certificados e-CNPJ são destinados a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ).

Os certificados e-CNPJ são utilizados para assinatura digital e autenticação do seu titular em sistemas e aplicações.

Não poderão ser emitidos certificados e-CNPJ para pessoas jurídicas cuja situação cadastral, perante o CNPJ, esteja enquadrada na condição de suspensa, inapta, baixada ou nula. A validação desta situação é realizada por intermédio do sistema Consulta Prévia, disponibilizado pela RFB às Autoridades Certificadoras Habilitadas.

O nome da empresa titular do certificado, é obtido do Cadastro Nacional da Pessoa Jurídica da RFB, utilizando o sistema Consulta Prévia.

Os certificados e-CNPJ atendem os seguintes requisitos:

3.1.1. Número de Versão

Os certificados digitais e-CNPJ implementam a versão 3 de certificados definida no padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 3280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

3.1.2. Campo *Issuer*

Todo certificado e-CNPJ possui neste campo o nome X.500 da Autoridade Certificadora habilitada pela RFB.

3.1.3. Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave

O algoritmo utilizado para a geração das chaves dos certificados e-CNPJ é o RSA.

São quatro os tipos de certificados admitidos:

Tipo	Tamanho de Chave	Processo de Geração de Chave Criptográfica
A1	1024	Software
A2	1024	Software
A3	1024	Hardware
A4	2048	Hardware

3.1.4. Algoritmo de Assinatura Digital

Os certificados e-CNPJ deverão ser assinados conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

3.1.5. Limite de tamanho

O tamanho máximo de cada componente do *Distinguished Name* (DN), CN, OU, L, ST, O e C, é de 64 caracteres.

3.1.6. Chave pública do titular do certificado

Conforme definido na RFC 3280.

3.1.7. Identificação do sistema criptográfico utilizado

Conforme definido na RFC 3280.

3.1.8. Conjunto de Caracteres

Salvo no item 3.2.5, todas as seqüências de caracteres nos certificados, inclusive as dos *Distinguished Name* (DN) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere ‘c’.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21

"	22
#	23
$	24
%	25
&	26
‘	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F

@	40
\	5C

3.1.9. Identificação e Assinatura Digital da Autoridade Certificadora Emitente

Conforme definido na RFC 3280.

3.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 3280.

3.1.11. Validade do Certificado Digital

Conforme definido na RFC 3280.

3.1.12. Composição do Distinguished Name (DN) do certificado e-CNPJ

CN=<Nome Empresarial> <:> <número de inscrição no CNPJ>
OU= <Identificação da AR >
OU=<RFB e-CNPJ ** >
OU=Secretaria da Receita Federal do Brasil – RFB
L = <cidade>
ST= <sigla da unidade da federação >
O=ICP-Brasil
C=BR

O *Common Name* (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com cumprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.

São três os campos *Organizational Unit* (OU) definidos no certificado, sendo assim constituídos:

Primeiro "OU" com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

Segundo "OU" com conteúdo variável conforme o tipo de certificado:

- Tipo A1 = "RFB e-CNPJ A1";
- Tipo A2 = "RFB e-CNPJ A2";
- Tipo A3 = "RFB e-CNPJ A3";
- Tipo A4 = "RFB e-CNPJ A4".

Terceiro "OU" com conteúdo fixo "Secretaria da Receita Federal do Brasil – RFB".

O campo *locality* (L) com conteúdo correspondente ao nome da cidade onde a empresa está localizada. O campo deve ser preenchido sem acentos nem abreviaturas.

O campo *state or province name* (ST) com conteúdo correspondente a sigla do estado onde a empresa está localizada.

O campo *Organization Name* (O) com conteúdo fixo igual a "ICP-Brasil".

O campo *Country Name* (C) com conteúdo fixo igual a "BR".

No formato os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

Exemplo:

CN=CASA LIQUIDACAO:12345678000199
OU= Autoridade de Registro
OU=RFB e-CNPJ A3
OU=Secretaria da Receita Federal do Brasil – RFB
L=PORTO ALEGRE
ST=RS
O=ICP-Brasil
C=BR

3.2. Extensões Obrigatórias.

3.2.1. Authority Key Identifier

Não crítica

O campo *key Identifier* deve conter o hash SHA-1 da chave pública da AC Habilitada que emitiu o certificado.

3.2.2. Key Usage

Crítica

Somente os seguintes bits devem estar ativados:

- *DigitalSignature* ;
- *NonRepudiation ; e*
- *keyEncipherment*.

3.2.3. Certificate Policies

Não crítica

- o campo *policyIdentifier* contém o OID da Política de Certificação (PC) correspondente;
- o campo *policyQualifiers* contém o endereço URL da página *Web* onde se obtém a Declaração de Praticas de Certificação (DPC) da AC Habilitada que emitiu o certificado.

3.2.4. CRL Distribution Points

Não crítica

Contém os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC Habilitada que assinou o certificado.

Deverão conter três (3) endereços *web* diferentes para busca da LCR.

3.2.5. Subject Alternative Name

Não crítica

Contendo 4 (quatro) campos *OtherName* obrigatórios:

OID = 2.16.76.1.3.2 com o seguinte conteúdo:

Nome do responsável pela Pessoa Jurídica, perante o CNPJ;

OID = 2.16.76.1.3.3 com o seguinte conteúdo:

Número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

OID = 2.16.76.1.3.4 com o seguinte conteúdo:

Nas primeiras 8 (oito) posições, a data de nascimento do responsável pela Pessoa Jurídica perante o CNPJ, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do responsável pela Pessoa Jurídica perante o CNPJ; nas 11 (onze) posições subseqüentes o número de inscrição no NIS (PIS, PASEP ou CI) do responsável pela Pessoa Jurídica perante o CNPJ; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pela Pessoa Jurídica perante o CNPJ; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF;

OID = 2.16.76.1.3.7 com o seguinte conteúdo:

Nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da Pessoa Jurídica titular do certificado.

O conjunto de informações definido em cada campo *OtherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING.

Os seguintes campos são de preenchimento obrigatório;

Da empresa:

- Nome Empresarial;
- Número de inscrição no CNPJ.

Do responsável pela pessoa jurídica perante o CNPJ:

- Número de inscrição no CPF;

- Data de nascimento;
- Nome do responsável pela Pessoa Jurídica perante o CNPJ.
- Email.

Quando os números de NIS (PIS/PASEP/CI), RG ou CEI não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.

Se o número do RG não estiver disponível, não se deve preencher os campos de órgão expedidor e UF.

Todas informações de tamanho variável, referentes a números, tais como RG, devem ser preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível.

As 6 (seis) posições das informações sobre órgão expedidor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita.

Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados no campo *OtherName*, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

O campo *rfc822 Name*, parte da extensão obrigatória *Subject Alternative Name*, contendo o endereço e-mail do responsável, perante o CNPJ, pela Pessoa Jurídica titular do certificado também deverá estar presente.

3.2.6. Basic Constraints

Não crítica

Opcional,

- Subject Type= End Entity, e
- Path Length Constraint-None.

3.2.7. Extended-Key-Usage

Não crítica

Deve conter os seguintes valores representados por seus respectivos OID:

Obrigatório

OID	Propósito
1.3.6.1.5.5.7.3.2	Autenticação de Cliente
1.3.6.1.5.5.7.3.4	Proteção de E-mail

3.2.8. Authority Information Access (opcional)

Não crítica

Com os seguintes campos:

- Endereço de acesso ao protocolo de OCSP (On-line Certificate Status Protocol), conforme definido na RFC 3280;
- Endereço na *web* onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.

4. Leiaute do Certificado de Equipamento - e-Servidor

4.1. Requisitos de Certificado

Os certificados emitidos pelas Autoridades Certificadoras subordinadas à Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) obedecem as Resoluções do Comitê Gestor da ICP-Brasil.

Os certificados e-Servidor são destinados a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ).

Os certificados e-Servidor são utilizados para a identificação de equipamentos servidores *WEB.*

Para a emissão de um certificado e-Servidor deverá ser emitida autorização do representante legal da Pessoa Jurídica perante o CNPJ e do responsável pelo endereço *Domain Name Service* (DNS) em nome de um representante da empresa que será o responsável pelo certificado.

Não poderão ser emitidos certificados e-Servidor para pessoas jurídicas cuja situação cadastral, perante o CNPJ, esteja enquadrada na condição de suspensa, inapta, baixada ou nula.

Não poderão ser emitidos certificados e-Servidor quando a situação cadastral da pessoa física responsável pelo certificado, perante o CPF, estiver enquadrada na condição de cancelada ou nula.

As validações dessas situações são realizadas por intermédio do sistema Consulta Prévia, disponibilizado pela RFB às Autoridades Certificadoras Habilitadas.

O nome empresarial da Pessoa Jurídica bem assim o nome da Pessoa Física responsável pelo certificado são obtidos no Cadastro Nacional da Pessoa Jurídica e Cadastro de Pessoa Física, respectivamente, utilizando o sistema Consulta Prévia.

Os certificados e-Servidor atendem os seguintes requisitos:

4.1.1. Número de Versão

Os certificados digitais e-Servidor implementam a versão 3 de certificados definida no padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 3280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

4.1.2. Campo Issuer

Todo certificado e-Servidor possui neste campo o nome X.500 da Autoridade Certificadora que o emitiu.

4.1.3. Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave

O algoritmo utilizado para a geração das chaves dos certificados e-Servidor é o RSA.

São quatro os tipos de certificados admitidos:

Tipo	Tamanho de Chave	Processo de Geração de Chave Criptográfica
A1	1024	Software
A2	1024	Software
A3	1024	Hardware
A4	2048	Hardware

4.1.4. Algoritmo de Assinatura Digital

Os certificados e-Servidor deverão ser assinados conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

4.1.5. Limite de tamanho

O tamanho máximo de cada componente do DN (CN, OU, O e C) é de 64 caracteres.

4.1.6. Chave pública do titular do certificado

Conforme definido na RFC 3280.

4.1.7. Identificação do sistema criptográfico utilizado

Conforme definido na RFC 3280.

4.1.8. Conjunto de Caracteres

Salvo o previsto no item 4.2.5. todas as seqüências de caracteres nos certificados, inclusive as dos *Distinguished Name* (DN) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere ‘c’.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
"	22
#	23
$	24
%	25
&	26
‘	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F

:	3A
;	3B
=	3D
?	3F
@	40
\	5C

4.1.9. Identificação e Assinatura Digital da Autoridade Certificadora Emitente

Conforme definido na RFC 3280.

4.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 3280.

4.1.11. Validade do Certificado Digital

Conforme definido na RFC 3280.

4.1.12. Composição do DN (Distinguished Name) do certificado e-Servidor

CN=<DNS do servidor>
OU= <Identificação da AR >
OU=<RFB e-Servidor Tipo ** >
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

O “Common Name” (CN) é composto pelo DNS do servidor.

São três os campos “Organizational Unit” (OU) definidos no certificado, sendo assim constituídos:

Primeiro “OU” com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

Segundo “OU” com conteúdo variável conforme o tipo de certificado:

Certificados e-Servidor:

- Tipo A1 = “RFB e-Servidor A1”;
- Tipo A2 = “RFB e-Servidor A2”;
- Tipo A3 = “RFB e-Servidor A3”;
- Tipo A4 = “RFB e-Servidor A4”.

Terceiro “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

O campo “Organization Name” (O) com conteúdo fixo igual a “ICP-Brasil”.

O campo “Country Name” (C) com conteúdo fixo igual a “BR”.

No formato os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

Exemplo:

CN=www.receita.fazenda.gov.br
OU= Autoridade de Registro
OU=RFB e-Servidor A1
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

4.2. Extensões Obrigatórias.

4.2.1. Authority Key Identifier

Não crítica

O campo key Identifier deve conter o hash SHA-1 da chave pública da AC Habilitada que emitiu o certificado.

4.2.2. Key Usage

Crítica

Somente os seguintes bits devem estar ativados;

- “digitalSignature”;
- “nonRepudiation” ; e
- “keyEncipherment”.

4.2.3. Certificate Policies

Não crítica

- o campo “policyIdentifier” contém o OID da PC (Política de Certificação) correspondente;
- o campo “policyQualifiers” contém o endereço URL da página *Web* onde se obtém a DPC (Declaração de Praticas de Certificação) da AC Habilitada que emitiu o certificado.

4.2.4. CRL Distribution Points

Não crítica

Contém os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC Habilitada que assinou o certificado.

Deverão conter três (3) endereços *web* diferentes para busca da LCR.

4.2.5. Subject Alternative Name

Não crítica

Contendo 4 (quatro) campos “otherName” obrigatórios:

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo Certificado.

OID = 2.16.76.1.3.3 e conteúdo = número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do responsável pelo certificado; nas 11 (onze) posições subseqüentes, o número de inscrição no NIS (PIS, PASEP ou CI) do responsável pelo certificado; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pelo certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

Campos Opcionais

OID = 1.3.6.1.4.1.311.25.1 com o seguinte conteúdo:

Identificador único de controlador de domínio *(GUID)* e a identificação DNS do servidor.

O conjunto de informações definido em cada campo *OtherName* deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING, Os seguintes campos são de preenchimento obrigatório;

Da empresa:

- Número de inscrição no CNPJ;
- Nome empresarial;
- Nome DNS do servidor.

Do responsável pelo certificado:

- Número de inscrição no CPF;
- Data de nascimento;
- Nome do responsável pelo certificado;
- Email do responsável pelo certificado.

Quando os números de NIS(PIS/PASEP ou CI), RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.

Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. Todas informações de tamanho variável, referentes a números, tais como RG, devem ser preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível.

As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita.

Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados nos campos otherName, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

O campo “rfc822 Name”, parte da extensão obrigatória “Subject AlternativeName”, contendo o endereço e-mail do responsável pelo certificado também deverá estar presente

4.2.6. Basic Constraints

Não crítica

Opcional,

- Subject Type= End Entity; e
- Path Length Constraint-None.

4.2.7. Extended-Key-Usage

Não crítica

Deve conter os seguintes valores representados por seus respectivos OID:

Obrigatório

OID	**Propósito**
1.3.6.1.5.5.7.3.1	Autenticação de Servidor

Opcional

OID	**Propósito**
1.3.6.1.5.5.7.3.2	Autenticação de Cliente

4.2.8. Authority Information Access (opcional)

Não crítica

Com os seguintes campos:

- Endereço de acesso ao protocolo de OCSP (*On-line Certificate Status Protocol),* conforme definido na RFC 3280.
- Endereço na *web* onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.

5. Leiaute do Certificado de Aplicação - e-Aplicação

5.1. Requisitos de Certificado

Os certificados emitidos pelas Autoridades Certificadoras subordinadas à Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) obedecem as Resoluções do Comitê Gestor da ICP-Brasil.

Os certificados e-Aplicação são destinados a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ).

Os certificados e-Aplicação são utilizados exclusivamente para autenticação de aplicações.

São considerados, em relação ao escopo das aplicações, como certificados e-Aplicação singulares, os certificados com propósitos de Carimbo de Tempo, Email Seguro e OCSP.

Os propósitos do certificado de aplicação são excludentes, o certificado utilizado para um propósito não poderá ser utilizado cumulativamente para outro.

Para a emissão de um certificado e-Aplicação deverá ser emitida autorização do representante legal da Pessoa Jurídica perante o CNPJ em nome de um representante da empresa que será o responsável pelo certificado.

Não poderão ser emitidos certificados e-Aplicação para pessoas jurídicas cuja situação cadastral, perante o CNPJ, esteja enquadrada na condição de suspensa, inapta, baixada ou nula.

Não poderão ser emitidos certificados e-Aplicação quando a situação cadastral da pessoa física responsável pelo certificado, perante o CPF, estiver enquadrada na condição de cancelada ou nula.

As validações dessas situações são realizadas por intermédio do sistema Consulta Prévia, disponibilizado pela RFB às Autoridades Certificadoras Habilitadas.

O nome empresarial da Pessoa Jurídica bem assim o nome da Pessoa Física responsável pelo certificado são obtidos no Cadastro Nacional da Pessoa Jurídica e Cadastro de Pessoa Física, respectivamente, utilizando o sistema Consulta Prévia.

Os certificados e-Aplicação atendem os seguintes requisitos;

5.1.1. Número de Versão

Os certificados digitais e-Aplicação implementam a versão 3 de certificados definida no padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 3280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

5.1.2. Campo Issuer

Todo certificado e-Aplicação possui neste campo o nome X.500 da Autoridade Certificadora que o emitiu.

5.1.3. Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave

O algoritmo utilizado para a geração das chaves dos certificados é o RSA.

São quatro os tipos de certificados admitidos:

Tipo	Tamanho de Chave	Processo de Geração de Chave Criptográfica
A1	1024	Software
A2	1024	Software
A3	1024	Hardware
A4	2048	Hardware

5.1.4. Algoritmo de Assinatura Digital

Os certificados e-Aplicação deverão ser assinados conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

5.1.5. Limite de tamanho

O tamanho máximo de cada componente do DN (CN, OU, O e C) é de 64 caracteres.

5.1.6. Chave pública do titular do certificado

Conforme definido na RFC 3280.

5.1.7. Identificação do sistema criptográfico utilizado

Conforme definido na RFC 3280.

5.1.8. Conjunto de Caracteres

Salvo o previsto no item 5.2.5. todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Name*) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere 'c'.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C

-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

5.1.9. Identificação e Assinatura Digital da Autoridade Certificadora Emitente

Conforme definido na RFC 3280.

5.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 3280.

5.1.11. Validade do Certificado Digital

Conforme definido na RFC 3280.

5.1.12. Composição do DN (Distinguished Name) do certificado e-Aplicação.

CN=<Nome da Aplicação> <:> <número de inscrição no CNPJ>
OU= <Identificação da AR >
OU=<RFB e-Aplicacao Tipo ** >
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil

C=BR

O “Common Name” (CN) é composto do nome da aplicação, acrescido do sinal de dois pontos (:) mais o número de inscrição no Cadastro de Pessoas Jurídica (CNPJ).

São três os campos “Organizational Unit” (OU) definidos no certificado, sendo assim constituídos:

Primeiro “OU” com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

Segundo “OU” com conteúdo variável conforme o tipo de certificado:

Certificados e-Aplicação.

- Tipo A1 = “RFB e-Aplicacao A1”;
- Tipo A2 = “RFB e-Aplicacao A2”;
- Tipo A3 = “RFB e-Aplicacao A3”;
- Tipo A4 = “RFB e-Aplicacao A4”.

Terceiro “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

O campo “Organization Name” (O) com conteúdo fixo igual a “ICP-Brasil”.

O campo “Country Name” (C) com conteúdo fixo igual a “BR”.

No formato os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

Exemplo:

CN=Aplicação XYZ:01672780838897
OU= Autoridade de Registro
OU=RFB e-Aplicacao A1
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil

C=BR

5.2. Extensões Obrigatórias.

5.2.1. Authority Key Identifier

Não crítica

O campo key Identifier deve conter o hash SHA-1 da chave pública da AC Habilitada que emitiu o certificado.

5.2.2. Key Usage

Crítica

Somente os seguintes bits devem estar ativados;

- “digitalSignature”,
- “nonRepudiation”; e
- “keyEncipherment”.

5.2.3. Certificate Policies

Não crítica

- o campo “policyIdentifier” contém o OID da PC (Política de Certificação) correspondente;
- o campo “policyQualifiers” contém o endereço URL da página *Web* onde se obtém a DPC (Declaração de Praticas de Certificação) da AC Habilitada que emitiu o certificado.

5.2.4. CRL Distribution Points

Não crítica

Contém os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC Habilitada que assinou o certificado.

Deverão conter três (3) endereços *web* diferentes para busca da LCR.

5.2.5. Subject Alternative Name

Não crítica

Contendo 4 (quatro) campos “otherName” obrigatórios:

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo Certificado.

OID = 2.16.76.1.3.3 e conteúdo = número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do responsável pelo certificado; nas 11 (onze) posições subseqüentes, o número de inscrição no NIS (PIS, PASEP ou CI) do responsável pelo certificado; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pelo certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

O conjunto de informações definido em cada campo “OtherName” deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING.

Os seguintes campos são de preenchimento obrigatório;

Da empresa:

- Número de inscrição no CNPJ;
- Nome empresarial da Pessoa Jurídica;
- Nome da aplicação.

Do responsável pelo certificado:

- Número de inscrição no CPF;
- Data de nascimento;
- Nome do responsável pelo certificado;
- Email do responsável pelo certificado ou da pessoa jurídica, em caso de email coorporativo.

- Quando os números de NIS(PIS/PASEP ou CI), RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.

Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. Todas informações de tamanho variável, referentes a números, tais como RG, devem ser preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível.

As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita.

Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados nos campos otherName, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

O campo “rfc822 Name”, parte da extensão obrigatória “Subject AlternativeName”, contendo o endereço e-mail do responsável pelo certificado ou da pessoa jurídica, em caso de email corporativo, também deverá estar presente

5.2.6. Basic Constraints

Não crítica

Opcional,

- Subject Type= End Entity ; e
- Path Length Constraint-None.

5.2.7. Extended-Key-Usage

5.2.7.1 Certificados e-Aplicação com o propósito de Carimbo de Tempo.

Crítica

Obrigatório

OID	Propósito
1.3.6.1.5.5.7.3.8	Carimbo de tempo.

5.2.7.2 Certificados e-Aplicação com o propósito de Email Seguro.

Não crítica

Obrigatório

OID	Propósito
1.3.6.1.5.5.7.3.4	Email Seguro

5.2.7.3 Certificados e-Aplicação com o propósito de OCSP.

Não crítica

Obrigatório

OID	Propósito
1.3.6.1.5.5.7.3.9	Assinatura de OCSP

5.2.7.4 Certificados e-Aplicação com o propósito de Autenticação das demais aplicações.

Não crítica

Obrigatório

OID	Propósito
1.3.6.1.5.5.7.3.2	Autenticação de Cliente

5.2.8. Authority Information Access (opcional)

Não crítica

Com os seguintes campos:

- Endereço de acesso ao protocolo de OCSP (On-line Certificate Status Protocol), conforme definido na RFC 3280;
- Endereço na *web* onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.

6. Leiaute do Certificado de Assinatura de Código - e-Código

6.1. Requisitos de Certificado

Os certificados emitidos pelas Autoridades Certificadoras subordinadas à Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB) obedecem as Resoluções do Comitê Gestor da ICP-Brasil.

Os certificados e-Código são destinados a todas as pessoas jurídicas que possuem registro no Cadastro Nacional da Pessoa Jurídica da Receita Federal do Brasil (CNPJ).

Os certificados e-Código são utilizados exclusivamente para assinatura de código de software.

Para a emissão de um certificado e-Código deverá ser emitida autorização do representante legal da Pessoa Jurídica perante o CNPJ em nome de um representante da empresa que será o responsável pelo certificado.

Não poderão ser emitidos certificados e-Código para pessoas jurídicas cuja situação cadastral, perante o CNPJ, esteja enquadrada na condição de suspensa, inapta, baixada ou nula.

Não poderão ser emitidos certificados e-Código quando a situação cadastral da pessoa física responsável pelo certificado, perante o CPF, estiver enquadrada na condição de cancelada ou nula.

As validações dessas situações são realizadas por intermédio do sistema Consulta Prévia, disponibilizado pela RFB às Autoridades Certificadoras Habilitadas.

O nome empresarial da Pessoa Jurídica bem assim o nome da Pessoa Física responsável pelo certificado são obtidos no Cadastro Nacional da Pessoa Jurídica e Cadastro de Pessoa Física, respectivamente, utilizando o sistema Consulta Prévia.

Os certificados e-Código atendem os seguintes requisitos

6.1.1. Número de Versão

Os certificados digitais e-Código implementam a versão 3 de certificados definida no padrão ITU-T X.509, de acordo com o perfil estabelecido na RFC 3280 (*Request for Comments – Internet X509 Public Key Infrastructure*).

6.1.2. Campo Issuer

Todo certificado e-Código possui neste campo o nome X.500 da Autoridade Certificadora que o emitiu.

6.1.3. Algoritmos de Criptografia, Tamanho e Processo de Geração de Chave

O algoritmo utilizado para a geração das chaves dos certificados é o RSA.

São quatro os tipos de certificados admitidos:

Tipo	Tamanho de Chave	Processo de Geração de Chave Criptográfica
A1	1024	Software
A2	1024	Software
A3	1024	Hardware
A4	2048	Hardware

6.1.4. Algoritmo de Assinatura Digital

Os certificados e-Código deverão ser assinados conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC ICP-01.01).

6.1.5. Limite de tamanho

O tamanho máximo de cada componente do DN (CN, OU, O e C) é de 64 caracteres.

6.1.6. Chave pública do titular do certificado

Conforme definido na RFC 3280.

6.1.7. Identificação do sistema criptográfico utilizado

Conforme definido na RFC 3280.

6.1.8. Conjunto de Caracteres

Salvo o previsto no item 6.2.5. todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Name*) devem obedecer ao Código NBR 9611, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na tabela abaixo. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere ‘c’.

Caractere	Código NBR 9611 (hexadecimal)
branco	20
!	21
"	22
#	23
$	24
%	25
&	26
‘	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F

:	3A
;	3B
=	3D
?	3F
@	40
\	5C

6.1.9. Identificação e Assinatura Digital da Autoridade Certificadora Emitente

Conforme definido na RFC 3280.

6.1.10. Número de Série Exclusivo do Certificado

Conforme definido na RFC 3280.

6.1.11. Validade do Certificado Digital

Conforme definido na RFC 3280.

6.1.12. Composição do DN (Distinguished Name) do certificado e-Código.

CN=<Nome Empresarial> <:> <número de inscrição no CNPJ>
OU= <Identificação da AR >
OU=<RFB e-Código Tipo ** >
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

O “Common Name” (CN) é composto do nome empresarial, acrescido do sinal de dois pontos (:) mais o número de inscrição no Cadastro de Pessoas Jurídica (CNPJ).

São três os campos “Organizational Unit” (OU) definidos no certificado, sendo assim constituídos:

Primeiro “OU” com conteúdo variável, informando o nome da Autoridade de Registro responsável pela aprovação do certificado, conforme o nome atribuído no credenciamento pelo ITI.

Segundo “OU” com conteúdo variável conforme o tipo de certificado:

Certificados e-Código.

- Tipo A1 = “RFB e-Código A1”;
- Tipo A2 = “RFB e-Código A2”;
- Tipo A3 = “RFB e-Código A3”;
- Tipo A4 = “RFB e-Código A4”.

Terceiro “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”.

O campo “Organization Name” (O) com conteúdo fixo igual a “ICP-Brasil”.

O campo “Country Name” (C) com conteúdo fixo igual a “BR”.

No formato os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

Exemplo:

CN=Nome Empresarial:01672780838897
OU= Autoridade de Registro
OU=RFB e-Código A1
OU=Secretaria da Receita Federal do Brasil – RFB
O=ICP-Brasil
C=BR

6.2. Extensões Obrigatórias.

6.2.1. Authority Key Identifier

Não crítica

O campo key Identifier deve conter o hash SHA-1 da chave pública da AC Habilitada que emitiu o certificado.

6.2.2. Key Usage

Crítica

Somente os seguintes bits devem estar ativados;

- "digitalSignature",
- "nonRepudiation"; e
- "keyEncipherment".

6.2.3. Certificate Policies

Não crítica

- o campo "policyIdentifier" contém o OID da PC (Política de Certificação) correspondente;
- o campo "policyQualifiers" contém o endereço URL da página *Web* onde se obtém a DPC (Declaração de Praticas de Certificação) da AC Habilitada que emitiu o certificado.

6.2.4. CRL Distribution Points

Não crítica

Contém os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC Habilitada que assinou o certificado.

Deverão conter três (3) endereços *web* diferentes para busca da LCR.

6.2.5. Subject Alternative Name

Não crítica

Contendo 4 (quatro) campos "otherName" obrigatórios:

OID = 2.16.76.1.3.2 e conteúdo = nome do responsável pelo Certificado.

OID = 2.16.76.1.3.3 e conteúdo = número de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

OID = 2.16.76.1.3.4 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do responsável pela certificado, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o número de inscrição no Cadastro de Pessoas Físicas (CPF) do responsável pelo certificado; nas 11 (onze) posições subseqüentes, o número de inscrição no NIS (PIS, PASEP ou CI) do responsável pelo certificado; nas 15 (quinze) posições subseqüentes, o número do Registro Geral (RG) do responsável pelo certificado; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF

OID = 2.16.76.1.3.8 e conteúdo = nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ) da Pessoa Jurídica titular do certificado.

O conjunto de informações definido em cada campo “OtherName” deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING.

Os seguintes campos são de preenchimento obrigatório;

Da empresa:

- Número de inscrição no CNPJ;
- Nome empresarial da Pessoa Jurídica.

Do responsável pelo certificado:

- Número de inscrição no CPF.
- Data de nascimento.
- Nome do responsável pelo certificado.
- Email do responsável pelo certificado.

Quando os números de NIS(PIS/PASEP ou CI), RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.

Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. Todas informações de tamanho variável, referentes a números, tais como RG, devem ser preenchidas com caracteres “zero” a sua esquerda para que seja completado seu máximo tamanho possível.

As 6 (seis) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita.

Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados nos campos otherName, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

O campo “rfc822 Name”, parte da extensão obrigatória “Subject AlternativeName”, contendo o endereço e-mail do responsável pelo certificado também deverá estar presente

6.2.6. Basic Constraints

Não crítica

Opcional,

- Subject Type= End Entity; e
- Path Length Constraint-None.

6.2.7. Extended-Key-Usage

Não crítica

Deve conter os seguintes valores representados por seus respectivos OID:

Obrigatório

OID	**Propósito**
1.3.6.1.5.5.7.3.3	Assinatura de Código.

6.2.8. Authority Information Access (opcional)

Não crítica

Com os seguintes campos:

- Endereço de acesso ao protocolo de OCSP (*On-line Certificate Status Protocol),* conforme definido na RFC 3280;

- Endereço na *web* onde se obtêm o arquivo p7b com os certificados da cadeia da Autoridade Certificadora, conforme definido na RFC 3280.