



Leiaute
dos
Certificados Digitais
Cert-JUS

Versão 2.1

Perfis e normas para emissão de
Certificados Digitais
na Cadeia de Certificação da
Autoridade Certificadora da Justiça
AC-JUS



1. Apresentação

A **Autoridade Certificadora da Justiça – AC-JUS** integra a Infra-estrutura de Chaves Públicas Brasileira – **ICP-Brasil** e é uma autoridade certificadora de primeiro nível.

Este documento descreve o perfil dos Certificados Digitais, ou seja, o conjunto de campos e extensões requeridos pela AC-JUS dentro de uma estrutura padrão *X.509* e de acordo com a *RFC3280* do *ITU-T*. Aqui são definidas a obrigatoriedade e criticidade dos campos e extensões, e descritas as informações que compõem os certificados emitidos sob a cadeia de certificação da **AC-JUS**, denominados certificados **Cert-JUS**.

As restrições e os requisitos documentais para emissão dos certificados **Cert-JUS**, também estão definidos neste documento.

Os modelos e normas deste documento aplicam-se a todas as Autoridades Certificadoras Subseqüentes à **AC-JUS** as quais deverão adotar as medidas necessárias para seu fiel cumprimento.

As ACs integrantes da cadeia **AC-JUS** utilizam a denominação **AC<espaço>nome_subseqüente-JUS**, e estão autorizadas a emitir apenas os certificados **Cert-JUS** definidos neste documento com o leiaute e denominação correspondente.

Cada leiaute de certificado **Cert-JUS** aqui descrito possui destinação e regras específicas para sua emissão.

2. Requisitos Gerais

Os certificados **Cert-JUS** identificam seus titulares relacionando-os a um determinado órgão público. Cada órgão público que desejar fazer uso de certificados **Cert-JUS** deverá responsabilizar-se pelas informações funcionais e institucionais constantes na **AUTORIZAÇÃO** e no certificado.

- 2.1 - Os certificados **Cert-JUS** destinam-se aos órgãos da administração pública direta e indireta.
- 2.2 - Órgãos **não pertencentes** ao Poder Judiciário deverão solicitar **CADASTRAMENTO** junto à AC-JUS, para a emissão de certificados **Cert-JUS**.
 - 2.2.1 - As Ac subseqüentes somente emitirão certificados para órgãos **não pertencentes** ao Poder Judiciário cujo **CADASTRAMENTO** tenha sido aprovado pela AC-JUS.
 - 2.2.2 - Para emissão de certificados **Cert-JUS** para órgãos do **Poder Judiciário** não é necessário **CADASTRAMENTO** prévio na AC-JUS.
- 2.3 - Para a emissão de qualquer certificado **Cert-JUS** é necessária **AUTORIZAÇÃO** da **autoridade competente** da instituição à qual o certificado está relacionado.
 - 2.3.1 - Para o disposto neste documento, entende-se como **autoridade competente**:
 - a autoridade máxima do órgão;
 - o representante legal do órgão;
 - outra pessoa expressamente designada para esta finalidade, por meio de documento oficial.



- 2.4 - A **AC-JUS** mantém em seu sítio em <http://www.acjus.gov.br> modelos do formulário para o **CADASTRAMENTO** de que trata o item 2.2 e da **AUTORIZAÇÃO** de que trata o item 2.3.
- 2.5 - Os certificados emitidos sob a cadeia **AC-JUS** seguem o padrão definido pela **ICP-Brasil** e obedecem às premissas de conformidade e interoperabilidade estabelecidas nas resoluções e normas da **ICP-Brasil** e da **AC-Raiz**.
- 2.6 - As autoridades certificadoras da cadeia de certificação da **AC-JUS** não estão autorizadas a emitirem certificados que possuam leiaute ou conteúdo diferente do definido neste documento.
 - 2.6.1 - Certificados já emitidos, que se encontrem fora das normas e regras aqui estabelecidas deverão ser imediatamente substituídos.
- 2.7 - Os certificados digitais, na cadeia de certificação da **AC-JUS**, recebem a denominação **Cert-JUS Modelo de Certificado**, onde **Modelo de Certificado** é o nome dado a cada leiaute descrito neste documento.
- 2.8 - A denominação dada por este documento a cada **Modelo de Certificado** deve ser seguida pelas integrantes da cadeia de certificação **AC-JUS**, inclusive em suas páginas de solicitação, revogação, renovação, material informativo, promocional e de divulgação.



3. Leiaute do Certificado **Cert-JUS** Institucional

O certificado **Cert-JUS** Institucional deve, obrigatoriamente, ser do **tipo A3 ou superior**. Deverá ser utilizado dispositivo criptográfico (ex.: token ou smartcard) para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado.

3.1 - Destinação

Os certificados digitais **Cert-JUS Institucional** destinam-se **exclusivamente** aos agentes públicos do **Poder Judiciário**, **autorizados** pela autoridade competente do seu órgão de lotação, a recebê-los.

O certificado **Cert-JUS Institucional** identifica o **titular** do certificado não só como **indivíduo**, mas também como **servidor** do órgão do **Poder Judiciário** em que está lotado.

3.1.1 - Os certificados **Cert-JUS Institucional** deverão ser utilizados nos atos praticados pelos agentes públicos no exercício de suas funções, tais como assinatura de documentos e mensagens de correio eletrônico, autenticação para acesso a sistemas e aplicações, login na rede e acesso remoto seguro .

3.1.2 - Os certificados **Cert-JUS Institucional** devido a sua natureza especial, que vincula o titular do certificado a uma instituição, podem ser revogados a pedido da instituição ou órgão de lotação do titular do certificado.

3.2 - Documentação Obrigatória

Os documentos obrigatórios para emissão de certificados **Cert-JUS Institucional** são:

- i. **AUTORIZAÇÃO** de que tratam o item 2.3;
- ii. Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE;
- iii. CPF e título de eleitor;
- iv. Comprovante de residência;
- v. Foto recente, caso as fotos nos documentos apresentados tenham mais de 3 anos.

3.2.1 - As informações de **lotação, cargo, matrícula e e-mail institucional**, devem, **obrigatoriamente**, constar na **AUTORIZAÇÃO**. A informação do **UPN** é opcional.

3.2.2 - Ao autorizar a emissão de um **Cert-JUS Institucional**, a autoridade competente se responsabilizará pela exatidão das informações fornecidas, bem como pela solicitação de revogação do certificado, em caso de alteração de alguma informação nele contida.

3.3 - Requisitos do Certificado

Os certificados **Cert-JUS** deverão obedecer ao formato definido no padrão internacional *ITU-T X.509* ou *ISO/IEC 9594-8*, devendo atender aos seguintes requisitos:



3.3.1 - Número de Versão

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

3.3.2 - Campo Issuer

Todo certificado **Cert-JUS** deve ter neste campo o nome *X.500* da Autoridade Certificadora que o emitiu.

3.3.3 - UniqueIdentifiers

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 3280*, os campos opcionais *UniqueIdentifiers* **não** devem ser incluídos.

3.3.4 - Algoritmos de Criptografia e tamanho das chaves

O algoritmo utilizado para a geração das chaves dos certificados de **Cert-JUS** deve ser o **RSA**, descrito na *RFC 2313* com *OID= 1.2.840.113549.1.1.1*, com chave assimétrica de no mínimo 1024 (hum mil e vinte e quatro) bits **ou** conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

3.3.5 - Algoritmo de Assinatura Digital e tamanho dos hashes.

Os certificados **Cert-JUS Institucional** deverão ser assinados com uso do algoritmo de assinatura digital **RSA com SHA-1** (*OID= 1.2.840.113549.1.1.5*) **ou** conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

3.3.6 - Chave pública do titular do certificado

Conforme definido na *RFC 3280*.

3.3.7 - Identificação do sistema criptográfico utilizado

Conforme definido na *RFC 3280*.

3.3.8 - Conjunto de caracteres

Salvo o previsto no item 3.4.5, todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Names*), devem obedecer ao Código *NBR9611*, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na *Tabela 1*. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere 'c'.

3.3.9 - Identificação e assinatura digital da Autoridade Certificadora emitente

Conforme definido na *RFC 3280*.

3.3.10 - Número de série exclusivo do certificado

Conforme definido na *RFC 3280*.



3.3.11 - Data, hora, minuto e segundo do início e fim de validade

Conforme definido na *RFC 3280*.

3.3.12 - Composição do DN:

O DN (*Distinguished Name*) do certificado **Cert-JUS Institucional** deve estar no seguinte formato:

C = BR, O=ICP-Brasil,
OU = Autoridade Certificadora da Justica – AC-JUS
OU = Cert-JUS Institucional – A3
OU = <Órgão de Lotação do Titular < - > Sigla do órgão >
OU = <Cargo do Titular>
CN = <Nome do Titular><:><#####>

- i. No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres “<” e “>” não devem ser incluídos.
- ii. Os caracteres “#” representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.
- iii. Os últimos **nove** caracteres do campo CN (*Common Name*) devem ser o nº de matrícula do titular no órgão de lotação, completado com caracteres brancos à direita, caso possua tamanho menor do que 9 caracteres.
- iv. O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
- v. No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite do tamanho do campo disponível, vedada a abreviatura.
- vi. Os dados necessários para preenchimento do DN serão os informados na **AUTORIZAÇÃO**.
- vii. As opções para o campo <Cargo do Titular> será preenchido com uma das seguintes opções:
 - a- MAGISTRADO;
 - b- SERVIDOR;
 - c- PRESTADOR DE SERVIÇO; ou
 - d- ESTAGIÁRIO.
- viii. A **AUTORIZAÇÃO** poderá conter também o UPN na forma usuário@domínio, se for do interesse da instituição.
- ix. Todos os campos do DN são obrigatórios e devem ser preenchidos.
- x. A lista contendo os nomes dos órgãos e respectivas siglas padronizadas está publicada no repositório da AC-JUS.
- xi. Em caso de dúvida sobre a padronização de nomes e siglas de órgãos não constantes da lista citada no item x, a unidade administrativa da AC-JUS deve ser consultada.

Exemplo:

Nome do Servidor ou Magistrado: José da Silva Valença
Matrícula: TR1-123.456 , Órgão de Lotação: CJF , Cargo: Técnico Judiciário



DN:

C = BR, O = ICP-Brasil,
OU = Autoridade Certificadora da Justiça – AC-JUS,
OU = Cert-JUS Institucional – A3
OU = Conselho da Justiça Federal – CJF
OU = Servidor
CN = Jose da Silva Valenca:TR123456

3.4 - Extensões Obrigatórias

3.4.1 - AuthorityKeyIdentifier

Não crítica.

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

3.4.2 - KeyUsage

Crítica.

Para certificados de assinatura, somente os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment* devem estar ativados.

3.4.3 - CertificatePolicies

Não crítica.

- o campo *policyIdentifier* contém o OID da PC correspondente;
- o campo *policyQualifiers* contém o endereço *URL* da página *Web* onde se obtém a DPC da AC que emitiu o certificado.

3.4.4 - CRLDistributionPoints

Não crítica.

Deve conter os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC que emitiu o certificado. O preenchimento deste campo e sua semântica devem obedecer a *RFC 3280*.

3.4.5 - SubjectAlternativeName

Não crítica, com o seguinte formato:

3.4.5.1 - 3 (três) campos *otherName*, **obrigatórios**, contendo:

- OID= 2.16.76.1.3.1 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subseqüentes, o Cadastro de Pessoas Físicas (CPF) do titular; nas 11 (onze) posições subseqüentes, o número de inscrição do titular no PIS/PASEP; nas 15 (quinze) posições subseqüentes, o número do registro Geral (RG) do titular; nas 6 (seis) posições subseqüentes, as siglas do órgão expedidor do RG e respectiva UF.



- ii. **OID= 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado.
- iii. **OID= 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subseqüentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subseqüentes, o município e a UF do Título de Eleitor.

3.4.5.2 - 2(dois) campos *otherName*, **não obrigatórios**, contendo:

- i. **OID= 2.16.76.1.4.n e conteúdo** = de 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 NA ICPBRASIL regulamenta a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.
- ii. **OID= 1.3.6.1.4.1.311.20.2.3 e conteúdo** = User Principal Name (UPN), necessário para login com uso de certificados digitais em redes Microsoft.

3.4.5.3 - Um campo **rfc822Name (OID= 2.5.29.17.1)**, de preenchimento obrigatório, contendo o e-mail institucional do titular do certificado. Este campo deverá estar no formato IA5string.

3.4.5.4 - O conjunto de informações em cada campo **otherName** deve estar de acordo com as seguintes especificações:

- i. Para emissão de certificado **Cert-JUS Institucional o preenchimento dos campos CPF, data de nascimento e Título de Eleitor é obrigatório.**
- ii. 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 *otherName* UPN, cuja cadeia de caracteres é do tipo UTF-8 String. O campo UPN deve estar na forma [usuario@dominio](#).
- iii. Quando os números de PIS/PASEP, CEI ou RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.
- iv. Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. Todas as 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.
- v. 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. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor.
- vi. 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.

3.4.6 - BasicConstraints



Não crítica, opcional, deve conter $cA=False$.

3.4.7 - Extended Key Usage (extendedKeyUsage)

Não crítica.

Deve conter os seguintes valores:

id-kp-clientAuth “client authentication” ($OID=1.3.6.1.5.5.7.3.2$),

id-kp-emailProtection “E-mail protection” ($OID=1.3.6.1.5.5.7.3.4$) e

“SmartCardLogon” ($OID= 1.3.6.1.4.1.311.20.2.2$) .

3.4.8 - Authority Information Access

Caso a Autoridade Certificadora disponibilize serviço de consulta on-line de situação de certificado (*On-line Certificate Status Protocol – OCSP*), esta extensão deve conter o endereço de acesso a esse serviço, conforme definido na *RFC 3280*.

Nesta extensão também poderá estar presente o campo id-ad- caIssuers contendo o protocolo e endereço de obtenção da cadeia de certificação do certificado.

3.4.9 - Outras Extensões

As extensões listadas na *Tabela II* não deverão estar presentes.



4. Leiaute do Certificado **Cert-JUS** Poder Público

O certificado **Cert-JUS Poder Público** para assinatura deve, obrigatoriamente, ser do **tipo A3 ou superior**, isto é, deve ser utilizado dispositivo criptográfico (ex.: token ou smartcard) para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado.

A emissão de certificados **Cert-JUS Poder Público** para determinado órgão só será iniciada após o **CADASTRAMENTO** de que tratam os itens 2.2 e 2.3.

4.1 - Destinação

Os certificados digitais **Cert-JUS Poder Público** destinam-se exclusivamente a agentes públicos, **autorizados** pela autoridade competente do seu órgão de lotação, a recebê-los.

O certificado **Cert-JUS Poder Público** identifica o titular do certificado não só como indivíduo, mas também como servidor do órgão público em que está lotado.

É vedada a emissão do **Cert-JUS Poder Público** para órgãos do Poder Judiciário.

4.1.1 - Os certificados **Cert-JUS Poder Público** deverão ser utilizados, nos atos praticados pelos agentes públicos no exercício de suas funções, tais como assinatura de documentos e mensagens de correio eletrônico, criptografia, autenticação para acesso a sistemas e aplicações, login na rede e acesso remoto seguro.

4.1.2 - Os certificados **Cert-JUS Poder Público** devido a sua natureza especial, que vincula o titular do certificado a uma instituição, podem ser revogados a pedido da instituição ou órgão de lotação do titular do certificado.

4.2 - Documentação Obrigatória

Os documentos obrigatórios para emissão de certificados **Cert-JUS Poder Público** são:

- i. **AUTORIZAÇÃO** de que trata o item 2.3;
- ii. Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE;
- iii. CPF;
- iv. Comprovante de residência;
- v. Foto recente, caso as fotos nos documentos apresentados tenham mais de 3 anos.

4.2.1 - As informações de **lotação, cargo, matrícula e e-mail institucional**, devem, obrigatoriamente, constar na **AUTORIZAÇÃO**. A informação do **UPN** é opcional.

4.2.2 - Ao autorizar a emissão de um **Cert-JUS Poder Público**, a autoridade competente se responsabilizará pela exatidão das informações fornecidas, bem como pela solicitação de revogação do certificado, em caso de alteração de alguma informação nele contida.

4.3 - Requisitos do Certificado



Os certificados **Cert-JUS** deverão obedecer ao formato definido no padrão internacional *ITU-T X.509* ou *ISO/IEC 9594-8*, devendo atender aos seguintes requisitos:

4.3.1 - Número de Versão

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

4.3.2 - Campo Issuer

Todo certificado **Cert-JUS** deve ter neste campo o nome *X.500* da Autoridade Certificadora que o emitiu.

4.3.3 - UniqueIdentifiers

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 3280*, os campos opcionais *UniqueIdentifiers* **não** devem ser incluídos.

4.3.4 - Algoritmos de Criptografia e tamanho das chaves

O algoritmo utilizado para a geração das chaves dos certificados de **Cert-JUS** deve ser o *RSA*, descrito na *RFC 2313* com *OID= 1.2.840.113549.1.1.1*, com chave assimétrica de no mínimo 1024 (hum mil e vinte e quatro) bits ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

4.3.5 - Algoritmo de Assinatura Digital e tamanho dos hashes.

Os certificados **Cert-JUS Poder Público** deverão ser assinados com uso do algoritmo de assinatura digital *RSA com SHA-1 (OID= 1.2.840.113549.1.1.5)* ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

4.3.6 - Chave pública do titular do certificado

Conforme definido na *RFC 3280*.

4.3.7 - Identificação do sistema criptográfico utilizado

Conforme definido na *RFC 3280*.

4.3.8 - Conjunto de caracteres

Salvo o previsto no item 4.4.5, todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Names*), devem obedecer ao Código *NBR9611*, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na *Tabela 1*. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e o cedilha deve ser substituído pelo caractere ‘c’.

4.3.9 - Identificação e assinatura digital da Autoridade Certificadora emitente

Conforme definido na *RFC 3280*.

4.3.10 - Número de série exclusivo do certificado



Conforme definido na *RFC 3280*.

4.3.11 - Data, hora, minuto e segundo do início e fim de validade

Conforme definido na *RFC 3280*.

4.3.12 - Composição do DN:

O DN (*Distinguished Name*) do certificado **Cert-JUS Poder Público** deve estar no seguinte formato:

C = BR, O=ICP-Brasil,

OU = Autoridade Certificadora da Justica – AC-JUS

OU = Cert-JUS Poder Público – A3

OU = <Órgão de Lotação do Titular ><-><Sigla do órgão>

OU = <Cargo do Titular>

CN = <Nome do Titular><:;><#####>

- i. No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres “<” e “>” não devem ser incluídos.
- ii. Os caracteres “#” representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.
- iii. Os últimos nove caracteres do campo CN (*Common Name*) devem ser o nº de matrícula do titular no órgão de lotação, completado com caracteres brancos à direita, caso possua tamanho menor do que 9 caracteres.
- iv. O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
- v. No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite do tamanho do campo disponível, vedada a abreviatura.
- vi. Os dados necessários para preenchimento do DN serão os informados na **AUTORIZAÇÃO**.
- vii. A **AUTORIZAÇÃO** poderá conter também o UPN na forma usuário@domínio, se for do interesse da instituição.
- viii. Todos os campos do DN são obrigatórios e devem ser preenchidos.
- ix. O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.

Exemplo:

Nome do Servidor: Antonio José da Silva

Matrícula: MPDF .12345 , Órgão de Lotação: Minsitério Publico do DF, Cargo: Procurador

DN:

C = BR, O = ICP-Brasil,

OU = Autoridade Certificadora da Justica – AC-JUS,

OU = Cert-JUS Poder Público – A3

OU = Ministerio Publico do DF -MPDF

OU = PROCURADOR



CN = Antonio Jose da Silva:MPDF12345

4.4 - Extensões Obrigatórias

4.4.1 - AuthorityKeyIdentifier

Não crítica.

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

4.4.2 - KeyUsage

Crítica.

Para certificados de assinatura, somente os bits *digitalSignature*, *nonRepudiation* e *keyEncipherment* devem estar ativados.

Para certificados de sigilo, somente os bits *keyEncipherment* e *dataEncipherment* devem estar ativados.

4.4.3 - CertificatePolicies

Não crítica.

- o campo *policyIdentifier* contém o OID da PC correspondente;
- o campo *policyQualifiers* contém os endereços *URL* das páginas *Web* onde se obtém a DPC da AC que emitiu o certificado.

4.4.4 - CRLDistributionPoints

Não crítica.

Deve conter o endereço na *Web* onde se obtém a Lista de Certificados Revogados (LCR) emitida pela AC que emitiu o certificado. O preenchimento deste campo e sua semântica devem obedecer a *RFC 3280*.

4.4.5 - SubjectAlternativeName

Não crítica, com o seguinte formato:

4.4.5.1 - 3 (três) campos *otherName*, **obrigatórios**, contendo:

- OID= 2.16.76.1.3.1 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato *ddmmaaaa*; nas 11 (onze) posições subsequentes, o Cadastro de Pessoas Físicas (CPF) do titular; nas 11 (onze) posições subsequentes, o número de inscrição do titular no PIS/PASEP; nas 15 (quinze) posições subsequentes, o número do registro Geral (RG) do titular; nas 6 (seis) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.
- OID= 2.16.76.1.3.6 e conteúdo** = nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado.
- OID= 2.16.76.1.3.5 e conteúdo** = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.



4.4.5.2 - 2(dois) campos *otherName*, **não obrigatórios**, contendo:

- i. **OID= 2.16.76.1.4.n e conteúdo** = de 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 NA ICP BRASIL regulamenta a correspondência de cada conselho de classe ou órgão competente ao conjunto de OID acima definido.
- ii. **OID= 1.3.6.1.4.1.311.20.2.3 e conteúdo** = User Principal Name (UPN), necessário para login com uso de certificados digitais em redes Microsoft.

4.4.5.3 - Um campo **rfc822Name (OID= 2.5.29.17.1)**, de preenchimento obrigatório, contendo o e-mail institucional do titular do certificado. Este campo deverá estar no formato IA5string.

4.4.5.4 - O conjunto de informações em cada campo *otherName* deve estar de acordo com as seguintes especificações:

- i. Para emissão de certificado **Cert-JUS Poder Público** o preenchimento dos campos CPF e data de nascimento é obrigatório.
- ii. 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 *otherName* UPN, cuja cadeia de caracteres é do tipo UTF-8 String. O campo UPN deve estar na forma *usuario@dominio*.
- iii. Quando os números de Título de Eleitor, PIS/PASEP, CEI ou RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.
- iv. Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF. Todas as 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.
- v. 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. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor.
- vi. Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados nos campos *otherName*, excetuando-se o UPN, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

4.4.6 - BasicConstraints

Não crítica, opcional, deve conter *cA=False*.

4.4.7 - Extended Key Usage (extendedKeyUsage)

Não crítica.

Deve conter os seguintes valores:

id-kp-clientAuth “client authentication” (*OID=1.3.6.1.5.5.7.3.2*),

id-kp-emailProtection “E-mail protection” (*OID=1.3.6.1.5.5.7.3.4*) e



“SmartCardLogon” (*OID= 1.3.6.1.4.1.311.20.2.2*).

4.4.8 - Authority Information Access

Caso a Autoridade Certificadora disponibilize serviço de consulta on-line de situação de certificado (*On-line Certificate Status Protocol – OCSP*), esta extensão deve conter o endereço de acesso a esse serviço, conforme definido na *RFC 3280*.

Nesta extensão também poderá estar presente o campo *id-ad-caIssuers* contendo o protocolo e endereço de obtenção da cadeia de certificação do certificado.

4.4.9 - Outras Extensões

As extensões listadas na *Tabela II* não deverão estar presentes.



5. Leiaute do Certificado **Cert-JUS** Equipamento Servidor

5.1 - Destinação

Os certificados digitais **Cert-JUS** Equipamento Servidor destinam-se **exclusivamente** para utilização em equipamentos que disponibilizem serviços ou informações do poder público, tais como web segura, SSH, e outros serviços que requeiram certificados digitais para autenticação de servidor.

Destina-se também a equipamentos que ofereçam serviços como **Carimbo de Tempo (timestamping), OCSP, ou outras aprovadas pela ICP-Brasil.**

O certificado **Cert-JUS** Equipamento Servidor poderá ser do tipo A1.

- 5.1.1 - A emissão de Certificados **Cert-JUS** Equipamento Servidor deve ser previamente autorizada pela autoridade competente.
- 5.1.2 - Os certificados **Cert-JUS** Equipamento Servidor devem ser utilizados somente em equipamentos servidores pertencentes a órgão do **Poder Judiciário, órgãos da administração pública direta e indireta** ou a empresas privadas que prestem serviços a órgãos públicos.
- 5.1.3 - O titular do **Cert-JUS** Equipamento Servidor será sempre um órgão público e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público, indicado e autorizado pela autoridade competente.
- 5.1.4 - A emissão de certificados **Cert-JUS** Equipamento Servidor para determinado órgão só será iniciado após o **CADASTRAMENTO** de que tratam os itens 2.2 e 2.3.

5.2 - Documentação Obrigatória

Os documentos obrigatórios para emissão de certificados **Cert-JUS** Equipamento Servidor são:

- i. **AUTORIZAÇÃO** de que trata o item 2.3.
 - ii. Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE da autoridade competente do órgão solicitante e do responsável pelo certificado.
 - iii. CPF da autoridade competente do órgão solicitante e do responsável pelo certificado.
 - iv. Comprovante de residência da autoridade competente do órgão solicitante e do responsável pelo certificado.
 - v. Comprovação de habilitação Jurídica e Fiscal do órgão solicitante, conforme as regras da ICP-Brasil.
 - vi. Comprovação de registro do domínio pela instituição solicitante.
- 5.2.1 - A **AUTORIZAÇÃO** deve designar o responsável pelo uso do certificado e informar: nome do órgão constante do CNPJ, número do CNPJ, unidade responsável, e-mail institucional e URL ou nome da aplicação, que constarão no certificado, bem como



nome, data de nascimento e CPF da autoridade competente e do responsável pelo certificado.

5.2.2 - Ao autorizar a emissão de um **Cert-JUS Equipamento Servidor**, a autoridade competente assume a responsabilidade pela exatidão das informações fornecidas .

5.3 - Requisitos do Certificado

Os certificados **Cert-JUS Equipamento Servidor** deverão obedecer ao formato definido no padrão internacional *ITU-T X.509* ou *ISO/IEC 9594-8*, devendo também atender aos seguintes requisitos:

5.3.1 - Número de Versão

Os certificados digitais **Cert-JUS** deverão implementar 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 X.509 Public Key Infrastructure)*.

5.3.2 - Campo Issuer

Todo certificado **Cert-JUS** deve ter neste campo o nome X.500 da Autoridade Certificadora que o emitiu.

5.3.3 - UniqueIdentifiers

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 3280*, os campos opcionais *UniqueIdentifiers* **não** devem ser incluídos.

5.3.4 - Algoritmos de Criptografia e tamanho das chaves

O algoritmo utilizado para a geração das chaves dos certificados **Cert-JUS Equipamento Servidor** deve ser o **RSA**, descrito na *RFC 2313* com *OID= 1.2.840.113549.1.1.1*, com chave assimétrica de no mínimo 1024 (hum mil e vinte e quatro) bits ou conforme definido no documento PADRÕES E ALGORÍTMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

5.3.5 - Algoritmo de Assinatura Digital e tamanho dos *hashes*.

Os certificados de **Cert-JUS Equipamento Servidor** deverão ser assinados com uso do algoritmo de assinatura digital **RSA com SHA-1** (*OID= 1.2.840.113549.1.1.5*) ou conforme definido no documento PADRÕES E ALGORÍTMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

5.3.6 - Chave pública do titular do certificado

Conforme definido na *RFC 3280*.

5.3.7 - Identificação do sistema criptográfico utilizado

Conforme definido na *RFC 3280*



5.3.8 - Conjunto de caracteres

Salvo o previsto no item 5.4.5, todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Names*), devem obedecer ao Código *NBR9611*, que inclui os caracteres alfanuméricos e os caracteres especiais, descritos na *Tabela 1*. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e a cedilha deve ser substituída pelo caractere 'c'.

5.3.9 - Identificação e assinatura digital da Autoridade Certificadora emitente

Conforme definido na *RFC 3280*.

5.3.10 - Número de série exclusivo do certificado

Conforme definido na *RFC 3280*.

5.3.11 - Data, hora, minuto e segundo do início e fim de validade

Conforme definido na *RFC 3280*.

5.3.12 - Composição do DN:

O DN (*Distinguished Name*) do certificado **Cert-JUS Equipamento Servidor** deve estar no formato:

C=BR, O=ICP-Brasil,

OU=Autoridade Certificadora da Justica – AC-JUS

OU=Cert-JUS Equipamento Servidor – <Tipo de Certificado>

OU=<Órgão a que pertence><-><Sigla>

OU=<nome da Unidade Organizacional responsável pelo equipamento>

CN=<nome DNS (*Domain Name Service*) do equipamento ou nome da aplicação>

- i. No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os “<<” e “>>” não devem ser incluídos.
- ii. O CN (*Common Name*) deve conter a URL correspondente ao equipamento servidor, ou o nome da aplicação ou serviço, a que esse certificado se refere.
- iii. Os dados necessários para preenchimento do DN deverão ser obtidos na **AUTORIZAÇÃO** de emissão do certificado, citada no item 5.2 e 5.2.1.
- iv. O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
- v. Todos os campos do DN são obrigatórios e devem ser preenchidos.
- vi. Para servidores do Poder Judiciário, a lista contendo os nomes dos órgãos e respectivas siglas padronizadas está publicada no repositório da AC-JUS.
- vii. Em caso de dúvida sobre a padronização de nomes e siglas de órgãos não constantes da lista citada no item x, a unidade administrativa da AC-JUS deve ser consultada.
- viii. Para servidores que não sejam do Poder Judiciário o nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.

Exemplo :



URL do Equipamento: www.cjf.gov.br

Órgão onde está instalado: Conselho da Justiça Federal

Unidade organizacional responsável: Divisão de Operação e Serviços de Rede

DN:

C=BR, O=ICP-Brasil,

OU= Autoridade Certificadora da Justica – AC-JUS,

OU=Cert-JUS Equipamento Servidor – A1

OU=Conselho da Justica Federal – CJF

OU=Divisao de Operacao e Servicos de Rede

CN=www.cjf.jus.br

5.4 - Extensões Obrigatórias

5.4.1 - AuthorityKeyIdentifier

Não crítica.

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

5.4.2 - KeyUsage

Crítica.

Os bits *digitalSignature* e *keyEncipherment* devem estar ativados.
O bit *nonRepudiation* é opcional

5.4.3 - CertificatePolicies

Não crítica:

- o campo *policyIdentifier* contém o OID da PC correspondente;
- o campo *policyQualifiers* contém o endereço URL da página *Web* onde se obtém a DPC da AC que emitiu o certificado.

5.4.4 - CRLDistributionPoints

Não crítica:

Deve conter os endereços na *Web* onde se obtém a LCR emitida pela AC que emitiu o certificado. O preenchimento deste campo e sua semântica devem obedecer a *RFC 3280*.

5.4.5 - SubjectAlternativeName

Não crítica com o seguinte formato:

5.4.5.1 - 4 (quatro) campos *otherName*, **obrigatórios**, contendo, na seguinte ordem :

- i. **OID= 2.16.76.1.3.8 e conteúdo** = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica) do órgão ou instituição, sem abreviações.;



- ii. **OID= 2.16.76.1.3.3 e conteúdo** = Numero do CNPJ;
- iii. **OID= 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;
- iv. **OID= 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoas Físicas (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Identificação Social-NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do registro Geral (RG) do responsável; nas 6 (seis) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

5.4.5.2 - Um campo **rfc822Name (OID= 2.5.29.17.1)**, de preenchimento obrigatório, contendo o e-mail institucional do responsável pelo certificado. Este campo deverá estar no formato IA5string.

5.4.5.3 - Os campos **otherName** devem estar de acordo com as seguintes especificações:

- i. O preenchimento dos campos: *nome empresarial constante do CNPJ, número do CNPJ, nome, CPF e data de nascimento do responsável pelo certificado*, é **obrigatório**.
- ii. O preenchimento do campo **rfc822Name**, contendo o e-mail institucional do responsável pelo certificado é **obrigatório**. Pode ser utilizado o e-mail da unidade organizacional responsável pelo certificado.
- iii. O conjunto de informações definido em cada campo **otherName** deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 **OCTET STRING**.
- iv. Quando os números de PIS/PASEP,CEI ou RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”.
- v. 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.
- vi. 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.
- vii. 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.

5.4.6 - BasicConstraints

Não crítica, opcional, deve conter **cA=False**.

5.4.7 - ExtKeyUsage

Não crítica.

Deve conter o seguinte valor: **id-kp-serverAuth**, **OID= 1.3.6.1.5.5.7.3.1**, para uso na



autenticação de equipamento servidor.

O campo *id-kp-clientAuth*, **OID= 1.3.6.1.5.5.7.3.2**, para uso na autenticação de cliente é **opcional**.

Em se tratando de certificado para **aplicação de carimbo de tempo**, deve conter o valor *id-kp-serverAuth*, acompanhado de ***id-kp-timestamping*, **OID= 1.3.6.1.5.5.7.3.8****.

Em se tratando de certificado para **assinatura de serviço OCSP**, deve conter o valor *id-kp-serverAuth* acompanhado de ***id-kp-OCSPSigning*, **OID= 1.3.6.1.5.5.7.3.9****.

Poderá ser utilizado outro identificador de objeto que tenha sido aprovado pela ICP-Brasil, desde que a **AC-JUS** autorize a utilização em sua cadeia de certificação.

5.4.8 - Authority Information Access

Caso a Autoridade Certificadora disponibilize serviço de consulta on-line de situação de certificado (*On-line Certificate Status Protocol – OCSP*), esta extensão deve conter endereço de acesso a esse serviço, conforme definido na *RFC 3280*.

Nesta extensão também poderá estar presente o campo *id-ad-caIssuers* contendo o protocolo e endereço de obtenção da cadeia de certificação do certificado.

5.4.9 - Outras Extensões

As extensões listadas na *Tabela II* não deverão estar presentes.



6. Leiaute do Certificado **Cert-JUS** Código Seguro

O certificado digital **Cert-JUS** Código Seguro pode ser do tipo A1 ou A3.

6.1 - Destinação

- 6.1.1 - O certificado **Cert-JUS** Código Seguro destina-se, exclusivamente, para assinatura de código de software, desenvolvido, disponibilizado ou contratado por órgão do **Poder Judiciário e órgãos da administração pública direta e indireta**,
- 6.1.2 - O **Cert-JUS** Código Seguro deverá ser emitido sempre para PESSOA JURÍDICA. O responsável pelo certificado deverá ser indicado pela autoridade competente, na **AUTORIZAÇÃO** para emissão do certificado.
- 6.1.3 - O titular do **Cert-JUS** Código Seguro será sempre um órgão do **Poder Judiciário ou órgão da administração pública direta e indireta** e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público, indicado e autorizado pela autoridade competente.

6.2 - Documentação Obrigatória

Os documentos obrigatórios para emissão de certificados **Cert-JUS** Código Seguro são:

- i. **AUTORIZAÇÃO** de que trata o item 2.3.
 - ii. Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE da autoridade competente do órgão solicitante e do responsável pelo certificado.
 - iii. CPF da autoridade competente do órgão solicitante e do responsável pelo certificado.
 - iv. Comprovante de residência da autoridade competente do órgão solicitante e do responsável pelo certificado.
 - v. Comprovação de habilitação Jurídica e Fiscal do órgão solicitante.
- 6.2.1 - A **AUTORIZAÇÃO** deve designar o responsável pelo uso do certificado e informar: nome do órgão constante do CNPJ, número do CNPJ, unidade responsável, e-mail institucional do responsável pelo certificado ou de sua unidade; nome, data de nascimento e CPF da autoridade competente e do responsável pelo certificado.

6.3 - Requisitos de Certificado

Os certificados **Cert-JUS** Código Seguro deverão obedecer ao formato definido no padrão internacional *ITU-T X.509* ou *ISO/IEC 9594-8*, devendo também atender aos seguintes requisitos:

6.3.1 - Número de Versão

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

6.3.2 - Campo Issuer



Todo certificado **Cert-JUS** deve ter neste campo o nome X.500 da Autoridade Certificadora que o emitiu.

6.3.3 - UniqueIdentifiers

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 3280*, os campos opcionais *UniqueIdentifiers* **não** devem ser incluídos.

6.3.4 - Algoritmos de Criptografia e tamanho das chaves

O algoritmo utilizado para a geração das chaves dos certificados **Cert-JUS Código Seguro** deve ser o **RSA**, descrito na *RFC 2313* com *OID= 1.2.840.113549.1.1.1*, com chave assimétrica de no mínimo 1024 (hum mil e vinte e quatro) bits ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

6.3.5 - Algoritmo de Assinatura Digital e tamanho dos hashes

Os certificados **Cert-JUS Código Seguro** deverão ser assinados com uso do algoritmo de assinatura digital **RSA com SHA-1** (*OID= 1.2.840.113549.1.1.5*) ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

6.3.6 - Chave pública do titular do certificado

Conforme definido na *RFC 3280*.

6.3.7 - Identificação do sistema criptográfico utilizado

Conforme definido na *RFC 3280*.

6.3.8 - Conjunto de caracteres

Salvo o previsto no item 6.4.5, todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Names*), devem obedecer ao Código *NBR9611*, que inclui os caracteres alfanuméricos e os caracteres especiais descritos na *Tabela I*. Os acentos não são suportados e devem ser substituídos pelo caractere não acentuado e a cedilha deve ser substituída pelo caractere 'c'.

6.3.9 - Identificação e assinatura digital da Autoridade Certificadora emitente

Conforme definido na *RFC 3280*.

6.3.10 - Número de série exclusivo do certificado

Conforme definido na *RFC 3280*.

6.3.11 - Data, hora, minuto e segundo do início e fim de validade

Conforme definido na *RFC 3280*.

6.3.12 - Composição do DN

O DN (*Distinguished Name*) do certificado **Cert-JUS Código Seguro** deve estar no formato:



C = BR, O = ICP-Brasil,

OU = Autoridade Certificadora da Justiça – AC-JUS

OU = Cert-JUS Código Seguro – <Tipo de Certificado>

OU = <nome da Unidade Organizacional responsável >

CN = <nome do órgão constante do CNPJ>

- i. No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os “<” e “>” não devem ser incluídos.
- ii. O CN (*Common Name*) deve conter a nome do órgão constante do CNPJ.
- iii. Os dados necessários para preenchimento do DN deverão ser obtidos na **AUTORIZAÇÃO** para emissão do certificado, citada no item 6.2, letra “a” e 6.2.1.
- iv. O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
- v. Todos os campos do DN são obrigatórios e devem ser preenchidos. Para titulares do Poder Judiciário, a lista contendo os nomes dos órgãos e respectivas siglas padronizadas está publicada no repositório da AC-JUS.
- vi. Em caso de dúvida sobre a padronização de nomes e siglas de órgãos não constantes da lista citada no item x, a unidade administrativa da AC-JUS deve ser consultada.

Exemplo :

Unidade Organizacional Responsável: DESIN – Secretaria de Desenvolvimento de Sistemas Internos

Nome do órgão constante do CNPJ: CONSELHO DA JUSTIÇA FEDERAL

DN:

C=BR, O=ICP-Brasil,

OU= Autoridade Certificadora da Justiça – AC-JUS,

OU=Cert-JUS Código Seguro – A1

OU=DESIN - Secretaria de Desenvolvimento de Sistemas

CN=CONSELHO DA JUSTICA FEDERAL

6.4 - Extensões Obrigatórias

6.4.1 - AuthorityKeyIdentifier

Não crítica.

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

6.4.2 - KeyUsage

Crítica.

Somente os bits *digitalSignature* e *nonRepudiation* devem estar ativados.

6.4.3 - CertificatePolicies

Não crítica.



- o campo *policyIdentifier* contém o OID da PC correspondente;
- o campo *policyQualifiers* contém os endereços URL das páginas *Web* onde se obtém a DPC da AC que emitiu o certificado.

6.4.4 - CRLDistributionPoints

Não crítica.

Deve conter o endereço na *Web* onde se obtém a LCR emitida pela AC que emitiu o certificado. O preenchimento deste campo e sua semântica devem obedecer a RFC 3280.

6.4.5 - SubjectAlternativeName

Não crítica com o seguinte formato:

6.4.5.1 - 4 (quatro) campos *otherName* **obrigatórios**, contendo, na seguinte ordem :

- OID= 2.16.76.1.3.8 e conteúdo** = nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica).;
- OID= 2.16.76.1.3.3 e conteúdo** = Número do CNPJ;
- OID= 2.16.76.1.3.2 e conteúdo** = nome do responsável pelo certificado;
- OID= 2.16.76.1.3.4 e conteúdo** = nas primeiras 8 (oito) posições, a data de nascimento do responsável, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoas Físicas (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Identificação Social -NIS (PIS,PASP ou CI); nas 15 (quinze) posições subsequentes, o número do registro Geral (RG) do responsável; nas 6 (seis) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

6.4.5.2 - Um campo *rfc822Name* (**OID= 2.5.29.17.1**), obrigatório, contendo o e-mail institucional do responsável pelo certificado. Este campo deverá estar no formato *IA5string*.

6.4.5.3 - Os campos *otherName* devem estar de acordo com as seguintes especificações:

- O preenchimento dos campos: nome empresarial constante do CNPJ , número do CNPJ, nome, CPF e data de nascimento do responsável pelo certificado, é **obrigatório**.
- O preenchimento do campo *rfc822Name*, contendo o e-mail institucional do responsável pelo certificado é **obrigatório**. Poderá ser utilizado o e-mail da unidade organizacional responsável pelo certificado.
- O conjunto de informações definido em cada campo *otherName* deve ser armazenado como uma cadeia de caracteres do tipo *ASN.1 OCTET STRING*.
- Quando os números de PIS/PASEP,CEI ou 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.

- vi. 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.
- vii. 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.

6.4.6 - BasicConstraints

Não crítica, opcional, deve conter *cA=False*.

6.4.7 - ExtKeyUsage

Não crítica.

Deve conter o seguinte valor: *id-kp-codeSigning*, *OID= 1.3.6.1.5.5.7.3.3*, para uso em assinatura de código.

6.4.8 - Authority Information Access

Caso a Autoridade Certificadora disponibilize serviço de consulta on-line de situação de certificado (*On-line Certificate Status Protocol – OCSP*), esta extensão deve conter o endereço de acesso a esse serviço, conforme definido na RFC 3280.

Nesta extensão também poderá estar presente o campo *id-ad-caIssuers* contendo o protocolo e endereço de obtenção da cadeia de certificação do certificado.

6.4.9 - Outras Extensões

As extensões listadas na *Tabela II* não deverão estar presentes.



7. Leiaute do Certificado das Autoridades Certificadoras Subseqüentes à AC-JUS

7.1 - Requisitos de Certificado

Os certificados emitidos para as Autoridades Certificadoras Subseqüentes obedecem ao formato definido no padrão internacional *ITU-T X.509* ou *ISO/IEC 9594-8* e implementam a versão 3 de certificado de acordo com o perfil estabelecido na *RFC 3280 (Request for Comments – Internet X.509 Public Key Infrastructure)*. Os certificados das AC subseqüentes deverão atender aos seguintes requisitos:

7.1.1 - Campo issuer

Os certificados emitidos para as Ac subseqüentes têm neste campo o nome *X.500* da **Autoridade Certificadora da Justiça – AC-JUS**.

7.1.2 - Número de Versão

Os certificados das Ac subseqüentes implementam a versão 3 do padrão *ITU-T X.509*, de acordo com o perfil estabelecido na *RFC 3280*.

7.1.3 - UniqueIdentifiers

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 3280*, os campos opcionais UniqueIdentifiers **não** devem ser incluídos.

7.1.4 - Algoritmos de Criptografia e tamanho das chaves

O Algoritmo utilizado para geração do par de chaves dos certificados emitidos para as Ac subseqüentes, será o **RSA**, descrito na *RFC 2313* com *OID= 1.2.840.113549.1.1.1* conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL e a chave assimétrica dos certificados emitidos para as Ac subseqüentes terá no mínimo 2048 bits.

7.1.5 - Algoritmo de Assinatura Digital e tamanho dos hashes

Os certificados emitidos para as Ac subseqüentes serão assinados com o uso do algoritmo **RSA com SHA-1** (*OID= 1.2.840.113549.1.1.5*), conforme o padrão *PKCS#1 (RFC 2313)* ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

7.1.6 - Conjunto de caracteres

Todas as seqüências de caracteres nos certificados, inclusive as dos DN (*Distinguished Names*), devem obedecer ao Código *NBR9611*, 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 a cedilha deve ser substituída pelo caractere 'c'.

7.1.7 - Chave pública da Autoridade Certificadora Subseqüente titular do certificado

Conforme definido na *RFC 3280*.

7.1.8 - Identificação do sistema criptográfico utilizado



Conforme definido na *RFC 3280*.

7.1.9 - Identificação e assinatura digital da AC-JUS

Conforme definido na *RFC 3280*.

7.1.10 - Número de série exclusivo do certificado

Conforme definido na *RFC 3280*.

7.1.11 - Data, hora, minuto e segundo do início e fim de validade

Conforme definido na *RFC 3280*.

7.1.12 - Composição do DN:

O DN (*Distinguished Name*) da Autoridade Certificadora Subseqüente estará no formato:

C=BR

O=ICP-Brasil,

OU=Autoridade Certificadora da Justiça – AC-JUS,

CN=AC <Nome da Autoridade Certificadora Subseqüente><->JUS

- i. No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os “<” e “>” não devem ser incluídos.
- ii. O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
- iii. O CN deve ser preenchido com o nome empresarial da Autoridade Certificadora Subseqüente, com comprimento máximo de 64 caracteres.
- iv. O CN deverá ser composto da seguinte forma:
AC <nomedaACSubseqüente>-JUS.
A expressão “AC” seguida de um espaço, o nome da AC, seguido de um hífen e a expressão JUS.
- v. O traço (hífen) antes da expressão JUS é obrigatório. Exemplo: AC EXEMPLO-JUS

Exemplo de DN:

C=BR, O=ICP-Brasil,
OU=Autoridade Certificadora da Justiça – AC-JUS,
CN=AC <subsequente>-JUS

7.2 - Extensões Obrigatórias

7.2.1 - AuthorityKeyIdentifier



Não crítica:

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

7.2.2 - SubjectKeyIdentifier

Não crítica:

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

7.2.3 - KeyUsage

Crítica.

Somente os bits *keyCertSign* e *cRLSign* devem estar ativados. Os demais devem estar desativados.

7.2.4 - CertificatePolicies

Não crítica.

- o campo *policyIdentifier* contém o OID das PC que a AC titular do certificado implementa ;
- o campo *policyQualifiers* contém o endereço URL da página *Web*: <http://www.acjus.gov.br/acjus/>, onde se obtém a DPC da AC-JUS.

7.2.5 - CRLDistributionPoints

Não crítica.

Deve conter os endereços na *Web* onde se obtém a LCR gerada e publicada pela AC-JUS. O preenchimento deste campo e sua semântica devem obedecer a *RFC 3280*.

7.2.6 - BasicConstraints

Crítica: deve conter *cA=True*.

7.2.7 - Outras Extensões

As extensões listadas na *Tabela II* não deverão estar presentes.



LISTA DE ACRÔNIMOS

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM-SEI	<i>Capability Maturity Model do Software Engineering Institute</i>
CMVP	<i>Cryptographic Module Validation Program</i>
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas -
COBIT	<i>Control Objectives for Information and related Technology</i>
COSO	<i>Comitee of Sponsoring Organizations</i>
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IDS	Sistemas de Detecção de Intrusão
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>On-line Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	<i>Proof of Possession</i>
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SNMP	<i>Simple Network Management Protocol</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Location</i>



ANEXO I

Tabela I

branco	20	‘	27	.	2E
!	21	(28	/	2F
“	22)	29	:	3A
#	23	*	2A	;	3B
\$	24	+	2B	=	3D
%	25	,	2C	?	3F
&	26	-	2D	@	40
				\	5C

Tabela II

<i>Nome</i>	<i>OID</i>
Private Key Usage Period	2.5.29.16
Policy Mappings	2.5.29.33
Name Constraints	2.5.29.30
Policy Constraints	2.5.29.36
Issuer Alternative Name	2.5.29.18
Subject Alternative Attributes	2.5.29.9
Inhibit Any-Policy	2.5.39.54



Anexo II

Resumo de requisitos e leiaute

Cert-JUS Institucional - TIPO A3 (emissão somente do tipo A3)	
Público Alvo	Servidores e Autoridades do Poder Judiciário
Documentos Obrigatórios	1. Autorização da Autoridade Competente 2. Identidade, Passaporte ou CNE 3. CPF 4. Título de eleitor, 5. Foto, 6. Informação de cargo, matrícula e lotação, e-mail institucional 7. Comprovante de residência
DN (obs . As opções de cargo definidas pela COTEC são APENAS : Magistrado, Servidor, Prestador de Serviço, Estagiário)	C = BR, O=ICP-Brasil, OU = Autoridade Certificadora da Justiça – AC-JUS, OU = Cert-JUS Institucional – A3 OU = <Órgão de Lotação do Titular > <-> <Sigla> OU = <Cargo do Titular> CN = <Nome do Titular><:><#####> As informações de órgão , cargo, lotação, nome e matrícula(#) são obrigatórios
Subject Alternative Name Dados obrigatórios: Dt Nascimento, CPF, título de eleitor, rfc822Name	OID's: 2.16.76.1.3.1 -> *Data Nascimento(8), *CPF(11), NIS(11), RG (15), órgão e UF (6) 2.16.76.1.3.6 -> INSS (12) 2.16.76.1.3.5 -> *Título de eleitor(12), *Zona Eleitoral (3), *Seção (4), 2.5.29.17.1 -> *rfc822Name - e-mail institucional 1.3.6.1.4.1.311.20.2.3 -> UPN – usuario@dominio-login na rede (opcional) Os campos marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO . Todos os campos, exceto o UPN, são obrigatórios, isto é, devem existir no certificado.
Uso (KeyUsage)	<i>digitalSignature (assinatura digital)</i> <i>nonRepudiation (não repúdio) e</i> <i>keyEncipherment (cifragem de chave)</i>
Uso estendido (extendedKeyUsage)	<i>“client authentication” (autenticação de cliente) (OID 1.3.6.1.5.5.7.3.2)</i> <i>“E-mail protection” (proteção de e-mail) (OID 1.3.6.1.5.5.7.3.4) e</i> <i>“SmartCardLogon” (logon com smartcard rede MS) (OID 1.3.6.1.4.1.311.20.2.2)</i>
Dados que devem constar na “Autorização de Emissão”	<i>Nome do titular, Lotação, cargo, matrícula, Nome de login na rede na forma (UPN) <u>usuario@dominio</u>, e-mail institucional</i>

Cert-JUS Poder Público - TIPO A3 (emissão somente do tipo A3) – Obrigatório cadastramento de cada órgão solicitante	
Público Alvo	Servidores e Autoridades do Poder Publico
Documentos Obrigatórios	1. Autorização da Autoridade Competente 2. Identidade, Passaporte ou CNE 3. CPF



Cert-JUS Poder Público - TIPO A3 (emissão somente do tipo A3) – Obrigatório cadastramento de cada órgão solicitante	
	4. Foto, 5. Informação de cargo, matrícula e lotação, e-mail institucional 6. Comprovante de residência
DN	C = BR, O=ICP-Brasil, OU = Autoridade Certificadora da Justiça – AC-JUS, OU = Cert-JUS Institucional – A3 OU = <Órgão de Lotação do Titular ><-><Sigla> OU = <Cargo do Titular> CN = <Nome do Titular><:><#####> As informações de órgão , cargo, lotação, nome e matrícula(#) são obrigatórios
Subject Alternative Name Dados obrigatórios: Dt Nascimento, CPF, rfc822Name	OID's: 2.16.76.1.3.1 -> *Data Nascimento(8), *CPF(11), NIS(11), RG (15), órgão e UF (6) 2.16.76.1.3.6 -> INSS (12) 2.16.76.1.3.5 -> Titulo de eleitor(12), Zona Eleitoral (3), Seção (4), 2.5.29.17.1 -> *rfc822Name - e-mail institucional 1.3.6.1.4.1.311.20.2.3 -> UPN – usuario@dominio-login na rede (opcional) Os campos marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO . Todos os campos, exceto o UPN, são obrigatórios, isto é, devem existir no certificado.
Uso (KeyUsage)	<i>digitalSignature (assinatura digital)</i> <i>nonRepudiation (não repúdio) e</i> <i>keyEncipherment (cifragem de chave)</i>
Uso estendido (extendedKeyUsage)	<i>“client authentication” (autenticação de cliente) (OID 1.3.6.1.5.5.7.3.2)</i> <i>“E-mail protection” (proteção de e-mail) (OID 1.3.6.1.5.5.7.3.4) e</i> <i>“SmartCardLogon” (logon com smartcard rede MS) (OID 1.3.6.1.4.1.311.20.2.2)</i>
Dados que devem constar na “Autorização de Emissão”	<i>Nome do titular, Lotação, cargo, matrícula, Nome de login na rede na forma (UPN) usuario@dominio, e-mail institucional</i>



Cert-JUS Equipamento Servidor TIPO A1 Certificado p/ Equipamento - Pessoa Jurídica –	
Publico Alvo	Equipamentos servidores de aplicação de órgãos públicos
Documentos Obrigatórios	Identificação da Instituição: Ato Constitutivo e CNPJ ou CEI Identificação da autoridade competente e do responsável pelo certificado: Documentos para identificação: 1. Autorização e indicação do responsável pela Autoridade Competente 2. ID (Passaporte, CNE), 3. CPF 4. Foto, 5. Informação de cargo, matrícula, lotação e e-mail institucional 6. Comprovante de residência
DN _____ Dados Obrigatórios: Órgão, Unidade Organizacional, Url do servidor	C=BR, O=ICP-Brasil, OU=Autoridade Certificadora da Justiça – AC-JUS OU=Cert-JUS Equipamento Servidor – A1 OU=<Órgão a que pertence><->Sigla> OU=<nome da Unidade Organizacional responsável pelo equipamento> CN=<URL, nome DNS (<i>Domain Name Service</i>) oficial do equipamento> <i>As informações de órgão , unidade organizacional e URL do equipamento são obrigatórias</i>
subjectAlternativeName _____ Dados Obrigatórios: Nome empresarial, CNPJ, Nome do Responsável, dt nasc. responsável, CPF responsável, rfc822Name	OID's: 2.16.76.1.3.8 -> * Nome empresarial 2.16.76.1.3.3 -> *CNPJ, 2.16.76.1.3.2 -> *Nome do responsável 2.16.76.1.3.4 -> *data de nascimento do responsável(8), *CPF(11), NIS(11), RG(15), emitente e UF(6). e ainda, 2.5.29.17.1 -> *rfc822Name - e-mail institucional do responsável (pode ser utilizada e-mail departamental) Todos os campos do subject alternative name marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO
USO (KeyUsage)	<i>digitalSignature (assinatura digital), keyEncipherment (cifragem de chave) , nonRepudiation (opcional)</i>
Uso Estendido (extendedKeyUsage)	<i>id-kp-serverAuth, OID = 1.3.6.1.5.5.7.3.1 - autenticação de equipamento servidor, acompanhado de id-kp-timestamping, OID= 1.3.6.1.5.5.7.3.8, para aplicação de carimbo de tempo,</i> <i>ou</i> <i>id-kp-OCSPSigning, OID= 1.3.6.1.5.5.7.3.9 para assinatura de serviço OCSP</i> <i>“id-kp-clientAuth” OID= 1.3.6.1.5.5.7.3.2 autenticação de cliente</i> <i>(opcional)</i>
Dados que devem constar na “Autorização de Emissão”	URL(nome DNS), Órgão, Unidade responsável, Dados Pessoa Jurídica, Dados Responsável, Dados Representante Legal, e-mail institucional



Cert-JUS Código Seguro – Tipo A1 ou A3 Certificado Pessoa Jurídica para assinatura de código executável.	
Publico Alvo	Código executável para download e execução
Documentos	Identificação da Instituição: Ato Constitutivo e CNPJ ou CEI Identificação de representante legal e responsável, documentos para identificação: <ol style="list-style-type: none"> 1. Autorização e indicação do responsável pela Autoridade Competente 2. ID (Passaporte, CNE), 3. CPF 4. Título de eleitor, 5. Foto, 6. Comprovante de residência
DN	C = BR, O = ICP-Brasil, OU = Autoridade Certificadora da Justiça – AC-JUS OU = Cert-JUS Código Seguro – A3 OU = <nome da Unidade Organizacional responsável > CN = <nome do órgão constante do CNPJ>
Dados Obrigatórios	<i>As informações de órgão e unidade responsável pelo código são de</i> Preenchimento Obrigatório.
Unidade Organizacional Nome do órgão	
subjectAlternativeName	OID's: 2.16.76.1.3.8 -> *Nome empresarial 2.16.76.1.3.3 -> *CNPJ, 2.16.76.1.3.2 -> *Nome do responsável 2.16.76.1.3.4 -> *data de nascimento do responsável(8), *CPF(11), NIS(11), RG(15), emitente e UF(6).
Dados obrigatórios:	e ainda,
Nome empresarial CNPJ Dt Nascimento responsável CPF responsável rfc822Name	2.5.29.17.1 -> *rfc822Name - e-mail institucional do responsável (pode ser utilizado e-mail departamental) Todos os campos marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO
USO (KeyUsage)	digitalSignature e nonRepudiation
Uso Estendido (extendedKeyUsage)	id-kp-codeSigning, OID= 1.3.6.1.5.5.7.3.3 , assinatura de código..
Dados que devem constar da "Autorização de Emissão"	Órgão, Unidade responsável, Dados Pessoa Jurídica, Dados Responsável, Dados Representante Legal, e-mail institucional