



Leiaute
dos
Certificados Digitais
Cert-JUS
Versão 4.0

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

Sumário

1. Apresentação.....	3
2. Considerações Gerais.....	3
3. Requisitos Comuns dos Certificados Cert-JUS.....	6
4. Leiaute do Certificado Cert-JUS Institucional.....	9
5. Leiaute do Certificado Cert-JUS Poder Público.....	14
6. Leiaute do Certificado Cert-JUS Equipamento Servidor.....	19
7. Leiaute do Certificado Cert-JUS Código Seguro.....	24
8. Leiaute do Certificado Cert-JUS Carimbo de Tempo.....	28
9. Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS.....	32



1. APRESENTAÇÃO

A **Autoridade Certificadora da Justiça – AC-JUS** integra a Infraestrutura de Chaves Públicas Brasileira – **ICP-Brasil** como autoridade certificadora de primeiro nível.

Este documento descreve o perfil dos certificados digitais, ou seja, o conjunto de campos e extensões requerido pela AC-JUS dentro de uma estrutura padrão *X.509* e de acordo com a *RFC5280* do *ITU-T*. Aqui são definidas, a obrigatoriedade e criticidade dos campos, extensões e as informações que compõem os certificados emitidos sob a cadeia de certificação da **AC-JUS**.

Os certificados digitais emitidos sob a cadeia da AC-JUS são 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 subsequentes 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_subsequente-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. CONSIDERAÇÕES GERAIS

Os certificados *Cert-JUS* destinam-se aos órgãos do Poder Judiciário e da administração pública direta e indireta e identificam seus titulares relacionando-os a determinado órgão público. Cada órgão público que desejar fazer uso de certificados *Cert-JUS* é responsável pelas informações funcionais e institucionais constantes no certificado digital.

2.1 - 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.

2.2 - 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**.

2.3 - 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.

2.4 - Certificados já emitidos, que se encontrem fora das normas e regras aqui estabelecidas deverão ser imediatamente substituídos.

2.5 - DENOMINAÇÃO

2.5.1 - 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.

2.5.2 - A denominação definida neste documento 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.

2.6 - CADASTRAMENTO DE ÓRGÃOS NÃO PERTENCENTES AO PODER JUDICIÁRIO.

2.6.1 - Órgãos **não pertencentes** ao Poder Judiciário deverão solicitar **CADASTRAMENTO** junto à AC-JUS, para a emissão de certificados *Cert-JUS*.

2.6.2 - O cadastramento deve ser solicitado por ofício da autoridade competente do órgão interessado, endereçado à AC-JUS

2.6.3 - Após a aprovação do cadastro a AC-JUS oficiará as AC subsequentes para que incluam o órgão cadastrado nos seus sistemas de certificação.

2.6.4 - As AC da cadeia AC-JUS somente emitirão certificados digitais para órgãos **não pertencentes** ao Poder Judiciário após o **CADASTRAMENTO** ter sido aprovado pela **AC-JUS**.

2.6.5 - Para órgãos do Poder Judiciário **não é necessário cadastramento** prévio.

2.6.6 - A lista de órgãos autorizados e respectivas siglas padronizadas está publicada no repositório da AC-JUS e é divulgada para todas as Autoridades Certificadoras da cadeia AC-JUS.



2.6.7 - Em caso de dúvida sobre a padronização de nomes e siglas de órgãos não constantes da lista publicada, a unidade administrativa da AC-JUS deve ser consultada.

2.7 - AUTORIZAÇÃO

2.7.1 - Para a emissão de qualquer certificado ***Cert-JUS*** é necessária **AUTORIZAÇÃO** da **autoridade competente** da instituição à qual o certificado está relacionado.

2.7.2 - Ao autorizar a emissão de um certificado *Cert-JUS* a autoridade competente se responsabilizará pela exatidão das informações fornecidas,

2.7.3 - A Autorização conterá todas as informações institucionais obrigatórias, necessárias para a emissão do certificado digital, tais como *nome, matrícula, lotação, nome do órgão, cargo*, etc., além dos campos opcionais de interesse da instituição.

2.7.4 - A **AC-JUS** mantém em seu sítio em <http://www.acjus.jus.br> modelos de formulário para AUTORIZAÇÃO

2.8 - REVOGAÇÃO

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

2.8.2 - É obrigação do titular solicitar a revogação do certificado se vier a não mais fazer parte do quadro funcional do órgão autorizante.

2.8.3 - Cabe à instituição ou órgão de lotação do titular do certificado certificar-se da revogação do certificado, se o titular não mais fizer parte dos seus quadros e em caso de alteração de alguma informação nele contida



3. REQUISITOS COMUNS DOS CERTIFICADOS *Cert-JUS*

Os requisitos seguintes são comuns a todos os certificados da cadeia AC-JUS.

3.1 - Os certificados *Cert-JUS* deverão obedecer ao formato definido no padrão internacional *ITU-T X.509* versão 3 de acordo com o perfil estabelecido na *RFC 5280 (Request for Comments – Internet X.509 Public Key Infrastructure)* devendo atender aos seguintes requisitos:

3.2 - *Campo Issuer*

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

3.3 - *UniqueIdentifiers*

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 5280*, os campos opcionais *UniqueIdentifiers* **não** devem ser incluídos.

3.4 - *Algoritmos de Criptografia e tamanho das chaves*

O algoritmo utilizado para a geração das chaves dos certificados *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 até 31/12/2011, 2048 (dois mil e quarenta e oito) bits a partir de janeiro de 2012 ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

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

Os certificados *Cert-JUS* deverão ser assinados com uso do algoritmo de assinatura digital ***RSA com SHA-256*** (*OID= 1.2.840.113549.1.1.11*) ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

3.6 - *Conjunto de caracteres*

Salvo o previsto no item 3.4.5, todas as sequências 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 o cedilha deve ser substituído pelo caractere ‘c’.



3.7 - EXTENSÕES OBRIGATÓRIAS

3.7.1 - *AuthorityKeyIdentifier*

Não crítica.

O campo *keyIdentifier* deve conter o *hash SHA1* da chave pública da AC que emitiu o certificado.

3.7.2 - *KeyUsage*

Crítica.

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

3.7.3 - *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.

3.7.4 - *CRLDistributionPoints*

Não crítica.

Deve conter os endereços na *Web* onde se obtém a Lista de Certificados Revogados (LCR) gerada pela AC que emitiu o certificado. O preenchimento deste campo e sua semântica devem obedecer a *RFC 5280*.

3.7.5 - *BasicConstraints*

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

3.7.6 - *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 5280*.

Nesta extensão também poderá estar presente o campo *id-ad-caIssuers* OID=1.3.6.5.5.7.48.2 contendo o protocolo e endereço de obtenção da cadeia de certificação do certificado.

3.7.7 - *Outras Extensões*



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



4. 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.

4.1 - 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 e identificam o **titular** do certificado não só como indivíduo, mas também como servidor do órgão do Poder Judiciário em que está lotado.

4.1.1 - Os certificados *Cert-JUS Institucional* serão 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.

4.2 - DOCUMENTAÇÃO OBRIGATÓRIA

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

- i. AUTORIZAÇÃO de que trata o item 2.7;
- ii. Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE;
- iii. CPF ;
- iv. Comprovante de residência ou domicílio;
- v. Foto recente, caso as fotos nos documentos apresentados tenham mais de 5 anos.

4.3 - REQUISITOS ESPECÍFICOS DOS CERTIFICADOS *CERT-JUS* INSTITUCIONAL

Além dos requisitos gerais descritos no item 3 os certificados *Cert-JUS Institucional* deverão atender os seguintes requisitos específicos.:

4.3.1 - 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 Justiça – AC-JUS

OU = Cert-JUS Institucional – A3

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

OU = <Cargo do Titular>

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

- vi. No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres “<” e “>” não devem ser incluídos.
- vii. Os caracteres “#” representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.
- viii. 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.
- ix. O tamanho máximo de cada componente do DN (C, CN, O, OU, etc) é de 64 caracteres.
- x. No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura.
- xi. Os dados necessários para preenchimento do DN serão os informados na AUTORIZAÇÃO.
- xii. Para o certificado *Cert-JUS* Institucional, exclusivo para o Poder Judiciário, a informação <Cargo do Titular> deverá ser preenchido com uma das seguintes opções:
- MAGISTRADO;
 - SERVIDOR;
 - PRESTADOR DE SERVIÇO; ou
 - ESTAGIÁRIO.
- xiii. Todos os campos do DN são obrigatórios e devem ser preenchidos.
- xiv. O UPN (nome de login do Windows) deverá ser informado na autorização, na forma usuário@domínio, se for do interesse da instituição



Exemplo de um DN:

Nome do Servidor : José da Silva Valença

Matrícula: TR1-123.456 , Órgão de Lotação: TRF1 , Cargo: Técnico Judiciário

DN:

C = BR, O = ICP-Brasil,

OU = Autoridade Certificadora da Justiça – AC-JUS,

OU = Cert-JUS Institucional – A3

OU = Tribunal Regional Federal da 1ª Região - TRF1

OU = Servidor

CN = Jose da Silva Valenca:TR1123456

Extensões Obrigatórias

4.3.2 - KeyUsage

Crítica.

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

4.3.3 - SubjectAlternativeName

Não crítica, com o seguinte formato:

4.3.3.1 - 3 (três) campos *otherName*, **obrigatórios**, contendo:

- i. **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 subsequentessubsequentes, o Cadastro de Pessoas Físicas (CPF) do titular; nas 11 (onze) posições subsequentessubsequentes, o número de inscrição do titular no PIS/PASEP; nas 15 (quinze) posições subsequentessubsequentes, o número do registro Geral (RG) do titular; nas 6 (seis) posições subsequentes, 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 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.

4.3.3.2 - 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.

4.3.3.3 - 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.

4.3.3.4 - 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 é obrigatório.**
- ii. O conjunto de informações definido em cada campo *otherName* deve ser armazenado como O UPN (nome de login do Windows) deverá ser informado na autorização, na forma `usuário@domínio`, se for do interesse da instituição 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.

4.3.4 - 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*) .



5. LEIAUTE DO CERTIFICADO *CERT-JUS* PODER PÚBLICO

O certificado *Cert-JUS* **Poder Público** 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 trata o item 2.6

5.1 - 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 servidores de órgãos do Poder Judiciário.

5.1.1 - Os certificados *Cert-JUS* Poder Público serão 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.

5.1.2 - Por ser instrumento de identificação pessoal e institucional bem como de assinatura digital pessoal do titular, o uso do *Cert-JUS* Poder Público não é exclusivo para fins institucionais e profissionais, podendo ser utilizado para qualquer operação no meio digital que utilize a tecnologia de certificação digital.

5.2 - DOCUMENTAÇÃO OBRIGATÓRIA

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

- i. AUTORIZAÇÃO de que trata o item 2.7;
- ii. Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE;
- iii. CPF;



- iv. Comprovante de residência ou domicílio;
- v. Foto recente, caso as fotos nos documentos apresentados tenham mais de 5 anos.

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

5.2.2 - Cada órgão autorizado pela AC-JUS a emitir certificados *Cert-JUS* Poder Público poderá fazer acordos com as Autoridades Certificadoras da Cadeia AC-JUS para padronização do campo cargo, facilitando assim o processo de emissão dos certificados digitais.

5.3 - REQUISITOS DO CERTIFICADO

5.3.1 - 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 Justiça – 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. Todos os campos do DN são obrigatórios e devem ser preenchidos.
- viii. O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.
- ix. O UPN (nome de login do Windows) deverá ser informado na autorização, na forma `usuário@domínio`, se for do interesse da instituição

Exemplo:

Nome do Servidor: Antonio José da Silva

Matrícula: MPDFT .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 e Territorios -MPDFT

OU = PROCURADOR

CN = Antonio Jose da Silva:MPDF12345

5.4 - EXTENSÕES OBRIGATÓRIAS

5.4.1 - KeyUsage

Crítica.

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

5.4.2 - SubjectAlternativeName



Não crítica, com o seguinte formato:

5.4.2.1 - 3 (três) campos *otherName*, **obrigatórios**, contendo:

- i. **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.
- 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 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.

5.4.2.2 - 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.

5.4.2.3 - 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.

5.4.2.4 - 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.

5.4.3 - BasicConstraints

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

5.4.4 - 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*) .



6. LEIAUTE DO CERTIFICADO *CERT-JUS* EQUIPAMENTO SERVIDOR

6.1 - 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, VPN e outros serviços que requeiram certificados digitais para autenticação de servidor.

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

6.1.1 - A emissão de Certificados *Cert-JUS* Equipamento Servidor deve ser previamente autorizada pela autoridade competente.

6.1.2 - 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.

6.1.3 - 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.

6.1.4 - A emissão de certificados *Cert-JUS* Equipamento Servidor para determinado órgão só será iniciado após o CADASTRAMENTO de que trata o item 2.5.

6.2 - DOCUMENTAÇÃO OBRIGATÓRIA

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

- i. **AUTORIZAÇÃO** de que trata o item 2.7.
- 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 ou domicílio 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.

6.3 - REQUISITOS DO CERTIFICADO

6.3.1 - 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 Justiça – 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 2.7
- 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. 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.jus.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

6.4 - EXTENSÕES OBRIGATÓRIAS

6.4.1 - KeyUsage

Crítica.

Os bits *digitalSignature* e *keyEncipherment* devem estar ativados.

O bit *nonRepudiation* é opcional

6.4.2 - SubjectAlternativeName

Não crítica com o seguinte formato:

6.4.2.1 - 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.

6.4.2.2 - 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.

6.4.2.3 - 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.

6.4.3 - BasicConstraints

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

6.4.4 - 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 ***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.

6.4.5 - Outras Extensões

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



7. LEIAUTE DO CERTIFICADO *CERT-JUS* CÓDIGO SEGURO

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

7.1 - DESTINAÇÃO

7.1.1 - 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.

7.1.2 - 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.

7.1.3 - 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.

7.2 - 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 ou domicílio da autoridade competente do órgão solicitante e do responsável pelo certificado.
- v. Comprovação de habilitação Jurídica e Fiscal do órgão solicitante.

7.2.1 - 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.

7.2.2 - 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 Justica – AC-JUS,

OU=Cert-JUS Codigo Seguro – A1

OU=DESIN - Secretaria de Desenvolvimento de Sistemas

CN=CONSELHO DA JUSTICA FEDERAL

7.3 - EXTENSÕES OBRIGATÓRIAS

7.3.1 - *KeyUsage*

Crítica.

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

7.3.2 - *SubjectAlternativeName*

Não crítica com o seguinte formato:

7.3.2.1 - 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).;
- ii. **OID= 2.16.76.1.3.3 e conteúdo** = Número 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,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.

7.3.2.2 - 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*.

7.3.2.3 - 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**. Poderá 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

7.3.3 - 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.



8. LEIAUTE DO CERTIFICADO *CERT-JUS* CARIMBO DE TEMPO

O certificado digital *Cert-JUS Carimbo de Tempo* pode ser do tipo T3 (2048 bits) ou T4 (4096 bits)

8.1 - DESTINAÇÃO

8.1.1 - O certificado *Cert-JUS Carimbo de Tempo* destina-se, exclusivamente, para uso no Servidores de Carimbo de Tempo (SCT) de Autoridades Certificadoras de Tempo (ACT), autorizadas pela ICP-Brasil e pela AC-JUS.

8.1.2 - O *Cert-JUS Carimbo de Tempo* deverá ser emitido sempre para PESSOA JURÍDICA. O responsável pelo certificado deverá ser indicado pela autoridade competente, na **AUTORIZAÇÃO** para emissão do certificado.

8.1.3 - O titular do *Cert-JUS Carimbo de Tempo* 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.

8.2 - DOCUMENTAÇÃO OBRIGATÓRIA

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

- i. **AUTORIZAÇÃO** de que trata o item 2.7.
- 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 ou domicílio da autoridade competente do órgão solicitante e do responsável pelo certificado.
- v. Comprovação de habilitação Jurídica e Fiscal do órgão solicitante.
- vi. Cópia da publicação do ato de autorização de funcionamento do SCT e da ACT solicitantes.

8.2.1 - 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 Carimbo de Tempo – <Tipo de Certificado>

OU = < Nome da ACT>

CN = <nome do Servidor Carimbo do tempo >

- 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 2.7.
- 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

Exemplo :

ACT: Autoridade Certificadora de Tempo da Justiça

Servidor Carimbo de Tempo: ctempo.stf.jus.br

Tipo de Certificado:T4

DN:

C=BR, O=ICP-Brasil,

OU= Autoridade Certificadora da Justiça- ACJUS

OU= Cert-JUS Carimbo de Tempo-T4

OU= < Nome da ACT>

CN=<nome do Servidor Carimbo do tempo>



8.3 - EXTENSÕES OBRIGATÓRIAS

8.3.1 - *KeyUsage*

Crítica.

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

8.3.2 - *SubjectAlternativeName*

Não crítica com o seguinte formato:

8.3.2.1 - 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).;
- ii. **OID= 2.16.76.1.3.3 e conteúdo** = Número 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,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.

8.3.2.2 - 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*.

8.3.2.3 - 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**. Poderá 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. 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.
- 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.
- 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.

8.3.3 - ExtKeyUsage

Não crítica.

Deve conter o seguinte valor: *id-kp-timestamping*, *OID= 1.3.6.1.5.5.7.3.8*, para uso em sistemas de carimbo de tempo.



9. LEIAUTE DO CERTIFICADO DAS AUTORIDADES CERTIFICADORAS SUBSEQUENTES À AC-JUS

9.1 - REQUISITOS DE CERTIFICADO

Os certificados emitidos pela AC-JUS para as Autoridades Certificadoras subsequentes 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 5280 (Request for Comments – Internet X.509 Public Key Infrastructure)*. Os certificados das AC subsequentes deverão atender aos seguintes requisitos:

9.1.1 - Campo issuer

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

9.1.2 - Número de Versão

Os certificados das AC subsequentes implementam a versão 3 do padrão *ITU-T X.509*, de acordo com o perfil estabelecido na *RFC 5280*.

9.1.3 - UniqueIdentifiers

Em consonância com a recomendação constante na seção 4.1.2.8 da *RFC 5280*, os campos opcionais UniqueIdentifiers **não** devem ser incluídos.

9.1.1 - Algoritmos de Criptografia e tamanho das chaves

O Algoritmo utilizado para geração do par de chaves dos certificados emitidos para as AC subsequentes, 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 terá no mínimo 4096bits.

9.1.2 - Algoritmo de Assinatura Digital e tamanho dos hashes

Os certificados emitidos para as AC subsequentes serão assinados com o uso do algoritmo ***RSA com SHA-512*** (*OID= 1.2.840.113549.1.1.13*), conforme o padrão *PKCS#1 (RFC 4055)* ou conforme definido no documento PADRÕES E ALGORÍTMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

9.1.3 - Composição do DN:

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



C=BR

O=ICP-Brasil,

OU=Autoridade Certificadora da Justiça – AC-JUS,

CN=AC <Nome da Autoridade Certificadora Subsequente>->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 Subsequente, 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

9.2 - EXTENSÕES OBRIGATÓRIAS

9.2.1 - *AuthorityKeyIdentifier*

Não crítica:

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

9.2.2 - *SubjectKeyIdentifier*



Não crítica:

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

9.2.3 - KeyUsage

Crítica.

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

9.2.4 - 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.jus.br/acjus/>, onde se obtém a DPC da AC-JUS.

9.2.5 - 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 5280*.

9.2.6 - BasicConstraints

Crítica: deve conter *cA=True*.

9.2.7 - Outras Extensões

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



LISTA DE ACRÔNIMOS

AC	Autoridade Certificadora
ACT	Autoridade de Carimbo de Tempo
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ASR	Autenticação de Sincronização de relógio
AR	Autoridades de Registro
BIPM	Bureau International des Poids e Mesures
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
DPCT	Declaração de Práticas de Carimbo de Tempo
EAT	Entidade de Auditoria de Tempo
FCT	Fonte Confiável de Tempo
FIPS	Federal Information Processing Standards Publication
HLB	Hora Legal do Brasil
ICP-Brasil	infraestrutura 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>
NTP	<i>Network time Protocol</i>
OCSP	<i>On-line Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
ON	<i>Observatório Nacional</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



PCT	Política de Carimbo de tempo
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
SAS	Sistema de Auditoria e Sinconismo
SCT	Servidor de Carimbo de Tempo
SINMETRO	Sistema Nacional de Metrologia
<i>SNMP</i>	<i>Simple Network Management Protocol</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
<i>TSDM</i>	<i>trusted Software Development Methodology</i>
<i>TSP</i>	<i>Time Stamp Protocol</i>
<i>TSQ</i>	<i>Requisição de Carimbo de Tempo(Timestamp-query-request)</i>
<i>TSR</i>	<i>Carimbo de tempo(Timestamp response)</i>
<i>TSDM</i>	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Location</i>
UTC	<i>Tempo Universal Coordenado</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	
Público Alvo	Servidores e Autoridades do Poder Judiciário
Documentos Obrigatórios	1. Autorização da Autoridade Competente 2. Identidade, Passaporte ou CNE 3. CPF 4. Foto, 5. Informação de cargo, matrícula e lotação, e-mail institucional 6. Comprovante de residência ou domicílio
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><:> <#####> <i>As informações de órgão , cargo, lotação, nome e matrícula(#) são obrigatórios</i>
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	<i>Nome do titular, Lotação, cargo, matrícula, Nome de login na rede (UPN) na forma <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 4. Foto, 5. Informação de cargo, matrícula e lotação, e-mail institucional 6. Comprovante de residência ou domicílio
DN	C = BR, O=ICP-Brasil, OU = Autoridade Certificadora da Justica – AC-JUS, OU = Cert-JUS Institucional – A3 OU = <Órgão de Lotação do Titular><-><Sigla> OU = <Cargo do Titular> CN = <Nome do Titular><.><#####> <i>As informações de órgão , cargo, lotação, nome e matrícula(#) são obrigatórios</i>
Subject Alternative Name	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)
Dados obrigatórios: Dt Nascimento, CPF, rfc822Name	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	<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 ou Aplicação - Pessoa Jurídica –	
Publico Alvo	Equipamentos servidores de aplicação de órgãos publicos
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 ou domicílio
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 (Domain Name Service) 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 <i>(pode ser utilizada e-mail departamental)</i> 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 deou</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 (opcional)</i>
Dados que devem constar na “Autorização de Emissão”	URL 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: 1. Autorização e indicação do responsável pela Autoridade Competente 2. ID (Passaporte, CNE), 3. CPF 4. Foto, 5. Comprovante de residência ou domicílio
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 Preenchimento Obrigatório.</i>
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: Nome empresarial CNPJ Dt Nascimento responsável CPF responsável rfc822Name	e ainda, 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



<i>Cert-JUS</i> Carimbo de Tempo Certificado p/ SCT – T3 ou T4	
Publico Alvo	Equipamentos de carimbo de tempo
Documentos Obrigatórios	Identificação da Instituição: Autorização de funcionamento fornecida pelo ITI/ACT-RAIZ 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 ou domicílio
DN	C=BR, O=ICP-Brasil,
Dados Obrigatórios:	OU= Autoridade Certificadora da Justiça- ACJUS
Nome da ACT, Nome do servidor	OU= Cert-JUS Carimbo de Tempo-T4 OU= < Nome da ACT> CN=<nome do Servidor Carimbo do tempo>
subjectAlternativeName	OID's:
Dados Obrigatórios:	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), , nonRepudiation</i>
Uso Estendido (extendedKeyUsage)	<i>id-kp-timestamping, OID= 1.3.6.1.5.5.7.3.8, para aplicação de carimbo de tempo,</i>
Dados que devem constar na “Autorização de Emissão”	Nome do SCT, Nome da ACT, Unidade responsável, Dados Pessoa Jurídica, Dados Responsável, Dados Representante Legal, e-mail institucional