Leiaute dos Certificados Digitais

Cert-JUS

Versão 5.0

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

Sumário

1. Apresentação 3
2. Considerações Gerais 3
3. Requisitos Comuns dos Certificados Cert-JUS 8
4. Leiaute do Certificado *Cert-JUS* Institucional 10
5. Leiaute do Certificado *Cert-JUS* Poder Público 14
6. Leiaute do Certificado *Cert-JUS* Equipamento Servidor 19
8. Leiaute do Certificado *Cert-JUS* Código Seguro 23
9. Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS 26

1. APRESENTAÇÃO

A **Autoridade Certificadora da Justiça – AC-JUS** integra a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil como autoridade certificadora de primeiro nível. A AC-JUS define e normatiza a emissão de certificados digitais para uso no âmbito da Administração Pública Direta e Indireta no geral e no âmbito do Poder Judiciário em particular.

Este documento descreve o perfil dos certificados digitais definidos pela AC-JUS**,** tomando como base as definições da ICP-Brasil e a aderência à estrutura padrão *X.509,* de acordo com a *RFC 5280* do *ITU-T*. Todos os Certificados Cert-JUS têm como base a definição básica da ICP-Brasil, com requisitos ou preenchimento de campos ou extensões adicionais.

São definidas a obrigatoriedade dos campos e extensões bem como as informações que devem ser inseridas, as regras, restrições e requisitos documentais para emissão dos certificados sob a cadeia de certificação da AC-JUS**.**

Os certificados digitais emitidos sob a cadeia da AC-JUS são denominados certificados ***Cert-JUS***.

As Autoridades Certificadoras integrantes da cadeia **AC-JUS** utilizam a denominação AC<espaço>*nome_subsequente*-JUS e estão autorizadas a emitir apenas os certificados ***Cert-JUS*** conforme definidos neste documento. Devem utilizar o leiaute e denominação correspondente, seguindo as regras específicas para emissão, aqui descritas.

2. CONSIDERAÇÕES GERAIS

Os certificados digitais ***Cert-JUS*** destinam-se a servidores, equipamentos e aplicações dos órgãos do Poder Judiciário e da administração pública direta e indireta. Cada certificado identifica seu titular, equipamento ou aplicação, **relacionando-os a determinado órgão público.**

O órgão público que desejar fazer uso dos certificados *Cert-JUS*, deve autorizar a emissão para cada titular, equipamento ou aplicação e é responsável pelo fornecimento das informações funcionais e institucionais que devem constar

no certificado digital.

O órgão é responsável também por garantir a revogação do certificado digital ou a destruição da sua chave privada em caso de desligamento do titular do certificado.

NOTA: No caso de certificados digitais emitidos para Magistrados, não se faz necessária a revogação em caso de mudança de jurisdição ou atuação em outro órgão.

2.1 - Para o disposto neste documento, entende-se como **autoridade competente**:

- a autoridade máxima do órgão;
- o representante legal do órgão ou pessoa com delegação formal para representação administrativa do órgão;
- servidores com responsabilidade delegada para representação administrativa do órgão por meio de ato oficial ou pela natureza de suas atribuições, descritas em regimento interno ou semelhante.
- servidores designados para esta finalidade, por meio de ato oficial.

2.2 - Os certificados emitidos sob a cadeia **AC-JUS** seguem os padrões definidos 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** somente emitirão certificados que possuam leiaute e conteúdo conforme definido neste documento.

2.4 - As autoridades certificadoras da cadeia de certificação da **AC-JUS** somente emitirão certificados para os órgãos previamente cadastrados junto à AC-JUS conforme o item 2.9.

2.5 - Todos os órgãos autorizados a utilizarem certificados ***Cert-JUS*** estão relacionados no documento *Lista de Órgãos Autorizados – AC-JUS*, disponível no site da AC-JUS em http://www.acjus.jus.br/ .

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

2.7 - Não é permitida a emissão de certificado digitais de SIGILO e CFe-SAT no âmbito da AC-JUS.

2.8 - DENOMINAÇÃO

2.8.1 - 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.

2.8.2 - 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.

2.9 - CADASTRAMENTO DE ÓRGÃOS NÃO PERTENCENTES AO PODER JUDICIÁRIO.

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

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

2.9.3 - 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**.

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

2.9.5 - A lista de órgãos cadastrados, bem como as respectivas siglas padronizadas, está publicada no repositório da AC-JUS e é

divulgada para todas as Autoridades Certificadoras da cadeia AC-JUS.

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

2.9.7 - Todos os órgãos do Poder Judiciário estão automaticamente cadastrados.

2.10 - AUTORIZAÇÃO

2.10.1 - Para a emissão de qualquer certificado ***Cert-JUS*** é necessária autorização da autoridade competente da instituição ou órgão à qual o titular do certificado está relacionado.

2.10.2 - A autorização conterá todas as informações institucionais obrigatórias, necessárias para a emissão do certificado digital, conforme cada leiaute definido, além dos campos opcionais de interesse da instituição.

2.10.3 - A AC-JUS mantém em seu sítio em http://www.acjus.jus.br modelos de AUTORIZAÇÃO para diversos tipos de certificado

2.10.4 - As autorizações para emissão de certificados, não necessitam ser individualizadas. Podem ser utilizadas listas ou outros meios acordados entre o órgão e a Autoridade Certificadora emitente, desde que sejam assinadas pela autoridade competente. (Ver item 2.1)

2.11 - REVOGAÇÃO

2.11.1 - 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.

2.11.2 - É obrigação do titular solicitar a revogação do certificado se

vier a não mais fazer parte do quadro funcional do órgão que autorizou a emissão do certificado.

2.11.3 - Cabe à instituição ou órgão de lotação do titular de um certificado Cert-JUS, garantir a revogação do certificado se aquele titular não mais fizer parte dos seus quadros ou em caso de alteração de alguma informação contida no certificado.

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 também os requisitos definidos pela ICP-Brasil.

3.2 - 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 2048 (dois mil e quarenta e oito) bits ou conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL.

3.3 - 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.

3.4 - FORMATO DO CAMPO DN

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

3.5 - EXTENSÕES OBRIGATÓRIAS

3.5.1 - AuthorityKeyIdentifier

Não crítica.

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

3.5.2 - KeyUsage e extendedKeyUsage

a) Para certificados de Assinatura de Código:

"Key Usage", crítica: somente o bit digitalSignature deve estar ativado;

"Extended Key Usage", não crítica: somente propósito codeSigning OID=1.3.6.1.5.5.7.3.3 deve estar presente.

b) Para certificados de Autenticação de Servidor:

"Key Usage", crítica: os propósitos *digitalSignature* e *keyEncypherment* devem estar presentes;

O propósito *nonRepudiation* é opcional

"Extended Key Usage", não crítica: deve conter o propósito *serverAuthentication* OID = 1.3.6.1.5.5.7.3.1.

Pode conter o propósito *clientAuthentication* OID = 1.3.6.1.5.5.7.3.2.

c) Para certificados de assinatura de resposta OCSP:

"Extended Key Usage", não crítica: somente o propósito *OCSPSigning*, OID =1.3.6.1.5.5.7.3.9 deve estar ativado.

d) Para os demais certificados de Assinatura e/ou Proteção de e-mail:

"Key Usage", crítica: os propósitos *digitalSignature, nonRepudiation* e *keyEnciphernment* devem estar ativados;

"Extended Key Usage", não crítica: os propósitos clientAuthentication OID = 1.3.6.1.5.5.7.3.2 e *emailProtection* OID = 1.3.6.1.5.5.7.3.4 deve estar ativado.

3.5.3 - 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.

3.5.4 - 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*.

3.5.5 - Authority Information Access

Não crítica.

Na primeira entrada deve conter 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.

Na segunda entrada pode conter o método de acesso *id-ad-ocsp* e o respectivo endereço de acesso ao serviço OCSP, caso a autoridade certificadora emitente o implemente.

4. LEIAUTE DO CERTIFICADO *CERT-JUS* INSTITUCIONAL

O certificado ***Cert-JUS*** Institucional deve preferencialmente ser do tipo A3 ou superior.

Será admitida a utilização de certificados do tipo A1 (A1 Mobile), somente para dispositivos móveis (tablets e celulares) , desde que:

a) o certificado esteja associado a um único dispositivo.
b) o par de chaves criptográfica e a requisição de certificado devem ser gerados no dispositivo associado.
c) o software de geração e gerenciamento das chaves privadas, instalado no dispositivo, não deve permitir a exportação da chave privada.
d) a AC emitente não deve permitir a configuração pelo usuário dos parâmetros referentes à exportação da chave privada, que deve estar marcada como “não exportável”.
e) a AC deve se certificar de que o dispositivo utilizado não esteja em modo “root” ou jailbreak ou qualquer modo equivalente de desbloqueio do Sistema Operacional do dispositivo, no momento da geração das chaves, que permita ou facilite o acesso ao material criptográfico além do próprio aplicativo móvel que o gerou no momento da geração das chaves .

Para os certificados 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.

A validade de certificados de no máximo 1 ano para A1 e 3 anos para A3 e A4.

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 os **titulares** 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. Demais requisitos determinados pela ICP-Brasil.

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 Justica – AC-JUS

OU = Cert-JUS Institucional – <A3> ou <A4> <A1 Mobile>

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. Os dados necessários para preenchimento do DN deverão ser os informados na AUTORIZAÇÃO.

v. Para o certificado *Cert-JUS* Institucional, exclusivo para o Poder Judiciário, a informação <*Cargo do Titular*> deverá ser preenchido **SOMENTE** com uma das seguintes opções:

- MAGISTRADO;
- SERVIDOR;
- PRESTADOR DE SERVIÇO; ou
- ESTAGIÁRIO.

vi. Todos os campos do DN são obrigatórios e devem ser preenchidos.

vii. No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura

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 Justica – AC-JUS,
OU = Cert-JUS Institucional – A3

OU = Tribunal Regional Federal da 1a Região - TRF1

OU = Servidor

CN = Jose da Silva Valenca:TR1123456

_____

4.4 - EXTENSÕES OBRIGATÓRIAS

4.4.1 - SubjectAlternativeName

4.4.1.1 - Devem ser obrigatoriamente preenchidas as informações:

a) Data de Nascimento, CPF e RG presentes no OID 2.16.76.1.3.1

4.4.1.2 - Informações opcionais

b) PIS/PASP presente no OID 2.16.76.1.3.1

c) CEI presente OID 2.16.76.1.3.6

d) Título de eleitor presentes no OID 2.16.76.1.3.5

e) Número da identificação profissional é opcional no OID= 2.16.76.1.4.n

f) O OID= 1.3.6.1.4.1.311.20.2.3, User Principal Name (UPN), necessário para *login com uso de certificados digitais. O UPN (nome de login do Windows) deverá ser informado na AUTORIZAÇÃO, na forma usuário@domínio_institucional, se for do interesse da instituição*

No preenchimento dos demais campos e informações devem ser seguidas as normas definidas pela ICP Brasil nos DOC-ICP 05 e 04

4.4.2 - Extended Key Usage (extendedKeyUsage)

Não crítica.

a) Os seguintes propósitos devem estar ativados:

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*).

b) “*SmartCardLogon*” (OID= 1.3.6.1.4.1.311.20.2.2) é opcional e deve estar presente sempre que for solicitado e fornecido o UPN.

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

O certificado *Cert-JUS* Poder Público deve preferencialmente ser do tipo A3 ou superior.

Será admitida a utilização de certificados do tipo A1 (A1 Mobile), somente para dispositivos móveis (tablets e celulares), desde que:

f) o certificado esteja associado a um único dispositivo.

g) o par de chaves criptográfica e a requisição de certificado devem ser gerados no dispositivo associado.

h) o software de geração e gerenciamento das chaves privadas, instalado no dispositivo, não deve permitir a exportação da chave privada.

i) a AC emitente não deve permitir a configuração pelo usuário dos parâmetros referentes à exportação da chave privada, que deve estar marcada como “não exportável”.

j) a AC deve se certificar de que o dispositivo utilizado não esteja em modo “root” ou jailbreak ou qualquer modo equivalente de desbloqueio do Sistema Operacional do dispositivo, no momento da geração das chaves, que permita ou facilite o acesso ao material criptográfico além do próprio aplicativo móvel que o gerou no momento da geração das chaves .

Para os certificados 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.

A validade de certificados de no máximo 1 ano para A1 e 3 anos para A3 e A4.

A emissão de certificados *Cert-JUS* Poder Público para determinado órgão só será iniciada pela Autoridade Certificadora emitente, 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

Além dos documentos obrigatórios para emissão de certificados para pessoa física definidos pela ICP Brasil, é obrigatória a apresentação de:

i. AUTORIZAÇÃO de que trata o item 2.7;

ii. CPF;

iii. Demais requisitos determinados pela ICP-Brasil

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 Justica – AC-JUS

OU = Cert-JUS Poder Público – <A3> ou <A4> ou <A1 Mobile>

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. Os dados necessários para preenchimento do DN serão os informados na AUTORIZAÇÃO**.**

v. Todos os campos do DN são obrigatórios e devem ser preenchidos.

vi. O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.

vii. No CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura

Exemplo:

Nome do Servidor: Antonio José da Silva

Matrícula: MPDFT .12345, Órgão de Lotação: Ministério Público 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 - SubjectAlternativeName

5.4.1.1 - Informações Obrigatórias

a) Data de Nascimento, CPF e RG presentes no OID 2.16.76.1.3.1

5.4.1.2 - Informações opcionais

a) PIS/PASP presente no OID 2.16.76.1.3.1

b) CEI presente no OID 2.16.76.1.3.6

c) Título de eleitor presentes no OID 2.16.76.1.3.5

d) Número da identificação profissional é opcional no OID= 2.16.76.1.4.n

e) O OID= 1.3.6.1.4.1.311.20.2.3, User Principal Name (UPN), necessário para *login com uso de certificados digitais. O UPN (nome de login do Windows) deverá ser informado na AUTORIZAÇÃO, na forma usuário@domínio_institucional, se for do interesse da instituição*

No preenchimento dos demais campos e informações devem ser seguidas as normas definidas pela ICP Brasil nos DOC-ICP 05 e 04

5.4.2 - Extended Key Usage (extendedKeyUsage)

Não crítica.

a) Os seguintes propósitos devem estar ativados:

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*).

b) EKU “SmartCardLogon” (OID= 1.3.6.1.4.1.311.20.2.2) é opcional e deve estar presente sempre que for solicitado e fornecido o UPN.

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 e aplicações que disponibilizem serviços ou informações do poder público (órgãos do Poder Judiciário, órgãos da administração pública direta e indireta ou a empresas privadas que prestem serviços a órgãos públicos), tais como web segura, SSL, SSH, VPN, OCSP e outros serviços que requeiram certificados digitais para autenticação. 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 - 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.

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

6.1.4 - O certificado *Cert-JUS* Equipamento Servidor poderá ser do tipo mono-domínio ou multidomínio exceto para certificados de resposta OCSP.

6.1.5 - O certificado *Cert-JUS* Equipamento Servidor do tipo multidomínio poderá endereçar no máximo 25 servidores diferentes.

6.1.6 - O certificado *Cert-JUS* Equipamento Servidor do tipo multidomínio não poderá ser do tipo WILDCARD (infinitos domínios/servidores).

6.1.7 - Os certificados de resposta OCSP serão emitidos somente para autoridades certificadoras subsequentes à AC-JUS, pela própria AC subsequente, de forma viabilizar a autenticação do seu serviço OCSP. Para este certificado está dispensada a Autorização de que trata o item 2.7.

6.2 - DOCUMENTAÇÃO OBRIGATÓRIA

Além dos documentos obrigatórios para emissão de certificados para Equipamentos e aplicações, definidos pela ICP Brasil, é obrigatória a apresentação de:

i. **AUTORIZAÇÃO** de que trata o item 2.7.

ii. CPF da autoridade competente do órgão solicitante e do responsável pelo certificado.

iii. Comprovação de registro dos domínios pela instituição solicitante.

iv. Aplicam-se as exigências documentais e procedimentais dos DOC ICP 05 e 04.

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 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. Para certificados multidomínio o CN conterá a *url* principal do domínio,

essa *url* e demais *url*s endereçadas pelo certificado estarão em campos *dnsName* da extensão s*ubjectAlternativeName*.

iv. Os dados necessários para preenchimento do DN deverão ser obtidos na **AUTORIZAÇÃO** de emissão do certificado, citada no item 2.7, inclusive a relação de todas as *url* endereçadas pelo certificado.

v. A lista contendo os nomes dos órgãos e respectivas siglas padronizadas está publicada no repositório da AC-JUS.

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 - SubjectAlternativeName

a) Campos obrigatórios:
   i. nome empresarial constante no *OID 2.16.76.1.3.8*
   ii. número do CNPJ constante no *OID 2.16.76.1.3.3*
   iii. nome do responsável pelo certificado constante no *OID 2.16.76.1.3.2*
   iv. data de nascimento e número do Cadastro de Pessoas Físicas (CPF) do responsável constantes *no OID 2.16.76.1.3.4*
   v. e-mail do responsável constante no OID= 2.5.29.17.1 - rfc822Name.

Deve conter o endereço de e-mail institucional do responsável pelo certificado. Pode ser utilizado o e-mail da unidade organizacional do responsável pelo certificado.

b) Campos opcionais:

Número de Identificação Social-NIS (PIS, PASEP ou CI) e Registro Geral (RG) *constantes no OID= 2.16.76.1.3.4.*

c) Para Certificados MULTIDOMÍNIO

Poderão haver até 25 campos DnsName, contendo, 1 FQDN de equipamento ou aplicação, cada um.

d) Para os demais campos são aplicadas todas as definições padrão da ICP-Brasil quanto à obrigatoriedade e formatação.

6.4.2 - ExtKeyUsage

Não crítica.

Deve conter o propósito *id-kp-serverAuth*, **OID= 1.3.6.1.5.5.7.3.1**, para uso na autenticação de equipamento servidor.

O propósito *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 somente o propósito *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.

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

O certificado digital *Cert-JUS* **Código Seguro** pode ser do tipo A1, A3 ou A4.

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 **P**oder 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.

7.1.4 - Serão observados os requisitos complementares do DOC-ICP-01.02, que deverão ser incorporadas nas PC das AC subsequente para emissão desse tipo de certificado.

7.2 - DOCUMENTAÇÃO OBRIGATÓRIA

Além dos documentos constantes no DOC-ICP-05, para emissão de **CERTIFICADOS *CERT-JUS*** CÓDIGO SEGURO **SÃO** obrigatórios**:**

i. AUTORIZAÇÃO de que trata o item 2.7.

ii. CPF da autoridade competente do órgão solicitante e do responsável pelo certificado.

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 Justica – AC-JUS

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

OU = <nome da Unidade Organizacional responsável >

CN = <nome do órgão constante do CNPJ>

ST= estado da federação do titular do certificado.

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. Todos os campos do DN são obrigatórios e devem ser preenchidos.

v. 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, 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

ST= DF

_____

7.3 - EXTENSÕES OBRIGATÓRIAS

7.3.1 - SubjectAlternativeName

Não crítica com o seguinte formato**:**

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** = a data de nascimento do responsável, o Cadastro de Pessoas Físicas (CPF) do responsável, são obrigatórios;

i. Um campo ***rfc822Name***, obrigatório, contendo o e-mail institucional do responsável pelo certificado. Poderá ser utilizado o e-mail da unidade organizacional responsável pelo certificado.

7.3.2 - ExtKeyUsage

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

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

8.1 - 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*).

Conforme DOC ICP-01.02 de 15/07/2016, os certificados de confirmação de identidade e assinatura do tipo A1 a A4 devem ser separados por Autoridade Certificadoras (AC) emissora para cada tipo de uso, conforme descrito a seguir;

a) Autenticação de Servidor (SSL/TLS);

b) Assinatura Geral e Proteção de e-mail (S/MIME); e

c) Assinatura de Código (Code Signing).

Os certificados das AC subsequentes deverão atender aos seguintes requisitos:

8.1.1 - Campo issuer

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

8.1.2 - 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*.

8.1.3 - UniqueIdentifiers

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

8.1.4 - 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.

8.1.5 - 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.

8.1.6 - Composição do DN:

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

C=BR

O=ICP-Brasil,

OU=Autoridade Certificadora da Justica – AC-JUS,

OU=Tipo (propósito) de Uso dos certificados emitidos na Cadeia

CN=AC <*Nome da Autoridade Certificadora Subsequente*> <->JUS <identificador de tipo d ecertificado> <identificador de versão>

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, de acordo com a nomenclatura definida pela Instrução Normativa nº12 da ICP-Brasil e seus anexos, com comprimento máximo de 64 caracteres.

iv. O CN deverá ser composto da seguinte forma:

AC <*nomedaACSubseqüente* >-JUS <Tipo de certificado da cadeia> <identificador de versão da cadeia>.

A expressão “AC” seguida de um espaço, o nome da AC, seguido de um hífen e a expressão JUS seguido de espaço e do identificador do tipo de certificado que irá emitir, seguido de espaço e do identificador de versão da cadeia.

v. O traço (hífen) antes da expressão JUS é obrigatório. Exemplo: AC EXEMPLO**-**JUS SSL

Exemplo de DN:

_____

C=BR, O=ICP-Brasil,

OU=Autoridade Certificadora da Justiça – AC-JUS

OU= SSL

CN=AC Exemplo-JUS SSL v5

_____

8.2 - EXTENSÕES OBRIGATÓRIAS

8.2.1 - AuthorityKeyIdentifier

Não crítica:

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

8.2.2 - SubjectKeyIdentifier

Não crítica:

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

8.2.3 - KeyUsage

Crítica.

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

8.2.4 - 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.

8.2.5 - 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*.

8.2.6 - BasicConstraints

Crítica: deve conter *cA=True*.

8.2.7 - 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 Internacional des Poids e Mesures
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM-SEI	*Capability Maturity Model* do *Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas -
COBIT	*Control Objectives for Information and related Technology*
COSO	*Comitee of Sponsoring Organizations*
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
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	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITSEC	*European Information Technology Security Evaluation Criteria*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	*National Institute of Standards and Technology*
NTP	*Network time Protocol*
OCSP	*On-line Certificate Status Protocol*
OID	*Object Identifier*
ON	*Observatório Nacional*
OU	*Organization Unit*
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	*Proof of Possession*
PSS	Prestadores de Serviço de Suporte
RFC	*Request For Comments*
RG	Registro Geral
SAS	Sistema de Audiotoria e Sinconismo
SCT	Servidor de Carimbo de Tempo
SINMETRO	Sistema Nacional de Metrologia
SNMP	*Simple Network Management Protocol*
TCSEC	*Trusted System Evaluation Criteria*
TSDM	*trusted Software Development Methodology*
TSP	*Time Stamp Protocol*
TSQ	*Requisição de Carimbo de Tempo(Timestamp-query-request)*
TSR	*Carimbo de tempo(Timestamp response)*
TSDM	*Trusted Software Development Methodology*
UF	Unidade de Federação
URL	*Uniform Resource Location*
UTC	*Tempo Universal Coordenado*

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

Nome	***OID***
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 , A4 ou A1 mobile	
Público Alvo	**Servidores e Autoridades do Poder Judiciário**
Documentos Obrigatórios	1. Autorização da Autoridade Competente 2. Informação de cargo, matrícula, lotação e e-mail institucional e opcionais 3. Identidade, Passaporte ou CNE 4. CPF 5. Demais exigências ICP-Brasil
DN (Obs. Para o campo cargo somente podem ser utilizadas Magistrado, Servidor, Prestador de Serviço, Estagiário) O campo órgão deve seguir a tabela distribuída pela AC-JUS às subsequentes	**C = BR, O=ICP-Brasil,** **OU = Autoridade Certificadora da Justica – AC-JUS,** **OU = Cert-JUS Institucional** – A3 ou A4 ou A1 Mobile **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: Data Nascimento, CPF, rfc822Name	*OID's:* *2.16.76.1.3.1 -> *Data Nascimento (8), *CPF (11), NIS (11), RG (15), Órgão e UF (10)* *2.16.76.1.3.6 -> INSS (12) (opcional)* *2.16.76.1.3.5 -> Título de eleitor (12), Zona Eleitoral (3), Seção (4),* *1.3.6.1.4.1.311.20.2.3 -> UPN – usuario@dominio-login na rede (opcional)* *2.5.29.17.1 - *rfc822Name - e-mail institucional (iA5String)* *Os campos marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO.*
Uso (KeyUsage)	*digitalSignature (assinatura digital)* OID 2.5.29.15.0 *nonRepudiation (não repúdio)* OID 2.5.29.15.1 *e* *keyEncipherment (cifragem de chave)*
Uso estendido (extendedKeyUsage)	*"client authentication" (autenticação de cliente) (***OID 1.3.6.1.5.5.7.3.2***)* *"E-mail protection" (proteção de e-mail) (***OID 1.3.6.1.5.5.7.3.4***) e* *"SmartCardLogon" (logon com smartcard) (***OID 1.3.6.1.4.1.311.20.2.2***)*
Dados que devem constar na Autorização	*Nome do titular, Lotação, cargo, matrícula, Nome de login na rede (UPN) na forma* usuario@dominio*, e-mail institucional*

Cert-JUS **Poder Público** - TIPO A3, A4 ou A1 mobile (Obrigatório cadastramento de cada órgão solicitante	
Público Alvo	Servidores e Autoridades do Poder Publico
Documentos Obrigatórios	1. Autorização da Autoridade Competente 2. Informação de cargo, matrícula, lotação e e-mail institucional e opcionais 3. Identidade, Passaporte ou CNE 4. CPF 5. Demais exigências ICP-Brasil
DN O campo órgão deve seguir a tabela distribuída pela AC-JUS às subsequentes. Apenas os órgãos constantes da tabela oficial estão autorizados a emitirem Certificados Cert-JUS	C = BR, O=ICP-Brasil, OU = Autoridade Certificadora da Justica – AC-JUS, OU = Cert-JUS Poder Publico – A3 ou A1 Mobile 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 OID 2.5.29.17 _____ Dados obrigatórios: Data Nascimento, CPF, rfc822Name	*OID's:* *2.16.76.1.3.1 -> *Data Nascimento (8), *CPF (11), NIS (11), RG (15), Órgão e UF (10)* *2.16.76.1.3.6 -> INSS (12) (opcional)* *2.16.76.1.3.5 -> Título de eleitor (12), Zona Eleitoral (3), Seção (4),* *1.3.6.1.4.1.311.20.2.3 -> UPN – usuario@dominio-login na rede (opcional)* *2.5.29.17.1 -*rfc822Name - e-mail institucional (iA5String)* *Os campos marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO.*
Uso da Chave (KeyUsage)	*digitalSignature (assinatura digital)* *keyEncipherment (cifragem de chave)* *nonRepudiation (não repúdio)*
Uso estendido da chave (extendedKeyUsage)	*"client authentication" (autenticação de cliente) (*OID 1.3.6.1.5.5.7.3.2*)* *"E-mail protection" (proteção de e-mail) (*OID 1.3.6.1.5.5.7.3.4*) e* *"SmartCardLogon" (logon com smartcard) (*OID 1.3.6.1.4.1.311.20.2.2*) (opcional)*
Dados que devem constar na Autorização	*Nome do titular, Lotação, cargo, matrícula, Nome de login na rede na forma (UPN)* usuario@dominio*, e-mail institucional*

Cert-JUS **Equipamento Servidor** TIPO A1 ou superior Certificado p/ Equipamento ou Aplicação - Pessoa Jurídica –	
Público 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 pelo certificado 2. Informação de matrícula lotação e e-mail institucional do responsável pelo certificado 3. ID (Passaporte, CNE), 4. CPF 5. Demais exigências da ICP-Brasil
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 ou nome da aplicação> *As informações de órgão, unidade organizacional e URL do equipamento são obrigatórias*
subjectAlternativeName _____ Dados Obrigatórios: Nome empresarial, CNPJ, Nome do responsável, data nasc.do responsável, CPF responsável, e-mail institucional	***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 (10), 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)	*DigitalSignature (assinatura digital),* keyEncipherment *(cifragem de chave), nonRepudiation (opcional)*
Uso Estendido (extendedKeyUsage)	id-kp-serverAuth, **OID = 1.3.6.1.5.5.7.3.1** - *autenticação de equipamento servidor, acompanhado de* *"id-kp-clientAuth"* **OID= 1.3.6.1.5.5.7.3.2** *autenticação de cliente (opcional)* *Para serviço OCSP* *Somente id-kp-OCSPSigning,* **OID= 1.3.6.1.5.5.7.3.9**
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 superior Certificado Pessoa Jurídica para assinatura de código executável.	
Público 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 pelo certificado 2. ID (Passaporte, CNE), 3. CPF responsável e CNPJ do órgão 4. Demais exigências da ICP-Brasil
DN _____ Dados Obrigatórios Unidade Organizacional Nome do órgão	**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> **ST =** Unidade da federação *As informações de órgão e unidade responsável pelo código são de* **Preenchimento Obrigatório**.
subjectAlternativeName _____ Dados obrigatórios: Nome empresarial CNPJ Data Nascimento 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 (10). E ainda, **rfc822Name - e-mail institucional do responsável* (pode ser utilizado e-mail departamental) Todos os campos marcados com (*) são de PREENCHIMENTO OBRIGATÓRIO
USO (KeyUsage)	digitalSignature
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

Alterações:

01/12/2016	Adequação à IN 07 e 12 e correções	Explicitar a admissibilidade dos certificado A4
05/09/2014 17:33	Para adequação à resolução 103/204 ICP Brasil:	– Ajustes no item 7.1.2.7 do DOC ICP- 04 v5.2 - Ajuste no tamanho do campo UF e emissor dos OIDs 2.16.76.1.3.1 e 2.16.76.1.3.4
20/09/2016	- adequação ao DOC-ICP 01.02 - adequação para possibilitar o uso de A1 Mobile, no sistema PJe - retirada certificados de Tempo	