LEIAUTE DOS CERTIFICADOS CERT-JUS

Versão 7.0

ABRIL DE 2019

AUTORIDADE CERTIFICADORA DA JUSTIÇA – AC-JUS

Sumário

Leiaute dos Certificados Digitais Cert-JUS

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**,** tendo 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 digitais Cert-JUS têm como base a definição básica da ICP-Brasil, com requisitos ou preenchimento de campos ou extensões adicionais.

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

Neste documento são definidos os campos, extensões e informações obrigatórias que devem ser constar em cada perfil de certificado especificado, bem como as regras, restrições e requisitos documentais para emissão dos certificados sob a cadeia de certificação da AC-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 digitais Cert-JUS conforme definidos neste documento. Devem utilizar o leiaute e a denominação correspondente, seguindo as regras específicas para emissão, aqui descritas.

2 Considerações Gerais

Os certificados digitais ***Cert-JUS*** destinam-se a servidores, magistrados, equipamentos e aplicações dos órgãos do Poder Judiciário e da Administração Pública direta e indireta. Cada certificado digital identifica seu titular, equipamento ou aplicação, **relacionando-os a determinado órgão público ou ao Poder Judiciário no caso do Certificado Cert-JUS Magistrado.**

O órgão público que desejar fazer uso dos certificados digitais *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.

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.
- recomenda-se a designação pelo órgão, dos servidores que responsáveis pela autorização no início da execução contratual, com renovação anual da designação.

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-Brasi**l 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 digitais Cert-JUS para os órgãos previamente cadastrados junto à AC-JUS conforme o item 2.9.

2.5 Todos os órgãos autorizados a utilizarem certificados digitais 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 Não é permitida a emissão de certificado digitais de SIGILO e CFe-SAT na cadeia da AC-JUS.

3 Denominação

3.1 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.

3.2 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.

4 Cadastramento de Órgãos não pertencentes ao Poder Judiciário.

A AC-JUS definiu um perfil de certificado digital específico, chamado *Cert-JUS Poder Público,* para ser utilizado por órgãos da Administração Pública direta e indireta, não pertencentes ao Poder Judiciário.

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

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**.

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

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

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.

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

Os órgãos do Poder Judiciário não necessitam fazer cadastramento desde que já constem na *Lista de órgãos autorizados*, distribuída às Autoridades Certificadoras e publicada no site da AC-JUS.

5 Autorização

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

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.

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

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 e contenham todas as informações institucionais requeridas. (Ver item 2.1)

6 Revogação

Os certificados digitais ***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.

É obrigação do titular solicitar a revogação do certificado digital quando for desligado do quadro funcional do órgão que autorizou a emissão do certificado.

Cabe à instituição ou órgão de lotação do titular de um certificado digital ***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.

7 Requisitos Comuns dos Certificados *Cert*-JUS

Os certificados digitais ***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.

8 Leiaute do Certificado *Cert*-JUS Institucional

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

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

- o certificado esteja associado a um único dispositivo.
- o par de chaves criptográfica e a requisição de certificado devem ser gerados no dispositivo associado.
- o software de geração e gerenciamento das chaves privadas, instalado no dispositivo, não deve permitir a exportação da chave privada.
- 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".
- a AC deve se certificar de que o dispositivo utilizado não esteja em modo "*root*", "*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 a qualquer outro aplicativo além do próprio aplicativo móvel utilizado para geração das chaves.

Para os certificados A3 ou superior, deverá ser utilizado dispositivo criptográfico para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado.

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

8.1 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. Identificam os titulares do certificado não só como indivíduo, mas também como servidor do órgão do Poder Judiciário em que está lotado.

Os certificados digitais ***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.

Os certificados digitais ***Cert-JUS* Institucional** PODEM ser emitidos para MAGISTRADOS do Poder Judiciário.

8.2 Documentação Obrigatória

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

- AUTORIZAÇÃO de que trata o item 5;
- Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE;
- CPF;
- Demais requisitos determinados pela ICP-Brasil.

8.3 Requisitos específicos dos certificados ***Cert*-JUS Institucional**

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

8.3.1 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= CNPJ da AR onde ocorreu a identificação presencial
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*><:><*#########*>

- Os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres "<" e ">" não devem ser incluídos.
- Os caracteres "#" representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.
- 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.
- Os dados necessários para preenchimento do DN deverão ser os informados na AUTORIZAÇÃO de que trata o item 5.
- Todos os campos do DN são obrigatórios e devem ser preenchidos.
- No campo CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura
- A informação <*Cargo do Titular*> deverá ser preenchido **SOMENTE** com uma das seguintes opções:
- MAGISTRADO;
- SERVIDOR;
- PRESTADOR DE SERVIÇO; ou
- ESTAGIÁRIO.

Exemplo de um DN do Cert-JUS Intitucional:
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= CNPJ da AR onde ocorreu a identificação presencial
OU = Cert-JUS Institucional – A3
OU = Tribunal Regional Federal da 1a Região - TRF1
OU = Servidor
CN = Jose da Silva Valenca:TR1123456

_____

8.3.2 Campos obrigatórios nas Extensões do certificado

SubjectAlternativeName

Nesta extensão o campo *otherName* com OID 2.16.76.1.3.1 deverá conter obrigatoriamente as informações Data de Nascimento, CPF e RG do titular.

Quando o <nome de login> for informado na AUTORIZAÇÃO de que trata o item 5, deve-se incluir um campo *otherName*, com OID=1.3.6.1.4.1.311.20.2.3, contendo *User Principal Name (UPN)* na forma usuário@domínio_institucional.

O preenchimento dos demais campos definidos no DOC-ICP-04 da ICP-Brasil são opcionais.

Extended Key Usage (extendedKeyUsage)

Além dos campos *id-kp-clientAuth "client authentication"* (OID=1.3.6.1.5.5.7.3.2) e *id-kp-emailProtection "E-mail protection"* (OID=1.3.6.1.5.5.7.3.4). Pode ainda, conter um campo *"SmartCardLogon"* (OID= 1.3.6.1.4.1.311.20.2.2) sempre que for solicitado e o *UPN* for fornecido.

9 Leiaute do Certificado *Cert*-JUS Magistrado (novo)

O certificado digital ***Cert*-JUS** Magistrado deve ser, preferencialmente, do tipo A3 ou superior e destina-se exclusivamente a Magistrados.

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

- o certificado esteja associado a um único dispositivo.
- o par de chaves criptográfica e a requisição de certificado devem ser gerados no dispositivo associado.
- o software de geração e gerenciamento das chaves privadas, instalado no dispositivo, não deve permitir a exportação da chave privada.
- 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".
- a AC deve se certificar de que o dispositivo utilizado não esteja em modo "*root*", "*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 a qualquer outro aplicativo além do próprio aplicativo móvel utilizado para geração das chaves.

Para os certificados A3 ou superior, deverá ser utilizado dispositivo criptográfico para a geração do par de chaves criptográficas e armazenamento da chave privada e do certificado.

A validade será de, no máximo, 1 ano para Certificados A1 e 3 anos para Certificados A3 e A4.

9.1 Destinação

Os certificados digitais ***Cert*-JUS Magistrado** destinam-se **exclusivamente** aos **MAGISTRADOS** do Poder Judiciário, autorizados pela autoridade competente do seu **atual órgão de atuação** a recebê-

los. Identificam os titulares não só como indivíduos, mas também como Magistrados do Poder Judiciário.

Os certificados digitais ***Cert*-JUS Magistrado** serão utilizados nos atos praticados pelos Magistrados 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.

9.2 Documentação Obrigatória

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

- AUTORIZAÇÃO de que trata o item 5;
- Documento oficial de identidade, passaporte ou Carteira Nacional de Estrangeiro – CNE;
- CPF;
- Demais requisitos determinados pela ICP-Brasil.

9.3 Requisitos específicos dos certificados ***Cert*-JUS *Magistrado***

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

9.3.1 Composição do DN:

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

C = BR, O=ICP-Brasil,
OU = Autoridade Certificadora da Justica – AC-JUS
OU = CNPJ da AR onde ocorreu a identificação presencial
OU = Cert-JUS Magistrado – <A3> ou <A4> <A1 Mobile>
OU =<*Órgão de Lotação do Titular*> = PODER JUDICIÁRIO
OU = <*Cargo do Titular*> = Magistrado

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

- Os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres "<" e ">" não devem ser incluídos.
- Os caracteres "#" representam os dígitos da matrícula do titular **no órgão que autorizou a emissão do certificado**. Todos os outros caracteres devem ser interpretados literalmente.
- Os últimos nove caracteres do campo CN (*Common Name*) devem ser o nº de matrícula do titular no atual órgão de atuação, que autorizou a emissão, completado com caracteres brancos à direita, caso possua tamanho menor do que 9 caracteres.
- **Os dados necessários para preenchimento do DN deverão ser os informados na AUTORIZAÇÃO de que trata o item 5**.
- Todos os campos do DN são obrigatórios e devem ser preenchidos.
- No campo CN, caso o nome completo do titular exceda os 54 caracteres, deverá ser escrito até o limite de 54 caracteres, vedada a abreviatura
- A informação <*Cargo do Titular*> deverá ser preenchido **SOMENTE** com a expressão **MAGISTRADO;**

Exemplo de um DN do Cert-JUS Magistrado:

Nome do Magistrado: José da Silva Valença
Matrícula: TR1-123.456,

_____

DN:
C = BR, O = ICP-Brasil,
OU = Autoridade Certificadora da Justica – AC-JUS,
OU= CNPJ da AR onde ocorreu a identificação presencial
OU = Cert-JUS Magistrado – A3
OU = PODER JUDICIARIO
OU = MAGISTRADO
CN = Jose da Silva Valenca:TR1123456

_____

9.3.2 Campos obrigatórios nas Extensões do certificado

SubjectAlternativeName

Nesta extensão o campo *otherName* com OID 2.16.76.1.3.1 deverá conter obrigatoriamente as informações Data de Nascimento, CPF e RG do titular.

Quando o <nome de login> for informado na AUTORIZAÇÃO de que trata o item 5, deve-se incluir um campo *otherName*, com OID=1.3.6.1.4.1.311.20.2.3, contendo *User Principal Name (UPN)* na forma usuário@domínio_institucional.

O preenchimento dos demais campos definidos no DOC-ICP-04 da ICP-Brasil são opcionais.

Extended Key Usage (extendedKeyUsage)

Além dos campos *id-kp-clientAuth "client authentication"* (OID=1.3.6.1.5.5.7.3.2) e *id-kp-emailProtection "E-mail protection"* (OID=1.3.6.1.5.5.7.3.4). Pode ainda, conter um campo *"SmartCardLogon"* (OID= 1.3.6.1.4.1.311.20.2.2) sempre que for solicitado e o *UPN* for fornecido.

10 Leiaute do Certificado *Cert-JUS* Poder Público

O certificado digital ***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:

- o certificado esteja associado a um único dispositivo.
- o par de chaves criptográfica e a requisição de certificado devem ser gerados no dispositivo associado.
- o software de geração e gerenciamento das chaves privadas, instalado no dispositivo, não deve permitir a exportação da chave privada.

- 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”.
- 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 4.

10.1 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.

Os certificados digitais ***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.

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.

10.2 Documentação Obrigatória

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

- AUTORIZAÇÃO de que trata o item 5;
- CPF;
- Demais requisitos determinados pela ICP-Brasil

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

Cada órgão autorizado pela AC-JUS a emitir certificados digitais ***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.

10.3 Requisitos do Certificado

10.3.1 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= CNPJ da AR onde ocorreu a identificação presencial
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*><:><##########>

- No formato acima, os caracteres "<" e ">" delimitam campos que serão substituídos pelos seus respectivos valores; os caracteres "<" e ">" não devem ser incluídos.
- Os caracteres "#" representam os dígitos da matrícula do titular. Todos os outros caracteres devem ser interpretados literalmente.
- 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.
- Os dados necessários para preenchimento do DN serão os informados na AUTORIZAÇÃO**.**
- Todos os campos do DN são obrigatórios e devem ser preenchidos.
- O nome e sigla do órgão deverão ser aquelas constantes da comunicação de cadastramento encaminhada pela AC-JUS à AC emitente.
- 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 do Cert-JUS Poder Público:
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= CNPJ da AR onde ocorreu a identificação presencial
OU = Cert-JUS Poder Público – A3
OU = Ministerio Publico do DF e Territorios -MPDFT
OU = PROCURADOR
CN = Antonio Jose da Silva:MPDF12345

_____

10.3.2 Campos obrigatórios nas Extensões do certificado

SubjectAlternativeName

Nesta extensão o campo *otherName* com OID 2.16.76.1.3.1 deverá conter obrigatoriamente as informações Data de Nascimento, CPF e RG do titular.

Quando o <nome de login> for informado na AUTORIZAÇÃO de que trata o item 5, deve-se incluir um campo *otherName*, com OID=1.3.6.1.4.1.311.20.2.3, contendo *User Principal Name (UPN)* na forma usuário@domínio_institucional.

O preenchimento dos demais campos definidos no DOC-ICP-04 da ICP-Brasil são opcionais.

Extended Key Usage (extendedKeyUsage)

Além dos campos *id-kp-clientAuth "client authentication"* (OID=1.3.6.1.5.5.7.3.2) e *id-kp-emailProtection "E-mail protection"* (OID=1.3.6.1.5.5.7.3.4), pode conter um campo *"SmartCardLogon"* (OID= 1.3.6.1.4.1.311.20.2.2) sempre que for solicitado e o UPN for fornecido.

11 Leiaute do Certificado *Cert-JUS* Equipamento Servidor (Monodomínio, Multidomínio e wildcard)

11.1 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, 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.

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

O titular do certificado digital ***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.

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

O certificado ***Cert*-JUS Equipamento Servidor** poderá ser do tipo *monodomínio*, *multidomínio* ou *wildcard* (curinga) exceto para certificados de resposta OCSP.

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

O certificado ***Cert*-JUS Equipamento Servidor** do tipo *wildcard* **não poderá** endereçar mais do que um domínio (tipo misto multidomínio/wildcard).

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 Autorizaçãoe o Cadastramento de que tratam os itens 4 e 5.

11.2 Documentação Obrigatória

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

- **AUTORIZAÇÃO** de que trata o item 5.
- CPF da autoridade competente do órgão solicitante e do responsável pelo certificado.
- Comprovação de registro dos domínios pela instituição solicitante.
- Aplicam-se as exigências documentais e procedimentais dos DOC ICP 05 e 04.

11.3 Requisitos do Certificado

11.3.1 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= CNPJ da AR onde ocorreu a identificação presencial
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> ou *.<nome_de_domínio>(para wildcard)

No perfil acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os “<” e “>” não devem ser incluídos.

- 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, no caso de certificado monodomínio.
- 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*.
- Para certificados *wildcard* o CN será da forma *.<nome do domínio>

Os dados necessários para preenchimento do DN deverão ser obtidos na **AUTORIZAÇÃO** de emissão do certificado, descrita no item 5, inclusive a relação de todas as *url* endereçadas pelo certificado, exceto para certificados *wildcard*, que conterá apenas o nome do domínio em que será utilizado.

A lista contendo os nomes dos órgãos autorizados 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= CNPJ da AR onde ocorreu a identificação presencial
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

_____

11.3.2 Extensões Obrigatórias

SubjectAlternativeName

Campos obrigatórios:

- nome empresarial presente no OID 2.16.76.1.3.8
- número do CNPJ presente no OID 2.16.76.1.3.3
- nome do responsável pelo certificado presente no OID 2.16.76.1.3.2
- data de nascimento e número do Cadastro de Pessoas Físicas (CPF) do responsável presente no OID 2.16.76.1.3.4
- e-mail do responsável presente no OID= 2.5.29.17.1 - *rfc822Name*.
  Este campo deve conter o endereço de e-mail institucional do responsável pelo certificado OU endereço de e-mail da unidade organizacional em que o responsável pelo certificado está lotado.

Para Certificados MULTIDOMÍNIO

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

Para Certificados WildCard

Campo *DnsName* contendo *.<nome_de_dominio> e *DnsName* contendo <nome_de_domínio>

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

ExtKeyUsage

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.

12 Leiaute do Certificado *Cert-JUS* Código Seguro

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

12.1 Destinação

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.

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.

O titular do ***Cert*-JUS Código Seguro** será sempre um órgão do Poder Judiciário ou da Administração Pública direta e indireta e o responsável pelo certificado deverá ser, obrigatoriamente, servidor público, indicado e autorizado pela autoridade competente.

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

12.2 Documentação Obrigatória

Além dos documentos constantes no DOC-ICP-05, para emissão de certificados digitais ***Cert*-JUS Código Seguro** são obrigatórios:

- AUTORIZAÇÃO de que trata o item 5.
- CPF da autoridade competente do órgão solicitante e do responsável pelo certificado.

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.

12.2.1 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 Justica – AC-JUS
OU= CNPJ da AR onde ocorreu a identificação presencial
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.

No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os “<” e “>” não devem ser incluídos.

O CN (*Common Name*) deve conter a nome do órgão constante do CNPJ.

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.

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

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

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= CNPJ da AR onde ocorreu a identificação presencial
OU=Cert-JUS Codigo Seguro – A1
OU=DESIN - Secretaria de Desenvolvimento de Sistemas
CN=CONSELHO DA JUSTICA FEDERAL
ST= DF

_____

12.3 Extensões Obrigatórias

SubjectAlternativeName

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

OID= 2.16.76.1.3.3 e conteúdo = Número do CNPJ;

OID= 2.16.76.1.3.2 e conteúdo = nome do responsável pelo certificado;

OID= 2.16.76.1.3.4 e conteúdo = a data de nascimento do responsável, o Cadastro de Pessoas Físicas (CPF) do responsável, são obrigatórios;

Deverá conter também campo *rfc822Name*, obrigatório, com endereço de e-mail institucional do responsável pelo certificado. Poderá ser utilizado o e-mail da unidade organizacional responsável pelo certificado.

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.

13 Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS

13.1 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 demais requisitos definidos pela ICp-Brasil

13.1.1 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 de certificado> <identificador de versão>
No formato acima, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores; os “<” e “>” não devem ser incluídos.

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

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.

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.

O traço (hífen) antes da expressão JUS é obrigatório. Exemplo: AC EXEMPLO-JUS SSL v5

Exemplo de DN:

_____

C=BR, O=ICP-Brasil,
OU=Autoridade Certificadora da Justiça – AC-JUS
OU= SSL
CN=AC Exemplo-JUS SSL v5

_____

13.2 Extensões Obrigatórias

De acordo com as normas ICP-Brasil.