



LEIAUTE DOS CERTIFICADOS DIGITAIS CERT-JUS

Versão 8.0

NOVEMBRO DE 2020
AUTORIDADE CERTIFICADORA DA JUSTIÇA – AC-JUS

Sumário

1	Apresentação	2
2	Considerações Gerais	2
3	Denominação	3
4	Cadastramento de Órgãos não pertencentes ao Poder Judiciário.	3
5	Autorização	4
6	Revogação	4
7	Requisitos Comuns dos Certificados <i>Cert-JUS</i>	5
8	Leiaute do Certificado <i>Cert-JUS</i> Institucional	5
9	Leiaute do Certificado <i>Cert-JUS</i> Magistrado	7
10	Leiaute do Certificado <i>Cert-JUS</i> Poder Público	9
11	Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS (até 2018)	12
12	Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS (após 2018)	13

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-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 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 SSL/TL, Codesigning, 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.

Para certificados digitais emitidos para Magistrados, não se faz necessária a revogação em caso de mudança de jurisdição ou atuação em outro órgão.

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*) e os requisitos definidos pela ICP-Brasil.

8 Leiaute do Certificado *Cert-JUS* Institucional

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

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 admitida a modalidade de certificado em nuvem.

A validade de certificados será de no máximo 3 anos.

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 NÃO PODERÃO mais ser emitidos para MAGISTRADOS do Poder Judiciário a partir de 1º de Janeiro de 2021.

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 que realizou a identificação presencial; ou CNPJ da AR cujo AGR operou videoconferência para emissão do certificado; ou, ainda, a expressão "Renovação Eletrônica", para os casos de renovação online com certificado digital válido

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

OU= <outras OU implementadas pela ICP-Brasil

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

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 pelo órgão 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:
 - SERVIDOR;
 - PRESTADOR DE SERVIÇO; ou
 - ESTAGIÁRIO.

Exemplo de um DN do Cert-JUS Institucional:

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= CNPJ da AR onde ocorreu a identificação presencial

OU= 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*

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

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, admitida a modalidade de certificado em nuvem

A validade será de, no máximo, 5 anos.

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 que realizou a identificação

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

OU= <outras OU implementadas pela ICP-Brasil

OU = Cert-JUS Magistrado – <A3>

OU =<Órgão de Lotação do Titular> = PODER JUDICIARIO

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 pelo órgão 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**;
- A informação <Orgão de Lotação do Titular> conterà sempre a expressão **Poder Judiciario**

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

OU= 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.

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 5 anos.

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 que realizou a identificação

OU = Tipo de identificação utilizada (presencial, videoconferência ou certificado digital)

OU= <outras OU implementadas pela ICP-Brasil

OU = Cert-JUS Poder Público – <A3>

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 pelo órgão na AUTORIZAÇÃO.
- Todos os campos do DN são obrigatórios e devem ser preenchidos.
- O nome e sigla do órgão deverão ser aquelas constantes na Lista de órgãos autorizados publicadas no site da AC-JUS.
- 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;

OU = Identificação por videoconferencia

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 das Autoridades Certificadoras Subsequentes à AC-JUS (até 2018)

11.1 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

11.1.1 Composição do DN:

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

C=BR

O=ICP-Brasil,

OU=Autoridade Certificadora da Justiça – 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= SMIME
CN=AC Exemplo-JUS v5

11.2 Extensões Obrigatórias

De acordo com as normas ICP-Brasil.

12 Leiaute do Certificado das Autoridades Certificadoras Subsequentes à AC-JUS (após 2018)

12.1 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. Na cadeia AC-JUS serão emitidos somente certificados S/MIME.

12.1.1 Composição do DN:

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

C=BR
O=ICP-Brasil,
OU=Autoridade Certificadora da Justiça – AC-JUS,
CN=AC <Nome da Autoridade Certificadora Subsequente> <->JUS <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 <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 de versão da cadeia.

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

Exemplo de DN:

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

12.2 Extensões Obrigatórias

De acordo com as normas ICP-Brasil.