# Política de Certificado de Assinatura Tipo A3

## PC A3 - AC LINK CD

## OID 2.16.76.1.2.3.80

**Versão 4.0**

**Abril de 2021**

# AC LINK CD
# POLÍTICA DE CERTIFICADO DE ASSINATURA - TIPO A3

## SUMÁRIO

## CONTROLE DE ALTERAÇÕES

| Resolução que aprovou a alteração | Itens alterados | Versão | Data |
|---|---|---|---|
| N/A | - | 1.0 | 14/09/2018 |
| Resolução 151, de 30/05/2019 que aprova a versão 7.0 do DOC-ICP-04 | Diversos | 2.0 | 09/08/2019 |
| Solicitado pelo ITI | 1.1.3, 1.1.4, 1.1.5, 1.4.1.4, 1.5.4, 6.8, 7, 7.1.2.2, 7.1.2.3 a.2) e a.4), 7.1.2.7, 7.1.3, 7.1.4, 10.1 | 3.0 | 31/07/2020 |
| Resolução 156 de 17/02/2020 | 7.1.2.3.a.2), 7.1.2.4.d | | |
| Resolução 169 de 17/04/2020 | 7.1.4.1 | | |
| - | 1.3.2.1, 1.3.5, 1.4.1.8, 1.5.1, 1.5.4, 3.2, 6.1.1.2, 6.1.1.4, 6.1.1.6, 6.1.1.7, 6.1.3, 6.1.4, 6.2, 6.2.1, 6.2.3, 6.2.4.2, 6.2.6, 6.2.9, 6.2.10, 6.4, 6.4.1, 6.4.2, 6.5.1, 6.6.1, 6.6.2, 6.6.3, 7.1.2.3 b1) nota, 7.1.2.4 nota, 7.3.1, 7.3.2, 9.12.1 | | |
| Resolução CG ICP-Brasil nº 179, de 20/10/2020. Aprova a versão 8.0 do DOC-ICP-04. | 1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7, 1.1.11, 1.1.12, 1.3.2.1 “b”, 1.6, 6.1.1.3, 6.1.1.4, Tabela 2, 6.1.4 “a”, 6.1.5.2, 6.1.6, 6.2.4.3,6.4.2”e”, 7.1.2.3 “a.2”, 7.1.2.4 “c”, 7.1.4.1, Nota 2, 9.17, 10.1, 10.2, 11 | 4.0 | 28/04/2021 |

# 1 INTRODUÇÃO

## *1.1 VISÃO GERAL*

O documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1] estabelece requisitos mínimos a serem obrigatoriamente observados pelas Autoridades Certificadoras (AC), integrantes da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), na elaboração de suas Políticas de Certificado (PC).

1.1.2 Esta Política de Certificado de Assinatura Digital tipo A3 da AC Link CD, a seguir designada simplesmente por "PC A3 da AC Link CD" adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [1].

1.1.3 A estrutura desta PC está baseada na RFC 3647.

1.1.4 Este documento compõe o conjunto da ICP-Brasil e nele são referenciados outros regulamentos dispostos nas demais normas da ICP-Brasil, conforme especificado no item 10.

1.1.5 O tipo de certificado de assinatura digital emitido sob essa PC é o Tipo A3.

1.1.6 Os certificados A3 de assinatura estão associados aos requisitos mais rigorosos de segurança.

1.1.7 Os certificados A3 de assinatura podem ser emitidos para pessoas físicas ou jurídicas.

1.1.8 Não se aplica.

1.1.9 Não se aplica.

1.1.10 Não se aplica.

1.1.11 Não se aplica.

1.1.12 Não se aplica.

## *1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO*

1.2.1 Esta Política de Certificado de Assinatura Digital é do tipo A3 da Autoridade Certificadora Link CD. O *Object Identifier* - OID da PC A3 da AC Link CD, atribuído para esta PC, após processo de credenciamento da AC junto à ICP-Brasil, é **2.16.76.1.2.3.80**.

1.2.2 Não se aplica.

## *1.3 PARTICIPANTES DA ICP-BRASIL*

### 1.3.1 AUTORIDADES CERTIFICADORAS

1.3.1.1 Esta PC se refere à AC Link CD, integrante da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil), sob a hierarquia da Autoridade Certificadora Safeweb (AC Safeweb), que por sua vez está subordinada hierarquicamente à Autoridade Certificadora Raiz Brasileira (AC Raiz).

1.3.1.2 As práticas e procedimentos de certificação da AC Link CD estão descritos na Declaração de Práticas de Certificação da AC Link CD (DPC - AC Link CD).

### 1.3.2 AUTORIDADES DE REGISTRO

1.3.2.1 Os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes são de competência das Autoridades de Registro (AR). As ARs vinculadas à AC Link CD, estão relacionadas na página: https://www.linkcertificacao.com.br/suporte/repositorio/ que contém:

a) Relação de todas as ARs credenciadas;

b) Relação de ARs que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

### 1.3.3 TITULARES DO CERTIFICADO

Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem ser titulares de certificado.

### 1.3.4 PARTES CONFIÁVEIS

Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital e chaves emitidas pela ICP-Brasil.

### 1.3.5 OUTROS PARTICIPANTES

A relação de todos os Prestadores de Serviços de Suporte (PSS), Prestadores de Serviços Biométricos (PSBios) e Prestadores de Serviço de Confiança (PSC), vinculados à AC Link CD estão relacionados na página https://www.linkcertificacao.com.br/suporte/repositorio/.

## *1.4 USABILIDADE DO CERTIFICADO*

### 1.4.1 USO APROPRIADO DO CERTIFICADO

1.4.1.1 Os certificados definidos por esta Política de Certificado têm sua utilização vinculada à assinatura digital, não repúdio, garantia de integridade da informação e autenticação de seu titular.

1.4.1.2 As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou superior, emitido por qualquer AC credenciada pela AC Raiz.

1.4.1.3 Na definição das aplicações para o certificado definido pela PC, a AC Link CD leva em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, frequência de emissão da correspondente Lista de Certificados Revogados - LCR e extensão do período de validade do certificado.

1.4.1.4 Certificados de tipo A3 emitidos pela AC Link CD são utilizados em aplicações como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

1.4.1.5 Não se aplica.

1.4.1.6 Não se aplica.

1.4.1.7 Não se aplica.

1.4.1.8 Não se aplica.

### 1.4.2 USO PROIBITIVO DO CERTIFICADO

Não se aplica**.**

## *1.5 POLÍTICA DE ADMINISTRAÇÃO*

### 1.5.1 ORGANIZAÇÃO ADMINISTRATIVA DO DOCUMENTO

Nome da AC: AC Link CD

### 1.5.2 CONTATOS

**Endereço:** Rua Visconde de Taunay, 173, sala 202 - São Lucas - 30.240.300 - Belo Horizonte/MG
**Página web:** www.linkcertificacao.com.br
**Telefone:** +55 31 3327 6670 | +55 31 3244 4800
**E-mail:** compliance@linkcertificacao.com.br
**Outros:** Setor de Compliance

### 1.5.3 PESSOA QUE DETERMINA A ADEQUABILIDADE DA DPC COM A PC

**Nome:** Mariana Borges
**Telefone:** +55 31 3327 6670 | +55 31 3244 4800
**E-mail:** compliance@linkcertificacao.com.br

**Outros:** Setor de Compliance

### 1.5.4 PROCEDIMENTOS DE APROVAÇÃO DA PC

Esta PC é aprovada pela AC Link e pelo ITI. Os procedimentos de aprovação da PC da AC Link CD são estabelecidos a critério do CG da ICP-Brasil.

## *1.6 DEFINIÇÕES E ACRÔNIMOS*

| SIGLA | DESCRIÇÃO |
|---|---|
| AC | Autoridade Certificadora |
| AC Raiz | Autoridade Certificadora Raiz da ICP-Brasil |
| ACT | Autoridade de Carimbo do Tempo |
| AR | Autoridades de Registro |
| CEI | Cadastro Específico do INSS |
| CF-e | Cupom Fiscal Eletrônico |
| CG ICP-Brasil | Comitê Gestor |
| *CMM-SEI* | *Capability Maturity Model do Software Engineering Institute* |
| *CMVP* | *Cryptographic Module Validation Program* |
| CN | *Common Name* |
| CNPJ | Cadastro Nacional de Pessoa Jurídica |
| CONFAZ | Conselho Nacional de Política Fazendária |
| CPF | Cadastro de Pessoas Físicas |
| CS | *Code Signing* |
| DMZ | Zona Desmilitarizada |
| DN | *Distinguished Name* |
| DPC | Declaração de Práticas de Certificação |
| EV | *Extended Validation* |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IDS | *Intrusion Detection System* |
| IEC | *International Electrotechnical Commission* |
| INMETRO | Instituto Nacional de Metrologia, Qualidade e Tecnologia |
| 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 |
| OCSP | *Online Certificate Status Protocol* |
| OID | *Object Identifier* |
| OM-BR | Objetos Metrológicos ICP-Brasil |
| OU | *Organization Unit* |

| | |
|---|---|
| PASEP | Programa de Formação do Patrimônio do Servidor Público |
| PC | Políticas de Certificado |
| PCN | Plano de Continuidade de Negócio |
| PIS | Programa de Integração Social |
| PS | Política de Segurança |
| PSS | Prestadores de Serviço de Suporte |
| RFC | *Request For Comments* |
| RG | Registro Geral |
| SAT | Sistema de Autenticação e Transmissão |
| SSL | *Secure Socket Layer* |
| TSDM | *Trusted Software Development Methodology* |
| UF | Unidade de Federação |
| URL | *Uniform Resource Locator* |

## 2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

Os itens seguintes estão referidos em seus correspondentes na DPC – AC Link CD.

### *2.1 REPOSITÓRIOS*

### *2.2 PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS*

### *2.3 TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO*

### *2.4 CONTROLE DE ACESSO AOS REPOSITÓRIOS*

## 3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão referidos em seus correspondentes na DPC – AC Link CD.

### *3.1 NOMEAÇÃO*

3.1.1 Tipos de nomes

3.1.2 Necessidade dos nomes serem significativos

3.1.3 Anonimato ou Pseudônimo dos Titulares do Certificado

3.1.4 Regras para interpretação de vários tipos de nomes

3.1.5 Unicidade de nomes

3.1.6 Procedimento para resolver disputa de nomes

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

### *3.2 VALIDAÇÃO INICIAL DE IDENTIDADE*

3.2.1 Método para comprovar a posse de chave privada

3.2.2 Autenticação da identificação da organização

3.2.3 Autenticação da identidade de um indivíduo

3.2.4 Informações não verificadas do titular do certificado

3.2.5 Validação das autoridades

3.2.6 Critérios para interoperação

3.2.7 Autenticação da identidade de equipamento ou aplicação

3.2.8 Procedimentos complementares

3.2.9 Procedimentos específicos

### *3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES*

3.3.1 Identificação e autenticação para rotina de novas chaves

3.3.2 Identificação e autenticação para novas chaves após a revogação

### *3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO*

## 4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Os itens seguintes estão referidos em seus correspondentes na DPC – AC Link CD.

### *4.1 SOLICITAÇÃO DO CERTIFICADO*

4.1.1 Quem pode submeter uma solicitação de certificado

4.1.2 Processo de registro e responsabilidades

### *4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO*

4.2.1 Execução das funções de identificação e autenticação

4.2.2 Aprovação ou rejeição de pedidos de certificado

4.2.3 Tempo para processar a solicitação de certificado

### *4.8 MODIFICAÇÃO DE CERTIFICADO*

4.8.1 Circunstâncias para modificação de certificado

4.8.2 Quem pode requisitar a modificação de certificado

4.8.3 Processamento de requisição de modificação de certificado

4.8.4 Notificação de emissão de novo certificado para o titular

4.8.5 Conduta constituindo a aceitação de uma modificação de certificado

4.8.6 Publicação de uma modificação de certificado pela AC

4.8.7 Notificação de uma emissão de certificado pela AC para outras entidades

### *4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO*

4.9.1 Circunstâncias para revogação

4.9.2 Quem pode solicitar revogação

4.9.3 Procedimento para solicitação de revogação

4.9.4 Prazo para solicitação de revogação

4.9.5 Tempo em que a AC deve processar o pedido de revogação

4.9.6 Requisitos de verificação de revogação para as partes confiáveis

4.9.7 Frequência de emissão de LCR

4.9.8 Latência máxima para a LCR

4.9.9 Disponibilidade para revogação/verificação de status on-line

4.9.10 Requisitos para verificação de revogação on-line

4.9.11 Outras formas disponíveis para divulgação de revogação

4.9.12 Requisitos especiais para o caso de comprometimento de chave

4.9.13 Circunstâncias para suspensão

4.9.14 Quem pode solicitar suspensão

4.9.15 Procedimento para solicitação de suspensão

4.9.16 Limites no período de suspensão

### *4.10 SERVIÇOS DE STATUS DE CERTIFICADO*

4.10.1 Características operacionais

### *5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE*

5.7.2 Recursos computacionais, *software*, e/ou dados corrompidos

5.7.3 Procedimentos no caso de comprometimento de chave privada de entidade

5.7.4 Capacidade de continuidade de negócio após desastre

### *5.8 EXTINÇÃO DA AC*

## 6 CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a PC define as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo esta PC. São também definidos outros controles técnicos de segurança utilizados pela AC Link CD e pelas ARs vinculadas na execução de suas funções operacionais.

### *6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES*

### 6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 Quando o titular de certificado é uma pessoa física, esta é a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado é uma pessoa jurídica, esta indica por seu(s) representante(s) legal(is), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

6.1.1.1.1 Não se aplica.

6.1.1.1.2. Não se aplica.

6.1.1.2 O processo de geração de chaves do tipo A3, contemplado nesta PC, exige:

a) A geração do par de chaves ocorre em cartão inteligente, token ou HSM com certificação INMETRO, protegidos por senha;

b) O responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado deve executar pessoalmente a geração dos pares de chaves criptográficas.

6.1.1.3 O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados é o RSA, conforme definido no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.1.4 Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, no meio de armazenamento

definido para cada tipo de certificado previsto pela ICP-Brasil, em hardware criptográfico, homologado junto à ICP-Brasil e com certificação INMETRO, conforme Tabela 2 a seguir.

6.1.1.5 A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e o repositório utilizado para o seu armazenamento.

6.1.1.6 A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada é única e seu sigilo é suficientemente assegurado;

b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7 A mídia de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8 O armazenamento de chaves privadas de terceiros em hardware criptográfico só poderá ser realizada por entidade credenciada como PSC, nos termos do documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL [3], ou no caso de soluções corporativas de armazenamento de chaves privadas de funcionários, em HSM de propriedade da instituição, mediante o conhecimento e concordância expressa do titular do certificado com a DPC da AC Link CD, que atendam as aplicações demandadas das organizações, com acesso exclusivo por meio da rede interna.

**Tabela 2 – Mídias Armazenadoras de Chaves Criptográficas**

| Tipo de Certificado | Mídia Armazenadora de Chave Criptográfica |
|---|---|
| A3 | Hardware criptográfico, homologado junto à ICP-Brasil e com certificação INMETRO. |

### 6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE

Não se aplica.

### 6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

A entrega da chave pública do solicitante do certificado, é feita por meio eletrônico, em formato PKCS#10, através de uma sessão segura SSL *Secure Socket Layer*.

### 6.1.4 ENTREGA DE CHAVE PÚBLICA DA AC LINK RFB ÀS TERCEIRAS PARTES

As formas para a disponibilização do certificado da AC Link CD, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

a) No momento da disponibilização de um certificado para seu titular, usando formato definido no DOC ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil;

b) Diretório;

c) Página Web da AC Link CD www.linkcertificacao.com.br/;

d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil;

e) Repositório da ICP-Brasil.

### 6.1.5 TAMANHOS DE CHAVE

6.1.5.1. O tamanho mínimo das chaves criptográficas associadas aos certificados da AC Link CD é de RSA 2048 bits para a hierarquia V5, conforme definido no DOC-ICP-01.01.

6.1.5.2. Os algoritmos e o tamanho de chaves criptográficas utilizados no certificado Tipo A3 da ICP-Brasil estão definidos no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

### 6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS E VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados atendem ao estabelecido no DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil.

### 6.1.7 PROPÓSITOS DE USO DE CHAVE (CONFORME CAMPO *"KEY USAGE"* NA X.509 V3)

Os pares de chaves correspondentes aos certificados emitidos pela AC Link CD podem ser utilizados para a assinatura digital (chave privada), para a verificação dela (chave pública), para a garantia do não repúdio e para cifragem de chaves. Para isso, os certificados emitidos segundo esta PC têm ativados os bits *digitalSignature, nonRepudiation* e *keyEncipherment.*

## *6.2 PROTEÇÃO DE CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO*

O repositório de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

a) A chave privada é única e seu sigilo é suficientemente assegurado;

b) A chave privada não pode, com uma segurança razoável, ser deduzida e é protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) A chave privada é eficazmente protegida pelo legítimo titular contra a utilização por terceiros, pois é gerada em cartão, token ou HSM com certificação INMETRO. Esses módulos criptográficos não permitem a exportação da chave privada e exigem senha para a sua utilização.

### 6.2.1 PADRÕES E CONTROLE PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1 O módulo criptográfico utilizado na geração e utilização de chaves criptográficas possui certificação INMETRO.

6.2.1.2 Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da entidade titular de certificado seguem os padrões definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

### 6.2.2 CONTROLE "N de M" PARA CHAVE PRIVADA

Não se aplica.

### 6.2.3 CUSTÓDIA (ESCROW) DE CHAVE PRIVADA

6.2.3.1 O agente de custódia (escrow) dos certificados emitidos pela AC Link CD, é o PSC Safeweb. As chaves privadas são armazenadas criptografadas em partições exclusivas em *hardware* criptográfico certificado pelo INMETRO. Estas chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e *push notification*).

6.2.3.2 A AC Link CD não implementa a recuperação de chaves privadas.

### 6.2.4 CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

6.2.4.1 Como diretriz geral, qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC Link CD não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, no entanto em casos em que o CD é emitido utilizando o PSC Safeweb, a guarda da cópia da chave privada é realizada pelo próprio PSC.

6.2.4.3 Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico aprovado pelo DOC-ICP-01.01, regulamento editado por instrução normativa da AC Raiz que define os padrões e algoritmos criptográficos da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.4.4 Através das tecnologias atualmente disponíveis, a entidade titular de certificado deve realizar a geração de cópia de segurança de sua chave privada.

### 6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 As chaves privadas das entidades titulares de certificados emitidos por esta PC não são arquivadas.

6.2.5.2 Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

### 6.2.6 INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

A AC Link CD gera os pares de chaves diretamente, sem inserções, em módulos de *hardware* criptográfico onde as chaves serão utilizadas.

### 6.2.7 ARMAZENAMENTO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

Ver item 6.1.

### 6.2.8 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

A chave privada é ativada, mediante senha solicitada pelo *software* de proteção da chave privada. A senha deve ser criada e mantida apenas pelo titular do certificado, sendo para seu uso e conhecimento exclusivo. O titular de certificado deverá adotar senha de proteção da chave privada, sendo recomendável que as senhas sejam alteradas no mínimo a cada 03 (três) meses.

### 6.2.9 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

A desativação da chave privada ocorre em função da expiração do certificado correspondente ou em função de sua revogação.

### 6.2.10 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

Para destruição da chave privada de certificados emitidos conforme esta PC, é preciso que o usuário acesse o software de proteção da chave privada, localize o certificado e o remova do repositório. A destruição da chave privada é irreversível e definitiva, não sendo mais possível a sua recuperação.

## *6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES*

### 6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

As chaves públicas da AC Link CD, dos titulares de certificados de assinatura digital e as LCRs por ela emitidas permanecem armazenadas após a expiração dos certificados correspondentes permanentemente para verificação de assinaturas geradas durante seu período de validade.

### 6.3.2 PERÍODOS DE OPERAÇÃO DO CERTIFICADO E PERÍODOS DE USO PARA AS CHAVES PÚBLICAS E PRIVADA

6.3.2.1 As chaves privadas dos respectivos titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Não se aplica.

6.3.2.3 O período máximo de uso das chaves correspondentes aos certificados emitidos pela PC A3 da AC Link CD é de 5 (cinco) anos.

6.3.2.4 Não se aplica.

6.3.2.5 Não se aplica.

## *6.4 DADOS DE ATIVAÇÃO*

Nos itens seguintes desta PC estão descritos os requisitos de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

### 6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

Os certificados emitidos conforme esta PC, se utilizam de *hardwares* criptográficos para manter a segurança de suas chaves privadas. Estes *hardwares* possuem certificação INMETRO e protegem as chaves privadas armazenando-as em partições exclusivas para este fim, com acesso restrito apenas através da utilização de senha criada pelo próprio titular, não necessitando de outros

dados de ativação para sua operação. Em casos de emissão através de PSC, as chaves estão acessíveis apenas a seus titulares através de duplo fator de autenticação (senha e *push notification*).

### 6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

Conforme descrito no item 6.4.1, os certificados emitidos conforme esta PC, não necessitam de outros dados de ativação para sua operação além da própria senha criada pelo titular e da posse do *hardware* criptográfico. Para uma maior proteção, os *hardwares* possuem a capacidade de bloquear o acesso à chave privada caso a quantidade de tentativas de utilização com a senha errada exceda o limite pré-definido. A AC Link CD recomenda:

a) Nunca fornecer senha a terceiros;

b) Escolher senhas de 8 ou mais caracteres;

c) Definir senhas com caracteres numéricos e alfanuméricos;

d) Memorizar a senha; e

e) Não a escrever.

### 6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

Não se aplica.

## *6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL*

### 6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

Nos equipamentos onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Link CD, recomenda-se o uso de mecanismos mínimos que garantam a segurança computacional, tais como:

a) Senha de *bios* ativada;

b) Controle de acesso lógico ao sistema operacional;

c) Exigência de uso de senhas fortes;

d) Diretivas de senha e de bloqueio de conta;

e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;

f) *Firewall* pessoal ou corporativo ativado, com permissões de acesso mínimas necessárias às atividades;

g) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches, hotfix*, etc.);

h) Proteção de tela acionada no máximo após 02 (dois) minutos de inatividade e exigindo senha do usuário para desbloqueio.

### 6.5.2 CLASSIFICAÇÃO DE SEGURANÇA COMPUTACIONAL

Não se aplica.

## *6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA*

### 6.6.1 CONTROLES DE DESENVOLVIMENTO DO SISTEMA

Como descrito no item correspondente da DPC AC Link CD.

### 6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

Como descrito no item correspondente da DPC AC Link CD.

### 6.6.3 CONTROLES DE SEGURANÇA DE CICLO DE VIDA

Como descrito no item correspondente da DPC AC Link CD.

### 6.6.4 CONTROLES NA GERAÇÃO DE LCR

Antes de publicadas, todas as LCRs geradas pela AC Link CD são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

## *6.7 CONTROLES DE SEGURANÇA DE REDE*

Não se aplica.

## *6.8 CARIMBO DO TEMPO*

Não se aplica.

# 7 PERFIS DE CERTIFICADO, LCR E OCSP

Os itens seguintes especificam os formatos dos certificados e das LCRs gerados segundo esta PC. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões. Os

requisitos mínimos estabelecidos nos itens seguintes são atendidos em todos os tipos de certificados admitidos no âmbito da ICP-Brasil.

### *7.1 PERFIL DO CERTIFICADO*

Os certificados emitidos pela AC Link CD, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

#### 7.1.1 NÚMERO DE VERSÃO

Os certificados emitidos pela AC Link CD, segundo esta PC, implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

#### 7.1.2 EXTENSÕES DE CERTIFICADO

7.1.2.1 Neste item, a PC descreve todas as extensões de certificado utilizadas e sua criticalidade.

7.1.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões:

a) **"*Authority Key Identifier*", não crítica:** o campo *keyIdentifier* contém o hash SHA-1 da chave pública da AC Link CD;

b) **"*Key Usage*", crítica:** configurados conforme disposto no item 7.1.2.7 deste documento;

c) **"*Certificate Policies*", não crítica:**

c.1) O campo *PolicyIdentifier* contém o OID desta PC **2.16.76.1.2.3.80**;

c.2) O campo *PolicyQualifiers* contém o endereço *Web* onde se obtém a DPC da AC Link CD: http://repositorio.linkcertificacao.com.br/ac-linkcd/ac-link-cd-dpc.pdf

d) **"*CRL Distribution Points*", não crítica:** contém o endereço na Web onde se obtém a LCR correspondente:

d.1) http://repositorio.linkcertificacao.com.br/ac-linkcd/lcr-ac-linkcd.crl

d.2) http://repositorio2.linkcertificacao.com.br/ac-linkcd/lcr-ac-linkcd.crl

e) **"*Authority Information Access*", não crítica:** a primeira entrada contém o método de acesso id-ad-caIssuer, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço: http://repositorio.linkcertificacao.com.br/ac-linkcd/ac-linkcd.p7b .

7.1.2.3 A ICP-Brasil define como obrigatória a extensão "*Subject Alternative Name*", não crítica, e com os seguintes formatos:

**a) PARA CERTIFICADOS DE PESSOA FÍSICA**

**a.1)** 3 (três) campos *otherName*, obrigatórios, contendo, nesta ordem:

I. **OID = 2.16.76.1.3.1 e conteúdo:** nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular; nas 11 (onze) posições subsequentes, o Número de Identificação Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do Registro Geral (RG) do titular; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

II. **OID = 2.16.76.1.3.6 e conteúdo:** nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa física titular do certificado.

III. **OID = 2.16.76.1.3.5 e conteúdo:** nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor da pessoa física titular do certificado; nas 3 (três) posições subsequentes, o número correspondente a Zona Eleitoral; nas 4 (quatro) posições seguintes, o número correspondente a Seção; nas 22 (vinte e duas) posições subsequentes, o nome do município e a UF do Título de Eleitor.

**NOTA:** O preenchimento dos campos abaixo, referentes à pessoa física titular do certificado, é obrigatório:

a) Nome;

b) Número de inscrição no CPF;

c) Data de nascimento;

d) E-mail.

**a.2)** Não se aplica.

**a.3)** Não se aplica.

**a.4)** Não se aplica.

**b) PARA CERTIFICADOS DE PESSOA JURÍDICA**

**b.1)** 4 (quatro) campos *otherName*, obrigatórios, contendo, nesta ordem:

I. **OID = 2.16.76.1.3.4 e conteúdo:** nas primeiras 8 (oito) posições, a data de nascimento do responsável pelo certificado, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do responsável; nas 11 (onze) posições subsequentes, o Número de Inscrição Social - NIS (PIS, PASEP ou CI); nas 15 (quinze) posições subsequentes, o número do RG do responsável; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

II. **OID = 2.16.76.1.3.2 e conteúdo:** nome do responsável pelo certificado.

III. **OID = 2.16.76.1.3.3 e conteúdo:** nas 14 (quatorze) posições o número do Cadastro Nacional de Pessoa Jurídica (CNPJ) da pessoa jurídica titular do certificado.

IV. **OID = 2.16.76.1.3.7 e conteúdo:** nas 12 (doze) posições o número do Cadastro Específico do INSS (CEI) da pessoa jurídica titular do certificado.

**NOTA:** Os seguintes campos são de preenchimento obrigatório:

Da empresa:

- Nome Empresarial;
- Número de inscrição no CNPJ.

Do responsável pela pessoa jurídica perante o CNPJ:

- Número de inscrição no CPF;
- Data de nascimento;
- Nome do responsável pela Pessoa Jurídica perante o CNPJ.
- E mail.

**c)** Não se aplica.

**d)** Não se aplica.

**e)** Não se aplica.

7.1.2.4 Os campos *otherName* definidos como obrigatórios pela ICP-Brasil devem estar de acordo com as seguintes especificações:

a) O conjunto de informações definido em cada campo otherName deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

b) Quando os números de CPF, NIS (PIS, PASEP ou CI), RG, CNPJ, CEI, ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG ou o número de inscrição do Título de Eleitor não estiver disponível, não se deve preencher os campos de órgão expedidor e UF ou os campos Zona Eleitoral, Sessão, Município e UF, respectivamente.

d) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente. No caso de múltiplas habilitações profissionais, deverão ser inseridos e preenchidos os campos (OID) correspondentes às identidades profissionais apresentadas;

e) Todas informações de tamanho variável referentes a números, tais como RG ou Título de Eleitor, devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado seu máximo tamanho possível;

f) As 10 (dez) posições das informações sobre órgão expedidor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF do Título de Eleitor;

g) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 7.1.5.2, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;

h) Não se aplica.

**Nota 1:** Para o preenchimento do campo "*Principal Name*" serão permitidos os caracteres de "A" a "Z", de "0" a "9" além dos caracteres "." (ponto), "(hífen) e "@" (arroba), necessários à formação do endereço de login do titular do certificado. Outros caracteres especiais, símbolos, espaços ou acentuação não são permitidos.

**Nota 2:** O campo rfc822Name, parte da extensão obrigatória "*Subject Alternative Name*", contendo o endereço e mail do titular do certificado também deverá estar presente.

7.1.2.5 Campos *otherName* adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC Link CD, poderão ser utilizados com OID atribuídos ou aprovados pela AC Raiz.

7.1.2.6 Os outros campos que compõem a extensão "*Subject Alternative Name*" poderão ser utilizados, na forma e com os propósitos definidos na RFC 5280.

7.1.2.7 As extensões *"Key Usage"* e *"Extended Key Usage"* para os referidos tipos de certificado são obrigatórias e obedecem aos propósitos de uso e a criticalidade conforme descrição abaixo:

a) para os demais certificados de Assinatura e/ou Proteção de e-Mail:

***"Key Usage"*, crítica:** contém o *bit digitalSignature* ativado, podendo conter os *bits keyEncipherment* e *nonRepudiation* ativados;

***"Extended Key Usage"*, não crítica:** no mínimo um dos propósitos *client authentication* OID = 1.3.6.1.5.5.7.3.2 *ou E-mail protection* OID = 1.3.6.1.5.5.7.3.4 está ativado, podendo implementar outros propósitos instituídos, desde que verificáveis e previstos nesta PC, em conformidade com a RFC 5280.

### 7.1.3 IDENTIFICADORES DE ALGORITMO

Os certificados emitidos pela AC Link CD às entidades titulares de certificado são assinados com o uso do algoritmo RSA com SHA-256 como função de *hash* (OID = 1.2.840.113549.1.1.11), conforme o padrão PKCS#1.

### 7.1.4 FORMATOS DE NOME

7.1.4.1 O nome do titular do certificado, constante do campo *"Subject"*, adota o *"Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = AC Link CD

OU = Link <e-PJ A3> ou <e-PF A3>

OU = <CNPJ da AR que realizou a identificação>

OU = <Tipo de identificação utilizada>

OU = <Referência>

CN = <Nome do titular do certificado>:<Documento do titular>

Onde:

I) Campo C (*Country Name*): Contém a UF do país emissor;

II) Campo O (*Organization Name*): Contém o nome da organização hierarquicamente responsável;

III) Primeiro campo OU (*Organizational Unit*): Nome da AC emitente;

IV) Segundo campo OU: Identificação do tipo de produto;

V) Terceiro campo OU: CNPJ da AR que realizou a identificação do titular.

VI) Quarto campo OU: Indica se a identificação foi presencial, videoconferência ou certificado digital;

VII) Quinto campo OU: Indica parâmetro adicional, que pode ser um nome, número, combinação de nome e número ou sequência alfanumérica;

VIII) Campo CN (Common Name): Para pessoa física - Nome do titular do certificado. Para pessoa jurídica - Nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ), ambos seguidos do número do documento do titular.

7.1.4.2 Não se aplica.

7.1.4.3 Não se aplica.

7.1.4.4 Não se aplica.

**Nota 1:** Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura.

### 7.1.5 RESTRIÇÕES DE NOME

7.1.5.1. Neste item estão descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.1.5.2. As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC Link CD são as seguintes:

a) Não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) Além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

| Caractere | Código NBR9611 (hexadecimal) | Caractere | Código NBR9611 (hexadecimal) |
|---|---|---|---|
| Branco | 20 | + | 2B |
| ! | 21 | , | 2C |
| “ | 22 | - | 2D |
| # | 23 | . | 2E |
| $ | 24 | / | 2F |
| % | 25 | : | 3A |
| & | 26 | ; | 3B |
| ´ | 27 | = | 3D |
| ( | 28 | ? | 3F |
| ) | 29 | @ | 40 |
| * | 2A | \ | 5C |

### 7.1.6 OID (OBJECT IDENTIFIER) DA PC

O OID (Object Identifier) desta PC é **2.16.76.1.2.3.80**. Todo certificado emitido segundo essa PC, contém o valor desse OID presente na extensão *Certificate Policies*.

### 7.1.7 USO DA EXTENSÃO "*POLICY CONSTRAINTS*"

Não se aplica.

### 7.1.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

Nos certificados emitidos segundo esta PC, o campo policyQualifiers da extensão “Certificate Policies” contém o endereço Web da DPC AC Link CD:

http://repositorio.linkcertificacao.com.br/ac-linkcd/ac-link-cd-dpc.pdf

### 7.1.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS DE PC

Extensões críticas são interpretadas conforme a RFC 5280.

## *7.2 PERFIL DE LCR*

### 7.2.1 NÚMERO DE VERSÃO

As LCR geradas pela AC Link CD implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

### 7.2.2 EXTENSÕES DE LCR E DE SUAS ENTRADAS

7.2.2.1 Neste item são descritas todas as extensões de LCR utilizadas pela AC Link CD e sua criticidade.

7.2.2.2 As LCRs da AC Link CD obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

a) **"*Authority Key Identifier*", não crítica:** contém o *hash* SHA-1 da chave pública da AC Link CD que assina a LCR;

b) **"CRL *Number*", não crítica:** contém um número sequencial para cada LCR emitida pela AC Link CD.

## *7.3 PERFIL DE OCSP*

### 7.3.1 NÚMERO DE VERSÃO

Não se aplica.

### 7.3.2 EXTENSÕES DE OCSP

Não se aplica.

# 8 AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Link CD.

Os itens seguintes estão referidos em seus correspondentes na DPC - AC Link CD.

## 9.12 *ALTERAÇÕES*

### 9.12.1 PROCEDIMENTO PARA EMENDAS

A AC Link CD segue um processo periódico de atualização de suas PCs, que contempla a revisão em duas etapas. A primeira realizada pela equipe de Compliance/Segurança da Informação e a segunda pela aprovação da Diretoria, visando a adequação dos documentos conforme as normas, procedimentos e regulamentos atuais da AC Safeweb e ICP-Brasil. Qualquer alteração nesta PC será submetida à aprovação da AC Raiz.

### 9.12.2 MECANISMO DE NOTIFICAÇÃO E PERÍODOS

A AC Link CD mantém a versão corrente desta PC para consulta pública em seu repositório *Web*, no endereço: http://repositorio.linkcertificacao.com.br/ac-linkcd/pc-a3-aclinkcd.pdf

### 9.12.3 CIRCUNSTÂNCIAS NA QUAL O OID DEVE SER ALTERADO

## 9.13 *SOLUÇÃO DE CONFLITOS*

## 9.14 *LEI APLICÁVEL*

## 9.15 *CONFORMIDADE COM A LEI APLICÁVEL*

## 9.16 *DISPOSIÇÕES DIVERSAS*

### 9.16.1 ACORDO COMPLETO

Esta PC representa as obrigações e deveres aplicáveis à AC Link CD e AR e outras entidades citadas. Havendo conflito entre esta PC e outras resoluções do CG da ICP-Brasil, prevalecerá sempre a última editada.

### 9.16.2 CESSÃO

### 9.16.3 INDEPENDÊNCIA DE DISPOSIÇÕES

### 9.16.4 EXECUÇÃO (HONORÁRIOS DOS ADVOGADOS E RENÚNCIA DE DIREITOS)

### 9.17 *OUTRAS PROVISÕES*

Esta PC foi submetida à aprovação, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2]. Como parte desse processo, além da conformidade com este documento, é verificada a compatibilidade entre a PC e a DPC da AC Link CD.

## 10 DOCUMENTOS REFERENCIADOS

***10.1*** Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio **https://www.gov.br/iti/pt-br** publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

| Ref. | Nome do documento | Código |
|---|---|---|
| [1] | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL<br>Aprovado pela Resolução CG ICP-Brasil nº 179, de 20 de outubro de 2020. | DOC-ICP-04 |
| [2] | CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL<br>Aprovado pela Resolução CG ICP-Brasil nº 178, de 20 de outubro de 2020. | DOC-ICP-03 |
| [3] | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇO DE CONFIANÇA DA ICP-BRASIL<br>Aprovado pela Resolução CG ICP-Brasil nº 180, de 20 de outubro de 2020. | DOC-ICP-17 |

## 11 REFERÊNCIAS BIBLIOGRÁFICAS

RFC 3647, IETF - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003.

RFC 5280, IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008.

RFC 2818, IETF - HTTP Over TLS, may 2000.

RFC 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.