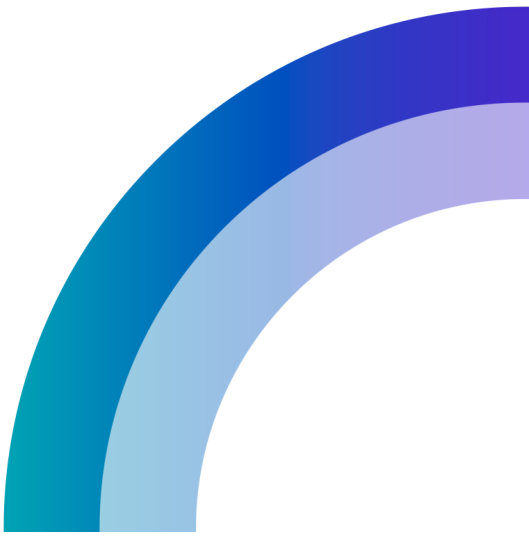
Política de Certificado
da
Autoridade Certificadora
do
SERPRO SSL A1

Autenticação de Servidor(SSL/TSL)

(PC AC SERPRO SSL A1)

Versão 3.2 de Junho 2022



Índice

Controle de Versão:

Versão	Data	Responsável	Motivo	Descrição
1.0	01/09/2019	Lucia Castelli	Versão Inicial	Versão Inicial
1.0	01/09/2019	Osni Bunn	Versão Inicial	Versão Inicial
1.1	22/11/2019	Lucia Castelli	Revisão	Inclusão requisitos CabForum 1.6.6.
1.1	22/11/2019	Osni Bunn	Aprovação	
1.2	26/02/2020	Lucia Castelli	Revisão	Apontamentos feitos pela Auditoria PKI;Alteração ***url*** para Suporte/Fraudes e o repositório da PC e DPC
1.2	26/02/2020	Osni/Alice	Aprovação	
1.3	13/03/2020	Lucia Castelli	Revisão	Alterado nome do ponto de distribuição da lcr – item 7.1.2 “d”
1.3	13/03/2020	Alice Vasconcellos	Aprovação	
2.0	12/05/2020	Lucia Castelli	Revisão	Alterado URL OCSP e OID OV SSL; Alteração conforme Res: 156 e 169; Apontamento do ITI;
2.0	12/05/2020	Alice Vasconcellos	Aprovação	
3.0	Novembro/2020	Lucia Castelli	Revisão	Atualização conforme resolução 179
3.0	Novembro/2020	Alice Vasconcellos	Aprovação	
3.1	Junho/2021	Lucia Castelli	Revisão	Alterado item 7.1.2.3. alinea c.1 e c.2; Inclusão tipo de certificado Open banking: item 7.1.2.7. e 7.1.4.4.
3.1	Junho/2021	Alice Vasconcellos	Aprovação	
3.2	Junho/2022	Lucia Castelli	Revisão	Alteração Referências Bibliográficas e Siglas e Acrônimos.
3.2	Junho/2022	Alice Vasconcellos	Aprovação	

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Este documento estabelece os requisitos a serem obrigatoriamente observados pela AC SERPRO SSL integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Políticas de Certificado – PC.
1.1.2. A PC SERPRO SSL A1 elaborada no âmbito da ICP-Brasil adota obrigatoriamente a estrutura dos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04), como também segue as atualizações dos documentos do WebTrust Principles and Criteria[6] e publicações do CA/Browser Forum[7].

No caso de qualquer inconsistência entre esse documento e os requisitos do CA/Browser Forum[7], estes terão precedência sobre o documento.

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 emitido sob esta PC é o certificado de assinatura do Tipo A1.

1.1.6. Não se aplica.

1.1.7 Não se aplica.

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 PC obedece às recomendações da ICP-Brasil para a emissão de certificados de assinatura do tipo A1.

1.2.2. Após o processo de credenciamento da AC SERPRO SSL foi atribuído a esta Política de Certificação, no âmbito da ICP-Brasil, o seguinte OID;

TIPO DE CERTIFICADO	OID
A1	**2.16.76.1.2.1.105.**

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

1.3.1.1. A Autoridade Certificadora do SERPRO SSL (AC SERPRO SSL) integra a Infraestrutura de Chaves Públicas Brasileira, ICP-Brasil, sob a hierarquia da Autoridade Certificadora Raiz Brasileira.

1.3.1.2 Esta PC é implementada pela Autoridade Certificadora SERPRO SSL cuja DPC encontra-se publicada em sua página *Web* no seguinte endereço: https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf.

1.3.2. Autoridades de Registro

1.3.2.1. A Autoridade de Registro, envolvida na emissão de certificados SSL, atende e segue os requisitos estabelecidas nas seções 4.2 e 5.3 desse documento.

O endereço da página *web* (*URL*) da AC é https://certificados.serpro.gov.br/serprossl onde estão publicados os dados abaixo referentes as Autoridades de Registro, responsáveis pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;

b) relação de AR que tenham sido descredenciadas da cadeia da AC, com a respectiva data do descredenciamento;

1.3.3. Titulares de Certificado

Os certificados são emitidos pela AC para equipamentos ou aplicações, sendo as pessoas físicas e pessoas jurídicas, detentoras dos certificados.

Em sendo o titular de certificado pessoa jurídica, será designado pessoa física como responsável pelo certificado, que será o detentor da chave privada.

Preferencialmente será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

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 AC utiliza o Serviço Federal de Processamento de dados (SERPRO) como Prestador de Serviço de Suporte – PSS e Prestador de Serviço Biométrico – PSBio, conforme disponibilizado no endereço: https://certificados.serpro.gov.br/serprossl.

Outros grupos que participaram do desenvolvimento dos requisitos do Cab/Browser Forum[15] incluem a AICPA / CICA, que é a força-tarefa do *WebTrust for AC[6]* e a *ETSI ESI*. A participação de tais grupos não implica endosso, recomendação ou aprovação do produto final.

1.4. Usabilidade do Certificado

1.4.1. Uso apropriado do certificado

1.4.1.1. Os certificados emitidos sob esta PC são apropriados ao uso apenas nas aplicações apresentadas na tabela descrita a seguir:

Política de Certificado	Aplicações Apropriadas
PC AC SERPRO SSL A1	Certificados emitidos sob essa política são considerados adequados para assinatura eletrônica, irretratabilidade, integridade e autenticação. Podem ser usados nas seguintes aplicações: • Confirmação de Identidade na *web*; • Correio eletrônico; • Transações *On-Line*; • Redes privadas virtuais (VPN); • Transações eletrônicas; • Criação de chave de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

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. As aplicações para o certificado definido nesta PC, devem levar 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 A1 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 há restrições de aplicações identificadas.

Os certificados SSL emitidos sob esta PC não garantem que o equipamento no qual o certificado foi instalado não esteja isento de defeitos, *malware* ou vírus.

1.5. Política de Administração

Esta PC é administrada pelo Centro de Certificação Digital do SERPRO(CCD-SERPRO).

1.5.1. Organização administrativa do documento

Autoridade Certificadora do SERPRO SSL – **AC SERPRO SSL**

1.5.2. Contatos

Administrativo:

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

Suporte / Fraudes

Nome: Central de Serviços SERPRO

Página Web: https://atendimento.serpro.gov.br/certificacaodigital

E-mail: css.serpro@serpro.gov.br

Telefone: 0800 7282323

1.5.3. Pessoa que determina a adequabilidade da DPC com a PC

Nome: Pedro Moacir Rigo Motta

Telefone: (61) 2021-7957

E-mail: certificados@serpro.gov.br

1.5.4. Procedimentos de aprovação da PC

Esta PC é aprovada pelo ITI.

Os procedimentos de aprovação da PC da AC são estabelecidos a critério do CG da ICP-Brasil.

As alterações feitas nesse documento estão identificadas na seção - Controle de Versões.

1.6. Definições e Acrônimos

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
ACME	Automatic Certificate Management Environment
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AICPA	American Institute of Certified Public Accountants
AR	Autoridades de Registro
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CICA	Canadian Institute of Chartered Accountants
CMM-SEI	*Capability Maturity Model do Software Engineering Institute*
CMVP	*Cryptographic Module Validation Program*
CN	*Common Name*
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
CS	Code Signing
DMZ	Zona Desmilitarizada
DN	*Distinguished Name*
DNS	Domain Name System
DPC	Declaração de Práticas de Certificação
ETSI	European Telecommunications Standards Institute
ESI	Electronic Signatures and Infrastructures
EV	Extended Validation (WebTrust for Certification Authorities)
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IETF PKIX	*Internet Engineering Task Force - Public-Key Infrastructured (X.509)*
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
NIST	*National Institute of Standards and Technology*
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
POP	Proof of Possession PS Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	Request For Comments
RG	Registro Geral
SAT	Sistema de Autenticação e Transmissão
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade de Federação
URL	Uniform Resource Locator

2. Responsabilidades de publicação e repositórios

Os itens seguintes estão descritos da DPC da AC.

2.1. Repositórios

2.2. Publicação de informações dos certificados

2.2.1. A AC está em conformidade com a versão atual dos Requisitos de Linha de Base para a Emissão e Gerenciamento de Certificados de confiança pública, publicados em http://www.cabforum.org. No caso de qualquer inconsistência entre este documento e esses requisitos, esses têm precedência sobre este documento.

2.3. Tempo ou Frequência de Publicação

2.4. Controle de Acesso aos Repositórios

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

Os itens seguintes estão descritos na DPC da AC.

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

3.3. 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 descritos na DPC da AC.

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

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.2. Publicação do certificado pela AC

4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades

4.5. Usabilidade do par de chaves e do certificado

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis

4.6. Renovação de Certificados

4.6.1. Circunstâncias para renovação de certificados

4.6.2. Quem pode solicitar a renovação

4.6.3. Processamento de requisição para renovação de certificados

4.6.4. Notificação para nova emissão de certificado para o titular

4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado

4.6.6. Publicação de uma renovação de um certificado pela AC

4.6.7. Notificação de emissão de certificado pela AC para outras entidades

4.7. Nova chave de certificado

4.7.1. Circunstâncias para nova chave de certificado

4.7.2. Quem pode requisitar a certificação de uma nova chave pública

4.7.3. Processamento de requisição de novas chaves de certificado

4.7.4. Notificação de emissão de novo certificado para o titular

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

4.7.6. Publicação de uma nova chave certificada pela AC

4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades

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

4.10.2. Disponibilidade dos serviços

4.10.3. Funcionalidades operacionais

4.11. Encerramento de atividades

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E INSTALAÇÕES

Os itens seguintes estão descritos na DPC da AC.

5.1. Controles físicos

5.1.1 Construção e localização das instalações de AC

5.1.2. Acesso físico

5.1.3. Energia e ar-condicionado

5.1.4. Exposição à água

5.1.5. Prevenção e proteção contra incêndio

5.1.6. Armazenamento de mídia

5.1.7. Destruição de lixo

5.1.8. Instalações de segurança (backup) externas (*off-site*) para AC

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.2. Número de pessoas necessário por tarefa

5.2.3. Identificação e autenticação para cada perfil

5.2.4. Funções que requerem separação de deveres

5.3. Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2. Procedimentos de verificação de antecedentes

5.3.3. Requisitos de treinamento

5.3.4. Frequência e requisitos para reciclagem técnica

5.3.5. Frequência e sequência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. Documentação fornecida ao pessoal

5.4. Procedimentos de Log de Auditoria

5.4.1. Tipos de eventos registrados

5.4.2. Frequência de auditoria de registros

5.4.3. Período de retenção para registros de auditoria

5.4.4. Proteção de registros de auditoria

5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria

5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)

5.4.7. Notificação de agentes causadores de eventos

5.4.8. Avaliações de vulnerabilidade

5.5. Arquivamento de Registros

5.5.1. Tipos de registros arquivados

5.5.2. Período de retenção para arquivo

5.5.3. Proteção de arquivo

5.5.4. Procedimentos de cópia de arquivo

5.5.5. Requisitos para datação de registros

5.5.6. Sistema de coleta de dados de arquivo (interno e externo)

5.5.7. Procedimentos para obter e verificar informação de arquivo

5.6. Troca de chave

5.7. Comprometimento e Recuperação de Desastre

5.7.1. Procedimentos gerenciamento de incidente e comprometimento

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, são definidas as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos segundo a PC.

São definidos também outros controles técnicos de segurança utilizados pela DPC e pelas AR 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 for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará, 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 Titular do Certificado gera a chave utilizando aplicativos com esta finalidade. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficos e pelo uso do certificado.

A chave privada é armazenada utilizando:

- Para certificados de pessoa física ou jurídica o solicitante deverá armazenar a chave privada com nível alto de segurança, isto é protegido por senha.

A AC recomenda que seja feito *backup* da chave privada, evitando assim perda do certificado.

6.1.1.3. O algoritmo a ser utilizado para as chaves criptográficas de titulares de certificados adota o padrão RSA conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

A AC rejeita uma solicitação de certificado se a chave pública solicitada não atender aos requisitos estabelecidos nas seções 6.1.5 e 6.1.6. Se tiver uma chave privada requeremos a suíte de assinatura sha2WithRSA, conforme orientação ICP-Brasil.

6.1.1.4. Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-Brasil[1], no meio de armazenamento definido para cada tipo de certificado A1 previsto pela ICP-Brasil.

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

6.1.1.6. A mídia de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, minimamente 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 deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

c) a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7. Essa 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. Não se aplica.

Nota: Não se aplica.

6.1.2. Entrega da chave privada à entidade titular

É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada. Caso a AC seja comunicada que uma chave privada de um certificado foi repassada a uma pessoa ou organização não autorizada, a AC providenciará a revogação imediata da chave pública referente.

6.1.3. Entrega da chave pública para o emissor de certificado

Chaves públicas são entregues à AC por meio de uma troca *on-line* utilizando funções automáticas do *software* de certificação da AC.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida na solicitação.

6.1.4. Disponibilização de chave pública da AC às terceiras partes

As formas para a disponibilização dos certificados da cadeia de certificação, para os usuários da AC, compreendem:

a) No momento da disponibilização de um certificado para seu titular, será utilizado o padrão PKCS#7, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1];

b) Página *web* da AC: https://certificados.serpro.gov.br/serprossl

c) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC é de, no mínimo, 2048 (dois mil e quarenta e oito) bits;

6.1.5.2. Os algoritmos e o tamanho das chaves utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.6. Geração de parâmetros de chaves assimétricas

Os parâmetros de geração e verificação de chaves assimétricas do usuário final adotam o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1].

6.1.7. Propósitos de uso de chave (conforme o campo "*key usage*" na X.509 v3)

Os certificados emitidos nesta PC têm ativado os bits *digitalSignature e keyAgreement*.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

Nos itens seguintes, são definidos os requisitos para a proteção das chaves privadas dos titulares de certificados emitidos segundo esta PC.

6.2.1. Padrão e controle para módulo criptográfico

6.2.1.1. Os padrões requeridos para os módulos de geração de chaves criptográficos, estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS da ICP-BRASIL [1].

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

6.2.2. Controle "n de m" para chave privada

Item não aplicável.

6.2.3. Custódia (*escrow*) de chave privada

Não se aplica.

6.2.4. Cópia de segurança (*backup*) de chave privada

6.2.4.1. Qualquer titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2. A AC não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido.

6.2.4.3. Não se aplica.

6.2.4.4. Não se aplica.

6.2.5. Arquivamento de chave privada

6.2.5.1. As chaves privadas dos titulares de certificados emitidos pela AC 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

Os Titulares de Certificados poderão optar por utilizar um *hardware* criptográfico, cartão inteligente ou *token*, para armazenar sua chave privada após a aceitação do certificado.

6.2.7. Armazenamento de chave privada em módulo criptográfico

Conforme subitem 6.1.1.1.

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 3 meses.

6.2.9. Método de desativação de chave privada

A desativação da chave privada ocorre no fechamento do “browser” utilizado para estabelecer uma conexão segura.

6.2.10. Método de destruição de chave privada

A eliminação da chave da mídia armazenadora do certificado deve ser feita através de opções disponibilizadas pelo “browser” utilizado para gerar o par de chaves. A opção permite apagar a chave privada.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, bem como as LCR emitidas, 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 pública e privada

6.3.2.1. A chave privada da AC e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2. Não se aplica.

6.3.2.3. Certificados do tipo A1, previsto nesta PC, tem validade de até 1 ano.

6.3.2.4. Não se aplica.

6.3.2.5. Não se aplica.

6.4. Dados de Ativação

Nos itens seguintes, estão descritos os requisitos gerais 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 dados de ativação da chave privada da AC são únicos e aleatórios.

6.4.2. Proteção dos dados de ativação

Os dados de ativação da AC são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha e são armazenados em ambiente de nível 6 de segurança.

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

6.5.1.1. A AC garante que a geração de seu par de chaves é realizada em ambiente *off-line*, para impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos gerais de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC estão descritos nessa PC.

6.5.1.3. Os computadores servidores, utilizados pela AC, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) Controle de acesso aos serviços e perfis da AC;

b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;

c) Acesso restrito aos bancos de dados da AC;

d) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

e) Geração e armazenamento de registros de auditoria da AC;

f) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e

g) Mecanismos para cópias de segurança (*backup*).

6.5.1.4. Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são

destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC, é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controles Técnicos do Ciclo de Vida

A AC não exige um software específico para utilização dos certificados emitidos segundo esta PC.

6.6.1. Controles de desenvolvimento de sistema

Conforme item 6.6.1. da DPC da AC.

6.6.2. Controles de gerenciamento de segurança

Conforme item 6.6.2. da DPC da AC.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Todas as LCR geradas pela AC 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

Os mesmos controles admitidos no item 6.7 da DPC.

6.8. Carimbo de Tempo

Não se aplica.

7. Perfis de Certificado e LCR

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

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

A AC atende a todos os requisitos estabelecidos nos itens 2.2, 6.1.5. e 6.1.6. desta PC.

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC, segundo esta PC, estão em conformidade com o formato definido pelo padrão ITU X.509 versão 3 ou ISO/IEC 9594-8.

7.1.1. Número de versão

Todos os certificados emitidos pela AC, segundo esta PC, implementam a versão 3 de certificado definida no 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:** contém o *hash* SHA-1 da chave pública da AC;

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

c) ***"Certificate Policies",* não crítica**: contém o **OID 2.16.76.1.2.1.105** da PC e o endereço *URL* da página *Web* https://repositorio.serpro.gov.br/docs/dpcserprossl.pdf com a DPC da AC;

Certificados de autenticação de servidores (SSL/TLS) devem conter ainda o OID da política de certificado de identificação dos requisitos do *CA/B Forum Guidelines*(**OV SSL = 2.23.140.1.2.2**).

d) ***"CRL Distribution Points",* não crítica:** contém o endereço *URL* da página *Web* onde se obtém a LCR da AC:

http://repositorio.serpro.gov.br/lcr/acserprosslv1.crl

http://certificados2.serpro.gov.br/lcr/acserprosslv1.crl

e) **"*Authority Information Access*"**, **não critica**, contendo o método de acesso id-ad-calssuer, utilizando o protocolo de acesso HTTP para a recuperação da cadeia de certificação no seguinte endereço: http://repositorio.serpro.gov.br/cadeias/serprossl.p7b

A segunda entrada contém o método de acesso *id-ad-ocsp*, com o respectivo endereço http://ocsp.serpro.gov.br/acserprosslv1 do respondedor OCSP, utilizando o protocolo de acesso, HTTP.

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

a) Não se aplica;

b) Não se aplica;

c) Para certificado de equipamento ou aplicação:

c.1) Para certificados do tipo SSL/TLS, cada entrada deverá ser um dNSName, obrigatório, contendo um FQDS(Fully Qualified Domain Name) ou iPAddress, contendo o endereço IP de um servidor, sendo que o(s) domínio(s) pertence(em) ou são controlados pelo titular, estando em conformidade com os princípios e critérios WebTrust[6] e os requisitos do CA/Browse Forum[7].

Os FQDN do tipo curinga são permitidos.

c.2) Não se aplica;

d) Não se aplica;

e) Não se aplica.

7.1.2.4. Todos os campos e extensões nos certificados da AC SERPRO SSL são definidos de acordo com a RFC 5280.

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

a) 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 não estiver disponível, não se deve preencher o campo de órgão emissor e UF. O mesmo ocorre para o campo de município e UF, se não houver número de inscrição do Título de Eleitor;

d) Não se aplica;

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

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

g) Apenas os caracteres de A a Z e de 0 a 9 poderão ser utilizados, não sendo permitidos caracteres especiais, símbolos, espaços ou quaisquer outros.

h) Não se aplica.

7.1.2.5. Campos otherName adicionais, contendo informações específicas e forma de preenchimento e armazenamento definidas pela AC, 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. A AC implementa as seguintes extensões, definidas como obrigatórias pela ICP-Brasil.

a) Não se aplica.

b) para certificados de Autenticação de Servidor (SSL/TLS):

"***Key Usage"*, crítica:** somente os bits *digitalSignature e keyAgreement* estão ativados;
"***Extended Key Usage"***, **não crítica**: contém o propósito *server authentication* **OID=1.3.6.1.5.5.7.3.1.** e também o propósito: *client authentication,* **OID = 1.3.6.1.5.5.7.3.2;**

para certificados Open Banking Transporte:

"*Key Usage"*, crítica: somente os bits *digitalSignature e keyEncipherment* estão ativados;
"*Extended Key Usage"*, **não crítica**: contém o propósito: *client authentication,* **OID = 1.3.6.1.5.5.7.3.2;**

c) Não se aplica.

d) Não se aplica.

e) Não se aplica.

f) Não se aplica.

g) Não se aplica.

7.1.3. Identificadores de algoritmo

7.1.3.1. Os algoritmos criptográficos utilizados para assinatura dos certificados pela AC são os admitidos no âmbito da ICP-Brasil, conforme documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]:

7.1.3.1.1. Os certificados emitidos pela AC são assinados com o uso do algoritmo criptográfico SHA-256 com função de *hash* (**OID = 1.2.840.113549.1.1.1**).

7.1.4. Formatos de nome

7.1.4.1. Não se aplica.

7.1.4.2. Não se aplica;

7.1.4.3. Não se aplica;

7.1.4.4.

a) O certificado digital emitido para Autenticação de Servidor (SSL/TLS) adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ)

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular

ST = unidade da federação do endereço físico do titular do certificado

L = cidade do endereço físico do titular

Business Category (OID 2.5.4.15) = tipo de categoria comercial, devendo conter: "Private Organization" ou "Government Entity" ou "Business Entity" ou "NonCommercial Entity"

Serial Number(OID 2.5.4.5) = CPF ou CNPJ, conforme o tipo de pessoa;

Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR

b) Certificado SSL Open Banking (Transporte):

O certificado digital SSL Open Banking (Transporte), adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, com os seguintes conteúdos:

C = BR;

O = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do Cadastro Nacional de Pessoa Jurídica (CNPJ);

CN = se presente, este campo deve conter um único nome de domínio pertencente ou controlado pelo titular;

ST = unidade da federação do endereço físico do titular do certificado;

L = cidade do endereço físico do titular;

OU = Código de Participante associado ao CNPJ listado no Serviço de Diretório do OpenBanking Brasil;

UID = Software Statement ID cadastrado no Serviço de Diretório do OpenBanking Brasil e pertencente ao CNPJ e Código de Participante.

Business Category(OID 2.5.4.15), = tipo de categoria comercial, devendo conter: "Private Organization" ou "Government Entity" ou "Business Entity" ou "NonCommercial Entity"**;**

Jurisdiction Country Name (OID: 1.3.6.1.4.1.311.60.2.1.3) = BR;

Serial Number(OID 2.5.4.5) = Cadastro Nacional de Pessoal Jurídica (CNPJ) da pessoa jurídica titular do certificado e associado ao atributo organizational UnitName e Software Statement ID, durante validação junto ao Serviço de Diretório do OpenBanking Brasil;

NOTA: 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 da PC, são descritas as restrições aplicáveis para os nomes dos titulares de certificados

7.1.5.2. A ICP-Brasil estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados:

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

b) além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

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

\	5C

Tabela 3 - Caracteres especiais admitidos em nomes

7.1.6. OID (*Object Identifier*) de Política de Certificado

O OID atribuído a esta Política de Certificado é: **2.16.76.1.2.1.105.**

Todo certificado emitido segundo esta PC deverá conter, na extensão "*Certificate Policies*", o OID correspondente.

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 da página *Web* (*URL*) com a DPC da AC, a saber: http://repositorio.serpro.gov.br/docs/dpcserprossl.pdf

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número de versão

As LCR geradas por essa AC, segundo a PC, implementam a versão 2 de LCR definida no 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. A AC SERPRO SSL adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

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

b) ***"CRL Number"***, ***não crítica***: contém número sequencial para cada LCR emitida.

7.2.2.2. Conforme o item 7.2.2.1.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Serviços de respostas OCSP implementa a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP

O campo **"*Authority Information Access*"**, **não critica**, contem 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.serpro.gov.br/cadeias/serprossl.p7b.

A segunda entrada contém o método de acesso id-ad-ocsp, com o respectivo endereço http://ocsp.serpro.gov.br/serprossl do respondedor OCSP, utilizando o protocolo de acesso, HTTP.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens seguintes são referidos os itens correspondentes da DPC da AC.

9.5. Direitos de Propriedade Intelectual

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da AC

9.6.2. Declarações e Garantias da AR

9.6.3. Declarações e garantias do titular

9.6.4. Declarações e garantias das terceiras partes

9.6.5. Representações e garantias de outros participantes

9.7. Isenção de garantias

9.8. Limitações de responsabilidades

9.9. Indenizações

9.10. Prazo e Rescisão

9.10.1. Prazo

9.10.2. Término

9.10.3. Efeito da rescisão e sobrevivência

9.11. Avisos individuais e comunicações com os participantes

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração na PC deverá ser submetida à aprovação da AC Raiz.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta PC será publicado no site da AC.

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 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, durante o processo de credenciamento da AC SERPRO SSL, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3]. Como parte desse processo, além da conformidade com este documento, foi verificada a compatibilidade entre a PC e a DPC da AC SERPRO SSL.

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 http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[3]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-03**
[8]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	**DOC-ICP-04**
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	**DOC-ICP-12**

10.2. Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL	**DOC-ICP-01.01**

11. REFERÊNCIAS BIBLIOGRÁFICAS

Ref	Nome do documento	Link
[6]	*WebTrust Principles and Criteria for Registration Authorities e Certification Authorities*	https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services
[7]	Baseline Requirements – CA/Browser Forum	https://cabforum.org/

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.