



**Política de Certificado A1 da Autoridade Certificadora DOCLOUD RFB.
PC A1 da AC DOCLOUD RFB**

**OID: 2.16.76.1.2.1.58
Versão 7.1**

1. INTRODUÇÃO	11
1.1. VISÃO GERAL	11
1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO.	11
1.3. PARTICIPANTES DA ICP-BRASIL	11
1.3.1. Autoridades Certificadoras	12
1.3.2. Autoridades de Registro	12
1.3.3 Titulares do Certificado.....	12
1.3.4. Partis Confiáveis.....	12
1.3.5. Outros Participantes	12
1.4. USABILIDADE DO CERTIFICADO	12
1.4.1. Uso apropriado do certificado	12
1.4.2. Uso proibitivo do certificado	13
1.5. POLÍTICA DE ADMINISTRAÇÃO	13
1.5.1. Organização administrativa do documento	13
1.5.2. Contatos.....	13
1.5.3. Adequabilidade da DPC com PC's.....	13
1.5.4. Procedimentos de aprovação desta PC	123
1.6. DEFINIÇÕES E ACRÔNICOS	13
2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIOS	14
2.1. REPOSITÓRIOS	14
2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS	14
2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO	14
2.4. CONTROLE DE ACESSO AOS RESPOSITÓRIOS	14
3. IDENTIFICAÇÃO E AUTENTICAÇÃO	14
3.1. NOMEAÇÃO	14
3.1.1. Tipos de nomes.....	14
3.1.2. Necessidade de os nomes serem significativos	15
3.1.3. Anonimato ou Pseudônimo dos Titulares do certificado	15
3.1.4. Regras para interpretação de vários tipos de nomes	15
3.1.5. Unicidade de nomes	15
3.1.6. Procedimento para resolver disputa de nomes	15
3.1.7. Reconhecimento, autenticação e papel de marcas registradas	15
3.2. VALIDAÇÃO INICIAL DA IDENTIDADE	15
3.2.1. Método para comprovar a posse de chave privada	15
3.2.2. Autenticação da identidade de uma organização	15
3.2.3. Autenticação da identidade de equipamento ou aplicação	15
3.2.4. Autenticação da identidade de um indivíduo.....	15

3.2.5. Informações não verificadas do titular do certificado.....	15
3.2.6. Validação das autoridades.....	15
3.2.7. Critérios para interoperação.....	15
3.3. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES	15
3.3.1. Identificação e autenticação para rotina de novas chaves.....	15
3.3.2. Identificação e autenticação para rotina de novas chaves após revogação	15
3.4. IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO	15
4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO	15
4.1. SOLICITAÇÃO DO CERTIFICADO	15
4.1.1. Quem pode submeter uma solicitação de certificado.....	15
4.1.2. Processo de registro e responsabilidade	15
4.2. PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO	15
4.2.1. Execução das funções de identificação e autenticação.....	15
4.2.2. Aprovação ou rejeição de pedidos de certificado	15
4.2.3. Tempo para processar a solicitação de certificado	15
4.3. EMISSÃO DO CERTIFICADO.....	15
4.3.1. Ações da AC durante a emissão de um certificado	15
4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado.....	15
4.4. ACEITAÇÃO DO CERTIFICADO	15
4.4.1. Conduta sobre a aceitação do certificado	15
4.4.2. Publicação do certificado pela AC.....	15
4.4.3. Notificação de emissão do certificado pela AC Raiz do certificado pela AC.....	15
4.5. USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO	15
4.5.1. Usabilidade da chave privada e do certificado do titular	15
4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis.....	15
4.6. RENOVAÇÃO DE CERTIFICADOS.....	15
4.6.1. Circunstância para renovação de certificados	15
4.6.2. Quem pode solicitar renovação.....	15
4.6.3. Processamento de requisição para renovação de certificados	15
4.6.4. Notificação para nova emissão de certificado para o titular	15
4.6.5. Conduta constituindo a aceitação de uma renovação de um certificado	16
4.6.6. Publicação de uma renovação de um certificado pela AC.....	16
4.6.7. Notificação de emissão de certificado pela AC para outras entidades	16
4.7. NOVA CHAVE DE CERTIFICADO.....	16
4.7.1. Circunstâncias para nova chave de certificado.....	16
4.7.2. Quem pode requisitar a certificação de uma nova chave pública	16
4.7.3. Processamento de requisição de novas chaves de certificado	16
4.7.4. Notificação de emissão de novo certificado para o titular	16

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada	16
4.7.6. Publicação de uma nova chave certificada pela AC.....	16
4.7.7. Notificação de uma emissão de certificado pela AC para outra entidades.....	16
4.8. MODIFICAÇÃO DE CERTIFICADO	16
4.8.1. Circunstâncias para modificação de certificado	16
4.8.2. Quem pode requisitar a modificação de certificado	16
4.8.3. Processamento de requisição de modificação de certificado	16
4.8.4. Notificação de emissão de novo certificado para o titular	16
4.8.5. Conduta constituindo a aceitação de uma modificação de certificado	16
4.8.6. Publicação de uma modificação de certificado pela AC	16
4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades	16
4.9. SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO	16
4.9.1. Circunstâncias para revogação	16
4.9.2. Quem pode solicitar revogação	16
4.9.3. Procedimento para solicitação de revogação.....	16
4.9.4. Prazo para solicitação de revogação.....	16
4.9.5. Tempo em que a AC deve processar o pedido de revogação.....	16
4.9.6. Requisitos de verificação de revogação para as partes confiáveis.....	16
4.9.7. Frequência de emissão de LCR	16
4.9.8. Latência máxima para a LCR	16
4.9.9. Disponibilidade para revogação/verificação de status on-line	16
4.9.10. Requisitos para verificação de revogação on-line	16
4.9.11. Outras formas disponíveis para divulgação de revogação	16
4.9.12. Requisitos especiais para o caso de comprometimento de chave.....	16
4.9.13. Circunstâncias para suspensão	16
4.9.14. Quem pode solicitar suspensão.....	16
4.9.15. Procedimento para solicitação de suspensão	16
4.9.16. Limites no período de suspensão	16
4.10. Serviços de status de certificado	16
4.10.1. Características operacionais	16
4.10.2. Disponibilidade dos serviços.....	16
4.10.3. Funcionalidades operacionais.....	16
4.11. Encerramento de atividades	16
4.12. Custódia e recuperação de chave.....	16
4.12.1. Política e práticas de custódia e recuperação de chave	16
4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão	16
5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES.....	16
5.1. CONTROLES FÍSICOS.....	17

5.1.1. Construção e localização das instalações	17
5.1.2. Acesso físico	17
5.1.3. Energia e ar-condicionado	17
5.1.4. Exposição à água.....	17
5.1.5. Prevenção e proteção contra incêndio.....	17
5.1.6. Armazenamento de mídia	17
5.1.7. Destruição de lixo	17
5.1.8. Instalações de segurança (backup) externas (off-site) para AC.....	17
5.2. CONTROLES PROCEDIMENTAIS.....	17
5.2.1. Perfis qualificados	17
5.2.2. Número de pessoas necessário por tarefa	17
5.2.3. Identificação e autenticação para cada perfil.....	17
5.2.4. Funções que requerem separação de deveres.....	17
5.3. CONTROLES DE PESSOAL	17
5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade	17
5.3.2. Procedimentos de verificação de antecedentes.....	17
5.3.3. Requisitos de treinamento	17
5.3.4. Frequência e requisitos para reciclagem técnica	17
5.3.5. Frequência e sequência de rodízio de cargos	17
5.3.6. Sanções para ações não autorizadas	17
5.3.7. Requisitos para contratação de pessoal	17
5.3.8. Documentação fornecida ao pessoal.....	17
5.4. PROCEDIMENTOS DE LOG DE AUDITORIA	17
5.4.1. Tipos de eventos registrados	17
5.4.2. Frequência de auditoria de registros	17
5.4.3. Período de retenção para registros de auditoria.....	17
5.4.4. Proteção de registros de auditoria	17
5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria	17
5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)	17
5.4.7. Notificação de agentes causadores de eventos	17
5.4.8. Avaliações de vulnerabilidade	17
5.5. ARQUIVAMENTO DE REGISTRO	17
5.5.1. Tipos de registros arquivados	17
5.5.2. Período de retenção para arquivo	17
5.5.3. Proteção de arquivo.....	17
5.5.4. Procedimentos de cópia de arquivo	17
5.5.5. Requisitos para datação de registros.....	17
5.5.6. Sistema de coleta de dados de arquivo (interno e externo)	17

5.5.7. Procedimentos para obter e verificar informação de arquivo	17
5.6. TROCA DE CHAVE.....	17
5.7. COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	17
5.7.1. Procedimentos de gerenciamento de incidente e comprometimento	17
5.7.2. Recursos computacionais, software, e/ou dados corrompidos	17
5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade	17
5.7.4. Capacidade de continuidade de negócio após desastre	18
5.8. EXTINÇÃO DA AC	18
6. CONTROLE TÉCNICOS DE SEGURANÇA	18
6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....	18
6.1.1. Geração do par de chaves.....	18
6.1.2. Entrega da chave privada à entidade titular.....	19
6.1.3. Entrega da chave pública para o emissor do certificado.....	19
6.1.4. Entrega de chave pública da AC às terceiras partes	19
6.1.5. Tamanhos de chave	19
6.1.6. Geração de parâmetros de chaves assimétricas, verificação da qualidade dos parâmetros	20
6.1.7. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3.....)	20
6.2. PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO.....	20
6.2.1. Padrões e controle para módulo criptográfico.....	20
6.2.2. Controle n de m para chave privada.....	20
6.2.3. Custódia (escrow) de chave privada	20
6.2.4. Cópia de segurança (backup) de chave privada	20
6.2.5. Arquivamento de chave privada.....	21
6.2.6. Inserção de chave privada em módulo criptográfico	21
6.2.7. Armazenamento de chave privada e módulo criptográfico	21
6.2.8. Método de ativação de de chave privada.....	21
6.2.9. Método de desativação de de chave privada	21
6.2.10. Método de destruição de de chave privada	21
6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES.....	21
6.3.1. Arquivamento de chave pública	21
6.3.2. Períodos de operação do certificado e períodos de uso para as chaves Pública e Privada	21
6.4. DADOS DE ATIVAÇÃO.....	22
6.4.1. Geração e instalação dos dados de ativação de chave pública	22
6.4.2. Proteção dos dados de ativação	22
6.4.3. Outros aspectos dos dados de ativação	22
6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL.....	22

6.5.1. Requisitos técnicos específicos de segurança computacional	22
6.5.2. Classificação da segurança computacional	22
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA	22
6.6.1. Controles de desenvolvimento de sistema	22
6.6.2. Controles de gerenciaento de segurança	22
6.6.3. Classificação de segurança do ciclo de vida	23
6.6.4. Controle na geração da LCR antes de publicadas	23
6.7. CONTROLES DE SEGURANÇA DE REDE.....	23
6.8. CARIMBO DE TEMPO	23
7. PERFIS DE CERTIFICAOD, LCR E OCSP	23
7.1. PERFIL DO CERTIFICADO.....	23
7.1.1. Número de versão	23
7.1.2. Extensões de certificados	23
7.1.3. Identificadores de algoritimo.....	26
7.1.4. Formatos de nome.....	26
7.1.5. Restrições de nome	28
7.1.6. OID (Object Identifer) de Política de Certificado	29
7.1.7. Uso da extensão "Policy Constraints"	29
7.1.8. Sintaxe e Semântica dos qualificadores de políticas	29
7.1.9. Semântica de processamento para extensões críticas	29
7.2. PERFIL DE LCR.....	29
7.2.1. Número de versão	29
7.2.2. Extensões de LCR e suas entradas	29
7.3. PERFIL DE OCSP	29
7.3.1. Número(s) de versão	29
7.3.2. Extensões de OCSP.....	30
8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES.....	30
8.1. FREQUÊNCIA E CIRCUNSTÂNCIA DAS AVALIAÇÕES.....	30
8.2. IDENTIFICAÇÃO E QUALIFICAÇÃO DO AVALIADOR	30
8.3. RELAÇÃO DO AVALIADOR COM A ENTRADA AVALIADA.....	30
8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO.....	30
8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA.....	30
8.6. COMUNICAÇÃO DOS RESULTADOS	30
9. OUTROS ASSUNTOS JURÍDICOS	30
9.1. TARIFAS.....	30
9.1.1. Tarifas de emissão e renovação de certificados	30
9.1.2. Tarifas de acesso ao certificado.....	30
9.1.3. Tarifas de revogação ou de acesso à informação de status	30

9.1.4. Tarifas para outros serviços	30
9.1.5. Política de reembolso	30
9.2. RESPONSABILIDADE FINANCEIRA	30
9.2.1. Cobertura do seguro	30
9.2.2. Outros ativos.....	30
9.2.3. Cobertura de seguros ou garantia para entidades finais.....	30
9.3. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO	30
9.3.1. Escopo de informações confidenciais.....	30
9.3.2. Informações fora do escopo de informações confidenciais	30
9.3.3. Responsabilidade em proteger a informação confidencial	30
9.4. PRIVACIDADE DA INFORMAÇÃO DA INFORMAÇÃO PESSOAL	30
9.4.1. Plano de privacidade.....	30
9.4.2. Tratamento de informação como privadas	30
9.4.3. Informações não consideradas privadas	30
9.4.4. Responsabilidade para proteger a informação privadas.....	30
9.4.5. Aviso e consentimento para usar informações privadas.....	30
9.4.6. Divulgação em processo judicial ou administrativo	30
9.4.7. Outras circunstâncias de divulgação de informação	30
9.5. DIREITOS DE PROPRIEDADE INTELECTUAL	31
9.6. DECLARAÇÕES E GARANTIAS.....	31
9.6.1. Declarações e Garantias da AC	31
9.6.2. Declarações e Garantias da AR	31
9.6.3. Declarações e garantias do titular	31
9.6.4. Declarações e garantias das terceiras partes	31
9.6.5. Representações e garantias de outros participantes	31
9.7. ISENÇÃO DE GARANTIAS	31
9.8. LIMITAÇÕES DE RESPOSABILIDADE.....	31
9.9. INDENIZAÇÕES.....	31
9.10. PRAZO E RESCISÃO.....	31
9.10.1. Prazo	31
9.10.2. Término.....	31
9.10.3. Efeito da rescisão e sobrevivência.....	31
9.11. AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES.....	31
9.12. ALTERAÇÕES.....	31
9.12.1. Procedimento para emendas	31
9.12.2. Mecanismo de notificação e períodos.....	31
9.12.3. Circunstâncias na qual o OID deve ser alterado	31
9.13. SOLUÇÃO DE CONFLITOS.....	31

9.14. LEI APLICÁVEL	31
9.15. CONFORMIDADE COM A LEI APLICÁVEL.....	31
9.16. DISPOSIÇÕES DIVERSAS.....	31
9.16.1. Acordo completo	31
9.16.2. Cessão	31
9.16.3. Independência de disposições.....	31
9.16.4. Execução (honorários dos advogados e renúncia de direitos)	32
9.17. OUTRAS PROVISÕES.....	32
10. DOCUMENTOS REFERENCIADOS.....	32
11. REFERÊNCIAS BIOGRÁFICAS	32

CONTROLE DE ALTERAÇÕES

RESPONSÁVEL	APROVAÇÃO	DESCRIÇÃO DA ALTEAÇÃO	VERSÃO	DATA
Compliance	Versão Inicial		1.0	12.06.2015
Compliance	Resolução 116 - 2015	Referência à autoridade certificadora Raiz V5 e suas cadeias subsequentes	2.0	29.08.2018
Compliance	Resolução 118 - 2015	Aprova a retirada do campo AIA da LCR e define a obrigatoriedade de dois pontos de obtenção da LCR em novas cadeias de certificação digital ICP-Brasil	2.0	29.08.2018
Compliance	IN nº 07 - 2016	conformidade aos requisitos do programa de raízes confiáveis para manutenção dos certificados da AC RAIZ da ICP-Brasil nos repositórios dos navegadores de internet	2.0	29.08.2018
Compliance	Resolução 119 - 2017	Obrigatoriedade de realização de auditorias WebTrust.	2.0	29.08.2018
Compliance	Resolução 123 - 2017	Procedimentos de validação fora do ambiente físico da AR.	2.0	29.08.2018
Compliance		Atualização das Informações de contato da AC.	2.1	05.12.2018
Compliance	Resolução 150 - 2018	7.1.4	3.0	04.04.2019
Compliance	Resolução 151 e 154 - 2019	Atualização das informações conforme resoluções	4.0	21.10.2019
Compliance	Instruções Normativas 02 e 03 de 2020	Solicitação de Certificado Digital por videoconferência e Procedimentos para aprovação de normativos da AC.	5.0	07.05.2020
Compliance	Resolução 169	Adequação de Conteúdo	6.0	05.08.2020
Compliance	Resolução 179/2020	Atualização das informações conforme resolução	7.0	12.03.2021
Compliance		Informações administrativas da AC DOCCLOUD RFB	7.1	02.09.2021

1. INTRODUÇÃO

1.1. VISÃO GERAL

1.1.1. 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 ICP-Brasil, na elaboração de suas Políticas de Certificado (PC).

1.1.2 Esta Política de Certificado de Assinatura Digital tipo A1 da AC Doccloud RFB, a seguir designada simplesmente por "PC A1 da AC DOCCLOUD RFB" 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 A1

1.1.6 Os certificados A1 de assinatura estão associados aos requisitos menos rigorosos de segurança.

1.1.7 Os certificados A1 de assinatura podem ser emitidos para pessoas físicas ou jurídicas

1.1.8 Item não aplicável.

1.1.9 Item não aplicável.

1.1.10 Item não aplicável.

1.1.11 Item não aplicável.

1.1.12 Item não aplicável.

1.2. NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1. Esta PC é chamada “Política de Certificado de assinatura digital Tipo A1 da Autoridade Certificadora DOCCLOUD para a Secretaria da Receita Federal do Brasil” e referida como “PC A1 da AC DOCCLOUD RFB”. Esta PC descreve os usos relacionados ao certificado de assinatura digital correspondente ao tipo A1 no DOC-ICP-04 do Comitê Gestor da ICP-Brasil. O **OID** (object identifier) desta PC é **2.16.76.1.2.1.58**.

1.2.2 Item não aplicável.

1.3. PARTICIPANTES DA ICP-BRASIL

1.3.1. Autoridade Certificadora

1.3.1.1. Esta PC se refere à AC Doccloud RFB, integrante da ICP-Brasil, sob a hierarquia da Autoridade Certificadora Secretaria da Receita Federal do Brasil (AC RFB), 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 DOCLOUD RFB estão descritos na Declaração de Práticas de Certificação da AC DOCLOUD RFB - DPC da AC DOCLOUD RFB.

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 DOCLOUD RFB estão relacionados na página doccloud.com.br/repositorios/acdoccloudfb que contém:

- a) Relação de todas as ARs credenciadas;
- b) Relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento.

1.3.3 Titulares do Certificado

Pessoas físicas inscritas no CPF, desde que não enquadradas na situação cadastral de CANCELADA ou NULA, e pessoas jurídicas inscritas no CNPJ, desde que não enquadradas na condição de INAPTA, SUSPENSA, BAIXADA ou NULA conforme o disposto no Anexo I da Portaria RFB/Sucor/Cotec nº 42, de 07 de agosto de 2020 (Leiute dos Certificados Digitais da Secretaria da Receita Federal do Brasil - Versão 5.0). Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será o detentor da chave privada. Obrigatoriamente, o responsável pelo certificado é o mesmo responsável pela pessoa jurídica cadastrada no CNPJ da RFB. 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

Os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviços de Confiança - PSC vinculados à AC DOCLOUD RFB estão relacionados em sua página web doccloud.com.br/repositorios/acdoccloudfb

1.4. USABILIDADE DO CERTIFICADO

1.4.1. Uso apropriado do certificado

1.4.1.1 Neste item são relacionadas as aplicações para as quais os certificados definidos nesta PC são adequados.

1.4.1.2 As aplicações e demais programas que admitem 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 A AC DOCLOUD RFB leva em conta o nível de segurança previsto para o certificado definido por esta PC na definição das aplicações para o certificado. Esse nível de segurança é caracterizado pelos requisitos 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 Os certificados de tipos A1 emitidos pela AC DOCLOUD RFB serão utilizados em aplicações

como confirmação de identidade e assinatura de documentos eletrônicos com verificação da integridade de suas informações

1.4.1.5 Item não aplicável.

1.4.1.6 Item não aplicável.

1.4.1.7 Item não aplicável.

1.4.1.8 Item não aplicável.

1.4.2. Uso proibitivo do certificado.

Item não aplicável.

1.5. POLÍTICA DE ADMINISTRAÇÃO

1.5.1. Organização administrativa do documento.

AC DOCCLOUD RFB

DOCCLOUD SOLUÇÃO DIGITAL

1.5.2. Contatos

Endereço: Rua Gonçalves Dias, 519 – Jardim Girassol - Americana/SP - CEP: 13.465-670.

Telefone: (19) 3477-1144

Página Web: www.doccloud.com.br

1.5.3. Adequabilidade da DPC com PC's

AC DOCCLOUD RFB

Nome: Lucas Carvalho dos Santos

Departamento: NORMAS & COMPLIANCE

Telefone: (19) 3477-1144 Ramal 2214 **E-mail:** compliance@doccloud.com.br

1.5.4. Procedimentos de aprovação desta PC

Este documento foi analisado pela alta gestão da AC DOCCLOUD RFB e submetido ao Instituto de Tecnologia da Informação – ITI para aprovação. Os procedimentos de aprovação da PC da AC DOCCLOUD RFB são estabelecidos a critério do CG da ICP-Brasil.

1.6. DEFINIÇÕES E ACRÔNICOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridade de Registro
CEI	Cadastro Específico do INSS
CF-e	Cupom Fiscal Eletrônico
CG ICP-Brasil	Comitê Gestor da ICP-Brasil
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNPJ	Cadastro Nacional de Pessoas Jurídicas
CPF	Cadastro de Pessoas Físicas
CS	Code Signing

DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
EV	Extended Validation (WebTrust for Certification Authorities)
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
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
PSS	Prestador de Serviço de Suporte
RFC	Request For Comments
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 PUBLICAÇÕES E REPOSITÓRIO

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

2.1. REPOSITÓRIOS

2.2. PUBLICAÇÃO DE INFORMAÇÕES DOS CERTIFICADOS

2.3. TEMPO OU FREQUÊNCIA DE PUBLICAÇÃO

2.4. CONTROLE DE ACESSO OS REPOSITÓRIOS

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

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

3.1. NOMEAÇÃO

3.1.1. Tipos de nomes

3.1.2. Necessidade de os 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 DA 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 equipamento ou aplicação**
- 3.2.4. Autenticação da identidade de um indivíduo**
- 3.2.5. Informações não verificadas do titular do certificado**
- 3.2.6. Validação das autoridades**
- 3.2.7. Critérios para interoperação**

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

Nos itens correspondentes a lista abaixo são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

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 DA 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 DO 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 DE INSTALAÇÕES

Nos itens correspondentes a lista abaixo são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

5.1. CONTROLES FISÍCOS

- 5.1.1. Construção e localização das instalações
- 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. CONTROLE 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 de 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 esta PC A1 da AC DOCCLLOUD RFB. São definidos também outros controles técnicos de segurança utilizados pela AC DOCCLLOUD RFB e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

Compete à AC Raiz acompanhar a evolução tecnológica e, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, publicando nova versão do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP BRASIL [3].

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. Item não aplicável.

6.1.1.1.2. Item não aplicável.

6.1.1.2. O processo de geração de chaves do tipo A1, contemplado nesta PC, exige:

- a) A instalação de software relacionado ao repositório armazenador do certificado selecionado pelo cliente;
- b) O par de chaves será gerado em repositório protegido por senha e/ou identificação biométrica e cifrado por software;
- c) 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 do titular do certificado deve ser gravada cifrada, por algoritmo simétrico aprovado no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [1]. As chaves privadas correspondentes aos certificados poderão ser armazenadas em repositório protegido por senha, cifrado por software no meio de armazenamento definido para o tipo de certificado A1.

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 utilizado pelo titular assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a) A chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- b) A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e
- c) a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

6.1.1.7. Esta mídia de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6.1.1.8. O tipo de certificado emitido pela AC DOCCLLOUD RFB e descrito nesta PC é o A1.

Tabela 2 – Mídias Armazenadoras de Chaves Criptográficas

TIPO DE CERTIFICADO	MÍDIA ARMAZENADORA DE CHAVE CRIPTOGRÁFICA (Requisitos Mínimos)
A1	<i>Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima.</i>

6.1.2. Entrega da chave privada à entidade titular

Item não aplicável.

6.1.3. Entrega da chave pública para o 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 às terceiras partes

As formas para a disponibilização do certificado da AC DOCCLLOUD RFB, e de todos os certificados da cadeia V2 e da cadeia V5 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:

<http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv2.p7b> (para cadeia V2) e

<http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv5.p7b> (para cadeia V5).

d) outros meios seguros aprovados pelo CG ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Os certificados emitidos de acordo com esta PC situam-se sob a cadeia da Autoridade Certificadora Raiz Brasileira (V2 e V5). O tamanho das chaves criptográficas associadas é de 2048 bits.

6.1.5.2. Os algoritmos e os tamanhos de chaves a serem utilizados nos diferentes tipos de certificados da ICP-Brasil estão definidos em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

6.1.6 Geração de parâmetros de chaves assimétricas verificação da qualidade dos parâmetros

Os parâmetros de geração e verificação de chaves assimétricas dos titulares de certificados atendem ao padrão 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 o campo “key usage” na X.509 v3)

Os pares de chaves correspondentes aos certificados emitidos pela AC DOCCLLOUD RFB 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 DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

A chave privada de certificados emitidos conforme esta PC, é armazenada no repositório de certificados do sistema operacional utilizado pelo usuário no momento da emissão do certificado. 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 pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros através de recursos nativos do próprio sistema operacional. Também podem ser utilizados recursos adicionais de proteção como a definição de senhas para utilização e exportação da chave privada. Fica a critério do titular a configuração e utilização destes recursos adicionais de proteção.

6.2.1. Padrões e controle para módulo criptográfico

Item não aplicável.

6.2.2. Controle “n de m” para chave privada

Item não aplicável.

6.2.3. Custódia (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

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 DOCCLOUD RFB responsável por esta PC não mantém cópia de segurança de chave privada de titular.

6.2.4.3. Em qualquer caso, a cópia de segurança deverá ser armazenada cifrada por algoritmo simétrico aprovado em regulamento editado por instrução normativa da AC Raiz que defina 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. O titular do certificado, quando realizar uma cópia de segurança da sua chave privada, deve observar que esta cópia deve ser efetuada com, no mínimo, os mesmos requerimentos de segurança da chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1. A AC DOCCLOUD RFB não arquivava cópias de chaves privadas de assinatura digital de titulares de certificados.

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

Ver item 6.1

6.2.8. Método de ativação de chave privada

O titular de certificado de e-CPF ou e-CNPJ deve obrigatoriamente utilizar senha para a proteção de sua chave privada, de acordo com o art. 5. da Instrução Normativa RFB N.1077, de 29 de outubro de 2010.

6.2.9. Método de desativação de chave privada

O titular do certificado pode definir procedimentos necessários para a desativação de sua chave privada.

6.2.10. Método de destruição de chave privada

O titular do certificado pode definir procedimentos necessários para a destruição de sua chave privada.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

As chaves públicas da AC DOCLOUD RFB, de titulares dos certificados de assinatura digital e as LCRs emitidas pela AC DOCLOUD RFB são armazenadas 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. As chaves privadas dos respectivos Titulares são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 Item não aplicável.

6.3.2.3 Certificados do tipo A1 previstos nesta PC podem ter a validade de minutos, horas, dias e até **1 ano**.

6.3.2.4 Item não aplicável.

6.3.2.5 Item não aplicável.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes desta PC são 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

Para certificados de tipo A1, a geração e armazenamento do par de chaves são realizados em software, com capacidade de geração de chave, sendo ativado e protegido por senha, e/ou identificação biométrica.

6.4.2 Proteção dos dados de ativação

Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 Requisitos técnicos específicos de segurança computacional

O titular do certificado é responsável pela segurança computacional dos sistemas nos quais são geradas e utilizadas as chaves privadas e deve zelar por sua integridade. O equipamento onde são gerados os pares de chaves criptográficas do titular do Certificado deve dispor de mecanismos mínimos que garantam a segurança computacional, com proteção anti-vírus e criptografia 3DES para a chave privada, armazenada no HD.

6.5.2 Classificação da segurança computacional

Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

A AC DOCCLOUD RFB desenvolve sistemas apenas com finalidade relacionada à operação de suas AR vinculadas.

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC DOCCLOUD RFB utiliza os modelos clássico espiral e SCRUM no desenvolvimento dos sistemas, de acordo com a melhor adequação destes modelos ao projeto em desenvolvimento. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a AC DOCCLOUD RFB utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC DOCCLOUD RFB provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC DOCCLOUD RFB.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1. A AC DOCCLOUD RFB verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2. A AC DOCCLOUD RFB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificações de segurança de ciclo de vida

Item não aplicável.

6.6.4 Controles na geração da LCR antes de publicadas

Antes de publicadas, todas as LCRs geradas pela AC DOCCLOUD RFB 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

Item não aplicável.

6.8 CARIMBO DE TEMPO

Item não aplicável.

7. PERFIS DE CERTIFICADO, LCR E OSCP

Os itens seguintes especificam os formatos dos certificados e das LCRs geradas 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

Todos os certificados emitidos pela AC DOCCLOUD RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão

Todos os certificados emitidos pela AC DOCCLOUD RFB, 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. A AC DOCCLOUD RFB implementa as mesmas extensões definidas como obrigatórias na ICP-Brasil, descritas no item 7.1.2.2.

7.1.2.2. A AC DOCCLOUD RFB implementa nos certificados emitidos segundo esta PC as seguintes extensões, definidas como obrigatórias pela ICP-Brasil:

- a) **“Authority Key Identifier”, não crítica:** contém o resumo SHA-1 da chave pública da AC DOCCLOUD RFB;
- b) **“Key Usage”, crítica:** somente os bits digitalSignature, nonRepudiation e keyEncipherment são ativados;
- c) **“Certificate Policies”, não crítica,** contém
 - c.1) o campo *policyIdentifier* contém o OID desta PC **2.16.76.1.2.1.58**;
 - c.2) o campo *PolicyQualifiers* contém o endereço *Web* onde se obtém a DPC da AC DOCCLOUD RFB, onde: <http://repositorio.acdoccloud.com.br/ac-doccloudrfb/dpc-acdoccloudrfb.pdf>
- d) **“CRL Distribution Points”, não crítica:** contém o endereço *URL* das páginas *Web* onde se obtém a LCR da AC DOCCLOUD RFB:

Para Certificados Digitais emitidos na cadeia V2:

- d.1) <http://repositorio.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv2.crl>
- d.2) <http://repositorio2.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv2.crl>
- d.3) <http://acrepositorio.icpbrasil.gov.br/lcr/doccloud/lcr-ac-doccloudrfbv2.crl>

Para Certificados Digitais emitidos da cadeia V5:

- d.1) <http://repositorio.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv5.crl>
- d.2) <http://repositorio2.acdoccloud.com.br/ac-doccloudrfb/lcr-ac-doccloudrfbv5.crl>

e) **"Authority Information Access", não crítica:** contém o método de acesso **id-ad-calssuer**, utilizando o protocolo de acesso HTTP, para a recuperação da cadeia de certificação no seguinte endereço:

e1) **Para Certificados Digitais emitidos na cadeia V2:**

<http://repositorio.acdoccloud.com.br/acdoccloudrfb/ac-doccloudrfbv2.p7b>

e2) **Para Certificados Digitais emitidos na cadeia V5:**

<http://repositorio.acdoccloud.com.br/acdoccloudrfb/ac-doccloudrfbv5.p7b>

A segunda entrada pode conter o método de acesso **id-ad-ocsp**, com o respectivo endereço do respondedor OCSP, utilizando o protocolo de acesso HTTP, nos seguintes endereços, onde estas extensões somente serão aplicáveis para certificados de usuário final: <http://ocsp.acdoccloud.com.br>

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

a) Para certificado de pessoa física:

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

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.

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

OID = 2.16.76.1.3.5 e conteúdo = nas primeiras 12 (doze) posições, o número de inscrição do Título de Eleitor; nas 3 (três) posições subsequentes, a Zona Eleitoral; nas 4 (quatro) posições seguintes, a Seção; nas 22 (vinte e duas) posições subsequentes, o município e a UF do Título de Eleitor.

a.2) Item não aplicável;

a.3) Item não aplicável;

a.4) Item não aplicável;

b) Para certificado de pessoa jurídica:

4 (quatro) campos otherName, obrigatórios, contendo, nesta ordem:

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 Identificação 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;

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

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;

OID = 2.16.76.1.3.7 e conteúdo = nas 12 (doze) posições o número do Cadastro Especifico do INSS (CEI) da pessoa jurídica titular do certificado

c) Item não aplicável;

d) Item não aplicável;

e) Item não aplicável;

7.1.2.4 Os campos otherName definidos como obrigatórios pela ICP-Brasil estão 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 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) Quando a identificação profissional não estiver disponível, não deverá ser inserido o campo (OID) correspondente, exceto nos casos de certificado digital cuja titularidade foi validada pela AR de conselho de classe profissional;

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

h) Item não aplicável.

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. As extensões “Key Usage” e “Extended Key Usage” para os referidos tipos de certificado são obrigatórias e devem obedecer aos propósitos de uso e a criticalidade conforme descrição abaixo:

- a) Item não aplicável.
- b) Item não aplicável.
- c) Item não aplicável.
- d) Item não aplicável.
- e) Item não aplicável.
- f) Para os demais certificados de Assinatura e/ou Proteção de e-Mail:
 - i. “Key Usage”, crítica: somente os seguintes bits devem estar ativados: digitalSignature, nonRepudiation e keyEncipherment.
 - ii. “Extended Key Usage”, não crítica: deve conter os seguintes valores representados por seus respectivos OID:
 - ✓ “client authentication”, obrigatória: OID = 1.3.6.1.5.5.7.3.2, para autenticação de cliente;
 - ✓ “e-mail protection”, obrigatória: OID = 1.3.6.1.5.5.7.3.4, para proteção de e-mail.
- g) item não aplicável.

7.1.3. Identificadores de algoritmo

Os certificados emitidos pela AC DOCCLOUD RFB são assinados utilizando o algoritmo RSA com SHA-256 como função de hash (OID = 1.2.840.113549.1.1.11) conforme o regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil.

7.1.4 Formatos de nome

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:

a) Para certificados e-CPF

C = BR

O = ICP-Brasil

OU = Secretaria da Receita Federal do Brasil – RFB

OU = RFB e-CPF A1

OU = Domínio do certificado (Opcional)

OU = CNPJ da AR onde ocorreu a identificação presencial

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

CN = Nome da Pessoa Física: número de inscrição no CPF

Onde

I - O Common Name (CN) é composto do nome da pessoa física, obtido do Cadastro de Pessoas Físicas (CPF) da RFB, com comprimento máximo de 52 (cinquenta e dois) caracteres, acrescido do sinal de dois

pontos (:) mais o número de inscrição da pessoa física do titular neste cadastro composto por 11 (onze) caracteres.

São cinco os campos Organizational Unit (OU) definidos no certificado, assim constituídos:

II - São cinco os campos Organizational Unit (OU) definidos no certificado, assim constituídos:

- a) Primeiro “OU” informando o tipo de identificação utilizada (presencial, videoconferência ou certificado digital);
- b) Segundo “OU” informando o CNPJ da AR que realizou a identificação do titular;
- c) Terceiro “OU” com conteúdo variável, informando no campo domínio a identificação da empresa ou órgão fornecedor do certificado, quando o titular for seu empregado, funcionário ou servidor. Caso esse “OU” não seja utilizado, o mesmo deverá ser grafado com o texto “EM BRANCO”;
- d) Quarto “OU” com conteúdo fixo “RFB e-CPF A1”;
- e) Quinto “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”

III - O campo Organization Name (O) com conteúdo fixo igual a “ICP-Brasil”.

IV - O campo Country Name (C) com conteúdo fixo igual a “BR”.

b) Para Certificados e-CNPJ

C = BR

O = ICP-Brasil

ST= <Sigla da unidade da federação>

L = cidade

OU = CNPJ da AR onde ocorreu a identificação presencial

OU = Secretaria da Receita Federal do Brasil – RFB

OU = RFB e-CNPJ A1

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

CN = Nome Empresarial: número de inscrição no CNPJ

Onde:

I - O Common Name (CN) é composto do nome empresarial da pessoa jurídica, obtido do Cadastro Nacional da Pessoa Jurídica (CNPJ) da RFB, com comprimento máximo de 49 (quarenta e nove) caracteres, acrescido do sinal de dois pontos (:) mais o número de inscrição da empresa titular do certificado neste cadastro composto por 14 (quatorze) caracteres.

II - São quatro os campos Organizational Unit (OU) definidos no certificado, sendo assim constituídos:

- a) Primeiro “OU” informando o tipo de identificação utilizada (presencial, videoconferência ou certificado digital);
- b) Segundo “OU” com conteúdo fixo “RFB e-CNPJ A1”;
- c) Terceiro “OU” com conteúdo fixo “Secretaria da Receita Federal do Brasil – RFB”;

d) Quarto “OU” informando o CNPJ da AR que realizou a identificação do titular.

III - O campo locality (L) com conteúdo correspondente ao nome da cidade onde a empresa está localizada. O campo deve ser preenchido sem acentos nem abreviaturas.

IV - O campo state or province name (ST) com conteúdo correspondente a sigla do estado onde a empresa está localizada.

V - O campo Organization Name (O) com conteúdo fixo igual a “ICP-Brasil”.

VI - O campo Country Name (C) com conteúdo fixo igual a “BR”.

NOTA: No formato, os caracteres “<” e “>” delimitam campos que serão substituídos pelos seus respectivos valores, não devendo ser incluídos no conteúdo do certificado.

7.1.4.2 Item não aplicável.

7.1.4.3 Item não aplicável.

7.1.4.4 Item não aplicável.

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, 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 certificado emitidos pela AC DOCCLOUD RFB são as seguintes:

- 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

7.1.6 OID (Object Identifier) de Política de Certificado

O OID atribuído a esta Política de Certificado é: **2.16.76.1.2.1.58**.

7.1.7 Uso da extensão “Policy Constraints”

Item não aplicável.

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 DOCLOUD RFB, sendo:

<http://repositorio.acdoccloud.com.br/ac-doccloudrfb/dpc-acdoccloudrfb.pdf>

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são ser interpretadas conforme a RFC 5280.

7.2. PERFIL DE LCR

7.2.1. Número de versão

As LCRs geradas pela AC DOCLOUD RFB 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 DOCLOUD RFB adota as extensões de LCR utilizadas e sua criticalidade:

- a) **“Authority Key Identifier”, não crítica:** contém o resumo SHA-1 da chave pública da AC DOCLOUD RFB que assina a LCR;
- b) **“CRL Number”, não crítica:** contém número sequencial para cada LCR emitida pela AC que assina a LCR.
- c) **“Authority Information Access”, não crítica:** contém o endereço web onde se poderá obter a cadeia de certificação:

Para Certificados Digitais emitidos na cadeia V2:

<http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv2.p7b>

Para Certificados Digitais emitidos na cadeia V5:

<http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloudrfbv5.p7b>

7.2.2.2 A AC DOCLOUD RFB adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

- a) **“Authority Key Identifier”, não crítica:** contém o resumo SHA-1 da chave pública da AC DOCLOUD RFB que assina a LCR; e

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

7.3. PERFIL DE OCSP

7.3.1. Número(s) de versão

Os serviços de respostas OCSP da AC DOCCLOUD RFB implementam a versão 1. do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960.

7.3.2. Extensões de OCSP

Os serviços de respostas OCSP da AC DOCCLOUD RFB estão em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

Nos itens correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

8.1. FREQUÊNCIA E CIRCUNSTÂNCIA DAS AVALIAÇÕES

8.2. IDENTIFICAÇÃO E QUALIFICAÇÃO DO AVALIADOR

8.3. RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.4. TÓPICOS COBERTOS PELA AVALIAÇÃO

8.5. AÇÕES TOMADAS COMO RESULTADO DE UMA DEFICIÊNCIA

8.6. COMUNICAÇÃO DOS RESULTADO

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

Nos itens correspondentes à lista abaixo são referidos os itens correspondentes da DPC da AC DOCCLOUD RFB.

9.1. TARIFAS

9.1.1. Tarifas de emissão e renovação de certificados

9.1.2. Tarifas de acesso ao certificado

9.1.3. Tarifas de revogação ou de acesso à informação de status

9.1.4. Tarifas para outros serviços

9.1.5. Política de reembolso

9.2. RESPONSABILIDADE FINANCEIRA

9.2.1. Cobertura do seguro

9.2.2. Outros ativos

9.2.3. Cobertura de seguros ou garantia para entidades finais

9.3. CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1. Escopo de informações confidenciais

9.3.2. Informações fora do escopo de informações confidenciais

9.3.3. Responsabilidade em proteger a informação confidencial

9.4. PRIVACIDADE DA INFORMAÇÃO DA INFORMAÇÃO PESSOAL

9.4.1. Plano de privacidade

9.4.2. Tratamento de informação como privadas

9.4.3. Informações não consideradas privadas

9.4.4. Responsabilidade para proteger a informação privadas

9.4.5. Aviso e consentimento para usar informações privadas

9.4.6. Divulgação em processo judicial ou administrativo

9.4.7. Outras circunstâncias de divulgação de informação

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 RESPONSABILIDADE

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

Alterações nesta PC podem ser solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da AC DOCCLOUD RFB. A aprovação e consequente adoção de nova versão estarão sujeitas à autorização da AC Raiz.

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

9.12.2. Mecanismo de notificação e períodos

A AC DOCCLOUD RFB mantém página específica com a versão corrente desta PC para consulta pública, a qual está disponibilizada no endereço Web

<http://repositorio.acdoccloud.com.br/ac-doccloudrfb/ac-doccloud-rfb-pc-a1.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 DOCCLOUD RFB 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 da AC DOCCLOUD RFB foi submetida à aprovação, durante o processo de credenciamento da AC DOCCLOUD RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

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.it.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
[4]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[5]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DOS PRESTADORES DE SERVIÇOS DE CONFIANÇA DA ICP-BRASIL	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 6960, IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.