



Declaração de Práticas de Certificação da Autoridade Certificadora Certisign OM-BR

DPC da AC Certisign OM-BR

Versão 2.0 – 09/04/2025





Sumário

| | |
|---|----|
| CONTROLE DE ALTERAÇÕES | 11 |
| 1. INTRODUÇÃO..... | 12 |
| 1.1. Visão Geral..... | 12 |
| 1.2. Nome do documento e identificação | 12 |
| 1.3. Participantes da ICP-Brasil | 12 |
| 1.3.1. Autoridades Certificadoras..... | 12 |
| 1.3.2. Autoridades de Registro..... | 12 |
| 1.3.3. Titulares do Certificado | 13 |
| 1.3.4. Partes Confiáveis | 13 |
| 1.3.5. Outros Participantes..... | 13 |
| 1.4. Usabilidade do Certificado | 13 |
| 1.4.1 Uso apropriado do certificado | 13 |
| 1.4.2 Uso proibitivo do certificado | 13 |
| 1.5 Políticas de Administração | 14 |
| 1.5.1 Organização administrativa do documento..... | 14 |
| 1.5.2 Contatos | 14 |
| 1.5.3 Pessoa que determina a adequabilidade da DPC com a PC | 14 |
| 1.5.4 Procedimentos de aprovação da DPC..... | 14 |
| 1.6 Definições e Acrônimos | 14 |
| 2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO..... | 16 |
| 2.1. Repositórios | 16 |
| 2.2. Publicação de informações dos certificados | 17 |
| 2.3. Tempo ou Frequência de Publicação | 17 |
| 2.4. Controle de Acesso aos Re却positórios..... | 17 |
| 3. IDENTIFICAÇÃO E AUTENTICAÇÃO | 18 |
| 3.1. Atribuição de Nomes..... | 18 |
| 3.1.1. Tipos de nomes | 18 |
| 3.1.2. Necessidade dos nomes serem significativos | 18 |
| 3.1.3. Anônimo ou Pseudônimo dos Titulares do Certificado..... | 18 |
| 3.1.4. Regras para interpretação de vários tipos de nomes | 18 |
| 3.1.5. Unicidade de nomes..... | 18 |
| 3.1.6. Procedimento para resolver disputa de nomes | 18 |



| | |
|---|-----------|
| 3.1.7. Reconhecimento, autenticação e papel de marcas registradas | 18 |
| 3.2. Validação inicial de identidade | 19 |
| 3.2.1. Método para comprovar a posse de chave privada..... | 19 |
| 3.2.2. Autenticação da identificação da organização..... | 19 |
| 3.2.3. Autenticação da identidade de um indivíduo | 19 |
| 3.2.4. Informações não verificadas do titular do certificado..... | 20 |
| 3.2.5. Validação das autoridades | 20 |
| 3.2.6. Critérios para interoperabilidade..... | 20 |
| 3.2.7. Autenticação da identidade de equipamento ou aplicação | 20 |
| 3.2.8 Procedimentos complementares..... | 21 |
| 3.2.9. Procedimentos específicos | 22 |
| 3.3. Identificação e autenticação para pedidos de novas chaves..... | 23 |
| 3.4. Identificação e Autenticação para solicitação de revogação | 23 |
| 4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO | 23 |
| 4.1. Solicitação do certificado | 23 |
| 4.1.1. Quem pode submeter uma solicitação de certificado..... | 24 |
| 4.1.2. Processo de registro e responsabilidades | 24 |
| 4.2. Processamento de Solicitação de Certificado | 26 |
| 4.2.1. Execução das funções de identificação e autenticação | 26 |
| 4.2.2. Aprovação ou rejeição de pedidos de certificado | 26 |
| 4.2.3. Tempo para processar a solicitação de certificado | 27 |
| 4.3. Emissão de Certificado | 27 |
| 4.3.1. Ações da AC durante a emissão de um certificado | 27 |
| 4.3.2. Notificações para o titular do certificado pela AC na emissão do certificado | 27 |
| 4.4. Aceitação de Certificado | 27 |
| 4.4.1. Conduta sobre a aceitação do certificado..... | 27 |
| 4.4.2. Publicação do certificado pela AC | 28 |
| 4.4.3. Notificação de emissão do certificado pela AC Raiz para outras entidades .. | 28 |
| 4.5. Usabilidade do par de chaves e do certificado | 28 |
| 4.5.1. Usabilidade da Chave privada e do certificado do titular..... | 28 |
| 4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis | 29 |
| 4.6. Renovação de Certificados | 29 |
| 4.6.1. Circunstâncias para renovação de certificados | 29 |
| 4.6.2. Quem pode solicitar a renovação | 29 |





| | |
|---|----|
| 4.6.3. Processamento de requisição para renovação de certificados | 29 |
| 4.6.4. Notificação para nova emissão de certificado para o titular | 29 |
| 4.6.5. Conduta constituindo a aceitação de uma renovação de um..... | 29 |
| 4.6.6. Publicação de uma renovação de um certificado pela AC | 29 |
| 4.6.7. Notificação de emissão de certificado pela AC para outras entidades .. | 29 |
| 4.7. Nova chave de certificado (Re-key)..... | 29 |
| 4.7.1. Circunstâncias para nova chave de certificado | 29 |
| 4.7.2. Quem pode requisitar a certificação de uma nova chave pública | 29 |
| 4.7.3. Processamento de requisição de novas chaves de certificado..... | 29 |
| 4.7.4. Notificação de emissão de novo certificado para o titular | 29 |
| 4.7.5. Conduta constituindo a aceitação de uma nova chave certificada | 29 |
| 4.7.6. Publicação de uma nova chave certificada pela AC..... | 30 |
| 4.7.7. Notificação de uma emissão de certificado pela AC para outras entidades .. | 30 |
| 4.8. Modificação de certificado | 30 |
| 4.8.1. Circunstâncias para modificação de certificado | 30 |
| 4.8.2. Quem pode requisitar a modificação de certificado..... | 30 |
| 4.8.3. Processamento de requisição de modificação de certificado..... | 30 |
| 4.8.4. Notificação de emissão de novo certificado para o titular | 30 |
| 4.8.5. Conduta constituindo a aceitação de uma modificação de certificado..... | 30 |
| 4.8.6. Publicação de uma modificação de certificado pela AC..... | 30 |
| 4.8.7. Notificação de uma emissão de certificado pela AC para outras entidades .. | 30 |
| 4.9. Suspensão e Revogação de Certificado | 30 |
| 4.9.1. Circunstâncias para revogação..... | 30 |
| 4.9.2. Quem pode solicitar revogação | 31 |
| 4.9.3. Procedimento para solicitação de revogação | 31 |
| 4.9.4. Prazo para solicitação de revogação | 32 |
| 4.9.5. Tempo em que a AC deve processar o pedido de revogação | 32 |
| 4.9.6. Requisitos de verificação de revogação para as partes confiáveis..... | 32 |
| 4.9.7. Frequência de emissão de LCR..... | 33 |
| 4.9.8. Latência máxima para a LCR..... | 33 |
| 4.9.9. Disponibilidade para revogação/verificação de status on-line..... | 33 |
| 4.9.10. Requisitos para verificação de revogação on-line | 34 |
| 4.9.11. Outras formas disponíveis para divulgação de revogação..... | 34 |
| 4.9.12. Requisitos especiais para o caso de comprometimento de chave | 34 |





| | |
|--|----|
| 4.9.13. Circunstâncias para suspensão | 34 |
| 4.9.14. Quem pode solicitar suspensão..... | 34 |
| 4.9.15. Procedimento para solicitação de suspensão | 34 |
| 4.9.16. Limites no período de suspensão | 34 |
| 4.10. Serviços de status de certificado | 35 |
| 4.10.1. Características operacionais..... | 35 |
| 4.10.2. Disponibilidade dos serviços..... | 35 |
| 4.10.3. Funcionalidades operacionais..... | 35 |
| 4.11. Encerramento de atividades | 35 |
| 4.12. Custódia e recuperação de chave | 36 |
| 4.12.1. Política e práticas de custódia e recuperação de chave | 36 |
| 4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão | 36 |
| 5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES | 36 |
| 5.1 Controles Físicos | 36 |
| 5.1.1. Construção e localização das instalações de AC | 36 |
| 5.1.2. Acesso físico | 37 |
| 5.1.3. Energia e ar-condicionado | 40 |
| 5.1.4. Exposição à água | 41 |
| 5.1.5. Prevenção e proteção contra incêndio | 41 |
| 5.1.6. Armazenamento de mídia | 41 |
| 5.1.7. Destriuição de lixo | 41 |
| 5.1.8. Instalações de segurança (<i>backup</i>) externas (<i>off-site</i>) para AC | 41 |
| 5.2. Controles Procedimentais | 42 |
| 5.2.1. Perfis qualificados | 42 |
| 5.2.2. Número de pessoas necessário por tarefa | 43 |
| 5.2.3. Identificação e autenticação para cada perfil..... | 43 |
| 5.2.4. Funções que requerem separação de deveres | 44 |
| 5.3. Controles de Pessoal | 44 |
| 5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade | 44 |
| 5.3.2. Procedimentos de verificação de antecedentes | 44 |
| 5.3.3. Requisitos de treinamento..... | 44 |
| 5.3.4. Frequência e requisitos para reciclagem técnica | 45 |
| 5.3.5. Frequência e sequência de rodízio de cargos | 45 |
| 5.3.6. Sanções para ações não autorizadas..... | 45 |





| | |
|--|----|
| 5.3.7. Requisitos para contratação de pessoal | 45 |
| 5.3.8. Documentação fornecida ao pessoal..... | 46 |
| 5.4. Procedimentos de Log de Auditoria..... | 46 |
| 5.4.1. Tipos de eventos registrados | 46 |
| 5.4.2. Frequência de auditoria de registros..... | 47 |
| 5.4.3. Período de retenção para registros de auditoria | 48 |
| 5.4.4. Proteção de registros de auditoria | 48 |
| 5.4.5. Procedimentos para cópia de segurança (Backup) de registros de auditoria | 48 |
| 5.4.6. Sistema de coleta de dados de auditoria (interno ou externo) | 48 |
| 5.4.7. Notificação de agentes causadores de eventos | 48 |
| 5.4.8. Avaliações de vulnerabilidade..... | 49 |
| 5.5. Arquivamento de Registros..... | 49 |
| 5.5.1. Tipos de registros arquivados | 49 |
| 5.5.2. Período de retenção para arquivo..... | 49 |
| 5.5.3. Proteção de arquivo | 49 |
| 5.5.4. Procedimentos de cópia de arquivo..... | 49 |
| 5.5.5. Requisitos para datação de registros..... | 50 |
| 5.5.6. Sistema de coleta de dados de arquivo (interno e externo) | 50 |
| 5.5.7. Procedimentos para obter e verificar informação de arquivo | 50 |
| 5.6. Troca de chave | 50 |
| 5.7. Comprometimento e Recuperação de Desastre | 50 |
| 5.7.1. Procedimentos de gerenciamento de incidente e comprometimento | 50 |
| 5.7.2. Recursos computacionais, software, e/ou dados corrompidos | 51 |
| 5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade | 51 |
| 5.7.4. Capacidade de continuidade de negócio após desastre | 52 |
| 5.8. Extinção da AC | 52 |
| 6. CONTROLES TÉCNICOS DE SEGURANÇA..... | 52 |
| 6.1. Geração e Instalação do Par de Chaves..... | 52 |
| 6.1.1. Geração do par de chaves | 52 |
| 6.1.2. Entrega da chave privada à entidade | 53 |
| 6.1.3. Entrega da chave pública para emissor de certificado | 53 |
| 6.1.4. Entrega de chave pública da AC às terceiras partes..... | 53 |
| 6.1.5. Tamanhos de chave | 53 |





| | |
|---|----|
| 6.1.6. Geração de parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros..... | 54 |
| 6.1.7. Propósitos de uso de chave (conforme o campo “key usage” na X.509 v3) .. | 54 |
| 6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico ... | 54 |
| 6.2.1. Padrões e controle para módulo criptográfico | 54 |
| 6.2.2. Controle “n de m” para chave privada | 55 |
| 6.2.3. Custódia (escrow) de chave privada..... | 55 |
| 6.2.4. Cópia de segurança de chave privada | 55 |
| 6.2.5. Arquivamento de chave privada..... | 55 |
| 6.2.6. Inserção de chave privada em módulo criptográfico | 55 |
| 6.2.7 Armazenamento de chave privada em módulo criptográfico | 55 |
| 6.2.8. Método de ativação de chave privada | 55 |
| 6.2.9. Método de desativação de chave privada | 56 |
| 6.2.10. Método de destruição de chave privada | 56 |
| 6.3. Outros Aspectos do Gerenciamento do Par de Chaves | 56 |
| 6.3.1. Arquivamento de chave pública | 56 |
| 6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada | 57 |
| 6.4. Dados de Ativação | 57 |
| 6.4.1. Geração e instalação dos dados de ativação | 57 |
| 6.4.2. Proteção dos dados de ativação | 57 |
| 6.4.3. Outros aspectos dos dados de ativação..... | 57 |
| 6.5. Controles de Segurança Computacional | 58 |
| 6.5.1. Requisitos técnicos específicos de segurança computacional..... | 58 |
| 6.5.2. Classificação da segurança computacional..... | 59 |
| 6.5.3. Controles de Segurança para as Autoridades de Registro | 59 |
| 6.6. Controles Técnicos do Ciclo de Vida | 60 |
| 6.6.1. Controles de desenvolvimento de sistema | 60 |
| 6.6.2. Controles de gerenciamento de segurança | 60 |
| 6.6.3. Controles de segurança de ciclo de vida | 60 |
| 6.6.4 Controles na Geração de LCR | 60 |
| 6.7. Controles de Segurança de Rede | 60 |
| 6.7.1 Diretrizes Gerais..... | 60 |
| 6.7.2. <i>Firewall</i> | 61 |





| | |
|--|----|
| 6.7.3. Sistema de detecção de intrusão (IDS) | 61 |
| 6.7.4. Registro de acessos não-autorizados à rede | 61 |
| 6.8. Carimbo de Tempo | 61 |
| 7. PERFIS DE CERTIFICADO, LCR E OCSP | 62 |
| 7.1. Perfil do Certificado..... | 62 |
| 7.1.1. Número de versão | 62 |
| 7.1.2. Extensões de certificado | 62 |
| 7.1.3. Identificadores de algoritmo | 62 |
| 7.1.4. Formatos de nome | 62 |
| 7.1.5. Não se aplica..... | 62 |
| 7.1.6. OID (<i>Object Identifier</i>) da DPC..... | 62 |
| 7.1.7. Uso da extensão “ <i>Policy Constraints</i> ”..... | 62 |
| 7.1.8. Sintaxe e semântica dos qualificadores de política | 62 |
| 7.1.9. Semântica de processamento para as extensões críticas de PC | 62 |
| 7.2. Perfil de LCR | 62 |
| 7.2.1. Número(s) de versão..... | 62 |
| 7.2.2. Extensões de LCR e de suas entradas | 62 |
| 7.3. Perfil de OCSP | 63 |
| 7.3.1. Número(s) de versão..... | 63 |
| 7.3.2. Extensões de OCSP | 63 |
| 8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES..... | 63 |
| 8.1. Frequência e circunstâncias das avaliações | 63 |
| 8.2. Identificação/Qualificação do avaliador | 63 |
| 8.3. Relação do avaliador com a entidade avaliada..... | 63 |
| 8.4. Tópicos cobertos pela avaliação | 64 |
| 8.5. Ações tomadas como resultado de uma deficiência | 64 |
| 8.6. Comunicação dos resultados..... | 64 |
| 9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS | 64 |
| 9.1. Tarifas | 64 |
| 9.1.1. Tarifas de emissão e renovação de certificados | 64 |
| 9.1.2. Tarifas de acesso ao certificado | 64 |
| 9.1.3. Tarifas de revogação ou de acesso à informação de status | 64 |
| 9.1.4. Tarifas para outros serviços | 65 |
| 9.1.5. Política de reembolso | 65 |





| | |
|--|----|
| 9.2. Responsabilidade Financeira..... | 65 |
| 9.2.1 Cobertura do seguro | 65 |
| 9.2.2 Outros ativos | 65 |
| 9.2.3 Cobertura de seguros ou garantia para entidades finais..... | 65 |
| 9.3 Confidencialidade da informação do negócio..... | 65 |
| 9.3.1 Escopo de informações confidenciais..... | 65 |
| 9.3.2 Informações fora do escopo de informações confidenciais..... | 65 |
| 9.3.3 Responsabilidade em proteger a informação confidencial | 66 |
| 9.4 Privacidade da informação pessoal..... | 67 |
| 9.4.1 Plano de privacidade..... | 67 |
| 9.4.2 Tratamento de informação como privadas | 67 |
| 9.4.3 Informações não consideradas privadas | 67 |
| 9.4.4 Responsabilidade para proteger a informação privadas | 67 |
| 9.4.5 Aviso e consentimento para usar informações privadas | 67 |
| 9.4.6 Divulgação em processo judicial ou administrativo | 67 |
| 9.4.7 Outras circunstâncias de divulgação de informação | 68 |
| 9.4.8 Informações a terceiros..... | 68 |
| 9.5 Direitos de Propriedade Intelectual..... | 68 |
| 9.6 Declarações e Garantias | 68 |
| 9.6.1 Declarações e Garantias da AC..... | 68 |
| 9.6.2 Declarações e Garantias da AR..... | 69 |
| 9.6.3 Declarações e garantias do titular..... | 69 |
| 9.6.4 Declarações e garantias das terceiras partes..... | 69 |
| 9.6.5 Representações e garantias de outros participantes | 70 |
| 9.7 Isenção de garantias | 70 |
| 9.8 Limitações de responsabilidades..... | 70 |
| 9.9 Indenizações | 70 |
| 9.10 Prazo e Rescisão | 70 |
| 9.10.1 Prazo | 70 |
| 9.10.2 Término | 70 |
| 9.10.3 Efeito da rescisão e sobrevivência..... | 70 |
| 9.11 Avisos individuais e comunicações com os participantes | 70 |
| 9.12. Alterações | 70 |
| 9.12.1. Procedimento para emendas | 70 |





| | |
|---|----|
| 9.12.2. Mecanismo de notificação e períodos | 71 |
| 9.12.3. Circunstâncias na qual o OID deve ser alterado | 71 |
| 9.13. Solução de conflitos | 71 |
| 9.14. Lei aplicável | 71 |
| 9.15. Conformidade com a Lei aplicável..... | 71 |
| 9.16. Disposições Diversas..... | 71 |
| 9.16.1. Acordo completo | 71 |
| 9.16.2. Cessão | 71 |
| 9.16.3. Independência de disposições..... | 71 |
| 9.16.4. Execução (honorários dos advogados e renúncia de direitos)..... | 72 |
| 9.17. Outras provisões | 72 |
| 10. DOCUMENTOS REFERENCIADOS | 72 |
| 11. REFERÊNCIAS BIBLIOGRÁFICAS | 73 |





CONTROLE DE ALTERAÇÕES

| Versão | Data | Resolução que Aprovou a alteração | Item Alterado | Descrição da Alteração |
|--------|------------|-----------------------------------|---------------|--|
| 1.0 | 25/03/2021 | -- | -- | Criação da AC. |
| 2.0 | 09/04/2025 | Resolução nº 211, de 31.10.2024 | Vários | Adequação para atender a nova resolução. |





Declaração de Práticas de Certificação da Autoridade Certificadora Certisign OM-BR

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora Certisign OM-BR (AC Certisign OM-BR) integrante na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços de certificação digital.

1.1.2. A estrutura desta DPC está baseada no DOC-ICP-05– REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICA DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL[5].

As referências a formulários presentes nesta DPC deverão ser entendidas também como referências a outras formas que a AC Certisign OM-BR ou entidades a ela vinculadas possa vir a adotar.

1.1.3 A estrutura desta DPC está baseada na RFC 3647.

1.1.4 A AC Certisign OM-BR mantém todas as informações da sua DPC sempre atualizadas.

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

1.2. Nome do documento e identificação

1.2.1. Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora Certisign OM-BR e referida como "DPC da AC Certisign OM-BR", cujo OID (*object identifier*) é 2.16.76.1.1.183.

1.2.2. A AC Certisign OM-BR emissora de certificados para Objetos Metrológicos (OM-BR) é exclusiva e separada de acordo com o propósito de uso de chaves de Assinatura de documento.

1.3. Participantes da ICP-Brasil

1.3.1. Autoridades Certificadoras

Esta DPC refere-se exclusivamente à AC Certisign OM-BR no âmbito da ICP-Brasil.

1.3.2. Autoridades de Registro

1.3.2.1. Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC Certisign OM-BR para os processos de recebimento, identificação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou





em página web da AC Certisign OM-BR (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html):

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

1.3.3. Titulares do Certificado

Certificados do tipo Objeto Metrológico - OM-BR só podem ser emitidos para equipamentos metrológicos regulados pelo INMETRO. O titular do certificado será o fabricante identificado no certificado digital ICP-Brasil de pessoa jurídica que assina a solicitação, associada ao número de identificação do equipamento detentor da chave privada.

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

1.3.5.1. A relação de todos os Prestadores de Serviços de Suporte – PSS, Prestadores de Serviços Biométricos – PSBios e Prestadores de Serviço de Confiança – PSC vinculados à AC Certisign OM-BR é publicada em serviço de diretório e/ou em página web da AC Certisign OM-BR (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html).

1.4. Usabilidade do Certificado

1.4.1 Uso apropriado do certificado

A AC Certisign OM-BR implementa a seguinte Políticas de Certificado Digital:

Para Certificados de Assinatura Digital:

- Política de Certificado de Assinatura Digital da Autoridade Certificadora Certisign OM-BR, PC da AC Certisign OM-BR, OID 2.16.76.1.2.550.5.

Na PC correspondente estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC Certisign OM-BR e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.4.2 Uso proibitivo do certificado

Quando cabível, as aplicações para as quais existam restrições ou proibições para o uso desses certificados estão listados nas PCs implementadas.





1.5 Política de Administração

Neste item estão incluídos nome, endereço e outras informações da AC Certisign OM-BR, assim como são informados o nome, os números de telefone e o endereço eletrônico de uma pessoa para contato.

1.5.1 Organização administrativa do documento

Nome da AC: AC Certisign OM-BR

1.5.2 Contatos

Endereço: Avenida Brigadeiro Faria Lima, 1485, Andar 06 – Torre Norte – Cond. C. E. Mario Garnero – São Paulo – 01452-002.

Telefone: (11) 99712-9924

Página web: http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html

E-mail: normas@certisign.com.br

Outros:

1.5.3 Pessoa que determina a adequabilidade da DPC com a PC

Nome: Márcio Fernandes Tolentino

Área: Auditoria e Normas

Telefone: (11) 99712-9924

E-mail: normas@certisign.com.br

Outros:

1.5.4 Procedimentos de aprovação da DPC

Esta DPC é aprovada pelo ITI.

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

1.6 Definições e Acrônimos

| SIGLA | Descrição |
|---------|---|
| AC | Autoridade Certificadora |
| ACME | <i>Automatic Certificate Management Environment</i> |
| AC Raiz | Autoridade Certificadora Raiz da ICP-Brasil |
| ACT | Autoridade de Carimbo do Tempo |
| AR | Autoridades de Registro |
| CEI | Cadastro Específico do INSS |
| CF-e | Cupom Fiscal Eletrônico |
| CG | Comitê Gestor |
| CMM-SEI | Capability Maturity Model do Software Engineering Institute |





| | |
|-------------------|---|
| CN | <i>Common Name</i> |
| CNE | Carteira Nacional de Estrangeiro |
| CNH | Carteira Nacional de Habilitação |
| CNPJ | Cadastro Nacional de Pessoas Jurídicas |
| CPF | Cadastro de Pessoas Físicas |
| CS | <i>Code Signing</i> |
| CSR | <i>Certificate Signing Request</i> |
| DETRAN | Departamento Nacional de Trânsito |
| DMZ | Zona Desmilitarizada |
| DN | <i>Distinguished Name</i> |
| DPC | Declaração de Práticas de Certificação |
| EV | <i>Extended Validation</i> |
| ICP-Brasil | Infraestrutura de Chaves Públicas Brasileira |
| IDS | <i>Intrusion Detection System</i> |
| IEC | <i>International Electrotechnical Commission</i> |
| IETF PKIX | <i>Internet Engineering Task Force - Public-Key Infrastructured (X.509)</i> |
| INMETRO | Instituto Nacional de Metrologia, Qualidade e Tecnologia |
| ISO | <i>International Organization for Standardization</i> |
| ITSEC | <i>European Information Technology Security Evaluation Criteria</i> |
| ITU | <i>International Telecommunications Union</i> |
| LCR | Lista de Certificados Revogados |
| NBR | Norma Brasileira |
| NIS | Número de Identificação Social |
| OCSP | Online Certificate Status Protocol |
| OID | <i>Object Identifier</i> |
| OM-BR | Objetos Metrológicos ICP-Brasil |
| OU | <i>Organization Unit</i> |
| PASEP | Programa de Formação do Patrimônio do Servidor Público |
| PC | Políticas de Certificado |
| PCN | Plano de Continuidade de Negócio |
| PIN | <i>Personal Identification Number</i> |
| PIS | Programa de Integração Social |
| PS | Política de Segurança |
| PSBIO | Prestadores de Serviço Biométrico |
| PSC | Prestador de Serviço de Confiança |
| PSS | Prestadores de Serviço de Suporte |
| PUK | <i>PIN Unbloking Key</i> |
| RFC | <i>Request For Comments</i> |
| RG | Registro Geral |
| SAT | Sistema de Autenticação e Transmissão |
| SIGEPE | Sistema de Gestão de Pessoal da Administração Pública Federal |
| SNMP | <i>Simple Network Management Protocol</i> |





| | |
|-------|---|
| SSL | <i>Secure Socket Layer</i> |
| TCSEC | <i>Trusted System Evaluation Criteria</i> |
| TSDM | <i>Trusted Software Development Methodology</i> |
| TSE | Tribunal Superior Eleitoral |
| UF | Unidade de Federação |
| URL | <i>Uniform Resource Locator</i> |

2. RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1. Repositórios

2.1.1 A AC Certisign OM-BR mantém disponível repositório atendendo as seguintes obrigações:

- a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC Certisign OM-BR e sua LCR/OCSP;
- b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- c) implementar os recursos necessários para a segurança dos dados nele armazenados.

2.1.2. O repositório da AC Certisign OM-BR possui os seguintes requisitos atendidos:

- a) localização lógica (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html)
- b) disponibilidade de 99,5% (noventa e nove e meio por cento), 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
- c) protocolos de acesso; e
- d) requisitos de segurança.

2.1.3. O repositório da AC Certisign OM-BR está disponível para consulta durante 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.1.4 A AC Certisign OM-BR disponibiliza 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCR/OCSP:

- a) <http://icp-brasil.certisign.com.br/repositorio/lcr/ACCertisignOM-BR/LatestCRL.crl>
- b) <http://icp-brasil.outralcr.com.br/repositorio/lcr/ACCertisignOM-BR/LatestCRL.crl>.





2.2. Publicação de informações dos certificados

2.2.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC Certisign OM-BR (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html), obedecendo as regras e os critérios estabelecidos nesta DPC.

2.2.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC Certisign OM-BR (http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html):

- a) seu próprio certificado;
- b) suas LCR/OCSP;
- c) esta DPC;
- d) as PC que implementa;
- e) uma relação, regularmente atualizada, contendo as AR vinculadas e seus respectivos endereços; e
- f) uma relação, regularmente atualizada, contendo os PSS, PSBio e PSC vinculados.

2.3. Tempo ou Frequência de Publicação

2.3.1. De modo a assegurar a disponibilização sempre atualizada de seus conteúdos:

- a) os certificados são publicados imediatamente após sua emissão;
- b) a publicação da LCR se dá conforme o item 4.4.9 da PC correspondente;
- c) as versões ou alterações desta DPC e da PC são atualizadas no web site da AC Certisign OM-BR após aprovação da AC Raiz da ICP-Brasil; e
- d) os endereços das AR vinculadas são atualizadas no web site da AC Certisign OM-BR

2.4. Controle de Acesso aos Repositórios

2.4.1. Não há qualquer restrição ao acesso para consulta a esta DPC, à lista de certificados emitidos, à LCR da AC Certisign OM-BR, às PC implementadas e aos endereços das AR vinculadas.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.





3. IDENTIFICAÇÃO E AUTENTICAÇÃO

A AC Certisign OM-BR, verifica a autenticidade da identidade e/ou atributos de Objetos Metrológicos (OM-BR) da ICP-Brasil antes da inclusão desses atributos em um certificado digital.

A AC reserva o direito, sem responsabilidade a qualquer solicitante, de rejeitar os pedidos.

3.1. Atribuição de Nomes

3.1.1. Tipos de nomes

3.1.1.1. O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o "*Distinguished Name*" do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular.

3.1.1.2. Não se aplica.

3.1.2. Necessidade dos nomes serem significativos

3.1.2.1. Os certificados emitidos pela AC Certisign OM-BR exigem o uso de nomes significativos que possibilitem determinar univocamente a identidade OM-BR titular do certificado a que se referem.

3.1.3. Anônimo ou Pseudônimo dos Titulares do Certificado

Não se aplica.

3.1.4. Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.5. Unicidade de nomes

Esta DPC estabelece que identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado emitido pela AC Certisign OM-BR.

Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo DN.

3.1.6. Procedimento para resolver disputa de nomes

A AC Certisign OM-BR se reserva o direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7. Reconhecimento, autenticação e papel de marcas registradas

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas são executados de acordo com a legislação em vigor.





3.2. Validação inicial de identidade

Neste e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pelas AR vinculadas a AC Certisign OM-BR para a primeira identificação e cadastramento de pessoas físicas titulares ou responsáveis por certificados digitais compreendendo os seguintes processos:

- a) Não se aplica.
- b) emissão do certificado: após solicitação de certificado ser feita pelo fabricante com seu certificado digital de Pessoa Jurídica, é liberada a emissão do certificado no sistema da AC Certisign OM-BR. A extensão *Subject Alternative Name* é considerada fortemente relacionada à chave pública contida no certificado, assim, todas as partes dessa extensão devem ser verificadas, devendo o solicitante do certificado comprovar que detém os direitos sobre essas informações junto aos órgãos competentes, ou que está autorizado pelo titular da informação a utilizá-las.

3.2.1. Método para comprovar a posse de chave privada

A AR verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital. As RFC 4210 e 6712 são utilizadas como referência para essa finalidade.

No caso em que sejam requeridos procedimentos específicos para as PCs implementadas, os mesmos são descritos nessas PCs, no item correspondente.

3.2.2. Autenticação da identificação da organização

3.2.2.1. Não se aplica.

3.2.2.1.1. Não se aplica.

3.2.2.1.2. Não se aplica.

3.2.2.1.3. Não se aplica.

Nota 01: Não se aplica.

3.2.2.1.4. Não se aplica;

3.2.2.1.5 Não se aplica.

3.2.2.2. Não se aplica.

Nota 01: Não se aplica.

3.2.2.3. Responsabilidade decorrente do uso do certificado de uma organização

Não se aplica.

3.2.3. Autenticação da identidade de um indivíduo

Não se aplica.





3.2.3.1 Procedimento para identificação de um indivíduo

Não se aplica.

Nota 1: Não se aplica.

3.2.3.1.1. Não se aplica.

3.2.3.1.2. Não se aplica.

3.2.3.1.3. Não se aplica.

3.2.3.1.4. Não se aplica.

3.2.3.1.5. Não se aplica.

3.2.3.1.6. Não se aplica.

3.2.3.1.7 Não se aplica.

3.2.3.1.8 Não se aplica.

3.2.3.1.8.1. Não se aplica.

3.2.4. Informações não verificadas do titular do certificado

Não se aplica.

3.2.5. Validação das autoridades

Não se aplica.

3.2.6. Critérios para interoperabilidade

Não se aplica.

3.2.7. Autenticação da identidade de equipamento ou aplicação

3.2.7.1 Disposições Gerais

3.2.7.1.1. Em se tratando de certificado emitido para aplicação, o titular será a pessoa jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

3.2.7.1.2. Não se aplica.

3.2.7.1.3. O titular do certificado será uma pessoa jurídica, com certificado emitido dentro dos padrões dos Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil - DOC-ICP-05.

3.2.7.1.4. Não se aplica.

3.2.7.1.5 Não se aplica.

3.2.7.2 Procedimentos para efeitos de identificação de um equipamento ou aplicação

3.2.7.2.1. Não se aplica.

3.2.7.2.2. Não se aplica.





3.2.7.3 Autenticação de identificação de equipamento para certificado CF-e-SAT

3.2.7.3.1 Disposições Gerais

3.2.7.3.1.1. Não se aplica.

3.2.7.3.1.2. Não se aplica.

3.2.7.3.1.3. Não se aplica.

3.2.7.4 Procedimentos para efeitos de identificação de um equipamento SAT

3.2.7.4.1. Não se aplica.

3.2.7.5 Autenticação de identificação de equipamentos para certificado OM-BR

3.2.7.5.1 Disposições Gerais.

3.2.7.5.1.1. Em se tratando de certificado emitido para equipamento OM-BR, o titular será representado pelo fabricante identificado no certificado digital ICP-Brasil de pessoa jurídica que assina a solicitação, associada ao número de identificação do equipamento detentor da chave privada.

3.2.7.5.1.2. Para certificados do tipo OM-BR, a confirmação da identidade do fabricante se dará conforme disposto no item 3.2.7.1 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.5.1.3. Para certificados do tipo OM-BR, por se tratar de certificado para equipamento metrológico específico de fabricante autorizado já identificado quando da emissão do certificado digital ICP-Brasil de pessoa jurídica válido que assina a requisição do certificado OM-BR, a confirmação da identidade se dará exclusivamente na forma do disposto no item 3.2.7.1 e com a assinatura do TERMO DE TITULARIDADE [4] específico de que trata o item 4.1.

3.2.7.6 Procedimentos para efeitos de identificação de um equipamento metrológico

3.2.7.6.1. Para certificados de equipamento metrológico, deve ser verificado se o CNPJ do fabricante que assina digitalmente a solicitação desse certificado está vinculado aos controles regulatórios do referido equipamento, o qual deve estar registrado e autorizado pelo INMETRO. Essas informações devem ser obtidas e confirmadas pela AC Certisign OM-BR.

3.2.8 Procedimentos complementares

3.2.8.1. A AC Certisign OM-BR mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro, bem como os Princípios e Critérios *WebTrust*.

3.2.8.2 Não se aplica.

3.2.8.2.1. Não se aplica.

3.2.8.3. Não se aplica.





3.2.8.3.1. Para os certificados OM-BR é mantida toda a documentação eletrônica utilizada no processo de validação e confirmação da identificação do equipamento objeto metrológico acreditado pelo INMETRO, observadas as condições definidas em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil.

3.2.8.3.2 Não se aplica.

3.2.8.3.3 Não se aplica.

3.2.8.4. Não se aplica.

3.2.8.4.1. Não se aplica.

3.2.8.4.2. Não se aplica.

3.2.9. Procedimentos específicos

3.2.9.1. Não se aplica.

3.2.9.2. Não se aplica.

3.2.9.3. Não se aplica.

3.2.9.3.1. Não se aplica.

3.2.9.3.2. Não se aplica.

3.2.9.3.3. Não se aplica.

3.2.9.3.4. Não se aplica.

3.2.9.4. Não se aplica.

3.2.9.4.1. Não se aplica.

3.2.9.5. Disposições para a Validação de Solicitação de Certificados do Tipo OM-BR:

A validação da solicitação de certificado do tipo OM-BR compreende:

a) validar o registro inicial por meio de verificação da assinatura digital do fabricante do equipamento metrológico realizada sobre a solicitação do certificado OM-BR e sobre o TERMO DE TITULARIDADE [4] específico de que trata o item 4.1. O certificado digital do fabricante que assina a solicitação e o termo de titularidade aqui referidos deve ser um certificado digital ICP-Brasil de pessoa jurídica válido;

b) realizar a verificação da solicitação, assinada digitalmente, contendo a requisição em conformidade com o formato estabelecido em regulamento editado por instrução normativa da AC Raiz que defina os padrões e algoritmos criptográficos da ICP-Brasil e confrontando com as informações de controle do órgão regulador e do certificado digital que assinou a requisição;

c) emissão do certificado digital sem que haja possibilidade de alteração dos dados constantes na requisição e disponibilização ao solicitante para instalação no equipamento OM-BR.





3.2.9.6. Não se aplica.

3.2.9.7. Não se aplica.

3.2.9.8 Não se aplica.

3.3. Identificação e autenticação para pedidos de novas chaves

3.3.1. No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC Certisign OM-BR para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.3.2 Não se aplica.

3.3.2.1 Não se aplica

3.3.3. Não existem procedimentos específicos para a PC implementada.

3.3.4. Não se aplica.

3.4. Identificação e Autenticação para solicitação de revogação

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC Certisign OM-BR está descrito no item 4.9.3.

Solicitações de revogação de certificados devem ser registradas.

4. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1. Solicitação do certificado

Neste item são descritos todos os requisitos e procedimentos operacionais estabelecidos pela AC Certisign OM-BR compreendem todas as ações necessárias tanto do indivíduo solicitante quanto das AC e AR no processo de solicitação de certificado digital e contemplam:

- a) Não se aplica;
- b) o uso de certificado digital do tipo A3 Pessoa Jurídica ICP-Brasil, a conferência das informações do equipamento e fabricante com a base da AC INMETRO para a emissão do certificado OM-BR;
- c) um termo de titularidade assinado digitalmente pelo certificado de Pessoa Jurídica do fabricante conforme o adendo referente ao TERMO DE TITULARIDADE [4] específico;





- d) Não se aplica;
- e) Não se aplica.

4.1.1. Quem pode submeter uma solicitação de certificado

A submissão da solicitação deve ser sempre pelo fabricante do equipamento, através do seu certificado de Pessoa Jurídica do tipo A3 ICP-Brasil.

- 4.1.1.1. Não se aplica.
- 4.1.1.2. Não se aplica.
- 4.1.1.3. Não se aplica.
- 4.1.1.4. Não se aplica.

4.1.2. Processo de registro e responsabilidades

Abaixo são descritas as obrigações gerais das entidades envolvidas. Não existem procedimentos específicos para a PC implementada.

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC Certisign OM-BR responde pelos danos a que der causa.

4.1.2.1.2 A AC Certisign OM-BR responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

4.1.2.1.3 Não se aplica.

4.1.2.2 Obrigações da AC

As obrigações da AC Certisign OM-BR são as abaixo relacionadas:

- a) operar de acordo com a sua DPC e com as PCs que implementa;
- b) gerar e gerenciar os seus pares de chaves criptográficas;
- c) assegurar a proteção de suas chaves privadas;
- d) notificar a AC INMETRO, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;
- e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- f) distribuir o seu próprio certificado;
- g) emitir, expedir e distribuir os certificados de AR a ela vinculadas e de usuários finais;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;





- j) emitir, gerenciar e publicar suas LCRs e, quando aplicável, disponibilizar consulta on-line de situação do certificado (*OCSP - On-line Certificate Status Protocol*);
- k) publicar em sua página web sua DPC e as PCs aprovadas que implementa;
- l) publicar, em sua página web, as informações definidas no item 2.2.2 deste documento;
- m) publicar, em página web, informações sobre o descredenciamento de AR;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, de acordo com as normas do CG da ICP-Brasil;
- u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
- v) informar à AC Raiz a quantidade de certificados digitais emitidos, conforme regulamentação da AC Raiz;
- w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
- x) realizar, ou delegar para seu PSS, as auditorias pré-operacionais e anualmente as auditorias operacionais de suas ARs, diretamente com seus profissionais, ou através de auditorias internas ou empresas de auditoria independente, ambas, credenciadas pela AC Raiz. O PSS deverá apresentar um único relatório de auditoria para cada AR vinculada às ACs que utilizam de seus serviços;





- y) garantir que todas as aprovações de solicitação de certificados sejam realizadas por agente de registro e estações de trabalho autorizados; e
- z) disponibilizar a AC-INMETRO, com atualização diária, lista dos certificados digitais emitidos e sua respectiva situação.

4.1.2.3 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

4.1.2.4 Obrigações das ARs

As obrigações das ARs vinculadas à AC Certisign OM-BR são as abaixo relacionadas:

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) encaminhar a solicitação de emissão ou de revogação de certificado, por meio de acesso remoto ao ambiente de AR hospedado nas instalações da AC responsável utilizando protocolo de comunicação seguro, conforme padrão definido em regulamento editado por instrução normativa da AC Raiz que defina as características mínimas de segurança para as AR da ICP-Brasil;
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1], bem como Princípios e Critérios *WebTrust* para AR[14];
- f) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- g) proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma do item 3.2.7; e
- h) divulgar suas práticas, relativas à cada cadeia de AC ao qual se vincular, em conformidade com o documento Princípios e Critérios *WebTrust* para AR[14].

4.2. Processamento de Solicitação de Certificado

4.2.1. Execução das funções de identificação e autenticação

A AC Certisign OM-BR e AR executam as funções de identificação e autenticação conforme item 3 desta DPC.

4.2.2. Aprovação ou rejeição de pedidos de certificado

4.2.2.1 Não se aplica.





4.2.2.2 A AC Certisign OM-BR e AR podem, com a devida justificativa formal, aceitar ou rejeitar pedidos de certificados de requerentes de acordo com os procedimentos descritos nesta DPC.

4.2.3. Tempo para processar a solicitação de certificado

A AC Certisign OM-BR cumpre os procedimentos determinados na ICP-Brasil.

Não há tempo máximo para processar as solicitações na ICP-Brasil.

4.3. Emissão de Certificado

4.3.1. Ações da AC durante a emissão de um certificado

4.3.1.1 A emissão de certificado depende do correto preenchimento de formulário de solicitação, da assinatura do “Termo de Titularidade”, no caso de certificados de pessoas jurídicas, ou aplicações e dos demais documentos exigidos. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e Titular é notificado da emissão e do método para a retirada do certificado.

4.3.1.2 O certificado é considerado válido a partir do momento de sua emissão.

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

O Titular é notificado da emissão do certificado através do Módulo Eletrônico de AR, que fará a comunicação entre o sistema de emissão da AC Certisign OM-BR e o fabricante do objeto metrológico.

4.4. Aceitação de Certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.1.1 O titular do certificado verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

- a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;
- b) garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;
- c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.2. A aceitação de todo certificado emitido é declarada pelo respectivo titular. Nos certificados emitidos para Objetos Metrológicos, a declaração deverá ser feita pelo fabricante responsável pelo certificado.





4.4.1.3 Eventuais termos de acordo, ou instrumentos similares, se necessários, são descritos neste item da PC correspondente.

4.4.2. Publicação do certificado pela AC

O certificado da AC Certisign OM-BR é publicado de acordo com item 2.2 desta DPC.

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

A notificação se dará de acordo com item 2.2 da DPC da AC Raiz.

4.5. Usabilidade do par de chaves e do certificado

O titular do certificado deve operar de acordo com essa Declaração de Práticas de Certificação (DPC) e com as Políticas de Certificado (PC) implementadas, estabelecidos em conformidade com este documento e com o documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

4.5.1. Usabilidade da Chave privada e do certificado do titular

4.5.1.1 O titular deve utilizar sua chave privada e garantir a proteção dessa chave conforme o previsto nesta DPC.

4.5.1.2 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos pela AC Certisign OM-BR constantes dos termos de titularidade de que trata o item 4.1 são os abaixo relacionados:

- a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- b) garantir a proteção e o sigilo de suas chaves privadas, código de ativação (PIN) e dispositivos criptográficos;
- c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
- d) conhecer os seus direitos e obrigações, contemplados pela DPC e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;
- e) informar à AC Certisign OM-BR qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente; e
- f) garantir a proteção do PUK, sendo permitido o gerenciamento por entidade autorizada pelo titular do certificado, mediante identificação presencial ou outro método com nível de segurança equivalente.

Nota: Nos certificados emitidos para Objetos Metrológicos estas obrigações se aplicam ao fabricante responsável pelo certificado.





4.5.2. Usabilidade da chave pública e do certificado das partes confiáveis
Em acordo com o item 9.6.4 desta DPC.

4.6. Renovação de Certificados

Não se aplica.

4.6.1. Circunstâncias para renovação de certificados

Não se aplica.

4.6.2. Quem pode solicitar a renovação

Não se aplica.

4.6.3. Processamento de requisição para renovação de certificados

Não se aplica.

4.6.4. Notificação para nova emissão de certificado para o titular

Não se aplica.

4.6.5. Conduta constituindo a aceitação de uma renovação de um

Não se aplica.

4.6.6. Publicação de uma renovação de um certificado pela AC

Não se aplica.

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

Não se aplica.

4.7. Nova chave de certificado (Re-key)

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica.

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

Não se aplica.

4.7.3. Processamento de requisição de novas chaves de certificado

Não se aplica.

4.7.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.7.5. Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica.





4.7.6. Publicação de uma nova chave certificada pela AC

Não se aplica.

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

Não se aplica.

4.8. Modificação de certificado

4.8.1. Circunstâncias para modificação de certificado

Não se aplica.

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica.

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica.

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica.

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica.

4.8.6. Publicação de uma modificação de certificado pela AC

Não se aplica.

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

Não se aplica.

4.9. Suspensão e Revogação de Certificado

4.9.1. Circunstâncias para revogação

4.9.1.1. O titular e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independente de qualquer circunstância.

4.9.1.2. O certificado deve ser obrigatoriamente revogado:

- a) Quando constatada emissão imprópria ou defeituosa do mesmo;
- b) Quando for necessária a alteração de qualquer informação constante no mesmo;
- c) Não se aplica;
- d) No caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.





4.9.1.3. A AC Certisign OM-BR define ainda que:

- a) A AC Certisign OM-BR deve revogar, no prazo definido no item 4.9.3.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil; e
- b) O CG da ICP-Brasil ou AC Raiz deverá determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.9.1.4. Todo certificado tem a sua validade verificada, na respectiva LCR ou OCSP, antes de ser utilizado.

4.9.1.4.1. Não se aplica.

4.9.1.4.2. Não se aplica.

4.9.1.5. A autenticidade da LCR/OCSP é também confirmada por meio das verificações da assinatura da AC Certisign OM-BR e do período de validade da LCR/OCSP.

4.9.2. Quem pode solicitar revogação

A revogação de um certificado somente poderá ser feita:

- a) Por solicitação do titular do certificado;
- b) Não se aplica;
- c) Não se aplica;
- d) Pela AC Certisign OM-BR;
- e) Não se aplica;
- f) Por determinação do CG da ICP-Brasil ou da AC Raiz; ou
- g) Não se aplica;
- h) Não se aplica;
- i) Pelo INMETRO, ou
- j) Não se aplica.

4.9.3. Procedimento para solicitação de revogação

4.9.3.1. A solicitação de revogação deverá ser feita pelo fabricante do equipamento diretamente a AC Certisign OM-BR. Essa solicitação será registrada por e-mail que conterá as informações do fabricante do equipamento e do equipamento que deverá ter o certificado revogado. Após o recebimento, a AC Certisign OM-BR avaliará a solicitação e revogará o certificado.

A revogação é realizada pela AC Certisign OM-BR de forma on-line contendo o motivo da solicitação de revogação mediante o fornecimento de dados.





O titular do certificado, neste caso o fabricante do equipamento, deverá assinar o termo de revogação com o certificado de pessoa jurídica tipo A3 ICP-Brasil.

4.9.3.2. Como diretrizes gerais:

- a) O Solicitante da revogação de um certificado é identificado;
- b) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas pela AC Certisign OM-BR;
- c) As justificativas para a revogação de um certificado são registradas;
- d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado e com a atualização do status do certificado na resposta OCSP à base de dados da AC Certisign OM-BR, quando aplicável.

4.9.3.3. O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 24 (vinte e quatro) horas.

4.9.3.4. Não se aplica.

4.9.3.5. A AC Certisign OM-BR responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da LCR correspondente.

4.9.3.6. Não se aplica.

4.9.4. Prazo para solicitação de revogação

4.9.4.1. A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.9.1 desta DPC.

O prazo para aceitação do certificado pelo seu titular é de 7 (sete) dias, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa de revogação.

4.9.4.2. Não se aplica.

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

Em caso de pedido formalmente constituído, de acordo com as normas da ICP-Brasil, a AC Certisign OM-BR processa a revogação imediatamente após a análise do pedido.

4.9.6. Requisitos de verificação de revogação para as partes confiáveis

Antes de confiar em um certificado, a parte confiável deve confirmar a validade de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de políticas de certificação e o status de revogação por meio de LCRs ou respostas OCSP identificados em cada certificado na cadeia de certificação.





4.9.7. Frequência de emissão de LCR

4.9.7.1. Neste item é definida a frequência para a emissão de LCR referente a certificados de usuários finais.

4.9.7.2. A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 horas.

4.9.7.3. Não se aplica.

4.9.7.4. Não se aplica.

4.9.8. Latência máxima para a LCR

A LCR é divulgada no repositório em no máximo 4 (quatro) horas após sua geração.

4.9.9. Disponibilidade para revogação/verificação de status on-line

A AC Certisign OM-BR suporta os processos de revogação de certificados de forma on-line quando aplicável por força de contratação específica.

A AC Certisign OM-BR suporta verificação da situação do estado de certificados de forma on-line por meio do protocolo OCSP (*On-line Certificate Status Protocol*), como maneira de obter informações atualizadas sobre o status de um certificado específico.

As respostas OCSP da AC Certisign OM-BR estão em conformidade com a RFC6960, e são assinadas por um certificado OCSP, assinado pela AC que emitiu o certificado cujo status de revogação está sendo verificado. Esse certificado de assinatura de Resposta OCSP contém a extensão *id-pkix-ocsp-nocheck*, conforme definido pela RFC6960.

As mensagens de Resposta OCSP da AC Certisign OM-BR, são compostas pelas informações a seguir, conforme definido pela RFC6960:

- a) versão da sintaxe de resposta;
- b) identificador do respondente OCSP;
- c) hora em que a resposta foi gerada;
- d) respostas para cada um dos certificados em uma solicitação;
- e) extensões opcionais;
- f) algoritmo de assinatura OID;
- g) assinatura calculada através de um hash da resposta;

A AC Certisign OM-BR utiliza as seguintes informações nas respostas OCSP, como valor do status de um certificado, conforme definido pela RFC6960:

- a) “*good*”: indica uma resposta positiva à consulta de status de um certificado;
- b) “*revoked*”: indica que o certificado foi revogado;





c) “*unknown*”: indica que o respondente não possui informações sobre o certificado que está sendo solicitado, geralmente porque o emissor não é reconhecido ou que o certificado não é suportado por este respondente.

4.9.10. Requisitos para verificação de revogação on-line

Não se aplica.

4.9.11. Outras formas disponíveis para divulgação de revogação

4.9.11.1 Não se aplica.

4.9.11.2 Não se aplica.

4.9.12. Requisitos especiais para o caso de comprometimento de chave

4.9.12.1. O titular de certificado deve notificar imediatamente, através de solicitação on-line de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.9.12.2. O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR Responsável, assinando formulário de solicitação de revogação, observado o item 4.4.3 desta DPC.

Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

4.9.13. Circunstâncias para suspensão

Não é permitida, salvo em casos específicos e determinados pelo Comitê Gestor, a suspensão de certificados de usuários finais.

4.9.14. Quem pode solicitar suspensão

A AC Certisign OM-BR pode solicitar suspensão quando aprovado pelo Comitê Gestor.

4.9.15. Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão serão dados por norma específica das DPC e PCs associadas.

4.9.16. Limites no período de suspensão

Os períodos de suspensão serão estabelecidos por norma específica das DPC e PCs associadas.





4.10. Serviços de status de certificado

4.10.1. Características operacionais

A AC Certisign OM-BR deve fornecer um serviço de status de certificado na forma de um ponto de distribuição da LCR nos certificados ou OCSP, conforme item 4.9.

4.10.2. Disponibilidade dos serviços

Ver item 4.9

4.10.3. Funcionalidades operacionais

Ver item 4.9

4.11. Encerramento de atividades

4.11.1. Observado o disposto no item sobre descredenciamento do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDECNIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6], este item da DPC descreve os requisitos e os procedimentos que serão adotados nos casos de extinção ou encerramento dos serviços da AC Certisign OM-BR , de uma AR, PSS ou PSBios a ela vinculados.

4.11.2. No caso de encerramento das atividades como AC da ICP-Brasil, a AC Certisign OM-BR segue os requisitos e procedimentos descritos no documento Plano de Encerramento. Esse plano tem abordagem multidisciplinar envolvendo aspectos de várias áreas da companhia, como jurídico, comercial, técnicos/tecnológicos, entre outros. De acordo com esse plano a AC Certisign OM-BR:

- a) Comunicará publicamente a extinção dos serviços da AC Certisign OM-BR, através de publicação em seu repositório.
- b) Revogará todos os certificados gerados pela AC Certisign OM-BR nos prazos estipulados nas PC implementadas após a publicação e comunicará às partes afetadas através de mensagem eletrônica.
- c) Extinguirá os serviços de emissão de certificados.
- d) Extinguirá os serviços de revogação, como emissão da LCR e/ou conservação dos serviços de status on-line após a revogação completa de todos os certificados.
- e) Destruirá a chave privada da AC Certisign OM-BR extinta seguindo o procedimento descrito na DPC Item 6.2.9.
- f) Transferirá os dados e gravações da AC Certisign OM-BR para a Autoridade Certificadora sucessora, aprovada pela AC Raiz.
- g) Transferirá as chaves públicas dos certificados emitidos pela AC Certisign OM-BR para serem armazenadas por outra AC aprovada pela AC Raiz. Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC Certisign OM-





BR. Caso as chaves públicas não sejam assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

- h) O responsável pela guarda desses dados e registros observará os mesmos requisitos de segurança exigidos para a AC Certisign OM-BR.
- i) Transferirá, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

4.11.2.1. No caso de falência, extinção da AR ou encerramento das atividades como AR vinculada a AC Certisign OM-BR a AR deverá seguir os seguintes requisitos e procedimentos:

- a) Comunicará publicamente a extinção dos serviços de AR vinculada AC Certisign OM-BR, através de publicação em seu repositório; e
- b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados.

4.11.2.2. No caso de encerramento das atividades como PSS vinculada a AC Certisign OM-BR, diretamente ou por intermédio da AR, deverá seguir os seguintes requisitos e procedimentos:

- a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;
- b) Manterá a guarda de toda a documentação comprobatória em seu poder.

4.12. Custódia e recuperação de chave

4.12.1. Política e práticas de custódia e recuperação de chave

A AC Certisign OM-BR não executa práticas de custódia e recuperação de chaves.

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

A AC Certisign OM-BR não executa tais práticas.

5. CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1 Controles Físicos

5.1.1. Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC Certisign OM-BR não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não existem ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.





5.1.1.2. As instalações para equipamentos de apoio, tais como máquinas de ar-condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares ficam em ambiente seguro.

As instalações para sistemas de telecomunicações, subestações e retificadores ficam em ambiente seguro com entrada e saída controlada.

Existem sistemas de aterramento e de proteção contra descargas atmosféricas

Existe iluminação de emergência em todos os ambientes de nível 4, além das áreas cobertas por câmeras de monitoramento.

5.1.2. Acesso físico

A AC Certisign OM-BR possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1. A AC Certisign OM-BR possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC Certisign OM-BR;

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC Certisign OM-BR. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC Certisign OM-BR transitam devidamente identificadas e acompanhadas.

Nenhum tipo de processo operacional ou administrativo da AC Certisign OM-BR é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Certisign OM-BR em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC Certisign OM-BR. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da AC Certisign OM-BR.

Qualquer atividade relativa ao ciclo de vida dos certificados digitais é executada a partir desse nível.





Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: identificação individual, por meio de cartão eletrônico, e identificação biométrica.

5.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC Certisign OM-BR, não são admitidos a partir do nível 3.

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Certisign OM-BR tais como emissão e revogação de certificados e emissão de LCR e a disponibilidade à resposta a consulta OCSP. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível, inclusive o sistema de AR. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver sendo ocupado.

5.1.2.1.9. No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto, são inteiros, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas foram sanadas por normas internacionais pertinentes.

5.1.2.1.11. Na AC Certisign OM-BR, existem ambientes de quarto nível para abrigar e segregar:

- a) equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infraestrutura - firewall, roteadores, switches e servidores - (Data Center);
- b) equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia).

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.





5.1.2.1.13. Para garantir a segurança do material armazenado, o cofre e o gabinete obedecem às seguintes especificações:

- a) confeccionado em aço;
- b) possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da AC Certisign OM-BR são armazenados nesses depósitos.

5.1.2.2 Sistemas físicos de detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24x7 deverão ser armazenadas por, no mínimo, 7 (sete) anos. Elas deverão ser testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, 1 (uma) fita referente a cada semana. Essas fitas deverão ser armazenadas em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

5.1.2.2.4. Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que o critério mínimo de ocupação deixa de ser satisfeito, devido à saída de um ou mais empregados, ocorre a reativação automática dos sensores de presença.

5.1.2.2.5. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.2.6. O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes estão localizados em ambiente de nível 3 e são permanentemente monitorados. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações.

5.1.2.3 Sistema de controle de acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.





5.1.2.4 Mecanismos de emergência

5.1.2.4.1. Mecanismos específicos são implantados pela AC Certisign OM-BR para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os mecanismos e procedimentos de emergência são verificados, semestralmente, por meio de simulação de situações de emergência.

5.1.3. Energia e ar-condicionado

5.1.3.1. A infraestrutura do ambiente de certificação da AC Certisign OM-BR está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC Certisign OM-BR e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da AC Certisign OM-BR.

5.1.3.2. Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados.

5.1.3.3. Existem tubulações, dutos, calhas, quadros e caixas – de passagem, distribuição e terminação – projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, telefonia e dados.

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

5.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8]. Qualquer modificação nessa rede é previamente documentada.

5.1.3.6. Não são admitidas instalações provisórias, fiação exposta ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

5.1.3.7. O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante à falhas.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9. O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC Certisign OM-BR é garantida, por meio de:





- a) gerador de porte compatível;
- b) gerador de reserva;
- c) sistemas de *no-breaks* redundantes;
- d) sistemas redundantes de ar-condicionado.

5.1.4. Exposição à água

A estrutura interiore do ambiente de nível 4 construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio

5.1.5.1. Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2. Nas instalações da AC Certisign OM-BR não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só abre quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC Certisign OM-BR, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6. Armazenamento de mídia

A AC Certisign OM-BR atende às normas NBR 11.515 e NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7. Destrução de lixo

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

5.1.7.2. Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos.

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

As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas.





5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.1.1. A AC Certisign OM-BR pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida dos certificados digitais, de forma a garantir a segurança da atividade de certificação e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo.

5.2.1.2. A AC Certisign OM-BR estabelece 4 perfis distintos para sua operação, atribuídos às seguintes áreas:

- Gerência de Operações Data Center:
 - Supervisão Operacional:
 - configuração e manutenção do hardware e do software da AC;
 - gerenciamento e controle da tecnologia empregada nos serviços de certificação da AC;
 - controle de acesso lógico dos funcionários à rede AC ;
 - gerenciamento dos operadores da AC;
 - controle de acesso ao sistema de certificação.
 - Supervisão de PKI:
 - administração e controle dos componentes criptográficos da AC;
 - verificação dos registros de acesso aos diferentes níveis de proteção das chaves privadas das AC (logs);
 - elaboração das cerimônias de geração de chaves de AC;
 - armazenamento dos registros de auditoria do sistema de certificação;
 - utilização de criptografia para segurança de acesso ao aplicativo de certificação.
- Gerência de Segurança:
 - implementação da Política de Segurança da AC;
 - verificação dos registros de auditoria;
 - supervisão do cumprimento das práticas e procedimentos determinados na Política de Segurança da AC;
 - acompanhamento das auditorias de segurança realizadas por terceiros;
 - verificação do cumprimento desta DPC;
 - autorização e concessão de acesso às instalações físicas e autorização de acessos lógicos ao sistema de certificação;
 - utilização de criptografia para a segurança da base de dados de registro de auditoria do sistema de certificação.





- Gerência de Operação:

- Gerenciamento e controle dos processos de validação, verificação, emissão e revogação de certificados.

5.2.1.3. Os operadores do sistema de certificação da AC Certisign OM-BR recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal (Política de Segurança da AC Certisign OM-BR), com base nas necessidades de cada perfil.

5.2.1.3.1. Não se aplica.

5.2.1.4. A AC Certisign OM-BR possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à AC Certisign OM-BR no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. Controle multiusuário é requerido para a geração e a utilização da chave privada da AC Certisign OM-BR, conforme o descrito em 6.2.2.

5.2.2.2. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Certisign OM-BR requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC Certisign OM-BR podem ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC Certisign OM-BR tem sua identidade e perfil verificados antes de:

- a) ser incluído em uma lista de acesso às instalações da AC Certisign OM-BR;
- b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC Certisign OM-BR;
- c) receber um certificado para executar suas atividades operacionais na AC Certisign OM-BR; e
- d) receber uma conta no sistema de certificação da AC Certisign OM-BR.

5.2.3.2. Os certificados, contas e senhas utilizados para identificação e autenticação dos empregados:

- a) são diretamente atribuídos a um único empregado;
- b) não são compartilhados; e
- c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC Certisign OM-BR adota padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.





5.2.4. Funções que requerem separação de deveres

A AC Certisign OM-BR implementa a segregação de atividades para o pessoal especificamente atribuído às funções definidas no item 5.2.1.

5.3. Controles de Pessoal

Todos os empregados da AC Certisign OM-BR, das AR e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- a) os termos e as condições do perfil que ocupam;
- b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
- c) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC Certisign OM-BR e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC Certisign OM-BR e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido, pelo menos, a:

- a) verificação de antecedentes criminais;
- b) verificação de situação de crédito;
- c) verificação de histórico de empregos anteriores; e
- d) comprovação de escolaridade e de residência.

5.3.2.2. Não se aplica.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC Certisign OM-BR e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

- a) princípios e mecanismos de segurança da AC Certisign OM-BR e das AR vinculadas;
- b) sistema de certificação em uso na AC Certisign OM-BR;
- c) procedimentos de recuperação de desastres e de continuidade do negócio;





- d) procedimento de solicitação conforme item 3.2.7; e
- e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

O pessoal da AC Certisign OM-BR e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC Certisign OM-BR.

5.3.5. Frequência e sequência de rodízio de cargos

Não estabelecido.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Certisign OM-BR ou de uma AR vinculada, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém, no mínimo, os seguintes itens:

- a) relato da ocorrência com “*modus operandis*”;
- b) identificação dos envolvidos;
- c) eventuais prejuízos causados;
- d) punições aplicadas, se for o caso; e
- e) conclusões.

5.3.6.3. Concluído o processo administrativo, a AC Certisign OM-BR encaminha suas conclusões à AC INMETRO.

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

- a) advertência;
- b) suspensão por prazo determinado; ou
- c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC Certisign OM-BR e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].





5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC Certisign OM-BR disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas:

- a) A DPC da AC Certisign OM-BR;
- b) a PC correspondente;
- c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8];
- d) documentação operacional relativa a suas atividades; e
- e) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela AC Certisign OM-BR e é mantida atualizada.

5.4. Procedimentos de Log de Auditoria

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC Certisign OM-BR com o objetivo de manter um ambiente seguro.

5.4.1. Tipos de eventos registrados

5.4.1.1. A AC Certisign OM-BR regista em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

- a) iniciação e desligamento do sistema de certificação;
- b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC Certisign OM-BR;
- c) mudanças na configuração dos sistemas AC Certisign OM-BR ou nas suas chaves;
- d) mudanças nas políticas de criação de certificados;
- e) tentativas de acesso (login) e de saída do sistema (*logoff*);
- f) tentativas não autorizadas de acesso aos arquivos do sistema;
- g) geração de chaves próprias da AC Certisign OM-BR ou de chaves de seus usuários finais;
- h) emissão e revogação de certificados;
- i) geração de LCR;
- j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;
- k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e





I) operações de escrita nesse repositório, quando aplicável.

5.4.1.1.1 Não se aplica.

5.4.1.2. A AC Certisign OM-BR também registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

- a) registros de acessos físicos;
- b) manutenção e mudanças na configuração de seus sistemas;
- c) mudanças de pessoal e perfis qualificados;
- d) relatórios de discrepância e comprometimento; e
- e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

5.4.1.3. As informações registradas pela AC Certisign OM-BR são todas as descritas nos itens acima.

5.4.1.4. Os registros de auditoria, eletrônicos ou manuais, contêm a data e a hora do evento registrado e a identidade do agente que o causou.

5.4.1.5. A documentação relacionada aos serviços da AC Certisign OM-BR é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.4.1.6. A AC Certisign OM-BR registram eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos são obrigatoriamente incluídos em arquivos de auditoria:

- a) não se aplica;
- b) data e hora das operações, incluindo a solicitação através de certificado digital de pessoa jurídica;
- c) não se aplica;
- d) a assinatura digital do executante.

5.4.1.6.1. Não se aplica.

5.4.1.7. A AC Certisign OM-BR a que esteja vinculada a AR define, em documento a estar disponível nas auditorias de conformidade, o local de arquivamento dos dossiês dos titulares.

5.4.2. Frequência de auditoria de registros

A periodicidade com que os registros de auditoria da AC Certisign OM-BR são analisados pelo pessoal operacional é de uma semana.





Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

5.4.3. Período de retenção para registros de auditoria

A AC Certisign OM-BR mantém localmente os seus registros de auditoria por, pelo menos, 2 (dois) meses e, subsequentemente, armazena-os da maneira descrita no item 5.5.

5.4.4. Proteção de registros de auditoria

5.4.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, através de permissões dadas pelo administrador do sistema de acordo com a função dos usuários ou aplicações e orientação do departamento de segurança.

O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

5.4.4.2. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso aos ambientes físicos onde são armazenados estes registros.

5.4.4.3. Os mecanismos de proteção descritos obedecem à Política de Segurança da AC Certisign OM-BR, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

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

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela AC Certisign OM-BR têm cópias de segurança semanais, feitas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

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

O sistema de coleta de dados de auditoria interno à AC Certisign OM-BR é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

5.4.7. Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Certisign OM-BR, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.





5.4.8. Avaliações de vulnerabilidade

Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC Certisign OM-BR, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC Certisign OM-BR e registradas para fins de auditoria.

5.5. Arquivamento de Registros

Nos itens seguintes da DPC está descrita a política geral de arquivamento de registros, para uso futuro, implementada pela AC Certisign OM-BR e pelas ARs a ela vinculadas.

5.5.1. Tipos de registros arquivados

Os tipos de registros arquivados são:

- a) Solicitações de certificados;
- b) Solicitações de revogação de certificados;
- c) Notificações de comprometimento de chaves privadas;
- d) Emissões e revogações de certificados;
- e) Emissões de LCR;
- f) Trocas de chaves criptográficas da AC Certisign OM-BR; e
- g) Informações de auditoria previstas no item 5.4.1.

5.5.2. Período de retenção para arquivo

Os períodos de retenção por tipo de registro arquivado são:

- a) As LCRs e os certificados de assinatura digital deverão ser retidos permanentemente, para fins de consulta histórica;
- b) Os dossiês dos titulares devem ser retidos, no mínimo, por 7 (sete) anos, a contar da data de expiração ou revogação do certificado; e
- c) As demais informações, inclusive os arquivos de auditoria, deverão ser retidas por, no mínimo, 7 (sete) anos.

5.5.3. Proteção de arquivo

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.5.4. Procedimentos de cópia de arquivo

5.5.4.1. A AC Certisign OM-BR estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à AC Certisign OM-BR, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.





5.5.4.2. As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

5.5.4.3. A AC Certisign OM-BR verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registros

Informações de data e hora nos registros baseiam-se no horário *Greenwich Mean Time (Zulu)*, incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero.

Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

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

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Certisign OM-BR em seus procedimentos operacionais são automatizados e manuais e internos.

5.5.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC Certisign OM-BR, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

5.6. Troca de chave

5.6.1. O titular do certificado digital pode solicitar a renovação antes do prazo de expiração por meio dos canais de vendas da AC Certisign OM-BR e de suas Autoridades de Registro.

Os avisos e instruções para a realização da renovação serão enviados pela AC Certisign OM-BR e por suas Autoridades de Registro, com antecedência mínima de 60 (sessenta) dias.

5.6.2. Não se aplica.

5.7. Comprometimento e Recuperação de Desastre

Nos itens seguintes da DPC estão descritos os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres, previstos no PCN da AC Certisign OM-BR, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], para garantir a continuidade dos seus serviços críticos.

5.7.1. Procedimentos de gerenciamento de incidente e comprometimento

5.7.1.1 A AC Certisign OM-BR deve possuir um Plano de Continuidade do Negócio – PCN, de acesso restrito, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos. Possui ainda um Plano de Resposta a Incidentes e um Plano de Recuperação de Desastres.





5.7.1.2 Os procedimentos previstos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, contém as seguintes informações:

- a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios, se for o caso;
- b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;
- c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários;
- d) Documentação dos processos e procedimentos acordados;
- e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e
- f) Teste e atualização dos planos.

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

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da AC Certisign OM-BR, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

5.7.3. Procedimentos no caso de comprometimento de chave privada de entidade

5.7.3.1 Certificado de entidade é revogado

Em caso de revogação do certificado da AC Certisign OM-BR o Gerente de Segurança, juntamente com a Supervisão de PKI da AC Certisign OM-BR, revogará todos os certificados subsequentes. Os titulares dos certificados revogados serão informados. A AC Certisign OM-BR emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

5.7.3.2 Chave de entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC Certisign OM-BR, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com a Supervisão de PKI da AC Certisign OM-BR, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

- a) Todos os certificados afetados serão revogados e as partes serão notificadas.





- b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC Certisign OM-BR estiver encerrando suas atividades.

5.7.4. Capacidade de continuidade de negócio após desastre

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infraestrutura, responsável pela contingência, notifica o Gerente de Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

- a) garantir a integridade física das pessoas que se encontram nas instalações da AC Certisign OM-BR;
- b) monitorar e controlar o foco da contingência;
- c) minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

5.8. Extinção da AC

Conforme CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, a DPC define as medidas de segurança implantadas pela AC Certisign OM-BR para proteger suas chaves criptográficas e os seus dados de ativação, bem como as chaves criptográficas dos titulares de certificados. São também definidos outros controles técnicos de segurança utilizados pela AC Certisign OM-BR e pelas ARs vinculadas na execução de suas funções operacionais.

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da AC Certisign OM-BR é gerado pela própria AC Certisign OM-BR, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. A geração do par de chaves de AC Certisign OM-BR é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC Certisign OM-BR, treinados para a função.

A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC Certisign OM-BR é gerado em módulo criptográfico de hardware no padrão obrigatório (Com NSH-2, Homologação da ICP-Brasil ou





Certificação do INMETRO - para a cadeia de certificação V5), conforme definido no DOC-ICP-01.01.

Somente os titulares dos certificados emitidos pela AC Certisign OM-BR geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC Certisign OM-BR.

6.1.1.3. Cada PC implementada pela AC Certisign OM-BR define o meio utilizado para armazenamento da chave privativa, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.1.1.4. O processo de geração do par de chaves da AC Certisign OM-BR é feito por hardware.

6.1.1.5. Cada PC implementada pela AC Certisign OM-BR caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.1.1.6. Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC Certisign OM-BR são os indicados no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Os procedimentos utilizados pela AC Certisign OM-BR para a entrega de sua chave pública à AC de nível hierárquico superior encarregada da emissão de seu certificado é definido pela AC superior.

6.1.3.2. 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. Os procedimentos específicos aplicáveis são detalhados em cada PC implementada.

6.1.4. Entrega de chave pública da AC às terceiras partes

A AC Certisign OM-BR disponibiliza o seu certificado, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, através de endereço Web: http://icp-brasil.certisign.com.br/repositorio/ac_certisign_om-br.html.

6.1.5. Tamanhos de chave

6.1.5.1. O tamanho das chaves criptográficas associadas aos certificados emitidos pela AC Certisign OM-BR, serão definidos por sua Política de Certificados em conformidade com o definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

6.1.5.2. Não se aplica.





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

6.1.6.1. Os parâmetros de geração de chaves assimétricas dos titulares de certificados adotam, no mínimo, o padrão estabelecido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.6.2. Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

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

6.1.7.1 Os certificados de assinatura emitidos pela AC Certisign OM-BR têm ativados os *bits digitalSignature, nonRepudiation e keyEncipherment*.

Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC Certisign OM-BR, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

6.1.7.2 A chave privada AC Certisign OM-BR é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

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

A AC Certisign OM-BR implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas.

A chave privada da AC Certisign OM-BR é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

Os titulares de certificados emitidos pela AC Certisign OM-BR, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado das suas chaves privadas.

6.2.1. Padrões e controle para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Certisign OM-BR adota o padrão com NSH-2, Homologação da ICP-Brasil ou Certificação do INMETRO, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.2.1.2. O módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão de homologação ICP-Brasil ou Certificação INMETRO.

Cada PC implementada descreve os padrões do módulo criptográfico a ser utilizado pela entidade titular de certificado.





6.2.2. Controle “n de m” para chave privada

6.2.2.1. A AC Certisign OM-BR exige controle múltiplo para utilização da sua chave privada.

6.2.2.2. É necessária a presença de pelo menos 3 (três) de um grupo de 10 (dez) funcionários de confiança, com perfis qualificados para a utilização da chave privada da AC Certisign OM-BR.

6.2.3. Custódia (escrow) de chave privada

A AC Certisign OM-BR não implementa tal prática.

6.2.4. Cópia de segurança de chave privada

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

6.2.4.2. A AC Certisign OM-BR mantém cópia de segurança de sua chave privada.

6.2.4.3. A AC Certisign OM-BR, não mantém cópia de segurança de chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC. Por solicitação do respectivo titular ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC Certisign OM-BR poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo 3DES – 112 bits ou AES – 128 ou 256 bits, conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC Certisign OM-BR não arquiva cópias de chaves privadas 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

A AC Certisign OM-BR gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7 Armazenamento de chave privada em módulo criptográfico

Ver item 6.1.

6.2.8. Método de ativação de chave privada

A ativação das chaves privadas das AC Certisign OM-BR é coordenada pela Supervisão de PKI, onde 3 de um grupo de 10 funcionários com perfis qualificados da





AC Certisign OM-BR, detentores de participação da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica.

Esse funcionários são identificados pelo crachá funcional emitido pela AC Certisign OM-BR contendo fotografia, nome, e departamento do funcionário.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

6.2.9. Método de desativação de chave privada

A chave privativa da AC Certisign OM-BR, instalada em ambiente de produção dos sistemas de certificação, localiza-se em nível de segurança 4, onde só é permitido o acesso ao ambiente em duplas devidamente autorizadas pelo sistema de controle de acesso da AC Certisign OM-BR.

Dentro deste ambiente, somente funcionários qualificados do departamento de operações têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação do sistema, após a sua devida identificação e autorização feita através de mecanismos nativos do sistema operacional.

Esses funcionários são identificados pelo crachá funcional emitido pela AC Certisign OM-BR contendo fotografia, nome, e departamento do funcionário.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.10. Método de destruição de chave privada

A Supervisão de PKI da AC Certisign OM-BR, de posse da chave privada original e suas cópias de segurança a serem destruídas, acompanhado do Gerente de Segurança e do representante legal da AC Certisign OM-BR, titular do certificado, conduz cerimônia específica, em ambiente de nível 4 de segurança, para reinicialização das mídias de armazenamento das chaves privadas, não deixando informações remanescente sensíveis nessas mídias.

O Gerente de Segurança e Supervisão de PKI são identificados pelo crachá funcional emitido pela AC Certisign OM-BR contendo fotografia, nome, e departamento do funcionário. O representante legal da AC Certisign OM-BR é identificado através de cédula de identidade ou passaporte, se estrangeiro.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC Certisign OM-BR e dos titulares dos certificados de assinatura digital por ela emitidos, bem como as LCR emitidas e sistemas de OCSP permanecem armazenadas após a expiração dos certificados correspondentes,





permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada

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

6.3.2.2. Não se aplica.

6.3.2.3. Cada PC implementada pela AC Certisign OM-BR define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.3.2.4. A validade admitida para certificados da AC Certisign OM-BR é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4. Dados de Ativação

Nos itens seguintes desta DPC 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

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC Certisign OM-BR são únicos e aleatórios.

6.4.1.2. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2. Proteção dos dados de ativação

6.4.2.1. A AC Certisign OM-BR garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra o uso não autorizado.

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 geração do par de chaves da AC Certisign OM-BR é realizada em ambiente próprio para a condução de Cerimônia de Geração de Chaves. O ambiente computacional é mantido off-line de modo a impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC Certisign OM-BR são descritos em cada PC implementada.

6.5.1.3. O ambiente computacional da AC Certisign OM-BR relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes funções:

- a) controle de acesso aos serviços e perfis da AC Certisign OM-BR;
- b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Certisign OM-BR;
- c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- d) geração e armazenamento de registros de auditoria da AC Certisign OM-BR;
- e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- f) 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 mecanismos de segurança física.

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC Certisign OM-BR, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC Certisign OM-BR. Todos esses eventos deverão ser registrados para fins de auditoria.

6.5.1.6. Equipamentos utilizados pela AC Certisign OM-BR são preparados e configurados como previsto na Política de Segurança da AC Certisign OM-BR ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.





6.5.2. Classificação da segurança computacional

A segurança computacional da AC Certisign OM-BR segue as recomendações *Common Criteria*.

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. Neste item estão descritos os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pelas AR para os processos de validação e aprovação de certificados.

6.5.3.2. Os requisitos abaixo correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL[1]:

- a) controle de acesso lógico ao sistema operacional;
- b) exigência de uso de senhas fortes;
- c) diretivas de senha e de bloqueio de conta;
- d) logs de auditoria do sistema operacional ativados, registrando:
 - i. iniciação e desligamento do sistema;
 - ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
 - iii. mudanças na configuração da estação;
 - iv. tentativas de acesso (login) e de saída do sistema (*logoff*);
 - v. tentativas não autorizadas de acesso aos arquivos de sistema;
 - vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.
- e) antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;
- f) firewall pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por *firewall* corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
- g) proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;
- h) sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);
- i) utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário;
- j) impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
- k) utilização de data e hora de Fonte Confiável do Tempo (FCT).

6.5.3.3. Não se aplica.





6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC Certisign OM-BR 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 Certisign OM-BR 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 Certisign OM-BR provêem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC Certisign OM-BR.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC Certisign OM-BR 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 Certisign OM-BR utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3. Controles de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

Antes de publicadas, todas as LCRs geradas pela AC Certisign OM-BR 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

6.7.1 Diretrizes Gerais

6.7.1.1. Neste item são descritos os controles relativos à segurança da rede da AC Certisign OM-BR, incluindo *firewalls* e recursos similares.

6.7.1.2. Nos servidores do sistema de certificação da AC Certisign OM-BR, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.7.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls*, e sistemas de detecção de intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.





6.7.1.4. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.7.1.5. O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2. *Firewall*

6.7.2.1. Mecanismos de *firewall* são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O *firewall* promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à AC Certisign OM-BR.

6.7.2.2. O software de *firewall*, entre outras características, implementa registros de auditoria.

6.7.3. Sistema de detecção de intrusão (IDS)

6.7.3.1. O sistema de detecção de intrusão está configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps* SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos *firewalls* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas ou ainda a reconfiguração dos *firewalls*.

6.7.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

6.7.3.3. O sistema de detecção de intrusão provê o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4. Registro de acessos não-autorizados à rede

As tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Carimbo de Tempo

Não se aplica.





7. PERFIS DE CERTIFICADO, LCR E OCSP

7.1. Perfil do Certificado

Todos os certificados emitidos pela AC Certisign OM-BR estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, de acordo com o perfil estabelecido na RFC 5280.

7.1.1. Número de versão

Os certificados emitidos pela AC Certisign OM-BR implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.1.2. Extensões de certificado

Não se aplica.

7.1.3. Identificadores de algoritmo

Não se aplica.

7.1.4. Formatos de nome

7.1.4.1. Não se aplica.

7.1.5. Não se aplica.

7.1.6. OID (*Object Identifier*) da DPC

O OID desta DPC é 2.16.76.1.1.183.

7.1.7. Uso da extensão “*Policy Constraints*”

Não se aplica.

7.1.8. Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.1.9. Semântica de processamento para as extensões críticas de PC

Extensões críticas são interpretadas conforme a RFC 5280.

7.2. Perfil de LCR

7.2.1. Número(s) de versão

As LCR geradas pela AC Certisign OM-BR 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. Neste item são descritas todas as extensões de LCR utilizadas pela AC Certisign OM-BR e sua criticalidade.

7.2.2.2. As LCR da AC Certisign OM-BR obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões de LCR:





- a) **Authority Key Identifier**, não crítica: contém o hash SHA-1 da chave pública da AC Certisign OM-BR;
- b) **CRL Number**, não crítica: contém um número sequencial para cada LCR emitida pela AC Certisign OM-BR.

7.3. Perfil de OCSP

7.3.1. Número(s) de versão

Os serviços de respostas OCSP da AC Certisign OM-BR 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 Certisign OM-BR estão em conformidade com a RFC 6960.

8. AUDITORIA DE CONFORMIDADE E OUTRAS AVALIAÇÕES

8.1. Frequência e circunstâncias das avaliações

As entidades integrantes da ICP-Brasil sofrem auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento.

8.2. Identificação/Qualificação do avaliador

8.2.1. As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2].

8.2.2. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

8.3. Relação do avaliador com a entidade avaliada

As auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].





8.4. Tópicos cobertos pela avaliação

8.4.1. As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPCs, PCs, PSs e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo *WebTrust*.

8.4.2. A AC Certisign OM-BR recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

8.4.3. As entidades da ICP-Brasil diretamente vinculadas à AC (AR e PSS), também receberam auditoria prévia, para fins de credenciamento. A AC é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

8.5. Ações tomadas como resultado de uma deficiência

A AC Certisign OM-BR age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

8.6. Comunicação dos resultados

A AC Certisign OM-BR age de acordo com os CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[2] e com os CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

Variável conforme definição interna Comercial.

9.1.2. Tarifas de acesso ao certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

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

Não são cobradas tarifas de revogação e de acesso à informação de status.





9.1.4. Tarifas para outros serviços

Não são cobradas tarifas de acesso à informação de status do certificado e à LCR, bem como tarifas de revogação e de acesso aos certificados emitidos.

9.1.5. Política de reembolso

Em caso de revogação do certificado por motivo de comprometimento da chave privada ou da mídia armazenadora da chave privada da AC Certisign OM-BR, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC Certisign OM-BR, será emitido gratuitamente outro certificado em substituição.

9.2. Responsabilidade Financeira

A responsabilidade da AC Certisign OM-BR será verificada conforme previsto na legislação brasileira.

9.2.1 Cobertura do seguro

Conforme item 4 desta DPC.

9.2.2 Outros ativos

Conforme regramento desta DPC.

9.2.3 Cobertura de seguros ou garantia para entidades finais

Conforme item 4 desta DPC.

9.3 Confidencialidade da informação do negócio

9.3.1 Escopo de informações confidenciais

9.3.1.1 Como princípio geral, todo documento, informação ou registro fornecido à AC ou às AR é sigiloso.

9.3.1.2. Nenhum documento, informação ou registro fornecido pelos titulares de certificado à AC Certisign OM-BR será divulgado.

9.3.2 Informações fora do escopo de informações confidenciais

As informações consideradas não sigilosas compreendem:

- a) os certificados e a LCR/OCSP emitidos pela AC Certisign OM-BR;
- b) informações corporativas ou pessoais que façam parte dos certificados ou em diretórios públicos;
- c) a PC correspondente;
- d) esta DPC;
- e) versões públicas da Política de Segurança;
- f) resultados finais de auditorias; e
- g) Termo de Titularidade ou solicitação de emissão do certificado.





A AC Certisign OM-BR e a AR a ela vinculada tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

- a) estejam na posse legítima da AC Certisign OM-BR ou da AR a ela vinculada antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;
- b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro(s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;
- c) sejam requisitados por determinação judicial ou governamental, desde que a AC Certisign OM-BR ou a AR a ela vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação.

Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC Certisign OM-BR e pela AR a ela vinculada, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

9.3.2.1 Certificados, LCR/OCSP, e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não confidenciais.

9.3.2.2 Os seguintes documentos da AC Certisign OM-BR também são considerados documentos não confidenciais:

- a) qualquer PC aplicável;
- b) qualquer DPC;
- c) versões públicas de Política de Segurança – PS; e
- d) a conclusão dos relatórios da auditoria.

9.3.2.3. A AC Certisign OM-BR também poderá divulgar, de forma consolidada ou segmentada por tipo de certificado, a quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-Brasil.

9.3.3 Responsabilidade em proteger a informação confidencial

9.3.3.1. Os participantes que receberem ou tiverem acesso a informações confidenciais devem possuir mecanismos para assegurar a proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

9.3.3.2. A chave privada de assinatura digital da AC Certisign OM-BR será gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade.





9.3.3.3. Os titulares de certificados emitidos para pessoas responsáveis pelo uso de certificados emitidos para equipamentos, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

9.3.3.4. Não se aplica.

9.4 Privacidade da informação pessoal

9.4.1 Plano de privacidade

A AC Certisign OM-BR assegurará a proteção de dados pessoais conforme sua Política de Privacidade.

9.4.2 Tratamento de informação como privadas

Como princípio geral, todo documento, informação ou registro que contenha dados pessoais fornecido à AC Certisign OM-BR será considerado confidencial, salvo previsão normativa em sentido contrário, ou quando expressamente autorizado pelo respectivo titular, na forma da legislação aplicável.

9.4.3 Informações não consideradas privadas

Informações sobre revogação de certificados de usuários finais são fornecidas na LCR/OCSP da AC Certisign OM-BR.

9.4.4 Responsabilidade para proteger a informação privadas

A AC Certisign OM-BR e AR são responsáveis pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5 Aviso e consentimento para usar informações privadas

As informações privadas obtidas pela AC Certisign OM-BR poderão ser utilizadas ou divulgadas a terceiros mediante expressa autorização do respectivo titular, conforme legislação aplicável.

O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

Autorizações formais podem ser apresentadas de duas formas:

- a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-Brasil; ou
- b) por meio de pedido escrito com firma reconhecida.

9.4.6 Divulgação em processo judicial ou administrativo

Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC Certisign OM-BR será fornecido a qualquer pessoa, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.





As informações privadas ou confidenciais sob a guarda da AC Certisign OM-BR poderão ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7 Outras circunstâncias de divulgação de informação

Não se aplica.

9.4.8 Informações a terceiros

Como diretriz geral, que nenhum documento, informação ou registro sob a guarda da AR ou da AC Certisign OM-BR deverá ser fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e corretamente identificada.

9.5 Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6 Declarações e Garantias

9.6.1 Declarações e Garantias da AC

A AC Certisign OM-BR declara e garante o quanto segue:

9.6.1.1 Autorização para certificado

A AC Certisign OM-BR implementa procedimentos para verificar a autorização da emissão de um certificado ICP-Brasil, contidas nos itens 3 e 4 desta DPC. A AC Certisign OM-BR, no âmbito da autorização de emissão de um certificado, analisa, audita e fiscaliza os processos das suas ARs em forma de suas DPCs, PCs e normas complementares.

9.6.1.2 Precisão da informação

A AC Certisign OM-BR implementa procedimentos para verificar a precisão da informação nos certificados, contidas nos itens 3 e 4 desta DPC. A AC Raiz, no âmbito da precisão da informação contida nos certificados que emite, analisa, audita e fiscaliza os processos das suas ARs na forma de suas DPCs, PCs e normas complementares.

9.6.1.3 Identificação do requerente

A AC Certisign OM-BR implementa procedimentos para verificar identificação dos requerentes dos certificados, contidas nos itens 3 e 4 desta DPC. A AC Certisign OM-BR, no âmbito da identificação do requerente contida nos certificados que emite, analisa, audita e fiscaliza os processos das suas ARs em forma de suas DPCs, PCs e normas complementares.





9.6.1.4 Consentimento dos titulares

A AC Certisign OM-BR implementa termos de consentimento ou titularidade, contidas nos itens 3 e 4 desta DPC.

9.6.1.5 Serviço

A AC Certisign OM-BR mantém 24x7 acesso ao seu repositório com a informação dos certificados próprios e suas LCRs/OCSP.

9.6.1.6 Revogação

A AC irá revogar certificados da ICP-Brasil por qualquer razão especificada nas normas da ICP-Brasil.

9.6.1.7 Existência Legal

Esta DPC está em conformidade legal com a MP 2.200-2, de 24 de agosto de 2001, e legislação aplicável.

9.6.2 Declarações e Garantias da AR

Em acordo com item 4 desta DPC.

9.6.3 Declarações e garantias do titular

9.6.3.1 Toda informação necessária para a identificação do titular de certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela AC Certisign OM-BR, o titular é responsável por todas as informações por ela fornecidas, contidas nesse certificado.

9.6.3.2 A AC Certisign OM-BR deve informar à AC Raiz qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4 Declarações e garantias das terceiras partes

9.6.4.1 As terceiras partes devem:

- a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
- b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2 O certificado da AC Certisign OM-BR é considerado válido quando:

- i. tiver sido emitido pela AC Certisign OM-BR;
- ii. não constar como revogado pela AC Certisign OM-BR;
- iii. não estiver expirado; e
- iv. puder ser verificado com o uso do certificado válido da AC Certisign OM-BR.

9.6.4.3 A utilização ou aceitação de certificados sem a observância das providências descritas é de conta e risco da terceira parte que usar ou aceitar a utilização do respectivo certificado.





9.6.5 Representações e garantias de outros participantes

Não se aplica.

9.7 Isenção de garantias

Não se aplica.

9.8 Limitações de responsabilidades

A AC Certisign OM-BR não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

9.9 Indenizações

A AC Certisign OM-BR responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

9.10 Prazo e Rescisão

9.10.1 Prazo

Esta DPC entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.2 Término

Esta DPC vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.10.3 Efeito da rescisão e sobrevivência

Os atos praticados na vigência desta DPC são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

9.11 Avisos individuais e comunicações com os participantes

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC deverá ser submetida à aprovação da AC Raiz.





9.12.2. Mecanismo de notificação e períodos

A AC Certisign OM-BR mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web: http://icp-brasil.certisign.com.br/repositorio/dpc/AC_Certisign_OM-BR/DPC_AC_Certisign_OM-BR.pdf.

9.12.3. Circunstâncias na qual o OID deve ser alterado

Não se aplica.

9.13. Solução de conflitos

9.13.1. Os litígios decorrentes desta DPC serão解决ados de acordo com a legislação vigente.

9.13.2. A DPC da AC Certisign OM-BR não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

9.14. Lei aplicável

Esta DPC é regida pela legislação da República Federativa do Brasil, notadamente a Medida Provisória Nº 2.200-2, de 24.08.2001, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas em vigor no Brasil.

9.15. Conformidade com a Lei aplicável

A AC Certisign OM-BR está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

9.16. Disposições Diversas

9.16.1. Acordo completo

Esta DPC representa as obrigações e deveres aplicáveis à AC Certisign OM-BR 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

Os direitos e obrigações previstos nesta DPC são de ordem pública e indisponíveis, não podendo ser cedidos ou transferidos a terceiros.

9.16.3. Independência de disposições

A invalidade, nulidade ou ineficácia de qualquer das disposições desta DPC não prejudicará as demais disposições, as quais permanecerão plenamente válidas e eficazes. Neste caso a disposição inválida, nula ou ineficaz será considerada como não escrita, de forma que esta DPC será interpretada como se não contivesse tal disposição, e na medida do possível, mantendo a intenção original das disposições remanescentes.





9.16.4. Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17. Outras provisões

Não se aplica.

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 |
|------|---|--------------|
| [1] | CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL Aprovado pela Resolução nº 07, de 19 de maio de 2006 | DOC-ICP03.01 |
| [2] | CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 25, de 24 de outubro de 2003 | DOC-ICP-09 |
| [3] | CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 24, de 29 de agosto de 2003 | DOC-ICP-08 |
| [6] | CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL Aprovado pela Resolução nº 06, de 22 de novembro de 2001 | DOC-ICP-03 |
| [7] | REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL Aprovado pela Resolução nº 07, de 12 de dezembro de 2001 | DOC-ICP-04 |
| [8] | POLÍTICA DE SEGURANÇA DA ICP-BRASIL Aprovado pela Resolução nº 02, de 25 de setembro de 2001 | DOC-ICP-02 |



| | | |
|-----|--|------------|
| [9] | REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL Aprovado pela Resolução nº 59, de 28 de novembro de 2008 | DOC-ICP-12 |
|-----|--|------------|

10.2 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio <http://www.iti.gov.br>.

| Ref. | Nome do documento | Código |
|------|-----------------------|--------------|
| [4] | TERMO DE TITULARIDADE | ADE-ICP-05.B |

11. REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. 11.515/NB 1334: Critérios de segurança física relativos ao armazenamento de dados. 2007.

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

RFC 4210, IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005.

RFC 5019, IETF - The Lightweight Online Certificate Status Protocol (OCSP) Profile for HighVolume Environments, september 2007.

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

RFC 6712, IETF - Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012.

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

