Infraestrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 11 – Volume I

Requisitos, Materiais e Documentos Técnicos para Homologação de Software de Autoridade Certificadora (AC) e Autoridade de Registro (AR) no Âmbito da ICP-Brasil

Verão 1.0

Brasília, 14 de maio de 2010

Sumário

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

Glossário

Os termos utilizados neste MCT se referem àqueles definidos no Glossário ICP-Brasil [8] conforme seção de referências normativas.

Lista de Acrônimos

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ANSI	*American National Standards Institute*
AR	Autoridade Registradora
BER	*Basic Encoding Rules*
CMS	*Cryptographic Message Syntax*
CPF	Cadastro de Pessoa Física
CRL	*Certificate Revocation List*
CSR	*Certificate Signing Request*
DER	*Distinguished Encoding Rules*
DPC	Declaração de Práticas de Certificação
HSM	*Hardware Security Module*
HTTP	*Hypertext Transfer Protocol*
ICP	Infra-Estrutura de Chaves Públicas
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IP	*Internet Protocol*
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
LEA	Laboratório de Ensaios e Auditoria
MCT	Manual de Condutas Técnicas
MSC	Módulo de Segurança Criptográfico
NSH	Nível de Segurança de Homologação
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
PC	Políticas de Certificado
PEM	*Privacy Enhanced Mail*
PKCS	*Public-Key Cryptography Standards*
PSC	Provedor de Serviços Criptográficos
RFC	*Request For Comments*
RG	Registro Geral
TI	Tecnologia da Informação

1. Introdução

Este documento descreve os requisitos técnicos que devem ser observados no processo de homologação de Softwares de Autoridade Certificadora (AC) e Autoridade de Registro (AR) no âmbito da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil).

1.1 Definições

Para uma melhor compreensão do disposto neste documento, adotam-se os termos Autoridade Certificadora (AC) e Autoridade de Registro (AR) conforme definição presente no glossário ICP-Brasil [8].

Entende-se que um Software de AC pode não implementar explicitamente as funcionalidades requeridas por uma AR. Entende-se também que o Software de AC e de AR precisa ser capaz de ser configurado para operar segundo as regulamentações definidas pela ICP-Brasil.

1.2 Objetivo da Homologação

O objetivo do processo de homologação de um Software de AC e AR é validar a interoperabilidade dos seus produtos gerados e sua relação com os usuários e por conseguinte constatar a operação segura do software para uma AC e uma AR, por meio da avaliação técnica de aderência aos requisitos técnicos definidos neste manual.

1.3 Descrição do Processo de Homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos definidos neste manual que devem ser atendidos por um Software de AC e AR para prover interoperabilidade nos seus produtos gerados e sua relação com os usuários e constatar a operação segura. Estes requisitos técnicos são avaliados segundo ensaios de aderência.
Para a realização dos ensaios, a Parte Interessada deve submeter ao processo de homologação um conjunto de materiais requisitados, através de um procedimento denominado depósito de material.

1.4 Estrutura do MCT 11 – Volume I

Este documento (MCT 11 – Volume I) está estruturado da seguinte forma:

- Parte 1: Descreve os requisitos técnicos que devem ser verificados no processo de homologação de um Software de AC e AR;
- parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de um Software de AC e AR;
- referências normativas: Descreve as referências normativas que foram utilizadas na elaboração deste documento.

1.1 Serviços oferecidos por uma ICP (Infra-estrutura de Chaves Públicas)

Imagine um grupo de pessoas que não se conhecem querendo se comunicar em sigilo. Com uso da criptografia assimétrica é possível enviar dados em sigilo para pessoas distintas, cada dado cifrado com a chave pública do destinatário. Assim, cifram-se os dados com a chave pública de cada destinatário. Somente o destinatário específico que detém a posse do par de chaves consegue abrir o pacote de dados cifrado destinado a ele, pois somente ele possui o acesso e conhecimento da sua chave privada correspondente a sua chave pública. Existe uma necessidade de se associar unicamente um determinado par de chaves assimétricas a uma identidade. O certificado digital é o elemento responsável por associar unicamente um par de chaves assimétricas a uma identidade. Portanto, uma ICP como uma infra-estrutura deve

definir normas e procedimentos de modo a assegurar por meio de controles rígidos o gerenciamento do ciclo de vida dos certificados digitais.

Como elementos principais que compõem uma ICP pode-se destacar: a AC responsável pela geração, emissão, renovação e revogação de certificados digitais e a AR responsável por registrar e validar a identidade dos titulares dos certificados digitais.

Conforme definido no glossário ICP-Brasil [8], os titulares dos certificados digitais são as entidades, pessoa física ou jurídica, para as quais foi emitido um certificado digital. O titular do certificado digital é o possuidor da chave privada correspondente à chave pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra. Os certificados digitais podem ser utilizados por uma pessoa, equipamento, instituição (empresa) ou aplicação.

Uma ICP possui uma estrutura hierárquica formada por uma AC raiz (âncora de confiança) e diversas AC´s intermediárias, sendo que cada AC intermediária deve confiar de forma hierárquica na AC raiz e nas AC´s de nível imediatamente superior. Uma AC pode emitir certificados digitais para outras AC´s de nível hierárquico inferior ou somente para usuários finais ou titulares dos certificados digitais conforme mostra a figura 1.

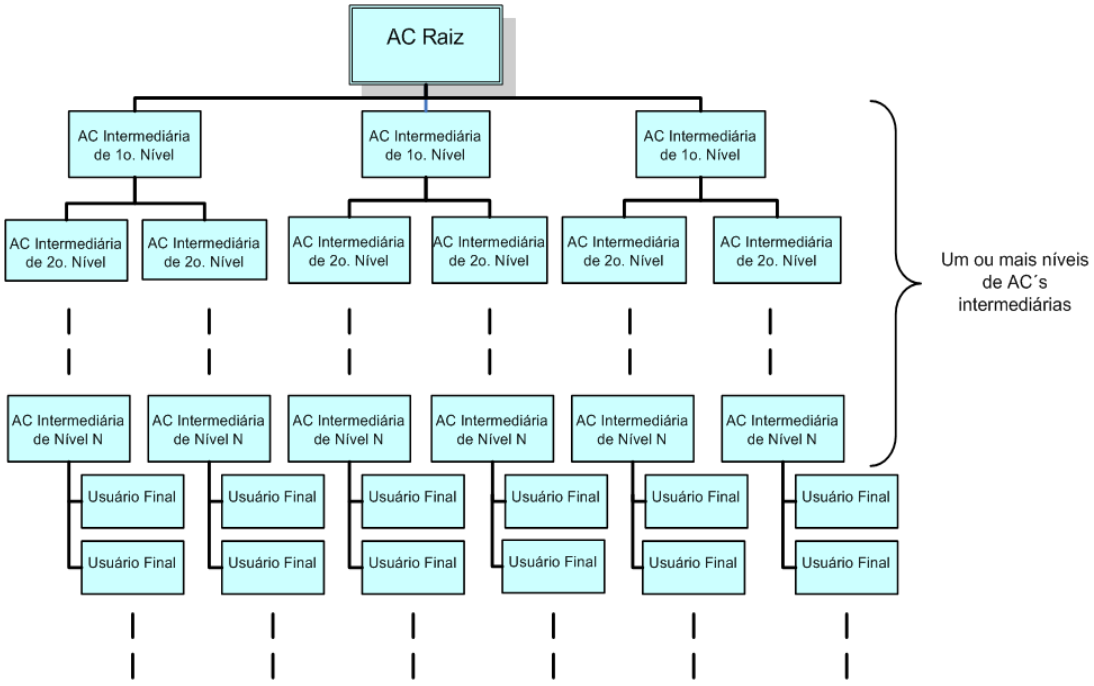

Figura 1: Hierarquia de uma ICP

2. Parte 1

Requisitos Técnicos para Homologação de Software de AC e AR no âmbito da ICP-Brasil

2.1 Introdução

A parte 1 deste manual apresenta os requisitos técnicos que devem ser verificados no processo de homologação de um Software de AC e AR.

Foram utilizadas as normas publicadas pela ICP-Brasil que estão citadas na seção de referências no final deste MCT para atender os requisitos dos Softwares de AC e AR.

Um Software de AC tem como principal objetivo gerenciar o ciclo de vida dos certificados digitais emitidos. Um Software de AC pode ser visto como um diagrama de blocos, onde cada bloco corresponde à funcionalidades específicas do sistema conforme pode ser visto na figura 2.

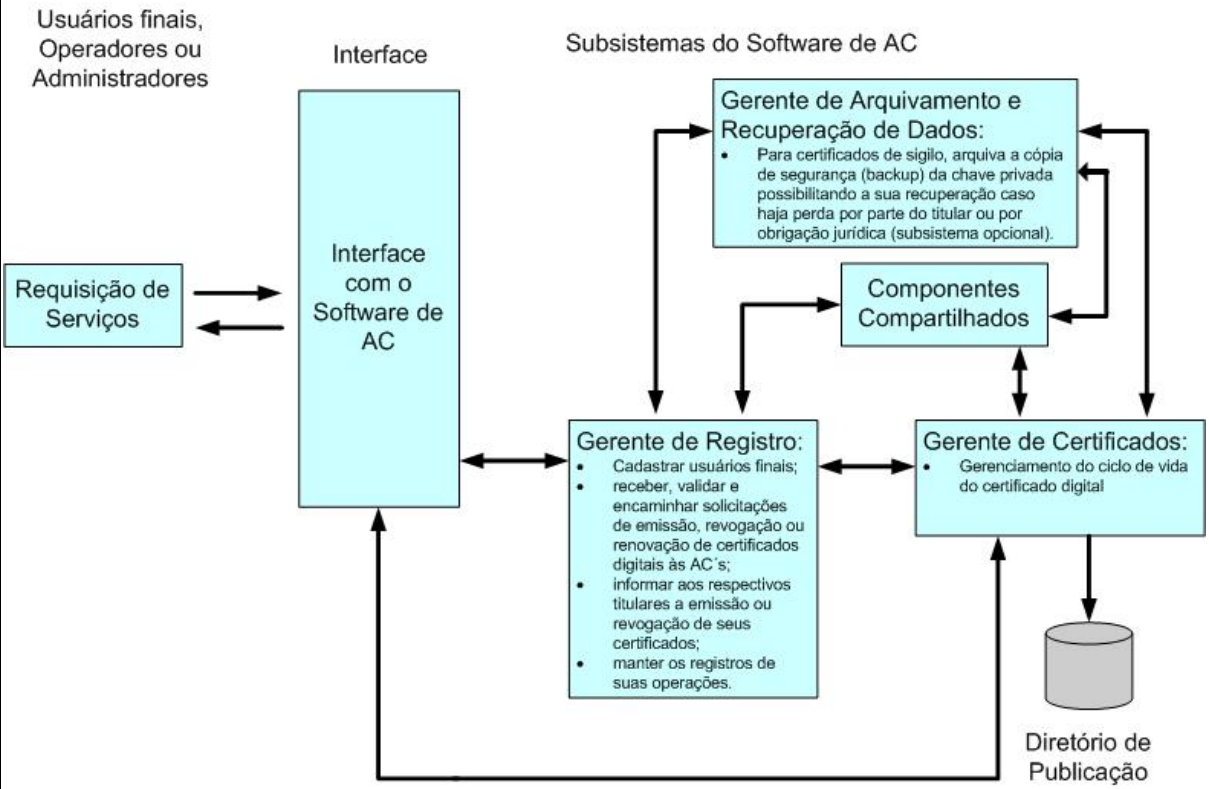

Figura 2: Arquitetura Genérica de um Software AC

Como mostra a figura 2, um Software de AC genérico é formado por três subsistemas principais mais os componentes compartilhados entre estes subsistemas, além do sistema operacional. Os três subsistemas principais são:

- Gerente de certificados digitais que funciona como uma autoridade certificadora principal com a funcionalidade básica de gerenciamento do ciclo de vida do certificado digital;

- gerente de registros que cadastra os dados obtidos do titular do certificado digital e os repassa para a AC com as seguintes funcionalidades básicas:

    - cadastrar os titulares dos certificados digitais;
    - receber, validar e encaminhar solicitações de emissão, revogação ou renovação de certificados digitais às AC´s;
    - informar aos respectivos titulares a emissão ou revogação de seus certificados;
    - manter os registros de suas operações;

- gerente de arquivamento e recuperação de dados que, para certificados de sigilo, arquiva a cópia de segurança (backup) da chave privada possibilitando a sua recuperação caso haja perda por parte do titular ou por obrigação jurídica (subsistema opcional).

Na arquitetura genérica de um Software de AC mostrada na figura 2, os titulares dos certificados digitais, operadores ou administradores do Software de AC fazem requisições de serviço por meio de uma interface com o Software de AC. Dependendo do tipo, as requisições de serviço são tratadas pelo subsistema de gerente de registro ou pelo subsistema de gerente de certificado. Ambos os subsistemas de gerente de registro e de gerente de certificado podem recuperar informações relacionadas aos serviços requisitados através do subsistema de gerente de recuperação de dados. Os três subsistemas podem ainda acionar componentes compartilhados para a execução dos serviços.

Os componentes compartilhados, conforme ilustrados na figura 3 são:

- Autorização: componente que serve para autorizar o acesso ao Software de AC, ao Software de AR e ao banco de dados interno;
- autenticação: componente que serve para confirmar a identidade de um titular do certificado digital, operador ou administrador do Software de AC e AR;
- políticas: componente responsável pela política de certificação, procedimentos e níveis de segurança adotados para o gerenciamento do ciclo de vida de um certificado digital;
- agendamento: componente que serve para agendar tarefas e notificações;
- *log* / registros: componente que serve para registrar as operações efetuadas no Software da AC e AR;
- diretório de publicação: componente que é um repositório utilizado para publicar certificados digitais emitidos e Listas de Certificados Revogados (LCR´s).
- banco de dados interno: componente que é utilizado para o armazenamento de informações administrativas dos Softwares de AC e AR, configurações etc;
- interfaces:

    - componente de interface para titular do certificado digital;
    - componente de interface para operador de AC e AR;
    - componente de interface para administrador de AC e AR.

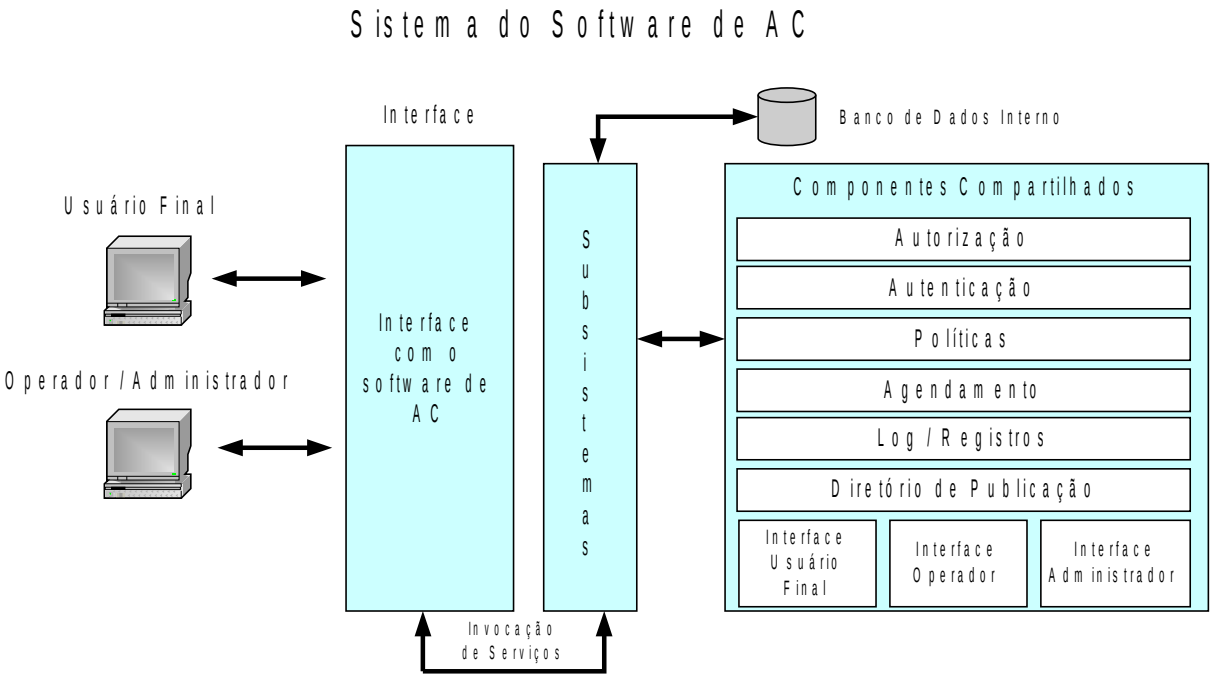

Figura 3: Componentes Compartilhados da Arquitetura Genérica de um Software de AC

Conforme podemos observar na figura 3, os componentes compartilhados são componentes auxiliares dos subsistemas para completar os serviços ICP e não são invocados diretamente por um titular do certificado digital, por um operador ou por um administrador, mas sim por meio dos subsistemas.

2.1.1 Ciclo de Vida do Certificado Digital

Um certificado digital possui as seguintes fases que definem o seu ciclo de vida:

- solicitação;
- validação;
- verificação;
- geração;
- emissão;
- publicação;
- aceitação;
- utilização;
- revogação;
- renovação;
- expiração.

Cada uma das fases do ciclo de vida do certificado digital envolve a troca de dados entre AC e titular. De acordo com as regulamentações específicas definidas pela ICP-Brasil, as fases de geração e emissão de certificados digitais requerem que um conjunto de dados adicional a CSR PKCS#10 [11] sobre o titular do certificado digital sejam informados para a AC. Esse conjunto de dados pode ser chamado de dados de solicitação do certificado digital na ICP-Brasil.

2.1.1.1 Dados de Solicitação do Certificado Digital na ICP-Brasil

Para possibilitar a geração e emissão correta de um certificado digital segundo as regras ICP-Brasil, os seguintes dados de solicitação do certificado digital devem ser informados pelo titular do certificado ao Software de AC e AR (ver figura 4):

- Dados da CSR PKCS#10 [11]: corresponde aos dados que devem ser informados segundo a especificação PKCS#10 [11], como por exemplo, a chave pública do titular do certificado digital;
- dados do titular do certificado digital: corresponde aos dados de identificação e os atributos que devem estar associados ao titular do certificado digital. Como dados de identificação e atributos entende-se aqueles descritos conforme DOC-ICP-04 [5] tais como, nome do proprietário do certificado digital, RG, CPF, data de nascimento etc; e
- dados do perfil do certificado digital ICP-Brasil: corresponde ao tipo de certificado digital ICP-Brasil solicitado pelo titular do certificado digital (por exemplo, A3 ou S3) que segundo o DOC-ICP-04 [5] define as regras quanto à validade do certificado, tamanho da chave, tipo de mídia armazenadora, o processo de geração de chave criptográfica etc.

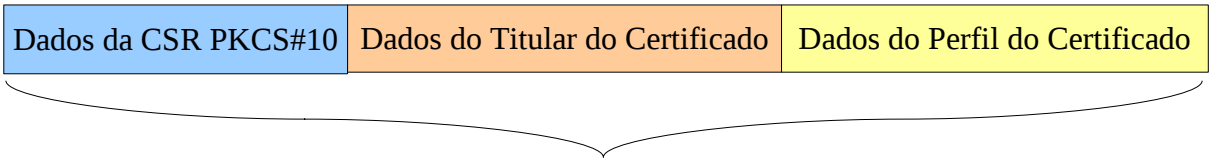

Figura 4: Dados de Solicitação do Certificado Digital na ICP-Brasil

2.1.1.2 Descrição dos Processos Associados ao Ciclo de Vida do Certificado Digital

Os processos associados ao ciclo de vida do certificado digital para o titular do certificado digital podem ser ilustrados pela figura 5. Um titular do certificado digital entra em contato com a AC via uma interface disponível para solicitar seu certificado digital. Após cadastramento inicial informando seus dados de titular e o tipo desejado do certificado digital, uma AR valida de forma presencial os dados do titular, e caso sejam verdadeiros, guarda uma cópia dos dados e aprova a emissão, por parte da AC, do certificado digital correspondente a solicitação prévia do titular do certificado digital. O titular do certificado digital então gera o par de chaves e a requisição de certificado digital (CSR PKSC#10 – *Certificate Signing Request*) que são enviados para a AC via canal seguro. Assim que a AC validar o conteúdo digital da CSR PKSC#10 e estar preparada para atender a política de certificado exigida pelo tipo ICP-Brasil escolhido, o certificado digital é gerado incluindo a chave pública do titular do certificado digital e depois assinado digitalmente pela chave privada da AC.

Após a emissão, o certificado digital do titular do certificado digital deve ser inserido pela AC no repositório de certificados digitais emitidos para futuras consultas. Depois de atingir o tempo de uso determinado pela validade do certificado, o certificado expira. Caso haja comprometimento da chave privada correspondente a chave pública do certificado ou qualquer outro problema durante a sua validade, o certificado deve ser revogado pelo titular do certificado digital e deve ser incluído pela AC em sua lista de certificados revogados publicada segundo as regras definidas pela ICP-Brasil.

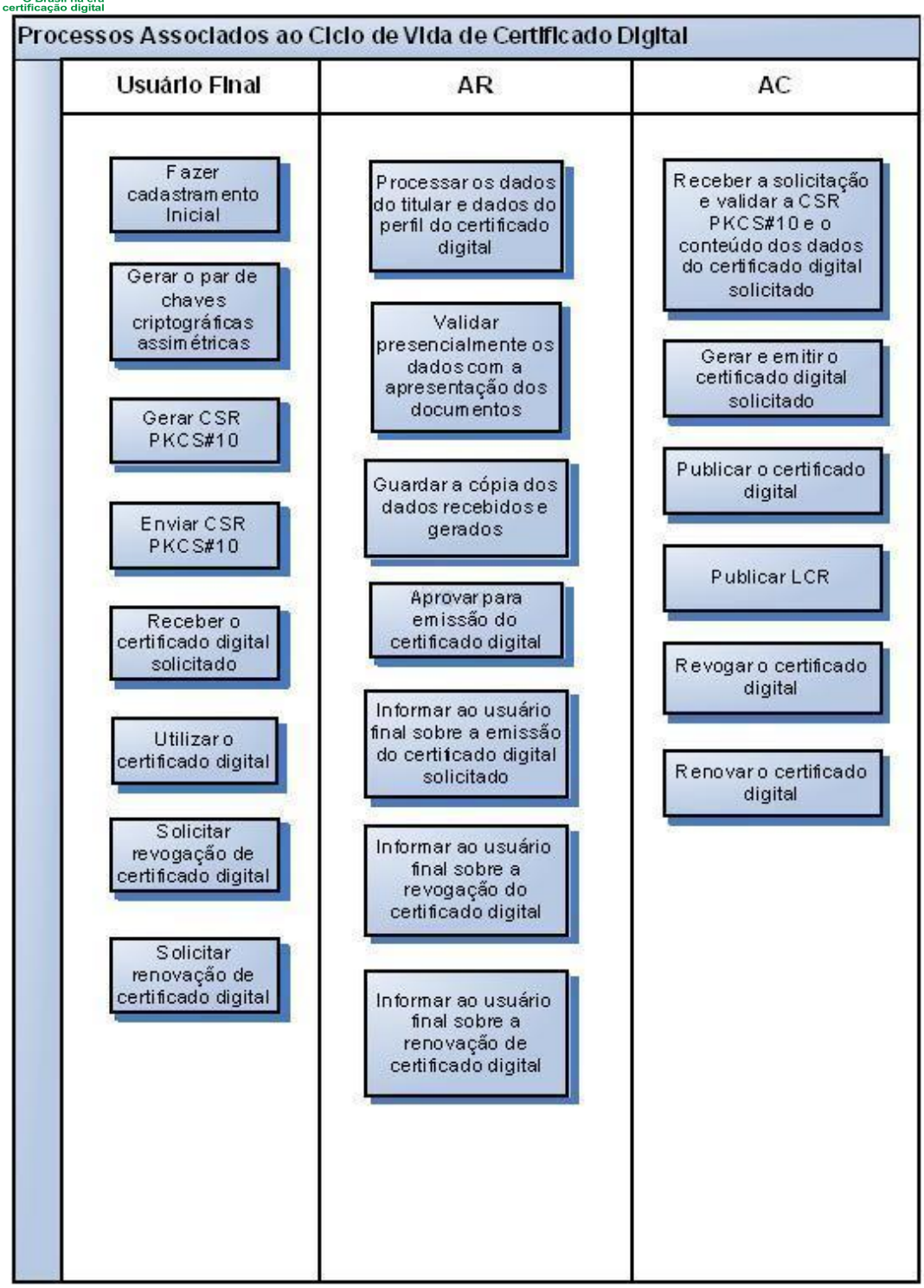

Figura 5: Ciclo de Vida Simples de um Certificado Digital

Antes de participar de serviços suportados por uma ICP, um titular do certificado digital deve inicialmente se cadastrar perante a AC. Este manual não tratará dos processos de verificação de documentação para validar o titular do certificado digital (responsabilidade da AR).

2.1.2 Organização da Parte 1 do MCT

A parte 1 deste MCT está organizada da seguinte forma:

- Requisitos aplicáveis somente ao Software de AC;
- Requisitos aplicáveis somente ao Software de AR;
- Requisitos aplicáveis ao Software de AC e AR.

2.2 Requisitos aplicáveis somente ao Software de AC

Nesta seção estão definidos os requisitos aplicáveis apenas a um Software de AC.

2.2.1 Requisitos Gerais de um Software de AC

REQUISITO I.01: Um Software de AC deve oferecer todas as funcionalidades necessárias para o gerenciamento completo do ciclo de vida do certificado digital.

RECOMENDAÇÃO I.01: Um Software de AC pode oferecer a funcionalidade de arquivamento e recuperação do par de chaves criptográficas assimétricas para certificados digitais ICP-Brasil de sigilo para os titulares dos certificados digitais.

RECOMENDAÇÃO I.02: Um Software de AC pode oferecer o serviço de OCSP [14].

REQUISITO I.02: Um Software de AC deve utilizar, no mínimo, os padrões e algoritmos criptográficos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4] para executar suas operações.

2.2.2 Requisitos de Solicitação de Certificados Digitais

A solicitação de certificado digital deve ser feita na AC por meio de um intermediário na forma de uma AR utilizando um canal seguro. Na solicitação, o titular do certificado digital fornece os dados da CSR PKCS#10, os seus dados de titular e os dados do perfil do certificado digital desejado. Os dados de titular devem ser validados por um agente de registro que depois terá a responsabilidade de aprovar ou negar a emissão do certificado digital.
A solicitação é recebida pelo Software de AC por meio de uma requisição formatada pela AR ou diretamente pelo titular do certificado digital por meio de uma interface que o Software de AC torna disponível.

REQUISITO I.03: Um Software de AC deve receber e validar uma requisição de certificado digital somente no formato CSR PKCS#10 [11] que contém a chave pública do titular do certificado digital.

REQUISITO I.04: Um Software de AC deve associar uma chave pública recebida com os dados do titular e os dados do perfil do certificado digital ambos informados pelo titular do certificado digital.

REQUISITO I.05: Um Software de AC deve, antes da emissão, controlar o período de validade dos certificados digitais emitidos para AC´s ou titulares dos certificados digitais solicitantes. Em termos de período de validade do certificado digital, os seguintes requisitos devem ser controlados pelo Software de AC:

- O período de validade deve estar de acordo com o tipo de certificado digital e com a PC da AC;

- o período de validade deve estar aninhado dentro do período de validade do certificado da AC emitente, obedecendo ao tipo do certificado digital.

2.2.3 Requisitos de Geração e Emissão de Certificados Digitais

REQUISITO I.06: Um Software de AC deve gerar um certificado digital no formato X.509v3 de acordo com os dados de solicitação do certificado digital do titular, após validados, a Política de Certificação (PC) e a Declaração de Práticas de Certificação (DPC) da AC segundo as regras definidas pela ICP-Brasil.

REQUISITO I.07: Ao decorrer de um processo de geração de certificado digital ICP-Brasil, um Software de AC deve verificar se o titular gerou uma chave pública diferente das chaves públicas presentes nos certificados digitais anteriores. Este requisito tem por finalidade evitar com que o titular consiga gerar o seu certificado digital utilizando a mesma chave pública de algum certificado digital anteriormente emitido por esta AC.

RECOMENDAÇÃO I.03: Ao decorrer de um processo de geração de certificado digital ICP-Brasil, um Software de AC pode também consultar e verificar se a chave pública utilizada pelo titular do certificado digital na geração é diferente das chaves públicas certificadas por todas as outras AC´s de mesmo nível credenciadas na ICP-Brasil. Este requisito tem por finalidade evitar com que o titular do certificado digital consiga gerar o seu certificado digital utilizando a mesma chave pública de algum certificado digital anteriormente emitido por uma AC diferente daquela escolhida para a solicitação atual.

REQUISITO I.08: Um Software de AC deve tornar disponível um certificado digital gerado ao titular do certificado digital solicitante.

RECOMENDAÇÃO I.04: Um Software de AC pode entregar um componente para o titular do certificado digital com a finalidade de gerar um par de chaves criptográficas assimétricas. Este componente deve ser capaz de verificar a midia de geração e armazenamento do par de chaves baseando-se no tipo de certificado digital ICP-Brasil (A1, A2, A3, A4, S1, S2, S3, S4, T3 ou T4) conforme definido no item 6.1 do DOC-ICP-04 [5].

REQUISITO I.09: Especificamente para certificados digitais ICP-Brasil de níveis de segurança 1 e 2, o componente do Software de AC responsável por gerar o par de chaves de forma aleatória deve utilizar métodos matemáticos seguros para esta finalidade. Por métodos matemáticos seguros entendem-se aqueles que atendem a norma ANSI X9.31 [18] em relação ao algoritmo RSA.

REQUISITO I.10: Um Software de AC deve permitir a emissão de certificados digitais ICP-Brasil contendo somente caracteres aceitos, conforme definido no DOC-ICP-04 [5].

REQUISITO I.11: Um Software de AC deve assinar certificados digitais ICP-Brasil utilizando os padrões e algoritmos definidos pela ICP-Brasil conforme DOC-ICP-01.01 [4].

REQUISITO I.12: Um Software de AC, conforme seu credenciamento, deve permitir a emissão de certificados digitais ICP-Brasil para AC Raiz [3], AC´s intermediárias ou titulares dos certificados digitais.

REQUISITO I.13: Um Software de AC deve possuir meios necessários para manter a relação unívoca entre um par de chaves criptográficas assimétricas e um titular do certificado

digital. Este requisito tem o objetivo de evitar com que titulares dos certificados digitais maliciosos solicitem certificados digitais diferentes a uma AC utilizando o mesmo par de chaves assimétricas, fato este que se ocorrer pode possibilitar a geração de assinaturas digitais idênticas (homônimas) que não evitam a irretratabilidade de conteúdo e de geração da assinatura digital.

2.2.4 Requisitos de Renovação de Certificados Digitais

REQUISITO I.14: Um Software de AC deve possuir a funcionalidade de renovar certificados digitais mediante requisição do titular ou responsável do certificado digital.

REQUISITO I.15: Um Software de AC deve oferecer uma interface e funcionalidades necessárias que permitam aos titulares dos certificados digitais renovarem seus certificados digitais. Conforme definido no glossário ICP-Brasil [8], renovação de certificado digital ICP-Brasil significa o processo para obter um certificado novo antes que o certificado existente tenha expirado. Na ICP-Brasil, é obrigatória a geração de novas chaves criptográficas distintas para cada certificado emitido.

REQUISITO I.16: Ao decorrer de um processo de renovação de certificado digital ICP-Brasil, um Software de AC deve verificar se o titular do certificado digital gerou uma chave pública diferente das chaves públicas presentes nos certificados digitais anteriores. Este requisito tem por finalidade evitar com que o titular do certificado consiga renovar o seu certificado digital utilizando a mesma chave pública de algum certificado digital anteriormente emitido.

RECOMENDAÇÃO I.05: Ao decorrer de um processo de renovação de certificado digital ICP-Brasil, um Software de AC pode também consultar e verificar se a nova chave pública utilizada pelo titular do certificado digital na renovação é diferente das chaves públicas certificadas por todas as outras AC´s de mesmo nível credenciadas na ICP-Brasil. Este requisito tem por finalidade evitar com que o titular do certificado digital consiga renovar o seu certificado digital utilizando a mesma chave pública de algum certificado digital anteriormente emitido por uma AC diferente daquela escolhida para a solicitação atual.

REQUISITO I.17: Um Software de AC deve controlar que o pedido de renovação seja feito dentro do período de validade do certificado digital.

2.2.5 Requisitos de Revogação de Certificados Digitais

Dentro do período de validade, um titular para certificados digitais de pessoa física ou um responsável para certificados digitais de pessoa jurídica, pode solicitar a revogação de um certificado digital por vários motivos, como comprometimento da própria chave privada, certificado digital gerado com dados errados do titular etc.
A AC que emitiu o certificado digital ou, também por uma AR vinculada, ambas podem revogar o certificado do titular ou do responsável por motivos de renovação do par de chaves da AC, comprometimento do par de chaves da AC etc.

REQUISITO I.18: Um Software de AC deve possuir a funcionalidade de revogar certificados digitais mediante requisição do titular ou responsável do certificado digital.

REQUISITO I.19: Um Software de AC deve fornecer ao titular do certificado digital uma interface de revogação de certificados digitais.

REQUISITO I.20: Um Software de AC deve receber requisições de revogação de certificados digitais ou por intermédio de uma AR ou diretamente pelo titular ou responsável do certificado digital.

REQUISITO I.21: Antes de permitir a revogação, um Software de AC, deve tornar disponível um mecanismo de autenticação para a revogação do certificado digital. Como consequencia, o Software de AC deve ser capaz de aceitar requisições de revogação somente após a entidade solicitante (AR, titular ou responsável) ter sido previamente autenticada.

RECOMENDAÇÃO I.06: Um Software de AC pode ter mecanismos de notificação para os titulares dos certificados digitais, por exemplo, por meio do envio de *e-mails*, quando ocorrer comprometimento da chave privada da AC, emissão de novo par de chaves e correspondente certificado, ou então o encerramento de suas atividades.

RECOMENDAÇÃO I.07: Recomenda-se que um Software de AC não retire da LCR um certificado digital que foi revogado e anteriormente expirado.

REQUISITO I.22: Um Software de AC deve gerar LCR´s de acordo com o DOC-ICP-04 [5].

REQUISITO I.23: Um Software de AC deve publicar a última LCR em repositórios internos e especificamente definidos pela AC para livre consulta. A publicação de uma LCR pode ser feita de forma manual ou automática. Antes da publicação de uma LCR, o Software de AC deve verificar se as seguintes condições foram satisfeitas:

- O certificado digital da AC que assina a LCR deve ser válido e possuir o campo *Key Usage* com valor *CRLSign* ativo;
- o repositório interno de publicação da AC deve ter o mesmo endereço do campo CRL Distribution Point informado nos respectivos certificados digitais emitidos para titulares dos certificados digitais.
- a LCR gerada pelo Software de AC deve ser verificada quanto à sua consistência de conteúdo e perfil conforme o DOC-ICP-05 [7] item 6.6.4.

REQUISITO I.24: Conforme o DOC-ICP-05 [7], um Software de AC deve fornecer interfaces de revogação de certificados digitais customizadas para cada entidade:

- Titular ou responsável;
- AR;
- própria AC.

REQUISITO I.25: Um Software de AC deve registrar as solicitações de revogação de certificados digitais.

2.2.5.1 Listas de Certificados Revogados

DEFINIÇÃO: Conforme definido no glossário ICP-Brasil [8], uma lista de certificados revogados é uma lista assinada digitalmente por uma Autoridade Certificadora, publicada periodicamente, contendo certificados que foram revogados antes de suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.

REQUISITO I.26: Um Software de AC deve permitir a configuração do caminho de publicação de LCR´s.

REQUISITO I.27: Um Software de AC deve garantir a gravação/publicação da LCR no repositório configurado.

REQUISITO I.28: Um Software de AC deve publicar uma LCR segundo os padrões e normas definidas pelo ICP-Brasil no DOC-ICP-04 [5] em função do tipo do certificado digital.

RECOMENDAÇÃO I.08: Um Software de AC pode configurar pontos distintos de distribuição da LCR para fins de contingência.

REQUISITO I.29: Um Software de AC deve assinar as LCR´s com a mesma chave privada usada para assinar os certificados digitais.

REQUISITO I.30: Um Software de AC deve emitir LCR´s, no máximo, até a data e hora estabelecidos pelo campo *nextUpdate* da LCR vigente que define a próxima data e hora de publicação.

REQUISITO I.31: Um Software de AC deve permitir a publicação automática ou manual de LCR´s. Por publicação automática entende-se uma publicação de LCR realizada diretamente pelo Software de AC sem a necessidade de intervenção do operador. Por publicação manual entende-se uma publicação de LCR realizada com a intervenção do operador.

2.2.6 Requisitos para a Utilização de OCSP

Os requisitos para a utilização do serviço de OCSP são requisitos condicionais que dependem de uma ICP ter tal serviço disponível para uso pelos titulares dos certificados digitais. Deve-se mencionar que conforme recomendação I.02, o serviço de OCSP é opcional e pode ser oferecido por uma ICP.

Dentro de uma ICP, o serviço de OCSP pode ser configurado como um componente separado do Software de AC ou como um componente integrante do Software de AC.

REQUISITO I.32: Caso uma ICP ofereça o serviço de OCSP, um Software de AC deve ter funcionalidade para publicar no repositório OCSP as informações sobre um certificado digital revogado.
OBSERVAÇÃO: Por repositório OCSP entende-se que representa um termo genérico que designa uma tecnologia específica que serve para concentrar as informações de revogação que podem ser consultadas via protocolo OCSP, podendo ser, por exemplo, ou um banco de dados ou um diretório LDAP internos ou extenos a uma AC.

REQUISITO I.33: Caso um Software de AC tenha um componente de software para prover o serviço de OCSP, o Software de AC deve controlar que todas as respostas OCSP sejam assinadas digitalmente utilizando um certificado digital válido com propósitos de uso também válidos. Além disso, o Software de AC deve assegurar que as respostas OCSP sejam geradas conforme as regras definidas na RFC 2560 [14].

2.2.7 Requisitos de Configuração do Software de AC

A seção de requisitos de configuração trata a administração e configuração do Software de AC.

REQUISITO I.34: Uma interface de administração do Software de AC deve permitir configurar o Software de AC e as operações de configuração devem ser realizadas por um administrador. Portanto, a interface de administração do Software de AC deve, no mínimo, permitir com que as seguintes operações sejam realizadas:

- Configuração do componente que emite certificados;
- configuração da hierarquia de certificação digital da AC;
- configuração de controle de acesso e autenticação;
- configuração de geração e monitoração de registros (logs);
- configuração de repositórios;
- configuração de publicações.

REQUISITO I.35: Um Software de AC deve gerar e manter os seguintes tipos de certificados:

- Certificados digitais com propósitos específicos para AC´s intermediárias; ou
- certificados digitais com propósitos específicos para utilização por titulares dos certificados digitais.

REQUISITO I.36: Um Software de AC deve permitir a criação, configuração e manutenção de modelos padronizados (*templates*) para a geração de certificados digitais em função do tipo de certificado definido pela ICP-Brasil.

REQUISITO I.37: Um certificado digital gerado e utilizado pelo Software de AC deve seguir as normas e os formatos definidos pela ICP-Brasil.

REQUISITO I.38: Baseando-se no tipo de certificado digital ICP-Brasil (A1, A2, A3, A4, S1, S2, S3, S4, T3 ou T4) e na PC definida pela AC, um Software de AC deve permitir sua configuração para atender o subconjunto de extensões X509v3 e os propósitos de uso que devem ser utilizados na emissão de um certificado digital.

REQUISITO I.39: Um Software de AC deve configurar a emissão de certificados digitais ICP-Brasil conforme definido pelo DOC-ICP-04 [5].

REQUISITO I.40: Um Software de AC deve permitir a configuração de políticas parametrizáveis para certificados e para LCR´s de acordo com o DOC-ICP-04 [5].

2.2.8 Requisitos de Interoperabilidade

REQUISITO I.41: Um Software de AC deve aceitar requisições e emitir certificados digitais, no mínimo, conforme um dos seguintes tipos de codificações:

- Binário:
  - BER [9];
  - DER [9].

- texto:
  - PEM [12];
  - Base64 [17].

RECOMENDAÇÃO I.09: Um Software de AC pode emitir certificados digitais ICP-Brasil que estejam contidos em um conteúdo CMS [15] ou PKCS#7 [10].

RECOMENDAÇÃO I.10: Um Software de AC pode permitir a entrega de um certificado digital ICP-Brasil para um titular do certificado digital que esteja contido em um conteúdo CMS [15] ou PKCS#7 [10] incluindo a respectiva cadeia de certificação.

2.2.9 Requisitos de Gerenciamento

Nesta seção serão abordados os requisitos sobre o gerenciamento de uma AC.

REQUISITO I.42: Um Software de AC deve dispor ao operador/administrador uma interface para gerenciar certificados. Esta interface deve atender, no mínimo, as seguintes funcionalidades:

- Requisições de certificados:

  - processar requisições:
    - aceitar;
    - rejeitar;
    - cancelar;

  - listar requisições de certificados.

- listar certificados:

  - emitidos;
  - expirados;
  - revogados.

- renovar e revogar certificados;
- gerenciar a lista de certificados revogados;
- publicação de certificados emitidos e LCR;
- recuperação de dados.

REQUISITO I.43: Uma interface entre o Software de AC e o titular do certificado digital deve permitir, no mínimo, a realização das seguintes funcionalidades:

- Solicitar um certificado digital;
- obter o certificado digital solicitado;
- consultar certificados digitais emitidos;
- requisitar a revogação de um certificado digital;
- obter informações de revogação do certificado digital (LCR ou OCSP);
- obter o caminho de certificação.

2.2.10 Requisitos de Segurança

Esta subseção descreve os requisitos relacionados com a segurança do Software de AC, tais como:

- Papel de acesso;
- auditoria;
- arquivamento da cópia de segurança (backup) de chaves privadas;
- interação com o hardware seguro.
- continuidade do serviço de uma AC e sua recuperação.

2.2.10.1 Requisitos de Papel de Acesso de um Software de AC

REQUISITO I.44: Um Software de AC deve permitir ao operador da AC se autenticar, no mínimo, por meio de *login* e senha.

REQUISITO I.45: Um Software de AC não deve permitir que um mesmo usuário autenticado no papel de acesso operador assuma simultaneamente um outro papel de acesso diferente.

REQUISITO I.46: Um Software de AC deve ter funcionalidade para a criação, alteração, suspensão temporária e exclusão de um perfil de operador da AC. Na criação ou na alteração do perfil de operador, o Software de AC deve vincular os dados do *login* ou do certificado digital que o operador da AC deve utilizar para acessar o software.

REQUISITO I.47: Um Software de AC deve ter funcionalidade para a criação, alteração, suspensão temporária e exclusão de um perfil de operador da AR. O Software de AC também deve ter a funcionalidade de autenticar o operador da AR por meio de certificado digital do tipo A3.

2.2.10.2 Requisitos de Auditoria de Software de AC

REQUISITO I.48: Um Software de AC deve gerar, no mínimo, os seguintes registros de auditoria para:

- Controle de acesso:
  - registros relacionados ao controle de acesso;
- autenticação:
  - registros relacionados às atividades de autenticação;

- autoridade certificadora:
    - registros relacionados às atividades desempenhadas pelo subsistema gerente de certificados;
- banco de dados:
    - registros relacionados às atividades desempenhadas com o banco de dados;
- HTTP:
    - registros relacionados às atividades desempenhadas com o servidor web que interage com os titulares dos certificados digitais;
- repositório de publicação:
    - registros relacionados às atividades dos repositório de publicação (certificados emitidos e LCR´s).

2.2.10.3 Requisitos de Arquivamento de Chaves Privadas no Software de AC

Conforme descrito no item 6.1.1 do DOC-ICP-04 [5] o responsável pela geração dos pares de chaves assimétricas e pelo uso do certificado digital é o titular do certificado quando pessoa física ou o seu representante legal quando o titular do certificado for pessoa jurídica.
Compreende-se que numa ICP é pressuposto que somente o titular do certificado digital tenha posse da sua chave privada. Entretanto no item 6.2.4 do DOC-ICP-04 [5] é permitida que uma AC possa manter uma cópia de segurança (backup) de chave privada correspondente a somente certificados de sigilo por ela emitido por solicitação do titular do certificado digital.

RECOMENDAÇÃO I.11: Um Software de AC pode oferecer um serviço de arquivamento da cópia de segurança (backup) de chaves privadas de certificado digital de sigilo por solicitação do respectivo titular, ou de empresa ou orgão, quando o titular do certificado for seu empregado ou cliente conforme descrito no item 6.2.4 do DOC-ICP-04 [5].

REQUISITO I.49: O serviço de arquivamento da cópia de segurança (backup) de chaves privadas para certificados digitais ICP-Brasil de sigilo, caso presente em um Software de AC. Os mecanismos de segurança utilizados no serviço de arquivamento devem ser robustos de tal forma que assegurem que:

- A guarda da chave privada do titular do certificado seja feita em repositório com acesso controlado na AC (fiel depositário);
- o conhecimento e uso da chave privada estejam obrigatoriamente sob o controle do titular do certificado, de tal forma que o Software de AC não tenha condições de utilizar a chave privada do titular;
- o uso de algoritmos criptográficos, métodos e protocolos seguros;
- segundo o DOC-ICP- 01.01 [4], também deve oferecer como proteção um nível de segurança não inferior àquele definido para a chave original.

2.2.10.4 Requisitos de Interação do Software de AC com Hardware Seguro

REQUISITO I.50: Um Software de AC deve utilizar hardware seguro (MSC ou HSM) para executar os serviços de ICP que necessitem utilizar a chave privada da AC (por exemplo,

assinar certificados digitais, assinar LCR's etc). O hardware seguro (MSC ou HSM) a ser utilizado pelo Software de AC deve estar de acordo com o DOC-ICP-01.01 [4] seção 3.

OBSERVAÇÃO: A ICP-Brasil regulamenta no DOC-ICP-05 [7] item 6.1.8.1 que o processo de geração do par de chaves criptográficas assimétricas da AC deve ser feito por hardware seguro (MSC ou HSM) ou por software. A geração por software é admitida apenas para chaves de AC utilizadas exclusivamente para assinatura de certificados dos tipos A1 ou S1. Entretanto, considera-se o DOC-ICP-01.01 seção 3 que afirma que a geração do par de chaves criptográficas assimétricas da AC deve ser feito sempre por hardware seguro (MSC ou HSM).

2.2.10.5 Requisitos para a Continuidade do Software de AC e sua Recuperação

REQUISITO I.51: Um Software de AC deve permitir a geração de cópia de segurança (backup) das suas chaves e dos seus dados críticos, que possibilite a execução de processo de recuperação colocando o Sistema de AC nas mesmas condições de operação que possuía no momento em que foi gerado a cópia.

REQUISITO I.52: Um Software de AC deve permitir que a cópia de segurança (backup) das suas chaves e dos seus dados críticos seja armazenada de forma segura, portanto, não sendo permitido o seu armazenamento em claro. Por armazenamento seguro, entende-se que a cópia de segurança das chaves e dos dados críticos seja protegida contra a indisponibilidade, e contra a divulgação, o acesso e as modificações não autorizadas.

2.2.11 Requisitos de Documentação para Software de AC

REQUISITO I.53: Um Software de AC deve ter as seguintes documentações em idioma português do Brasil ou inglês:

- Manual de usuário;
- manual de instalação;
- documentos de especificação técnica.

REQUISITO I.54: Um Software de AC deve possuir a configuração da sua interface em idioma português do Brasil ou inglês.

REQUISITO I.55: Um Software de AC deve possuir tópicos de ajuda em idioma português do Brasil ou inglês.

REQUISITO I.56: O manual de usuário ou o manual de instalação ou os documentos de especificação técnica deve informar quais as plataformas de sistema operacional suportadas pelo Software de AC e quais os requisitos de ambiente operacional necessários para sua operação.

REQUISITO I.57: Um Software de AC deve permitir ao operador ou administrador visualizar a versão do software e o nome do responsável pelo Software de AC.

REQUISITO I.58: De acordo com item 6.6 do DOC-ICP-05 [7], um Software de AC deve possuir documentação das práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao Software de AC ou a qualquer outro software desenvolvido ou utilizado pela AC.

2.3 Requisitos aplicáveis somente ao Software de AR

Nesta seção estão definidos os requisitos aplicáveis apenas a um Software de AR.

2.3.1 Requisitos Gerais de um Software de AR

Conforme o glossário ICP-Brasil [8], uma AR é definida como uma entidade responsável pela interface entre o usuário e a AC. Sendo vinculada a uma AC, a AR tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em um mesmo ambiente que uma AC ou em ambientes segregados.
Portanto, um Software de AR deve prover funcionalidades que permitam a uma AR desempenhar seus objetivos conforme definidos no glossário ICP-Brasil [8].

REQUISITO II.01: Um Software de AR deve oferecer, no mínimo, os seguintes componentes e funcionalidades:

- Cadastrar titulares dos certificados digitais;
- receber, validar e encaminhar solicitações de emissão ou renovação de certificados digitais às AC´s;
- realizar requisições de revogação de certificados digitais às AC´s;
- informar aos respectivos titulares a emissão ou revogação de seus certificados;
- gerar os registros de suas operações.

REQUISITO II.02: Caso uma AR desempenhe o papel de uma entidade intermediária na revogação de um certificado digital, então o Software de AC também deve oferecer as seguintes funcionalidades:

- Tornar disponível ao titular ou responsável uma interface de revogação de certificados digitais;
- autenticar a entidade solicitante antes de aceitar a sua requisição de revogação de certificado digital;
- receber, validar e encaminhar requisições de revogação de certificados digitais às AC´s.

2.3.2 Requisitos de Segurança

REQUISITO II.03: Um Software de AR deve possuir, no mínimo, as seguintes características de segurança:

1. Acesso permitido mediante autenticação por meio do certificado do Agente de Registro, no mínimo, do tipo A3;
2. acesso permitido somente a partir de equipamentos previamente autenticados ou cadastrados no Software de AR (ex. usando cadastramento prévio de endereço IP, ou outra solução que permita ao Software de AR autenticar o equipamento);
3. *timeout* de sessão;
4. registro de auditoria dos eventos citados no item 4.5.1 do DOC-ICP-05 [7];
5. histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;
6. se suportado pelo Software da AR, a funcionalidade de indicar se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR, para cada certificado digital emitido;

7. toda comunicação entre a AR e a AC e entre a AR e o titular do certificado digital deve ocorrer por meio de um canal seguro utilizando os padrões e algoritmos criptográficos da ICP-Brasil, conforme DOC-ICP-01.01 [4], que possibilitem o sigilo dos dados trafegados;

REQUISITO II.04: Um software de AR deve controlar a liberação de solicitação de certificados digitais por meio da autorização de dois ou mais agentes de registros conforme descrito no DOC-ICP-05 [7] item 3.1.1.1.

2.3.2.1 Requisitos de Auditoria de Software de AR

REQUISITO II.05: Um Software de AR deve gerar, no mínimo, os seguintes registros para:

- Controle de acesso:
  - registros relacionados ao controle de acesso;
- autenticação:
  - registros relacionados às atividades de autenticação;
- atividades:
  - registros relacionados às atividades desempenhadas pela AR;
- banco de dados:
  - registros relacionados às atividades desempenhadas com o banco de dados;
- HTTP:
  - registros relacionados às atividades desempenhadas com o servidor web que interage com os titulares dos certificados digitais.

2.3.3 Requisitos de Documentação para Software de AR

REQUISITO II.06: Um Software de AR deve ter as seguintes documentações em idioma português do Brasil ou inglês:

- Manual de usuário;
- manual de instalação;
- documentos de especificação técnica.

REQUISITO II.07: Um Software de AR deve possuir a configuração da sua interface em idioma português do Brasil ou inglês.

REQUISITO II.08: Um Software de AR deve possuir tópicos de ajuda em idioma português do Brasil ou inglês.

REQUISITO II.09: O manual de usuário ou o manual de instalação ou os documentos de especificação técnica deve informar quais as plataformas de sistema operacional suportadas

pelo Software de AR e quais os requisitos de ambiente operacional necessários para sua operação.

REQUISITO II.10: Um Software de AR deve permitir ao operador ou administrador visualizar a versão do software e o nome do responsável pelo Software de AR.

REQUISITO II.11: De acordo com item 6.6 do DOC-ICP-05 [8], um Software de AR deve possuir documentação das práticas de engenharia de software adotadas, metodologia de desenvolvimento de software, entre outros, aplicados ao Software de AR ou a qualquer outro software desenvolvido ou utilizado pela AR.

2.4 Requisitos aplicáveis ao Software de AC e AR

Nesta seção estão definidos os requisitos aplicáveis tanto para um Software de AC com para um Software de AR.

2.4.1 Requisitos de Papéis de Acesso

Nesta seção são abordados os requisitos sobre os papéis de acesso no Software de AC e de AR.

REQUISITO III.01: Um Software de AC ou AR deve dispor, no mínimo, dos seguintes papéis de acesso autenticados:

- Operador da AC ou AR: papel que realiza funções gerenciais e operacionais;
- administrador da AC ou AR: papel que configura a AC ou AR;
- auditor da AC ou AR papel que utiliza os eventos e logs registrados para fins de auditoria.

REQUISITO III.02: Um Software de AC ou AR deve tornar disponíveis interfaces de acordo com cada papel de acesso disponível, e possibilitar apenas o acesso aos seus serviços correspondentes. Portanto, com relação às interfaces, um Software de AC ou AR deve ter:

- Interface de titular do certificado digital;
- interface de operador;
- interface de administrador;
- interface de auditor.

2.4.2 Requisitos de Segurança

Esta subseção descreve os requisitos relacionados com a segurança dos Softwares de AC e AR.

REQUISITO III.03: Um Software de AC ou AR não deve permitir que sejam criados operadores com perfis iguais, garantido identidades únicas. Especificamente no Software de AC devem existir políticas de senhas que permitam controlar, no mínimo, a criação de senhas fortes, o bloqueio por número de tentativas erradas de senhas, a troca periódica de senhas, o tamanho mínimo de senhas e regras de formação de senhas.

REQUISITO III.04: Um Software de AC ou AR não deve permitir o acesso as suas funcionalidades quando ocorrer falhas na autenticação.

REQUISITO III.05: Um Software de AC ou AR deve exibir ao operador, após sua autenticação bem sucedida, informações sobre o último acesso realizado. Esse requisito presente no Software de AC ou AR tem como objetivo possibilitar ao operador alertar sobre possíveis acessos não autorizados que possam ter ocorrido com o seu papel.

REQUISITO III.06: Um Software de AC ou AR deve ter a opção para que o operador efetue o *logoff* quando for encerrar as suas atividades.

REQUISITO III.07: Um Software de AC ou AR deve possibilitar ao administrador a configuração de número de tentativas para bloqueio de acesso do operador.

REQUISITO III.08: Um Software de AC ou AR deve permitir que somente o administrador faça a criação, a alteração, a suspensão temporária, a exclusão e o desbloqueio do papel de acesso do operador.

REQUISITO III.09: Um Software de AC ou AR deve possibilitar a configuração de parâmetros de *timeout* para os casos de inatividade da sessão.

REQUISITO III.10: Um Software de AC ou AR não deve permitir que sejam efetuadas quaisquer operações após o tempo de *timeout* decorrido.

REQUISITO III.11: Um Software de AC ou AR deve solicitar que o operador efetue novo *login* após sua sessão ter sido encerrada devido à inatividade.

RECOMENDAÇÃO III.01: Um Software de AC ou AR pode permitir o gerenciamento de perfil por grupos de usuários (operadores e/ou administradores).

2.4.2.1 Requisitos de Auditoria de Software de AC ou AR

REQUISITO III.12: Um Software de AC ou AR deve gerar registros para finalidades de auditoria de acordo com a seção 4.5 do DOC-ICP-05 [7].

REQUISITO III.13: Um Software de AC ou AR deve prever regras para a rotação dos registros (*log*) baseado em tempo ou tamanho dos registros.

RECOMENDAÇÃO III.02: Um Software de AC ou AR pode ter a opção de assinar digitalmente os seus registros gerados.

3. Parte 2

Material e Documentos Técnicos que devem ser depositados para a execução do Processo de Homologação de Software de AC e AR no âmbito da ICP-Brasil

3.1 Introdução

Esta parte detalha os materiais e a documentação técnica que devem ser depositados pela Parte Interessada junto ao LEA para a execução dos processos de homologação de Software de AC e AR no âmbito da ICP-Brasil.

Os materiais e a documentação técnica referidos são classificados em duas categorias:

1. Documentação Técnica: corresponde aos documentos de natureza técnica referentes aos Softwares de AC e AR que devem ser submetidos ao processo de homologação. Devem ser depositados em formato impresso ou em formato eletrônico. No caso de formato eletrônico, devem estar armazenados, preferencialmente, em mídia tipo "leitura-somente" (*read-only*). Devem estar, obrigatoriamente, escritos nas línguas portuguesa ou inglesa;

2. componentes em Softwares Executáveis: corresponde a todo software executável, solicitado por este documento, referente ao funcionamento do objeto de homologação. Devem ser depositados, obrigatoriamente, em formato eletrônico e armazenados, preferencialmente, em mídia tipo "leitura-somente" (*read-only*).

   Três Níveis de Segurança de Homologação (NSH) diferentes foram estabelecidos para Software de AC e AR:

   - NSH 1: Este nível não requer depósito e análise de código-fonte associado ao objeto em homologação;
   - NSH 2: Este nível requer depósito e análise apenas de código-fonte de componentes específicos associados ao objeto em homologação.
   - NSH 3: Este nível requer depósito e análise de código-fonte completo associado ao objeto em homologação.

OBSERVAÇÃO: Para Software de AC e AR, a Parte Interessada deve indicar no formulário de depósito a plataforma de sistema operacional e sua versão a ser utilizada na análise de conformidade.

3.2 Materiais e Documentação Técnica Depositados

3.2.1 Documentação Técnica

- Nível de Segurança de Homologação 1
  Os seguintes documentos técnicos devem ser depositados junto ao LEA pela Parte Interessada:

- Projeto de Software, como por exemplo, casos de uso *(use cases)*, diagramas de sequência, diagramas de estado e outros documentos envolvidos na construção do software;
- manual de Usuário e Instalação que acompanha o objeto em homologação;
- manual de Instalação e Configuração de Softwares adicionais para interação com hardware seguro, tais como, provedores de serviço criptográficos (PSC) ;
- documentação Técnica de Homologações obtidas para o objeto e emitidas por entidades independentes, como por exemplo, *Common Criteria*;
- outros documentos: Projetos técnicos e suas especificações que a Parte Interessada julgar necessários para completar toda documentação técnica exigida;

- Níveis de Segurança de Homologação 2 e 3
  Adicionalmente à documentação técnica solicitada no NSH 1, os seguintes itens devem ser depositados junto ao LEA pela Parte Interessada:

  - Código-fonte do Software de AC e AR.

3.2.2 Componentes em Software Executável

Independentemente do NSH escolhido pela Parte Interessada, os seguintes componentes em softwares executáveis devem ser depositados junto ao LEA:

- Software de AC e AR: objeto a ser homologado;
- softwares de interação com hardware seguro: quando aplicável, a Parte Interessada deve fornecer todo software necessário para interação com hardwares seguros, como por exemplo, PSC para interação com cartões inteligentes ou *tokens* criptográficos.

3.2.3 Quantidade de Materiais e Documentos Técnicos Depositados para o Software de Assinatura Digital

A Tabela 1 apresenta a quantidade de materiais e documentos técnicos depositados pela Parte Interessada referente ao processo de homologação de Software de AC e AR que se resumem em:

- Documentos técnicos:

  - documentos Impressos: devem ser entregues cópias de igual teor (por exemplo, duas cópias impressas do manual do usuário do Software de AC e AR);
  - documentos eletrônicos: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por exemplo, dois CD-ROM com o mesmo conteúdo, apresentando como documentos técnicos o manual de usuário, manual de instalação/configuração e código-fonte do Software de AC e AR);

- componentes em softwares executáveis: devem ser entregues cópias de igual teor e armazenadas obrigatoriamente em mídias diferentes (por exemplo, dois CD-ROM´s com o mesmo conteúdo, apresentando como componentes em softwares executáveis o Software de AC e AR e software de interação com hardware seguro).

Requisito de depósito	Material e Documentos Técnicos depositados pela Parte Interessada – NSH 1	Quantidade
1	Projeto de Software	2 cópias
2	Manual de Usuário/Instalação	2 cópias
3	Manual de Instalação/Configuração de Softwares adicionais para interação com hardware seguro (quando aplicável)	2 cópias
4	Documentos Técnicos de Homologações obtidas	2 cópias
5	Outros documentos	2 cópias
Requisito de depósito	**Material e Documentos Técnicos depositados pela Parte Interessada – NSH 2 e 3**	**Quantidade**
6	Código-fonte do Software de AC e AR	2 cópias
Requisito de depósito	**Componentes em Software executável depositados pela Parte Interessada – NSH 1, 2 e 3**	**Quantidade**
7	Software de AC e AR	2 cópias
8	Softwares de interação com hardware seguro (MSC)	2 cópias

Tabela 1: Quantidade de Material e Documentos Técnicos depositados pela Parte Interessada junto ao LEA referente ao processo de homologação de AC e AR

Referências Normativas

[1] COMITÊ GESTOR DA ICP-BRASIL. Resolução N° 49, de 03 de Junho de 2008: Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil. Brasília. ICP-BRASIL, 2008. 23 p.

[2] COMITÊ GESTOR DA ICP-BRASIL. Resolução N° 41, de 18 de abril de 2006: Requisitos Mínimos para as Políticas de Certificados na Infraestrutura de Chaves Públicas Brasileira (ICP-BRASIL). Brasília. ICP-BRASIL, 2006. 20 p.

[3] COMITÊ GESTOR DA ICP-BRASIL. DOC-ICP-01: Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil. versão 4.0. Brasília. ICP-BRASIL, 2008. 34 p.

[4] COMITÊ GESTOR DA ICP-BRASIL. DOC-ICP-01.01: Padrões e Algoritmos Criptográficos da ICP-Brasil. versão 1.1. Brasília. ICP-BRASIL, 2008. 8 p.

[5] COMITÊ GESTOR DA ICP-BRASIL. DOC-ICP-04: Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil. versão 3.0. Brasília. ICP-BRASIL, 2008. 24 p.

[6] COMITÊ GESTOR DA ICP-BRASIL. DOC-ICP-04.01: Atribuição de OID na ICP-Brasil. versão 2.0. Brasília. ICP-BRASIL, 2009. 4 p.

[7] COMITÊ GESTOR DA ICP-BRASIL. DOC-ICP-05: Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil. versão 3.1. Brasília. ICP-BRASIL, 2009. 51 p.

[8] COMITÊ GESTOR DA ICP-BRASIL GLOSSÁRIO ICP-BR – INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS. Glossário ICP-Brasil. Versão 1.2. Brasília. ICP-BRASIL, 2007. 38 p.

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) – ISO/IEC 8825-1. Switzerland. ISO/IEC 8825-1:2002.

[10] RSA LABORATORIES. PKCS#7. Cryptographic Message Syntax Standard. version 1.5. 1993. 30p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>. Acesso em: 30.set.2009.

[11] RSA LABORATORIES PKCS#10: Certification Request Syntax Standard. Version 1.7. 2000. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf>. Acesso em: 05.out.2009.

[12] THE INTERNET ENGINEERING TASK FORCE. Linn, J. Privacy Enhancement for Internet Electronic Mail. Part I: Message Encryption and Authentication Procedures. RFC 1421. 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 30.set.2009.

[13] THE INTERNET ENGINEERING TASK FORCE. D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, Category: Standards Track. 2008. Disponível em <http://www.ietf.org/rfc/rfc5280.txt>. Acesso em: 10.set.2009.

[14] THE INTERNET ENGINEERING TASK FORCE. Myers, M.; Ankney, R.; Malpani, A.; Galperin, S. e Adams, C. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560, Category: Standards Track. 1999. Disponível em <http://www.ietf.org/rfc/rfc2560.txt>. Acesso em: 10.set.2009.

[15] THE INTERNET ENGINEERING TASK FORCE. Housley, R. Cryptographic Message Syntax (CMS). RFC 3852, Category: Standards Track. 2004. Disponível em <http://www.ietf.org/rfc/rfc3852.txt>. Acesso em: 30.set.2009.

[16] THE INTERNET ENGINEERING TASK FORCE. Housley, R.; Polk, W.; Ford, W. e Solo, D. Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, Category: Standards Track, April 2002. Disponível em <http://www.ietf.org/rfc/rfc3280.txt>. Acesso em: 20.set.2009.

[17] THE INTERNET ENGINEERING TASK FORCE. S. Josefsson. The Base16, Base32, and Base64 Data Encodings. RFC 4648, Category: Standards Track. 2006. Disponível em <http://www.rfc-editor.org/rfc/rfc4648.txt>. Acesso em: 07.out.2009.

[18] AMERICAN NATIONAL STANDARDS INSTITUTE. Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). ANSI. X9.31.1998.

[19] COMITÉ EUROPÉEN DE NORMALISATION WORKSHOP AGREEMENT. CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements