LEA

Manual de Condutas Técnicas 8 - Volume 1

Requisitos técnicos e material de depósito para homologação de Bibliotecas Criptográficas

versão 1.0 release 01

São Paulo, 30 de agosto de 2007

Título	Manual de Condutas Técnicas 8 - Volume 1
Versão	versão 1.0 release 01
Data	30 de agosto de 2007
Autor(es)	Mads Rasmussen, Marcelo Bortolotto, Igor Medeiros, Gerson Faria, Adilson Guelfi
Classificação	LEA:Interno
Proprietário	LEA
Autorização de acesso	LEA
Restrição de cópia	LEA

Sumário

Controle de versão

Versão revisada	Data de emissão	Alterações realizadas

Listas de ilustrações

Lista de figuras

Lista de Tabelas

1 Introdução

Este documento descreve os requisitos a serem observados no processo de homologação de softwares de bibliotecas criptográficas no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, ICP-Brasil [1].

De maneira geral, uma biblioteca criptográfica fornece serviços como suporte a padrões, serviços de protocolos, serviços de certificados digitais, serviços de confiança, serviços criptográficos, serviços de aplicação, etc.

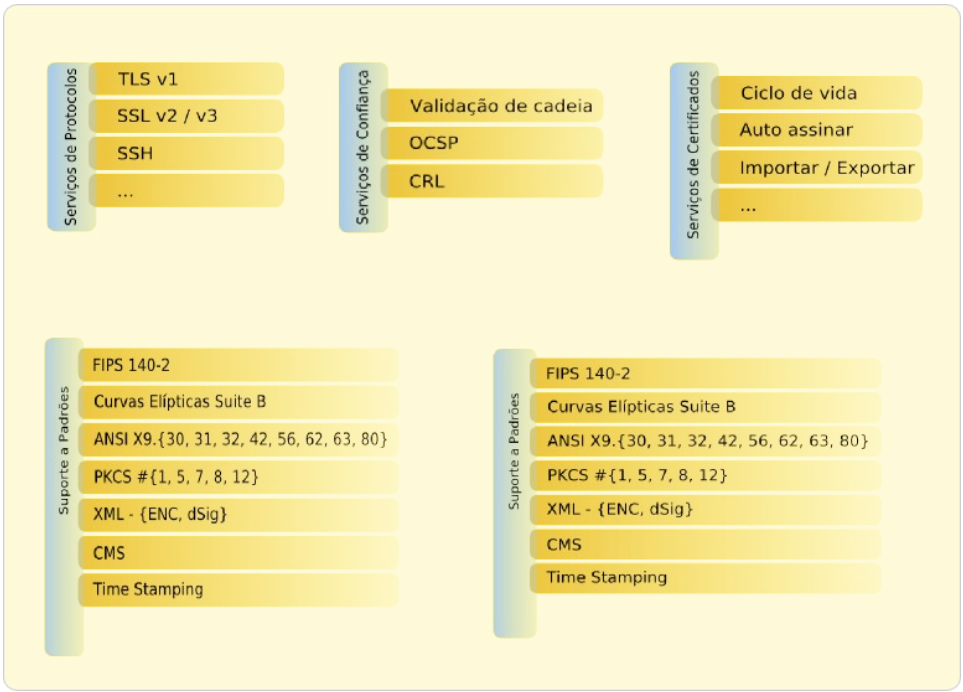

Figura 1. Serviços de uma biblioteca criptográfica

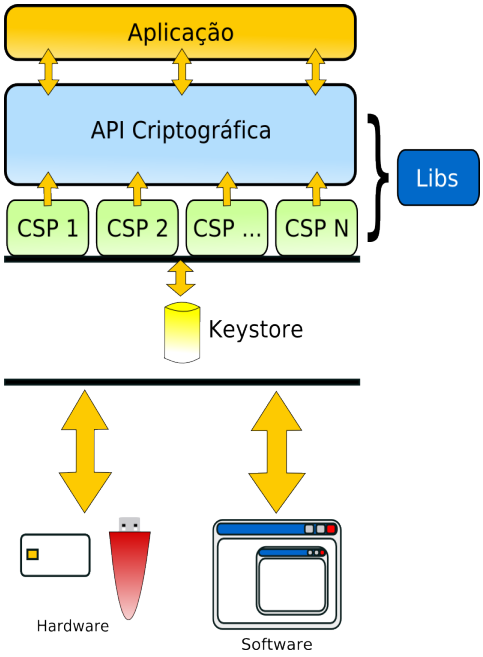

Figura 2. Definição de CSP

Uma biblioteca criptográfica fará uso do CSP (*Cryptographic Service Provider*) para o gerenciamento de chaves e serviços tais como cifrar e decifrar mensagens e formatação de assinatura digital como CMS [2] ou XML [3], de acordo com a figura acima.

A biblioteca criptográfica define uma API como um conjunto de convenções de chamadas aos serviços de tratamento de chaves criptográficas e certificados digitais.

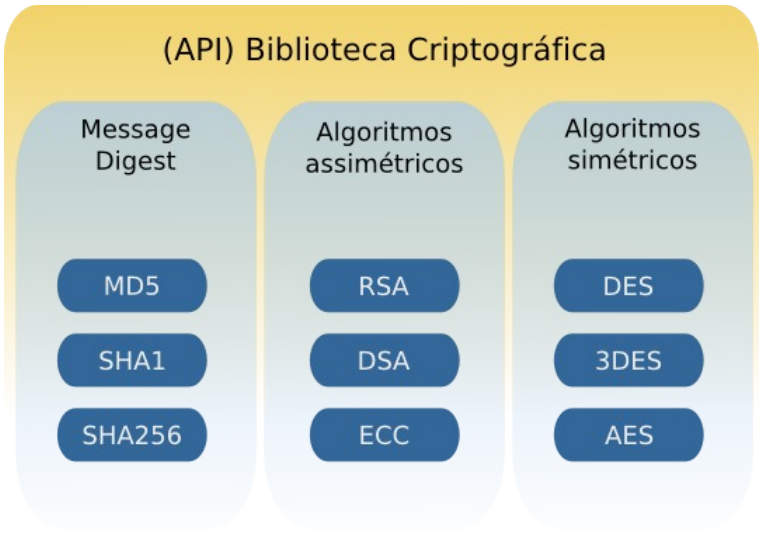

Figura 3. Definição de API

Neste documento, a não ser que seja explicitamente mencionado o contrário, o termo "biblioteca criptográfica" será usado como referência aos softwares de bibliotecas criptográficas no âmbito da ICP-Brasil.

1.1 Objetivo da homologação

O objetivo do processo de homologação de bibliotecas criptográficas é validar a interoperabilidade e operação segura das funções implementadas na biblioteca criptográfica oferecidas por meio da avaliação técnica de aderência aos requisitos técnicos definidos para este processo.

1.2 Descrição do processo de homologação

O processo de homologação é baseado em um conjunto de requisitos técnicos que devem ser atendidos por uma biblioteca criptográfica para garantia da interoperabilidade e operação segura.

Os requisitos técnicos englobam requisitos de segurança, requisitos de interoperabilidade, requisitos de documentação, requisitos específicos como algoritmos criptográficos mínimos, proteção de chaves em memória e requisitos funcionais que devem ser atendidos pela biblioteca criptográfica.

Estes requisitos técnicos são avaliados segundo ensaios de aderência aos requisitos técnicos. 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.

1.3 Escopo do processo de homologação

O escopo da avaliação considera as funções implementadas na biblioteca criptográfica, porém levando em consideração os possíveis riscos causados pela coexistência com outros serviços ou subsistemas.

O escopo dos requisitos técnicos e da avaliação são aplicados aos seguintes componentes:

- Documentação aderente
  - O produto corresponde ao descrito na documentação
- Avaliação dos algoritmos criptográficos
  - Implementação
  - Conformidade com as normas de especificação
  - Auto-testes
- Projeto de software
  - Documentos de design (Ex. UML)
  - Conformidade com os requisitos de segurança

1.4 Verificação de integridade externa

O conjunto de arquivos especificados na biblioteca criptográfica constitui o conjunto completo de código-fonte dessa biblioteca. Não haverão inserções, retiradas ou alterações desse conjunto de arquivos como definido na geração da biblioteca.

O código compilado da biblioteca criptográfica será verificado usando um tipo de algoritmo criptográfico como HMAC [5] utilizando função hash SHA-1 [6] e SHA-256.

Uma chave simétrica arbitrária será definida pelo ITI para ser usada na geração do valor HMAC utilizando função hash SHA-1 e SHA-256 para a checagem da integridade do sistema.

1.5 Estruturação do MCT-8

Este documento (MCT-8) está estruturado da seguinte forma:

- Parte 1: Descreve os requisitos técnicos que devem ser verificados no processo de homologação de bibliotecas criptográficas ICP;
- Parte 2: Descreve os materiais que devem ser depositados para a execução do processo de homologação de bibliotecas criptográficas ICP;
- Referências normativas: Descreve as referências normativas que foram utilizadas na elaboração deste documento.

Os termos e expressões usados neste documento estão referenciados no MCT – Glossário Geral [4].

2 PARTE 1

Requisitos técnicos para homologação de Bibliotecas Criptográficas

2.1 Introdução

A parte 1 deste documento apresenta os requisitos técnicos que devem ser verificados no processo de homologação de bibliotecas criptográficas.

Os requisitos técnicos descritos nesta parte englobam:

- Requisitos de documentação;
- requisitos de segurança;
- requisitos funcionais.

2.2 Requisitos de documentação

A documentação em geral envolve os seguintes itens:

- **Manual de instalação**: Manual especificando como será feita a instalação da biblioteca criptográfica.
- **Manual do usuário**: Manual do usuário, especificando como utilizar a biblioteca criptográfica.
- **Manual do desenvolvedor**: Manual da API para desenvolver aplicações utilizando a biblioteca criptográfica. Especificação do próprio fornecedor.
- **Manual de integração**: Manual especificando a utilização de hardwares específicos como *smart cards*, leitoras de *smart cards* ou *tokens* criptográficos para o acesso das funções da biblioteca criptográfica.
- **Exemplos com trechos de código-fonte:** Documento contendo trechos do código-fonte da biblioteca criptográfica.

A parte 2 deste documento terá um *check list* com uma lista completa de documentação requisitada para o processo de homologação de uma biblioteca criptográfica.

REQUISITO II.1: A documentação deve estar escrita nos idiomas português do Brasil ou inglês.

REQUISITO II.2: A PI deve fornecer manual de instalação e configuração, especificando os processos de instalação e configuração da biblioteca criptográfica. Além disso, o manual de instalação deve especificar os sistemas operacionais suportados pela biblioteca criptográfica.

REQUISITO II.3: A PI deve fornecer o manual do usuário, detalhando as ferramentas e recursos disponíveis aos operadores da biblioteca criptográfica.

REQUISITO II.4: A PI deve fornecer o manual de desenvolvedor detalhando a(s) API(s) para desenvolvimento de aplicações utilizando a biblioteca criptográfica.

REQUISITO II.5: A PI deve fornecer trechos de código-fonte para utilização da biblioteca criptográfica.

2.3 Requisitos de segurança

Esta seção descreve os requisitos mínimos de segurança que devem ser atendidos de forma comum pelas bibliotecas na sua utilização. Os requisitos foram divididos em duas seções:

1. Requisitos de segurança baseados no padrão FIPS [7]: define os requisitos de segurança derivados e complementares ao padrão FIPS;

2. requisitos específicos: define requisitos específicos de segurança para bibliotecas criptográficas.

2.3.1 Requisitos de segurança baseados no padrão FIPS

2.3.1.1 Especificação da biblioteca criptográfica

Uma biblioteca criptográfica pode ser um conjunto de serviços específicos como suporte a padrões, serviços de protocolos, serviços de certificados digitais, serviços de confiança, serviços criptográficos, serviços de aplicação, etc.

REQUISITO III.1.1: A documentação deve especificar cada subsistema empregado pela biblioteca criptográfica.

REQUISITO III.1.2: Caso a biblioteca criptográfica carregue dinamicamente subsistemas na hora de execução da biblioteca, deve existir um mecanismo de integridade da biblioteca, impedindo substituição de subsistemas por sistemas mal intencionados.

REQUISITO III.1.3: A documentação deve especificar o método para garantia de integridade da biblioteca criptográfica.

2.3.1.2 Interfaces da biblioteca criptográfica

REQUISITO III.1.4: A documentação técnica da biblioteca criptográfica deve especificar claramente as seguintes interfaces [8]:

- Entrada de dados: Parâmetros de entrada para todas as funções que aceitam entrada do invocador da API;
- saída de dados: Parâmetros de saída de funções que retorna dados como argumentos ou como valor de retorno da função;
- saída de estado: Informação retornada por meio de exceções (códigos de retorno ou *exit*).

2.3.1.3 Algoritmos criptográficos

REQUISITO III.1.5: A biblioteca criptográfica ICP-Brasil deve suportar no mínimo as seguintes funções criptográficas:

- Criptografia de dados:
  - DES (*Data Encryption Standard*) nos modos de operação ECB e CBC, apenas para uso legado, conforme padrão NIST FIPS PUB 46-3 [9];
  - *Triple*-DES (3DES ou TDES) nos modos de operação ECB e CBC, conforme padrão NIST FIPS PUB 46-3 [9];
  - AES (*Advanced Encryption Standard*) com tamanho de chave 128 bits nos modos de operação ECB e CBC (conforme padrão NIST FIPS PUB 197) [14];
  - RSA com utilização de chaves de comprimento maior do que 1024 bits, conforme padrões ANSI X9.31 [10]e PKCS#1 v. 1.5 [11].
- Autenticação de entidades com criptografia de Chave Pública:
  - RSA com tamanho mínimo de chaves de 1024 bits, conforme padrões NIST FIPS PUB 186 [12], FIPS PUB 196[13]e PKCS#1 v. 1.5 [11];
- Resumo criptográfico de dados (*Hash*) [6] :
  - SHA-1 (*Secure Hash Algorithm)*, apenas para uso legado (conforme padrão NIST FIPS PUB 180-2).

    SHA-256 (*Secure Hash Algorithm*) conforme padrão NIST FIPS PUB 180-2.

RECOMENDAÇÃO III.1.1: A biblioteca criptográfica ICP-Brasil também pode suportar a função AES (*Advanced Encryption Standard*) com utilização de chaves de comprimento de 192 e 256 bits, conforme padrão NIST FIPS PUB 197 [14], para cifração e decifração de dados.

RECOMENDAÇÃO III.1.2: A biblioteca criptográfica ICP-Brasil também pode suportar a função DSA (*Data Signature Algorithm*) com utilização de chaves de comprimento maior do que 512 bits, conforme padrão NIST FIPS PUB 186 [12], para autenticação e assinatura digital de dados.

RECOMENDAÇÃO III.1.3: A biblioteca criptográfica ICP-Brasil também pode suportar as seguintes funções para a geração de resumos criptográficos de dados, conforme padrão NIST FIPS PUB 180-2 [6] :

- SHA-224;
- SHA-256;
- SHA-384;
- SHA-512.

RECOMENDAÇÃO III.1.4: A biblioteca criptográfica ICP-Brasil também pode suportar as seguintes funções para a autenticação e integridade de dados:

- CBC-MAC baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38B [15];
- HMAC baseado nos algoritmos de resumos criptográficos implementados, conforme padrão NIST FIPS PUB 198 [5].
- CMAC baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38B [15];

- MAC-CCM baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38C [16].

RECOMENDAÇÃO III.1.5: Para a biblioteca criptográfica ICP-Brasil que suportar funções para derivação de chaves simétricas baseada em senha, é recomendável a seguinte função de derivação de chaves:

- Função 2 de derivação de chaves baseadas em senha, PBKDF2, como especificada em PKCS#5 [17].

2.3.1.4 Auto-testes

REQUISITO III.1.6: A biblioteca criptográfica deve executar um número de auto-testes para garantir a operação correta da biblioteca.

Podemos citar as seguintes classes de auto-testes para uma biblioteca criptográfica:

- Testes de algoritmos criptográficos
- Testes de pseudo números aleatórios
- Testes da integridade de software
- Testes de carregamento de software
- Testes de funções críticas
- Testes de respostas conhecidas

Algoritmos	Testes de resposta conhecida
AES	Cifração e decifração com chave de 128 bits
DES	Cifração e decifração
3DES (2 chaves)	Cifração e decifração
3DES	Cifração e decifração
RSA	• Teste de consistência de par de chaves de 1024 bits • Cifragem pública e decifragem privada com chave de 1024 bits

	• Teste de assinatura e verificação com chave de 1024 bits
PRNG	Geração de números pseudo aleatórios a partir de uma semente conhecida

REQUISITO III.1.7: Os testes de integridade devem utilizar um tipo de algoritmo criptográfico como HMAC-SHA-1, calculado em cima do código compilado de cada componente da biblioteca criptográfica.

REQUISITO III.1.8: Os auto-testes devem ser chamados na instanciação da biblioteca criptográfica. Adicionalmente devem ser possíveis chamar por meio de função API como por exemplo *Executar_auto_testes()*;

REQUISITO III.1.9: Se a biblioteca criptográfica apresentar falhas durante um auto-teste, a mesma deve ser conduzida a um estado de erro e emitir um indicador de erro via "Interface de Saída de Estado".

REQUISITO III.1.10: Nenhuma funcionalidade criptográfica deve estar disponível até a execução com sucesso dos auto-testes.

REQUISITO III.1.11: Quando um estado de erro ocorrer devido a falhas em um auto-teste, toda saída ou envio de dados via "Interface de Saída de Dados" deve ser impedido.

REQUISITO III.1.12: A documentação da biblioteca criptográfica deve especificar os seguintes itens:

- Os auto-testes realizados pela biblioteca;
- os estados de erro que a biblioteca criptográfica pode entrar quando um auto-teste falha;
- as condições e ações necessárias para sair dos estados de erro e reiniciar a operação normal da biblioteca criptográfica.

2.3.1.5 Garantia do projeto

REQUISITO III.1.13: A parte interessada deve fornecer documentação de utilização de ferramenta de controle de versão do código-fonte da biblioteca criptográfica.

REQUISITO III.1.14: A documentação da biblioteca criptográfica deve incluir diagramas de engenharia de software que representem a arquitetura do elemento de software.

REQUISITO III.1.15: A documentação da biblioteca criptográfica deve incluir diagramas que ilustrem sua relação de uso por outros elementos de software ou hardware.

Nível de Segurança de Homologação 2

REQUISITO III.1.16: No caso da biblioteca criptográfica ser *multi-threaded*, as funções que envolvem operações criptográficas devem ser *thread-safe*, ou seja, não devem colocar em risco nenhum tipo de informação protegida compartilhada contra divulgação, modificação e substituição não autorizada [8].

Nível de Segurança de Homologação 3

RECOMENDAÇÃO III.1.6: Os parâmetros de saída das funções das APIs da biblioteca criptográfica podem apresentar as seguintes características [8]:

- Nenhum destes parâmetros deve ser utilizado como variável temporária durante a sua execução, isto é, não devemos atribuir os valores dos parâmetros de uma função a uma variável temporária durante a execução desta função;

- todos os parâmetros de saída devem somente retornar os tipos que foram pré-determinados na API, isto é, não devemos modificar os parâmetros de saída de uma função na execução da mesma.

2.3.2 Requisitos específicos de segurança

Os requisitos descritos nesta seção correspondem aos requisitos específicos de segurança, que são aplicáveis às bibliotecas criptográficas.

2.3.2.1 *Requisitos de geração de pseudo números aleatórios*

A biblioteca criptográfica deve empregar geradores de números aleatórios (*Pseudo Random Number Generators* – PRNG [18]) determinísticos aprovados ou não determinísticos aprovados pela família de padrões FIPS para a geração de chaves criptográficas.

Os “geradores de números randômicos determinísticos aprovados” estão relacionados aos algoritmos referenciados no FIPS.

- FIPS 186-2 – apêndices 3.1 e 3.2 [12]
- ANSI X9.31 – apêndice A.2.4 com AES ou 3DES de 3 chaves [19]
- ANSI X9.62 – anexo A.4 [20]

Estes métodos são conhecidos como geradores de pseudo aleatoriedades e podem ser referenciados como métodos PRNG.

Os “geradores de números aleatórios não determinísticos” são os métodos de geração de números aleatórios por hardware específico ou coleta de informações de um sistema operacional (como movimento de mouse, teclado, lentidão de rede, tempo de acesso ao disco rígido, etc) que funcionarão como fontes de entropia.

REQUISITO III.2.1: Algoritmos PRNG determinísticos aprovados pela família de padrões FIPS devem ser usados para geração de chaves para funções criptográficas aprovadas.

REQUISITO III.2.2: A documentação deve especificar cada método de PRNG empregado na biblioteca criptográfica ICP-Brasil, seja ele aprovado ou não pelo padrão FIPS.

2.3.2.2 Requisitos de geração de chaves criptográficas

Uma biblioteca criptográfica ICP-Brasil pode gerar chaves criptográficas internamente.

REQUISITO III.2.3: A biblioteca criptográfica deve usar somente os métodos aprovados pela família de padrões FIPS para a geração de chaves criptográficas. Se um dos métodos de geração de chaves criptográficas necessitar como entrada o resultado de um algoritmo PRNG, então o algoritmo PRNG utilizado também deve ser aprovado pelo Comitê Gestor ICP-Brasil.

REQUISITO III.2.4: O esforço de comprometer a segurança de um método de geração de chaves criptográficas, deve ser, no mínimo, igual ao esforço de determinar o valor da chave gerada.

REQUISITO III.2.5: A documentação deve especificar cada um dos métodos de geração de chaves criptográficas empregados pela biblioteca criptográfica aprovados pelo Comitê Gestor ICP-Brasil.

REQUISITO III.2.6: [seção 2 do DOC ICP-01.01 - v1.0] A biblioteca criptográfica ICP-Brasil deve atender aos requisitos específicos de segurança estabelecidos, conforme descritos na seção 3.1.3.

2.4 Requisitos funcionais

Os requisitos funcionais dizem respeito à avaliação de funções relacionadas à biblioteca criptográfica ICP-Brasil que podem ser invocadas por aplicações de usuários por meio de uma interface de alto nível denominada de API (*Application Programming Interface*).

2.4.1 Requisitos gerais

REQUISITO IV.1.1: A biblioteca criptográfica deve ser capaz de reconhecer os OID´s (*Object Identifier*) mais comuns, reconhecidos pela ICP-Brasil, tais como CMS e os algoritmos da seção 3.1.3.

REQUISITO IV.1.2: A biblioteca criptográfica deve ser capaz de reconhecer OID´s (*Object Identifier*) adicionais configurados externamente.

2.4.2 Requisitos de CMS

REQUISITO IV.2.1: [referente à seção 2 do DOC ICP-01.01 - v1.0] Os seguintes requisitos funcionais de assinatura e certificação digital devem estar disponíveis por invocação da biblioteca criptográfica, onde as chaves são carregadas através de acesso a um CSP:

- Gerar requisição de certificado digital (CSR) [22] segundo formato PKCS#10 [21];
- realizar assinatura digital em mensagens, gerando pacote no formato CMS "*signed data*" [2], permitindo inserção de parâmetros autenticados e não autenticados;
- realizar sigilo de mensagens, gerando pacote no formato CMS "*enveloped data*" [2];
- realizar verificação de assinatura digital de mensagem no formato CMS "*signed data*";
- realizar extração de conteúdo de envelope digital no formato CMS "*enveloped data*";

- realizar co-assinatura digital em mensagens, inserindo a co-assinatura em um já existente, retornando um arquivo CMS novo ou como anexo no arquivo antigo;
- realizar contra-assinatura digital de uma assinatura já existente em uma mensagem sob as mesmas condições da co-assinatura;
- realizar assinatura digital simples para garantia de autenticidade de informações.

REQUISITO IV.2.2: Suportar o padrão DER e BER [26] para codificação e decodificação de ASN.1 com as estruturas definidas pelo ITU-T [23][24][25].

RECOMENDAÇÃO IV.2.1: Pode suportar o padrão PEM [27] para codificação de estruturas de chaves e certificados em texto ASCII.

REQUISITO IV.2.3: Suportar o padrão BASE64 [28] para codificação de dados binários em texto ASCII.

RECOMENDAÇÃO IV.2.2: Com relação a estrutura de chaves, é possível [8][27][29][30][31]:

- Suportar rotinas para conversão entre formatos PKCS#1 e PKCS#8;
- suportar rotinas para conversão entre formatos PKCS#1 e PEM e PKCS#8 e PEM;
- suportar rotinas para conversão entre formatos da própria biblioteca criptográfica e padrões como MS *CryptoAPI*, PKCS#11, Sun JCE, *OpenSSL*, entre outros.

2.4.3 Requisitos para S-MIME

REQUISITO IV.3.1: Os seguintes requisitos funcionais de assinatura e certificação digital devem estar disponíveis por invocação da biblioteca criptográfica para o protocolo S-MIMEv3 [32]:

- *CMS Enveloped Data*: conteúdo cifrado e chaves de sessão cifradas a serem usadas pelos destinatários;
- *CMS Signed Data:* assinatura digital do conteúdo. Codificação em base64 de assinatura e conteúdo;
- *CMS Clear-Signed Data:* assinatura digital do conteúdo, mas apenas esta é codificada em base64;
- *CMS Signed and Enveloped Data:* assinatura e cifragem da mensagem.

2.4.4 Requisitos de XML

REQUISITO IV.4.1: Se a biblioteca utilizar XML, então ela suporta os padrões W3C XMLSec (XML *security*) [33][34][35]:

- XMLDSig para assinatura digital;
- XMLEnc para cifragem;
- XKMS para gerenciamento de chaves em documentos que utilizam XMLSec.

3 PARTE 2

Material e documentos técnicos a serem depositados para a execução do processo de homologação de Bibliotecas Criptográficas

3.1 Introdução

O objetivo desta parte é detalhar o material e os documentos técnicos a serem depositados pela parte interessada junto ao LSITEC-LEA [36] para a realização dos processos de homologação de bibliotecas criptográficas no âmbito da ICP-Brasil [37][38].

O material e os documentos técnicos referidos são classificados em duas categorias:

1. Documentos técnicos: correspondem aos documentos de natureza técnica referentes às bibliotecas a serem submetidos ao processo de homologação. Devem ser depositados em formato impresso ou em formato eletrônico. No caso de formatos eletrônicos, devem estar armazenados, preferencialmente, em mídia tipo “leitura-somente” (*read-only*). Devem estar, obrigatoriamente, escritos nas línguas portuguesa ou inglesa;
2. Componentes em softwares: correspondem às bibliotecas de software, ferramentas de gerenciamento de dispositivo e/ou outros softwares executáveis, solicitados por este documento, referentes aos dispositivos a serem submetidos ao processo 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 as Bibliotecas Criptográficas:

- NSH 1: Este nível não requer depósito e análise de código-fonte 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.

Para os NSHs 2 e 3, a parte interessada pode depositar o código-fonte em linguagem C, C++ ou Java. Se o código-fonte estiver escrito em linguagem proprietária, ou mesmo em micro código, o respectivo manual desta linguagem deve estar contido na documentação como também simuladores para compilação e execução deste código-fonte;

3.2 Material e documentos técnicos a serem depositados

Segue abaixo a relação de materiais e documentos técnicos a serem depositados junto ao LSITEC-LEA.

3.2.1 Documentos técnicos

3.2.1.1 Nível de Segurança de Homologação 1

Os seguintes documentos técnicos devem ser depositados junto ao LSITEC-LEA pela parte interessada [3]:

- Projeto de software: Projeto de software da biblioteca criptográfica;
- Política de segurança não proprietária: Se a Biblioteca Criptográfica já tiver sido homologada pelo padrão FIPS;
- Manual de usuário/instalação: Manual de usuário/instalação idêntico ao fornecido ao usuário;
- Manuais das interfaces de programação (API): Manuais e documentos técnicos relacionados às APIs aplicáveis, como por exemplo:
    - Microsoft CSP (*CryptoAPI)*;

- PKCS#11 versão 2.11;
- Interfaces associadas à plataforma JCE/JCA, versões suportadas e procedimento de configuração no JRE (*Java Runtime Environment*);

- Manual da ferramenta de gerenciamento: Manual da ferramenta de gerenciamento da biblioteca criptográfica descrevendo claramente as funcionalidades disponíveis ao usuário;
- Projeto dos softwares de apoio: Documentos técnicos contendo a arquitetura, especificação técnica e o projeto de todo software de apoio, tais como, interfaces de programação (API), SDK (*Software Development Kits*), ferramenta de gerenciamento e bibliotecas de software suportadas;
- Relação de certificados obtidos: Relação de certificação e/ou licenças obtidas para a biblioteca criptográfica emitidas por entidades independentes;
- Outros documentos: Projetos técnicos e suas especificações que a parte interessada julgar necessários para completar toda documentação técnica exigida.

3.2.1.2 Nível de Segurança de Homologação 2

Adicionalmente aos documentos técnicos solicitados na seção 3.2.1.1, os módulos da biblioteca criptográfica em homologação devem ser depositados junto ao LSITEC-LEA pela parte interessada, tais como [3]:

- Código-fonte do componente PRNG *(Pseudo Random Number Generator);*
- Código-fonte do componente de geração de chaves;
- Código-fonte do componente de armazenamento de chaves;
- Código-fonte do componente de importação/exportação de chaves e sementes.

3.2.1.3 Nível de Segurança de Homologação 3

Adicionalmente aos documentos técnicos solicitados nas seções 3.2.1.1 e 3.2.1.2, os seguintes itens devem ser depositados junto ao LSITEC-LEA pela parte interessada [3]:

- Código-fonte da biblioteca criptográfica: Relação de todo código-fonte do software;
- Código-fonte de apoio: Relação de todo código-fonte de apoio relacionado às interfaces de programação (API), SDK (*Software Development Kits*), ferramenta de gerenciamento e bibliotecas de software suportadas pelos serviços criptográficos.

3.2.1.4 Componentes em software executável

Para os NSHs 1, 2 e 3, os seguintes componentes em softwares executáveis devem ser depositados junto ao LSITEC-LEA pela parte interessada:

- A biblioteca criptográfica compilada;
- ferramentas de gerenciamento da biblioteca criptográfica;
- outras bibliotecas de software e/ou programas.

3.2.1.5 Componentes físicos de apoio

Para os NSHs 1, 2 e 3, os seguintes componentes físicos devem ser depositados junto ao LSITEC-LEA pela parte interessada:

- Material de apoio: Caso a Biblioteca criptográfica submetida precise de hardware de apoio como cartão, leitora ou *token*:
  - Cartão criptográfico ICP: Amostras nas quantidades definidas por este documento;
  - Leitora de cartão inteligente: Amostras nas quantidades definidas por este documento;
  - *Token* criptográfico: Amostras nas quantidades definidas por este documento;

3.2.2 Quantidade de material de apoio e documentos técnicos a serem depositados

A Tabela 1 apresenta os materiais e documentos técnicos a serem depositados pela parte interessada junto ao LSITEC-LEA referente ao processo de homologação de bibliotecas criptográficas.

Tabela 1: Quantidade de material e documentos técnicos a serem depositados pela parte interessada junto ao LSITEC-LEA referente ao processo de homologação de bibliotecas criptográficas.

Requisito de depósito	Material e documentos técnicos a serem depositados pela parte interessada – NSH 1	Quantidade
1	Cartão inteligente – material de apoio	2
2	Leitora de cartão inteligente – material de apoio	1
3	*Token* de acesso (2 *tokens*) – material de apoio	2
4	PIN padrão	1
5	Projeto de software	2
6	Política de segurança não proprietária	2
7	Manual de usuário e manual de instalação	2
8	Manuais das interfaces de programação (APIs) e bibliotecas de desenvolvimento	2
9	Manual da ferramenta de gerenciamento	2
10	Projeto de software de apoio	2
11	Relação de certificados obtidos	2
12	Outros documentos	2
Requisito de depósito	**Material e documentos técnicos a serem depositados pela parte interessada – NSH 2**	
13	Código-fonte do componente PRNG *(Pseudo Random Number Generator*)	2
14	Código-fonte do componente de geração de chaves	2
15	Código-fonte do componente de armazenamento de chaves	2
16	Código-fonte do componente de importação/exportação de chaves	2
Requisito de depósito	**Material e documentos técnicos a serem depositados pela parte interessada – NSH 3**	
17	Código-fonte	2
18	Código-fonte de apoio	2
Requisito de depósito	**Componentes em software executável a serem depositados pela parte interessada – NSH 1, 2 e 3**	
19	Biblioteca Criptográfica compilada	2
20	Ferramentas de gerenciamento	
21	Outras bibliotecas de software e/ou programas	2

3.3 Plataformas para homologação

O fabricante pode escolher para qual plataforma deseja ser homologado como requisito do material a ser depositado.

Quando aplicável e possível, na arquitetura da biblioteca criptográfica, os requisitos funcionais podem estar disponíveis por invocação, via API, nas seguintes plataformas dos sistemas operacionais:

- “Linux kernel 2.4 ou versões superiores”;
- “Microsoft Windows 2000 ou versões superiores”

No caso de plataforma descontinuada (tais como Windows 98 SE) ou outra plataforma disponível específica (tais como Solaris, Mainframe, etc), o fabricante deverá fornecer o ambiente e treinamento (no caso em que a equipe de homologação do LSITEC-LEA não possua conhecimento da plataforma em questão) para que a homologação seja efetuada de acordo com a disponibilidade.

4 Referências normativas

[1] COMITÊ GESTOR DA ICP-BRASIL. **DOC ICP-01.01: Padrões e Algoritmos Criptográficos da Infra-Estrutura de Chaves Públicas Brasileira (ICP-BRASIL).** Versão 1.0. Brasília. ICP-BRASIL: 2006.

[2] THE INTERNET ENGINEERING TASK FORCE **CMS Cryptographic Message Syntax Standard. RFC 3852.** Russell Housley. 2004. Disponível em: <http://www.ietf.org/rfc/rfc3852.txt>. Acesso em: 27.abril.2007.

[3] [W3C] **Extensible Markup Language (XML) – Architecture Domain.** Disponível em <http://www.w3.org/XML/> Acesso em: 20.jul.2007.

[4] [ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Manual de Condutas Técnicas – Volume**: **Glossário Geral.** Versão 1.0.

[5] [NIST FIPS 198] **The Keyed-Hash Message Authentication Code (HMAC)**. 2002. Disponível em: <http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>. Acesso em: 20.jul.2007.

[6] [NIST FIPS 180-2] **Secure Hash Standard (SHA).** 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>. Acesso em: 20.jul.2007.

[7] [FIPS] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication.** Washington. US Government

Printing Office: May 25, 2001. Disponível em <http://www.itl.nist.gov/fipspubs/> Acesso em: 20.jul.2007.

[8] MESSIER, Matt e VIEGA, John. **Secure Programming Cookbook for C and C++**. O'Reilly Publisher: July, 2003. ISBN 0-596-00394-3.

[9] [NIST. FIPS 46-3]. **Data Encryption Standard (DES).** 1999. Disponível em: <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>. Acesso em: 20.jul.2007.

[10] [ANSI. X9.31] AMERICAN NATIONAL STANDARDS INSTITUTE. **Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).** 1998.

[11] [RSA LABORATORIES] **PKCS#1: RSA Cryptography Standard.** Version 2.1. 2002. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf>. Acesso em: 30.nov.2006.

[12] [NIST FIPS 186-2] **Digital Signatura Standard (DSS)**. 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf>. Acesso em: 20.jul.2007.

[13] [NIST FIPS 196] **Entity Authentication Using Public Key Criptography**. 1997. Disponível em: <http://csrc.nist.gov/publications/fips/fips196/fips196.pdf>. Acesso em: 20.jul.2007.

[14] [NIST FIPS 197] **Advanced Encryption Standard (AES)**. 2001. Disponível em: <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>. Acesso em: 20.jul.2007.

[15] [NIST Special Publication 800-38B] **Recommendation for Block Cipher Modes of Operation - The CMAC Mode for Authentication.** 2005. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf>. Acesso em: 20.jul.2007.

[16] [NIST / FIPS Special Publication 800-38C] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Counter with Cipher Block Chaining-Message Authentication Code (CCM)**. 2004. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-38C/SP800-38C.pdf>. Acesso em: 23.jul.2007.

[17] [RSA LABORATORIES] **PKCS#5: Password-Based Cryptography Standard.** Version 2.0. 1999. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2-0.pdf>. Acesso em: 30.nov.2006.

[18] [ANSI. X9.81-1] AMERICAN NATIONAL STANDARDS INSTITUTE. **Random Number Generation Part 1: Overview and Basic Principles.**

[19] [ANSI. X9.31] AMERICAN NATIONAL STANDARDS INSTITUTE. **Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).** 1998.

[20] [ANSI. X9.62] AMERICAN NATIONAL STANDARDS INSTITUTE. **Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA).** 2005.

[21] [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: 01.dez.2006.

[22] [RSA LABORATORIES] **PKCS#11: Cryptographic Token Interface Standard**. Version 2.0. 1997. 243p. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/pkcs11v2.pdf>. Acesso em: 04.jul.2007.

[23] [ITU-T X.680] **Information Technology: Abtract Syntax Notation One (ASN.1): Specification of Basic Notation.** 2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf>. Acesso em: 23.jul.2007.

[24] [ITU-T X.681] **Information Technology: Abtract Syntax Notation One (ASN.1): Information object specification.** 2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.681-0207.pdf>. Acesso em: 23.jul.2007.

[25] [ITU-T X.682] **Information Technology: Abtract Syntax Notation One (ASN.1): Constraint specification.** 2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.682-0207.pdf>. Acesso em: 23.jul.2007.

[26] [ITU-T X.690] **Information technology: ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).** 2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>. Acesso em: 23.jul.2007.

[27] THE INTERNET ENGINEERING TASK FORCE. Linn, J. **Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.** RFC 1421. February, 1993. Disponível em: <http://www.ietf.org/rfc/rfc1421.txt>. Acesso em: 30.jan.2006.

[28] THE INTERNET ENGINEERING TASK FORCE. Freed, N. e Borenstein, N. **Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies.** RFC 2045. Category: Standards Track. November, 1996. Disponível em: <http://www.ietf.org/rfc/rfc2045.txt>. Acesso em: 30.jan.2006.

[29] [RSA LABORATORIES] **PKCS#8: Private-Key Information Syntax Standard.** Version 1.2. 1993. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/ps/pkcs-8.ps>. Acesso em: 27.abril.2007.

[30] [OpenSSL FIPS 1402] **Security Policy Object Module: By the Open Source Software Institute.** Version 1.0a. March 24, 2006. Disponível em: <http://csrc.nist.gov/cryptval/140-1/140sp/140sp642.pdf>. Acesso em 20.jul.2007.

[31] [SUN JCE] **Java Cryptography Extension (JCE) for the Java 2 SDK.** versão 1.4. Disponível em: <http://java.sun.com/products/jce/index-14.html>. Acesso em 20.jul.2007.

[32] [S/MIME] Network Working Group, S. Dusse, P. Hoffman, B. Ramsdell e L. Lundblade, N. **S/MIME.** Version 2. Message Specification, RFC 2311. Category: Informational. March 1998. Disponível em: <http://www.ietf.org/rfc/rfc2311.txt>. Acesso em: 18.jul.2007.

[33] [W3C] **XMLSec: XML Signature Syntax and Processing.** W3C Recommendation. 12, February 2002. Disponível em: <http://www.w3.org/TR/xmldsig-core/>. Acesso em 20.jul.2007.

[34] [W3C] **XMLEnc: XML Encryption Syntax and Processing.** W3C Recommendation. 10, December 2002. Disponível em: **<**http://www.w3.org/TR/xmlenc-core/>. Acesso em 20.jul.2007.

[35] [W3C] **XKMS**: **XML Key Management Specification (XKMS)**. W3C Note 30. March 2001. Disponível em: **<**http://www.w3.org/TR/xkms/>. Acesso em 20.jul.2007.

[36] [LEA] LABORATÓRIO DE ENSAIOS E AUDITORIA. N**orma de Elaboração de Documentos**. versão 2.0. São Paulo. LEA: 2006.

[37] [ICP-BRASIL] COMITÊ GESTOR DA ICP-BRASIL. **Doc ICP-01.01. Padrões e Algoritmos Criptográficos da Infra-Estrutura de Chaves Públicas Brasileira (ICP-Brasil).** Versão 1.0. Brasília. ICP – Brasil: 2006.

[38] [ABNT] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 10520: Informação e Documentação: Citações em Documentos: Apresentação**. Rio de Janeiro. ABNT: 2002.