Estrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 8 - Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Bibliotecas Criptográficas no Âmbito da ICP-Brasil

versão 1.0

São Paulo, 22 de novembro de 2007

Sumário

Controle de versão

Versão revisada	Data de emissão	Alterações realizadas

1 Introdução

O objetivo deste documento é especificar os procedimentos de homologação que serão aplicados para verificar os requisitos de segurança, interoperabilidade, gerenciamento e funcionalidade para bibliotecas criptográficas no âmbito da Infra-Estrutura de Chaves Públicas Brasileira, ICP-Brasil [1] [40][41][42].

Os procedimentos de homologação fazem referência ao conjunto de métodos que serão usados para avaliar se uma biblioteca criptográfica está ou não em conformidade com os requisitos técnicos definidos pelo “Manual de Condutas Técnicas 8 - Volume I” [2].

Ao final de cada requisito avaliado, devem ser descritos os resultados dos ensaios realizados e emitido um relatório, cuja conclusão deve indicar a aderência ao respectivo requisito.

1.1 Organização deste documento

Cada seção deste documento contém um conjunto de requisitos que representam citações diretas do próprio texto do “Manual de Condutas Técnicas 8 - Volume I”. Os requisitos estão organizados da seguinte forma:

- “REQUISITO <número_do_requisito>.<número_de_seqüência_do_requisito>”
  - “número_do_requisito”: corresponde ao número de área definido no Manual de Condutas Técnicas 8 – Volume I;
  - “número_de_seqüência_do_requisito”: corresponde a um identificador seqüencial dos requisitos.

Os procedimentos de homologação visam a orientar sobre como proceder nos ensaios para bibliotecas criptográficas. Os procedimentos de ensaio estão classificados e agrupados por Níveis de Segurança de Homologação da seguinte forma:

- NSH 1: Este nível não requer depósito e análise de código-fonte associado à biblioteca em homologação;

- NSH 2: Este nível requer depósito e análise apenas de código-fonte de componentes específicos associados à biblioteca em homologação. Por exemplo, código-fonte do algoritmo gerador de números aleatórios;
- NSH 3: Este nível requer depósito e análise de código-fonte completo associado à biblioteca em homologação. Por exemplo, código-fonte de todo software da biblioteca criptográfica.

Os procedimentos de ensaio (EN) que devem ser desempenhados pelo analista LEA estão organizados da seguinte forma:

- EN.<número_do_requisito>.<número_de_seqüência_do_requisito>.<número_de_seqüência_do_ensaio>
  - “número_do_requisito”;
  - “número_de_seqüência_do_requisito”;
  - “número_de_seqüência_do_ensaio”: corresponde a um identificador seqüencial dos procedimentos que devem ser desempenhados.

Os termos usados neste documento estão referenciados no MCT – Glossário Geral [3].

2 PARTE 1

Procedimentos de ensaio a serem observados no processo de homologação de Bibliotecas Criptográficas

2.1 Introdução

Esta parte apresenta os procedimentos de ensaio que devem ser verificados no processo de homologação de bibliotecas criptográficas.

Os procedimentos de ensaio descritos nesta parte englobam:

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

2.2 Requisitos de documentação

REQUISITO II.01: A documentação deve estar escrita nos idiomas português do Brasil ou inglês.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.01.01: Verificar se a documentação está escrita nos idiomas português do Brasil ou inglês.

REQUISITO II.02: 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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.02.01: Analisar a documentação e verificar se o manual de instalação especifica corretamente o processo de instalação da biblioteca criptográfica que está sendo homologada.

EN.II.02.02: Analisar a documentação e verificar se o manual de instalação especifica quais procedimentos de inicialização devem ser adotados previamente a sua ativação.

EN.II.02.03: Analisar a documentação e verificar se o manual de instalação especifica quais componentes de software serão necessários para a ativação e configuração da biblioteca criptográfica, tais como, JVM e sistema operacional compatíveis.

EN.II.02.04: Analisar a documentação e verificar se o manual de instalação e configuração especifica os procedimentos que devem ser adotados para habilitação da biblioteca criptográfica na arquitetura criptográfica.

REQUISITO II.03: A PI deve fornecer o manual do usuário, detalhando as ferramentas e recursos disponíveis aos operadores da biblioteca criptográfica.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.03.01: Analisar a documentação e verificar se o manual do usuário detalha corretamente as ferramentas e recursos disponíveis da biblioteca criptográfica que está sendo homologada.

EN.II.03.02: Analisar a documentação e verificar se o manual do usuário especifica quais interfaces de administração e/ou configuração estão disponíveis, como por exemplo, arquivos-texto de configuração.

EN.II.03.03: Analisar a documentação e verificar se o manual do usuário especifica a versão e configuração da biblioteca criptográfica.

REQUISITO II.04: A PI deve fornecer o manual de desenvolvedor detalhando a(s) API(s) para desenvolvimento de aplicações utilizando a biblioteca criptográfica.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.04.01: Analisar a documentação e verificar se o manual do desenvolvedor especifica corretamente as funções da API da biblioteca criptográfica que está sendo homologada.

EN.II.04.02:: Analisar a documentação e verificar se o manual do desenvolvedor especifica a arquitetura do sistema.

EN.II.04.03:: Analisar a documentação e verificar se o manual do desenvolvedor especifica as SPIs implementadas da arquitetura criptográfica.

EN.II.04.04: Analisar a documentação e verificar se o manual do desenvolvedor especifica os tratamentos de erro das chamadas das funções da API.

REQUISITO II.05: A PI deve fornecer documenta contendo trechos de código-fonte que mostrem como utilizar as principais funções da biblioteca criptográfica ou aplicações de exemplo.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.II.05.01: Analisar a documentação e verificar se são fornecidos trechos de código-fonte da biblioteca criptográfica que está sendo homologada.

2.3 Requisitos de segurança

2.3.1 Requisitos de segurança baseados no padrão FIPS

2.3.1.1 Especificação da biblioteca criptográfica

REQUISITO III.01: A documentação deve especificar cada subsistema empregado pela biblioteca criptográfica [4].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.01.01: Verificar se a documentação descreve cada subsistema empregado pela biblioteca criptográfica.

REQUISITO III.02: 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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.02.01: Verificar se a biblioteca criptográfica carrega dinamicamente os subsistemas na hora de execução da biblioteca.

EN.III.02.02: Verificar se a biblioteca criptográfica possui um mecanismo de integridade da biblioteca, impedindo substituição de subsistemas por sistemas mal intencionados.

REQUISITO III.03: A documentação deve especificar o método para garantia de integridade da biblioteca criptográfica.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.03.01: Verificar se a documentação especifica o método para garantia de integridade da biblioteca criptográfica.

2.3.1.2 Interfaces da biblioteca criptográfica

REQUISITO III.04: A documentação técnica da biblioteca criptográfica deve especificar claramente as seguintes interfaces [5]:

- 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*).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.04.01: Verificar se a documentação descreve as interfaces presentes na biblioteca criptográfica. Para cada interface, é preciso verificar sua classificação quanto a:

- Interface de entrada de dados;
- interface de saída de dados;
- interface de saída de estado.

EN.III.04.02: Analisar a biblioteca criptográfica e suas interfaces de entrada de dados, verificando que os seguintes tipos de dados podem ser inseridos e processados:

- Dados em texto claro que deve ser cifrado ou assinado pela biblioteca criptográfica;
- texto cifrado ou assinado que deve ser decifrado ou verificado pela biblioteca criptográfica;
- chaves criptográficas em texto claro ou cifradas e outros dados de gerenciamento de chaves que são inseridos e utilizados pela biblioteca criptográfica, tais como, vetores e dados de iniciação, informação sobre particionamento de chaves, etc;

- dados de autenticação em texto claro ou cifrado que devem ser inseridos na biblioteca criptográfica, tais como, senhas, PINs, e/ou informações biométricas;
- informações de estado de fontes externas (por exemplo, dispositivo criptográfico);
- quaisquer outras informações que são inseridas na biblioteca criptográfica para processamento ou armazenamento.

EN.III.04.03: Analisar a biblioteca criptográfica e suas interfaces de saída de dados, verificando que os seguintes tipos de dados podem ser emitidos:

- Dados em texto claro que foram decifrados pela biblioteca criptográfica;
- texto cifrado que foi criptografado pela biblioteca criptográfica;
- assinaturas digitais que foram geradas pela biblioteca criptográfica;
- chaves criptográficas em texto claro ou cifradas e outros dados de gerenciamento de chaves que foram gerados pela biblioteca criptográfica, tais como, vetores e dados de iniciação, informação sobre particionamento de chaves, etc;
- informações de controle emitidas pela biblioteca criptográfica para entidades externas (por exemplo, dispositivo criptográfico);
- quaisquer outras informações que são emitidas pela biblioteca criptográfica após processamento ou armazenamento, exceto informações de estado.

EN.III.04.04: Analisar a biblioteca criptográfica e suas interfaces de saída de estado, verificando que todas as informações de estado utilizadas para mostrar o estado da biblioteca criptográfica podem ser emitidas, tais como:

- Informação retornada por meio de exceções (códigos de retorno ou *exit*);
- quaisquer outras informações de saída de estado.

2.3.1.3 Algoritmos criptográficos

REQUISITO III.05: A biblioteca criptográfica ICP-Brasil deve suportar 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 [8];
    - *Triple*-DES (3DES ou TDES) nos modos de operação ECB e CBC, conforme padrão NIST FIPS PUB 46-3 [8];
    - AES (*Advanced Encryption Standard*) com tamanho de chave 128 bits nos modos de operação ECB e CBC, conforme padrão NIST FIPS PUB 197 [17];
    - 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*) [15]:
    - 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.

Procedimentos de ensaio para NSH 1, 2 e 3 [6]:

EN.III.05.01: Verificar se a documentação descreve os algoritmos criptográficos suportados pela biblioteca criptográfica descritos no **REQUISITO III.05**.

EN.III.05.02: Executar testes de criptografia de dados verificando o suporte pela biblioteca criptográfica dos algoritmos DES e 3DES. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [7]. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes do DES e 3DES por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos. Para o modo de operação CBC, verificar a exatidão das operações de cifragem/decifração destes algoritmos.

EN.III.05.03: Executar testes de criptografia de dados verificando o suporte pela biblioteca criptográfica do algoritmo AES. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [16]. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes do AES por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos.

EN.III.05.04: Executar testes de criptografia de chave pública verificando o suporte pela biblioteca criptográfica do algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção

de referências normativas [9]. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de chave pública consistem em:

- Teste de geração de chaves, que avalia a habilidade de uma IUT de gerar os valores corretos dos componentes do algoritmo;
- teste de geração de assinaturas, que avalia a habilidade de uma IUT em gerar a assinatura correta que pode ser validada pela chave pública associada;
- teste de verificação de assinaturas, que avalia a habilidade da IUT em reconhecer assinaturas válidas e inválidas.

EN.III.05.05: Executar testes de resumo criptográfico de dados verificando o suporte pela biblioteca criptográfica dos algoritmos SHA-1 e SHA-256. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [14]. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de resumo criptográfico de dados consistem em:

- Testes de mensagens curtas (*Short Message Test*), que avaliam a exatidão na geração do resumo criptográfico de dados com relação ao tamanho da mensagem de entrada;
- testes de mensagens longas selecionadas (*Selected Long Message Test*), que avaliam a exatidão na geração do resumo criptográfico para mensagens que contêm múltiplos blocos;
- testes de mensagens geradas pseudo aleatoriamente (*Pseudorandomly generated messages test*), que verificam a exatidão dos resumos criptográficos de dados para mensagens geradas pseudo aleatoriamente.

EN.III.05.06: Executar testes de performance para a criptografia de dados verificando os resultados obtidos pela biblioteca criptográfica dos algoritmos do **REQUISITO III.05**. Os testes de performance para criptografia de dados consistem

em obter a velocidade em que os algoritmos são executados e verificar se esses valores são compatíveis para os algoritmos em questão.

No quadro abaixo temos alguns exemplos de valores obtidos a partir de códigos em C++, compilado com Microsoft Visual C++ 2005 SP1 e rodando em um Intel Core 2 1.83 GHz processor com Windows XP SP 2 em modo 32-bit.

Algoritmo	**MiB/Seg**	**Ciclos / Byte**
HMAC(SHA-1)	152	11.5
CBC-MAC/AES	86	20.2
DMAC/AES	82	21.3
SHA-1	155	11.3
SHA-256	81	21.5
AES/ECB (chave de 128-bit)	99	17.7
DES	34	51.1

Operação	**Miliseg/Operação**	**Megaciclos/Operação**
RSA 1024 Cifração	0.07	0.13
RSA 1024 Decifração	1.52	2.78
RSA 2048 Cifração	0.15	0.28
RSA 2048 Decifração	5.95	10.89
RSA 1024 Assinatura	1.42	2.60
RSA 1024 Verificação	0.07	0.13
RSA 2048 Assinatura	5.95	10.89
RSA 2048 Verificação	0.15	0.28

RECOMENDAÇÃO III.01: A biblioteca criptográfica ICP-Brasil também pode suportar a função AES (*Advanced Encryption Standard*) [17] com utilização de chaves de comprimento de 192 e 256 bits, conforme padrão NIST FIPS PUB 197, para cifração e decifração de dados.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.01.01: Verificar se a documentação descreve os algoritmos criptográficos suportados pela biblioteca criptográfica descritos na **RECOMENDAÇÃO III.01**.

EN.REC.III.01.02: Executar testes de criptografia de dados verificando o suporte pela biblioteca criptográfica do algoritmo AES. Este ensaio deve estar baseado nos

testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [16]. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes do AES por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos.

EN.REC.III.01.03: Executar testes de performance para a criptografia de dados verificando os resultados obtidos pela biblioteca criptográfica dos algoritmos AES (para 192 e 256 bits). Os testes de performance para criptografia de dados consistem em obter a velocidade em que os algoritmos são executados e verificar se esses valores são compatíveis para os algoritmos em questão.

No quadro abaixo temos alguns exemplos de valores obtidos a partir de códigos em C++, compilado com Microsoft Visual C++ 2005 SP1 e rodando em um Intel Core 2 1.83 GHz processor com Windows XP SP 2 em modo 32-bit.

Algoritmo	**MiB/Seg**	**Ciclos / Byte**
AES/ECB (chave de 192-bit)	86	20.2
AES/ECB (chave de 256-bit)	77	22.6

RECOMENDAÇÃO III.02: A biblioteca criptográfica ICP-Brasil também pode suportar a função DSA (*Data Signature Algorithm*) [10] 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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.02.01: Verificar se a documentação descreve os sistemas criptográficos suportados pela biblioteca criptográfica descritos na **RECOMENDAÇÃO III.02**.

EN.REC.III.02.02: Executar testes de c autenticação e assinatura digital de dados verificando o suporte pela biblioteca criptográfica do algoritmo DSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [12]. O documento de testes de validação está organizado para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de criptografia de chave pública consistem em:

- Teste de geração de chaves, que avalia a habilidade de uma IUT de gerar os valores corretos dos componentes do algoritmo;
- teste de geração de assinaturas, que avalia a habilidade de uma IUT em gerar a assinatura correta que pode ser validada pela chave pública associada;
- teste de verificação de assinaturas, que avalia a habilidade da IUT em reconhecer assinaturas válidas e inválidas.

EN.REC.III.02.03: Executar testes de performance para a criptografia de dados verificando os resultados obtidos pela biblioteca criptográfica dos algoritmos DSA. Os testes de performance para criptografia de dados consistem em obter a velocidade em que os algoritmos são executados e verificar se esses valores são compatíveis para os algoritmos em questão.
No quadro abaixo temos alguns exemplos de valores obtidos a partir de códigos em C++, compilado com Microsoft Visual C++ 2005 SP1 e rodando em um Intel Core 2 1.83 GHz processor com Windows XP SP 2 em modo 32-bit.

Operação	Miliseg/Operação	Megaciclos/Operação
DSA 1024 Assinatura	0.47	0.85
DSA 1024 Verificação	0.52	0.95

RECOMENDAÇÃO III.03: 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 [15]:

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

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.03.01: Verificar se a documentação descreve algoritmos opcionais para geração de resumos criptográficos de dados.

EN.REC.III.03.02: Repetir o ensaio **EN.III.05.05** para os algoritmos SHA-224, SHA-256, SHA-384 e SHA-512 [14].

EN.REC.III.03.03: Executar testes de performance para a criptografia de dados verificando os resultados obtidos pela biblioteca criptográfica dos algoritmos SHA-224, SHA-256, SHA-384 e SHA-512. Os testes de performance para criptografia de dados consistem em obter a velocidade em que os algoritmos são executados e verificar se esses valores são compatíveis para os algoritmos em questão.
No quadro abaixo temos alguns exemplos de valores obtidos a partir de códigos em C++, compilado com Microsoft Visual C++ 2005 SP1 e rodando em um Intel Core 2 1.83 GHz processor com Windows XP SP 2 em modo 32-bit.

Algoritmo	MiB/Seg	Ciclos / Byte
SHA-256	81	21.5
SHA-512	99	17.6

RECOMENDAÇÃO III.04: 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 [19];
- HMAC baseado nos algoritmos de resumos criptográficos implementados, conforme padrão NIST FIPS PUB 198 [18].
- CMAC baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38B [19];
- MAC-CCM baseado nos algoritmos 3DES ou AES, conforme padrão NIST PUB 800-38C [20].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.04.01: Verificar se a documentação descreve os algoritmos criptográficos suportados pela biblioteca criptográfica.

EN.REC.III.04.02: Executar testes de autenticação de dados verificando o suporte pela biblioteca criptográfica dos algoritmos CBC-MAC, HMAC, CMAC e MAC. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [6]. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de autenticação de dados consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes de CBC-MAC, HMAC, CMAC e MAC por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;

- testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos.

EN.REC.III.04.03: Executar testes de performance para a criptografia de dados verificando os resultados obtidos pela biblioteca criptográfica dos algoritmos CBC-MAC, HMAC, CMAC e MAC. Os testes de performance para criptografia de dados consistem em obter a velocidade em que os algoritmos são executados e verificar se esses valores são compatíveis para os algoritmos em questão.
No quadro abaixo temos alguns exemplos de valores obtidos a partir de códigos em C++, compilado com Microsoft Visual C++ 2005 SP1 e rodando em um Intel Core 2 1.83 GHz processor com Windows XP SP 2 em modo 32-bit.

Algoritmo	MiB/Seg	Ciclos / Byte
HMAC(SHA-1)	152	11.5
CBC-MAC/AES	86	20.2
CMAC/AES	82	21.3

RECOMENDAÇÃO III.05: 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 baseada em senha, PBKDF2, como especificada em PKCS#5 [21].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.III.05.01: Verificar se a documentação descreve os algoritmos criptográficos suportados pela biblioteca criptográfica.

EN.REC.III.05.02: Executar testes de derivação de chaves simétricas baseada em senha verificando o suporte pela biblioteca criptográfica do algoritmo PBKDF2. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências normativas [6]. Os documentos de testes de validação estão organizados para realizar testes automáticos em componentes denominados "*Implementation Under Test* (IUT)". Os testes de derivação de chaves simétricas baseadas em senha consistem em:

- Testes de respostas conhecidas (*Known Answer Tests*), que avaliam os componentes do PBKDF2 por meio dos parâmetros de entrada e de saída conhecidos. Estes testes também verificam a confiabilidade com relação aos erros de implementação nos componentes dos algoritmos;
- testes de modo de operação (*Modes of Operation Tests*), que avaliam a possibilidade de haver erros feitos deliberadamente ou de forma maliciosa nas implementações dos algoritmos;
- testes de mensagens de múltiplos blocos (*Multi-block message tests*), que avaliam os algoritmos no que se refere às mensagens com múltiplos blocos.

2.3.1.4 Auto-testes

REQUISITO III.06: A biblioteca criptográfica deve executar um número de auto-testes para garantir a operação correta da biblioteca [5].

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.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.06.01: Executar os auto-testes criptográficos de algoritmos criptográficos, de pseudo números aleatórios, de integridade de software, de carregamento de software, de funções críticas e de respostas conhecidas.

EN.III.06.02: Provocar erro nas funcionalidades da biblioteca criptográfica através dos auto-testes e verificar se a biblioteca criptográfica trata o erro devidamente.

EN.III.06.03: Para cada estado de erro dos auto-testes que não pôde ser alcançado, avaliar o código-fonte da biblioteca criptográfica e a documentação do projeto para determinar se há algum tipo de controle que impeça qualquer operação criptográfica de ser realizada enquanto o estado de erro persistir.

EN.III.06.04: Verificar se a documentação da biblioteca criptográfica especifica a utilização de ofuscação de código binário.

EN.III.06.05: Verificar, por meio de auto-testes, se o código binário da biblioteca criptográfica está utilizando ofuscação e estimar a qualidade disso.

EN.III.06.06: Verificar, por meio de auto-testes, a possibilidade de achar chaves em memória durante operações criptográficas.

REQUISITO III.07: 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.

Procedimentos de ensaio para NSH 2:

EN.III.07.01: Verificar se a biblioteca criptográfica executa auto-testes criptográficos utilizando um tipo de algoritmo criptográfico como HMAC-SHA-1 calculado em cima do código compilado de cada componente da biblioteca criptográfica.

EN.III.07.02: Executar os auto-testes e verificar se a integridade de cada componente de biblioteca criptográfica é mantida.

REQUISITO III.08: Os auto-testes devem ser chamados na instanciação da biblioteca criptográfica. Adicionalmente, devem ser possíveis chamar por meio de função da API como por exemplo *Executar_auto_testes()*;

Procedimentos de ensaio para NSH 3:

EN.III.08.01: Verificar se os auto-testes são chamados na instanciação da biblioteca criptográfica.

EN.III.08.02: Verificar se os auto-testes são chamados através de uma função da API da biblioteca criptográfica.

REQUISITO III.09: 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”.

Procedimentos de ensaio para NSH 1:

EN.III.09.01: Verificar a documentação que descreve os estados de erro dos auto-testes suportados pela biblioteca criptográfica, bem como o indicador de erro associado a cada estado de erro.

EN.III.09.02: Provocar os estados de erro dos auto-testes por meio de software específico, e analisar os indicadores de erro emitidos via “Interface de Saída de Estado”. Após a obtenção dos indicadores de erro dos auto-testes, verificar se os estados e indicadores de erro estão consistentes com a documentação.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.09.03: Para cada estado de erro dos auto-testes que não pôde ser alcançado, avaliar o código-fonte da biblioteca criptográfica e a documentação do projeto para determinar o respectivo indicador de erro que seria emitido via “Interface de Saída de Estado”.

REQUISITO III.10: Nenhuma funcionalidade criptográfica deve estar disponível até a execução com sucesso dos auto-testes.

Procedimentos de ensaio para NSH 1:

EN.III.10.01: Analisar a documentação, sendo que as seguintes funções criptográficas devem estar incluídas na lista de funções inibidas quando a biblioteca criptográfica estiver num estado de erro:

- Cifragem;
- decifração;
- geração segura de resumos criptográficos (*secure message hashing*);
- verificação e criação de assinaturas digitais;
- outras operações que necessitam do uso de criptografia.

EN.III.10.02: Provocar os estados de erro dos auto-testes suportados pela biblioteca criptográfica e, para cada estado de erro alcançado em um auto-teste, efetuar tentativas de realização de operações criptográficas específicas. Para cada tentativa realizada, verificar se as operações criptográficas não devem ser concluídas de forma bem sucedida.

EN.III.10.03: Verificar se quando a biblioteca criptográfica é conduzida para um estado de erro, não há qualquer saída de dados pela “Interface de Saída de Dados”.

Procedimentos de ensaio para NSH 2 e 3:

EN.III.10.04: Para cada estado de erro dos auto-testes que não pôde ser alcançado, avaliar o código-fonte da biblioteca criptográfica e a documentação do projeto para

determinar se há algum tipo de controle que impeça qualquer operação criptográfica de ser realizada enquanto o estado de erro persistir.

REQUISITO III.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.

Procedimentos de ensaio para NSH 1:

EN.III.11.01: Analisar a documentação, verificar se a biblioteca criptográfica impede a saída ou envio de dados via "Interface de Saída de Dados", enquanto houver um estado de erro devido a falhas num auto-teste.

EN.III.11.02: Provocar uma falha em cada auto-teste suportado pela biblioteca criptográfica e para cada estado de erro alcançado em um auto-teste efetuar testes em um sistema específico na "Interface de Saída de Dados". Durante a observação dos testes verificar se há qualquer evidência de tráfego pela "Interface de Saída de Dados".

Procedimentos de ensaio para NSH 2 e 3:

EN.III.11.03: Para cada estado de erro dos auto-testes que não pôde ser alcançado, avaliar o código-fonte da biblioteca criptográfica e a documentação do projeto, com o intuito de determinar se há algum tipo de controle que impeça que qualquer sinal trafegue pela "Interface de Saída de Dados".

REQUISITO III.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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.12.01: Verificar se a documentação atende ao **REQUISITO III.12**.

2.3.1.5 Garantia do projeto

REQUISITO III.13: A parte interessada deve fornecer documentação de utilização de ferramenta de controle de versão do código-fonte da biblioteca criptográfica.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.13.01: Verificar se a documentação inclui a utilização de alguma ferramenta de controle de versão do código-fonte da biblioteca criptográfica.

REQUISITO III.14: A documentação da biblioteca criptográfica deve incluir diagramas de engenharia de software que representem a arquitetura do elemento de software.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.14.01: Verificar se a documentação inclui diagramas de engenharia de software que representem a arquitetura do elemento de software.

REQUISITO III.15: A documentação da biblioteca criptográfica deve incluir diagramas que ilustrem sua relação de uso por outros elementos de software ou hardware.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.15.01: Verificar se a documentação inclui diagramas que ilustrem sua relação de uso por outros elementos de software ou hardware.

REQUISITO III.16: Em caso da biblioteca criptográfica ser *multi-threaded*, as funções que envolvem operações criptográficas devem ser *thread-safe*, ou seja, que não coloque em risco nenhum tipo de informação protegida compartilhada contra divulgação, modificação e substituição não autorizada [5].

Procedimentos de ensaio para NSH 2:

EN.III.16.01: Verificar se a documentação da biblioteca criptográfica descreve como sendo *multi-threaded.*

EN.III.16.02: Verificar se a biblioteca criptográfica apresenta operações criptográficas que sejam *thread-safe.*

EN.III.16.03: Analisar as operações criptográficas que sejam *thread-safe* do ensaio EN.III.16.02, por meio de aplicação específica e verificar se tais resultados das análises estão de acordo com os padrões especificados no **REQUISITO III.16.**

RECOMENDAÇÃO III.06: Os parâmetros de saída das funções das APIs da biblioteca criptográfica podem apresentar as seguintes características [5]:

- 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.

Procedimentos de ensaio para NSH 3:

EN.REC.III.06.01: Verificar nos parâmetros das funções da biblioteca criptográfica se os mesmos estão sendo utilizados como variável temporária.

EN.REC.III.06.02: Verificar nos parâmetros das funções da biblioteca criptográfica se os parâmetros de saída estão retornando os tipos que foram pré-determinados na API.

EN.REC.III.06.03: Analisar nos parâmetros das funções da biblioteca criptográfica dos ensaios EN.REC.III.06.01 e EN.REC.III.06.02, por meio de aplicação específica e verificar se tais resultados das análises estão de acordo com os padrões especificados na **RECOMENDAÇÃO III.06.**

2.3.2 Requisitos específicos de segurança

2.3.2.1 Geradores de pseudo números aleatórios

REQUISITO III.17: Algoritmos PRNG [22] determinísticos aprovados pela família de padrões FIPS devem ser usados para geração de chaves para funções criptográficas aprovadas.

Procedimentos de ensaio para NSH 1:

EN.III.17.01: Analisar a documentação referente a este requisito, verificando quais são os algoritmos PRNG determinísticos usados pela biblioteca criptográfica, e ainda, se tais algoritmos são aprovados ou não pela família de padrões FIPS. Algoritmos aprovados são listados no FIPS.

EN.III.17.02: Por meio de uma ferramenta específica que poderia utilizar uma interface disponível pela PI (por exemplo, API), realizar testes que permitam verificar

o comportamento estatístico dos algoritmos PRNG determinísticos suportados pela biblioteca criptográfica. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se o comportamento estatístico dos algoritmos PRNG determinísticos poderá ser executado nos NSHs 2 ou 3.

EN.III.17.03: Por meio de uma ferramenta específica que poderia utilizar uma interface disponível pela PI (por exemplo, API), realizar testes que permitam verificar o comportamento do algoritmo PRNG determinístico implementado pela biblioteca criptográfica, conforme listados no FIPS. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se o comportamento estatístico dos algoritmos PRNG determinísticos poderá ser executado nos NSHs 2 ou 3.

Procedimentos de ensaio para NSH 2:

EN.III.17.04: Verificar, por análise direta do código-fonte dos algoritmos PRNG determinísticos aprovados pela família de padrões FIPS, se tais algoritmos implementados estão em conformidade com a documentação.

Procedimentos de ensaio para NSH 3:

EN.III.17.05: Verificar, por análise direta do código-fonte da biblioteca criptográfica, se o algoritmo implementado PRNG determinístico aprovado pela família de padrões FIPS é utilizado para geração de chaves ou para geração de vetores de iniciação definidos em algoritmos criptográficos.

REQUISITO III.18: A documentação deve especificar cada método de PRNG empregado na biblioteca criptográfica ICP-Brasil, seja ele aprovado ou não pelo padrão FIPS.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.18.01: Verificar se a documentação atende ao **REQUISITO III.03.**

2.3.2.2 Geração de chaves criptográficas

REQUISITO III.19: 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.

Procedimentos de ensaio para NSH 1:

EN.III.19.01: Analisar a documentação referente a este requisito, verificando quais são os métodos de geração de chaves criptográficas usados pela biblioteca criptográfica, e ainda, se tais métodos são ou não aprovados pela família de padrões FIPS.

EN.III.19.02: Por meio de uma ferramenta específica que poderia utilizar uma interface disponível pela PI (por exemplo, API), realizar testes que permitam verificar se os métodos de geração de chaves criptográficas suportados pela biblioteca criptográfica são algoritmos aprovados pela família de padrões FIPS. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se a verificação dos métodos de geração de chaves criptográficas pode ser executada nos NSHs 2 ou 3.

Procedimentos de ensaio para NSH 2:

EN.III.19.03: Verificar, por análise direta do código-fonte dos métodos de geração de chaves, se tais métodos implementados estão em conformidade com a documentação.

Procedimentos de ensaio para NSH 3:

EN.III.19.04: Verificar, por análise direta do código-fonte do módulo criptográfico, se somente métodos aprovados pela família de padrões FIPS são usados para geração de chaves criptográficas. Além disso, verificar também se os métodos de geração de chaves criptográficas aprovados pela família de padrões FIPS, quando necessitarem como entrada o resultado de um algoritmo PRNG, utilizam somente algoritmos PRNG aprovados pela família de padrões FIPS .

REQUISITO III.20: 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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.20.01: Verificar se a documentação descreve o esforço necessário para comprometer a segurança de um método de geração de chaves criptográficas.

EN.III.20.02: Determinar o nível de clareza, raciocínio e exatidão de qualquer argumento ou parâmetro fornecido, verificando a existência de incertezas, pontos obscuros ou ambigüidades que possam comprometer o entendimento da documentação.

REQUISITO III.21: A documentação deve especificar cada um dos métodos de geração de chaves criptográficas empregados pela biblioteca criptográfica (aprovados pelo Comitê Gestor ICP-Brasil).

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.21.01: Verificar se a documentação atende ao **REQUISITO III.21.**

REQUISITO III.22: [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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.III.22.01: Verificar se a documentação atende ao **REQUISITO III.22.**

2.4 Requisitos funcionais

2.4.1 Requisitos gerais

REQUISITO IV.01: A biblioteca criptográfica deve ser capaz de reconhecer os OID´s (*Object Identifier*) mais utilizados, reconhecidos pela ICP-Brasil, tais como de CMS [24] e dos algoritmos da seção 2.3.1.3.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.01.01: Verificar se a documentação da biblioteca criptográfica descreve a geração dos OID´s (*Object Identifier*) mais comuns, reconhecidos pela ICP-Brasil, tais como de CMS [24] e dos algoritmos da seção 2.3.1.3.

EN.IV.01.02: Verificar se a biblioteca criptográfica reconhece os OID´s (*Object Identifier*) mais comuns, reconhecidos pela ICP-Brasil, tais como de CMS [24] e dos algoritmos da seção 2.3.1.3**.**

REQUISITO IV.02: A biblioteca criptográfica deve ser capaz de reconhecer OID´s (*Object Identifier*) adicionais configurados externamente.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.02.01: Verificar se a documentação da biblioteca criptográfica descreve a geração dos OID´s (*Object Identifier*) adicionais configurados externamente.

EN.IV.02.02: Verificar se a biblioteca criptográfica reconhece os OID´s (*Object Identifier*) adicionais configurados externamente**.**

2.4.2 CMS

REQUISITO IV.03: [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) segundo formato PKCS#10 [25];
- realizar assinatura digital em mensagens, gerando pacote no formato CMS "*signed data*", permitindo inserção de parâmetros autenticados e não autenticados;
- realizar sigilo de mensagens, gerando pacote no formato CMS "*enveloped data*" [24];
- realizar verificação de assinatura digital de mensagem no formato CMS "*signed data*" [24];
- 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 [26];
- realizar contra-assinatura digital de uma assinatura já existente em uma mensagem sob as mesmas condições da co-assinatura [26];
- realizar assinatura digital simples para garantia de autenticidade de informações [26].

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.03.01: Avaliar se a documentação descreve os requisitos de assinatura e certificação digital.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta de software ou utilitário desenvolvido pelo LEA, com base nas APIs e nas plataformas de sistemas operacionais.

EN.IV.03.02: Gerar requisição de certificado digital (CSR) segundo formato PKCS#10. Após tal procedimento, verificar se a requisição gerada está no formato PKCS#10.

EN.IV.03.03: Realizar assinatura digital em mensagens, gerando pacote no formato CMS "*signed data*". Após a assinatura digital de uma mensagem, verificar se o pacote resultante está no formato "CMS *signed data*" e se tal pacote permite que parâmetros autenticados e não autenticados sejam inseridos.

EN.IV.03.04: Realizar sigilo de mensagens, gerando pacote no formato CMS "*enveloped data*". Após o sigilo de uma mensagem, verificar se o pacote resultante está no formato CMS "*enveloped data*".

EN.IV.03.05: Realizar verificação de assinatura digital de mensagens no formato CMS "*signed data*".

EN.IV.03.06: Realizar extração de conteúdo de envelope digital no formato CMS "*enveloped data*".

EN.IV.03.07: Gerar um pacote CMS co-assinado, extrair a mensagem original deste pacote e assinar a mensagem extraída gerando um novo pacote no formato CMS ou um anexo no arquivo antigo. Após tal procedimento, verificar se o arquivo resultante está no formato CMS e com a nova assinatura inserida no pacote.

EN.IV.03.08: Realizar co-assinatura digital de mensagem, retornando um arquivo CMS co-assinado. Após tal procedimento, verificar se o arquivo está no formato CMS com a última assinatura inserida no pacote.

EN.IV.03.09: Escolher a assinatura que será contra-assinada. Realizar a contra-assinatura digital de mensagem, retornando um arquivo CMS. Após tal procedimento, verificar se o arquivo está no formato CMS com a última assinatura inserida no pacote.

EN.IV.03.10: Realizar verificação de assinatura digital simples para autenticidade de informações.

REQUISITO IV.4: Suportar o padrão DER e BER [30] para codificação e decodificação de ASN.1 com as estruturas definidas pelo ITU-T [27][28][29].

EN.IV.04.01: Realizar verificação de codificação e decodificação de ASN.1 para os padrões BER e DER.

RECOMENDAÇÃO IV.1: Pode suportar o padrão PEM [31] para codificação de estruturas de chaves e certificados em texto ASCII.

EN.REC.IV.01.01: Realizar verificação de codificação de estruturas de chaves e certificados em texto ASCII para o padrão PEM.

REQUISITO IV.5: Suportar o padrão BASE64 [32] para codificação de dados binários em texto ASCII.

EN.IV.05.01: Realizar verificação de codificação de dados binários em texto ASCII para o padrão BASE64.

RECOMENDAÇÃO IV.2: Com relação a sintaxe ASN.1 para estrutura de chaves, é possível:

- Suportar rotinas para conversão entre formatos PKCS#1 [11] e PKCS#8 [33];
- suportar rotinas para conversão entre formato PKCS#1 [11] e PEM [31] e PKCS#8 [33]e PEM;
- suportar rotinas para conversão entre formatos da própria biblioteca criptográfica e padrões como MS CryptoAPI, PKCS#11 [26], Sun JCE [35], OpenSSL [34], entre outros.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.REC.IV.02.01: Verificar se a documentação da biblioteca criptográfica descreve as estruturas de chaves descritas na **RECOMENDAÇÃO IV.2.**

EN.REC.IV.02.02: Gerar requisição de par de chaves segundo formato PKCS#1 e fazer a conversão para o formato PKCS#8. Após tal procedimento, verificar se a conversão gerada está no formato PKCS#8.

EN.REC.IV.02.03: Gerar requisição de formato PKCS#8 e fazer a conversão para o formato PKCS#1. Após tal procedimento, verificar se a conversão gerada está no formato PKCS#1.

EN.REC.IV.02.04: Gerar requisição de par de chaves segundo formato PKCS#1 e fazer a conversão para o formato PEM. Após tal procedimento, verificar se a conversão gerada está no formato PEM.

EN.REC.IV.02.05: Gerar requisição no formato PKCS#8 e fazer a conversão para o formato PEM. Após tal procedimento, verificar se a conversão gerada está no formato PEM.

EN.REC.IV.02.06: Gerar requisição de dados binários em texto ASCII e fazer a codificação para o padrão BASE64. Após tal procedimento, verificar se a codificação gerada está no padrão BASE64.

EN.REC.IV.02.07: Executar as rotinas de conversão para o(s) padrão(s) presente(s), tais como MS CryptoAPI, PKCS#11 [26], Sun JCE [35], OpenSSL [34] e verificar se a conversão é feita corretamente.

2.4.3 S/MIME

REQUISITO IV.6: Os seguintes requisitos funcionais de assinatura e certificação digital devem estar disponíveis por invocação da biblioteca criptográfica para o protocolo S/MIMEv3 [36]:

- *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.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.06.01: Analisar se a documentação descreve os requisitos de assinatura e certificação digital para o protocolo S-MIMEv3.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta de software ou utilitário desenvolvido pelo LEA, com base nas APIs e nas plataformas de sistemas operacionais.

EN.IV.06.02: Realizar assinatura digital do conteúdo com codificação BASE64 de assinatura e conteúdo, gerando pacote no formato CMS "*signed data*". Após a assinatura digital, verificar se o pacote resultante está no formato CMS "*signed data*".

EN.IV.06.03: Realizar cifragem de conteúdo e de chaves de sessão, gerando pacote no formato CMS "*enveloped data*". Após a operação, verificar se o pacote resultante está no formato CMS "*enveloped data*".

EN.IV.06.04: Realizar assinatura digital do conteúdo com codificação BASE64 de assinatura, gerando pacote no formato CMS "*clear-signed data*". Após a assinatura digital, verificar se o pacote resultante está no formato CMS "*clear-signed data*".

EN.IV.06.05: Realizar assinatura digital e cifragem de mensagem gerando pacote no formato CMS "*signed and enveloped data*". Após a assinatura digital e a cifragem, verificar se o pacote resultante está no formato CMS "*signed and enveloped data*".

2.4.4 XML

REQUISITO IV.7: Se a biblioteca utilizar XML, então ela suporta os padrões W3C XMLSec (XML *security*) [37]:

- XMLDSig para assinatura digital [37];
- XMLEnc para cifragem [38] ;
- XKMS [39] para gerenciamento de chaves em documentos que utilizam XMLSec.

Procedimentos de ensaio para NSH 1, 2 e 3:

EN.IV.07.01: Analisar a documentação e verificar se a biblioteca criptográfica utiliza XML.

EN.IV.07.02: Analisar a documentação e verificar se a biblioteca criptográfica suporta os padrões W3C XMLSec (XML *security*).

EN.IV.07.03: Realizar assinatura digital e verificar se é gerado conteúdo no padrão XMLDsig.

EN.IV.07.04: Realizar cifragem e verificar se é gerado conteúdo no padrão XMLEnc.

EN.IV.07.05: Verificar se o padrão XKMS está sendo utilizado para gerenciamento de chaves em documentos XMLSec.

3 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] [ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Manual de Condutas Técnicas 8 – Volume I**: **Detalhamento dos requisitos técnicos para bibliotecas criptográficas no âmbito da ICP-Brasil.** Versão 1.0.

[3] [ITI] GLOSSÁRIO ICP-BR – INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRAS. **Glossário ICP-Brasil.** Versão 1.2. Brasília. ICP – BR: 2007.

[4] [FIPS / NIST] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, [ITL] INFORMATION TECHNOLOGY LABORATORY. **Federal Information Processing Standards Publication.** Washington. US Government Printing Office: May 25, 2001. Disponível em: <http://www.itl.nist.gov/fipspubs/>

[5] MESSIER, Matt e VIEGA, John. **Secure Programming Cookbook For C And C++**. O'reilly Publisher: July 2003. ISBN 0-596-00394-3.

[6] [NIST SP 800-17] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.
Modes of Operation Validation System (MOVS): Requirements and Procedures. 1998. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-17/800-17.pdf> Acesso em: 25 jul. 2005.

[7] [NIST SP 800-20] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures.** 2000.

Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-20/800-20.pdf> Acesso em: 25 jul. 2005.

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

[9] [NIST] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The RSA Validation System (RSAVS).** 2004. Disponível em: <http://csrc.nist.gov/cryptval/dss/RSAVS.pdf>. Acesso em: 25 jul. 2005.

[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] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **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] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The Secure Hash Algorithm Validation System (SHAVS).** 2004. Disponível em: <http://csrc.nist.gov/cryptval/shs/SHAVS.pdf>. Acesso em: 25 jul. 2005.

[15] [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.

[16] [NIST] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **The Advanced Encryption Standard Algorithm Validation Suite (AESAVS).** 2002. 52 p. Disponível em: <http://csrc.nist.gov/cryptval/aes/AESAVS.pdf>. Acesso em: 25 jul. 2005.

[17] [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.

[18] [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.

[19] [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.

[20] [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

[21] [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.

[22] [ANSI. X9.81-1]. **Random Number Generation Part 1: Overview and Basic Principles.**

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

[24] [RSA LABORATORIES]. **CMS: Cryptographic Message Syntax Standard.** Version 1.5. 1993. Disponível em: <ftp://ftp.rsasecurity.com/pub/pkcs/ps/pkcs-7.ps>. Acesso em: 27.abril.2007.

[25] [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.

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

[27] [ITU-T X.680] **Information Technology: Abtract Syntax Notation One (ASN.1): Specification of Basic Notation.** 07.2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf>. Acesso em: 23.jul.2007

[28] [ITU-T X.681] **Information Technology: Abtract Syntax Notation One (ASN.1): Information object specification.** 07.2002. Disponível em <http://www.itu.int/ITU-T/studygroups/com17/languages/X.681-0207.pdf>. Acesso em: 23.jul.2007

[29] [ITU-T X.682] **Information Technology: Abtract Syntax Notation One (ASN.1): Constraint specification.** 07.2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.682-0207.pdf>. Acesso em: 23.jul.2007

[30] [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). 07.2002. Disponível em: <http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>. Acesso em: 23.jul.2007

[31] 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.

[32] 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.

[33] [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.

[34] [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.

[35] **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.

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

[37] [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.

[38] [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.

[39] [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.

[40] [IN 01/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 01/2007: Procedimentos administrativos a serem observados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito da ICP-Brasil.** DOC-ICP-10.01 versão 2.1. Brasília. ICP-Brasil: 2007

[41] [IN 02/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 02/2007: Estrutura normativa técnica e níveis de segurança de homologação a serem utilizados nos processos de homologação de sistemas e equipamentos de certificação digital no âmbito ICP-Brasil.** DOC-ICP-10.02 versão 2.0. Brasília. ICP-Brasil: 2007

[42] [IN 06/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 06/2007: Padrões e procedimentos técnicos a serem observados nos processos de homologação de bibliotecas criptográficas e softwares provedores de serviços criptográficos no âmbito da ICP-Brasil.** DOC-ICP-10.06 versão 1.0. Brasília. ICP-Brasil: 2007