Infraestrutura de Chaves Públicas Brasileira

Manual de Condutas Técnicas 3 - Volume II

Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de *Tokens* Criptográficos no Âmbito da ICP-Brasil

Versão 3.1

Brasília, 26 de setembro de 2017

SUMÁRIO

Controle de Versão

Versão atual	Data de emissão	Alterações realizadas
2.0.r.6	07/06/06	Revisões de ambiente operacional (seção 2.1.6) Revisões de classe de operação para cartão e leitora (seção 3.5 REQUISITO III.20). Revisão das funcionalidades do papel de acesso "usuário" (seção 2.2.12 REQUISITO II.21). Inclusão do termo "Módulo criptográfico multiaplicação" no glossário.
3.0.r.09	22/11/07	Revisão geral para os requisitos de cartões criptográficos ICP e leitoras de cartões inteligentes. Exclusão dos requisitos de *tokens* criptográficos. Revisão estrutural do Manual de Condutas Técnicas incluindo no desenvolvimento do mesmo documento os requisitos técnicos para cartões criptográficos ICP, leitoras de cartões inteligentes e materiais a serem depositados para a execução do processo de homologação.
3.1 IN 08/2017	26/09/2017	Previsão de autonomia para o OCP definir os ensaios nas Avaliações de Manutenção de Credenciamento; e Ajuste na obrigatoriedade dos comandos APDU.

Listas de Ilustrações

Lista de Figuras

Lista de Tabelas

1 Introdução

Este documento descreve os procedimentos de ensaio a serem aplicados no processo de homologação de *tokens* criptográficos no âmbito da Infraestrutura de Chaves Públicas Brasileira, a ICP-Brasil.

Os procedimentos de ensaio referem-se ao conjunto de métodos que serão usados para avaliar se *tokens* criptográficos estão ou não em conformidade com os requisitos técnicos definidos pelo Manual de Condutas Técnicas 3 - Volume I.

Em um Credenciamento Inicial e na Avaliação de Recertificação devem ser aplicados todos os ensaios definidos neste MCT. Em cada Avaliação de Manutenção, cabe ao OCP definir quais requisitos devem ser ensaiados. Uma Avaliação de Manutenção deve observar a proporção mínima de 20% (vinte por cento) do total dos requisitos previstos no Anexo I deste MCT para cada avaliação de manutenção no modelo 4 e de 33% (trinta e três por cento) do total dos requisitos previstos no Anexo I deste MCT para cada avaliação de manutenção no modelo 5. A avaliação de um requisito em uma Avaliação de Manutenção não impede sua reavaliação em Avaliações de Manutenção seguintes, mas ao longo das Avaliações da Manutenção o OCP deve garantir que todos os requisitos do Anexo I sejam avaliados.

Para uma melhor compreensão do disposto neste documento, entenda-se por *token* criptográfico um hardware instalado no computador que utiliza uma conexão física do tipo USB, com capacidade de geração e armazenamento de chaves criptográficas assimétricas e processamento criptográfico assimétrico e armazenamento de certificados digitais voltados para utilização em uma Infraestrutura de Chaves Públicas (ICP).

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 3 – Volume I. Os requisitos estão organizados da seguinte forma:

- *REQUISITO <número_do_requisito>.<número_de_sequência_do_requisito>*
    - “número_do_requisito”: corresponde ao número de área definido no Manual de Condutas Técnicas 3 – Volume I;

- "número_de_seqüência_do_requisito": corresponde a um identificador seqüencial dos requisitos.

Os procedimentos de ensaio visam orientar sobre como proceder nos testes elaborados sobre dispositivos. 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 ao dispositivo em homologação;
- NSH 2: Este nível requer depósito e análise de apenas código fonte de componentes específicos associados ao dispositivo em homologação. Por exemplo, código fonte do algoritmo gerador de números pseudo-aleatórios;
- NSH 3: Este nível requer depósito e análise de código fonte completo associado ao dispositivo em homologação. Por exemplo, código fonte de todo software e/ou firmware do módulo criptográfico.

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.

Este documento (MCT 3 – Volume II) está estruturado da seguinte forma:

- Parte 1: Descreve os procedimentos de ensaio que devem ser verificados no processo de homologação de *tokens* criptográficos ICP.

2 Parte 1

Procedimentos de ensaio para homologação de *tokens* criptográficos no âmbito da ICP-Brasil

2.1 Introdução

A parte 1 deste documento apresenta os procedimentos de ensaios que devem ser verificados no processo de homologação de *tokens* criptográficos.

Os procedimentos de ensaios descritos nesta parte englobam:

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

2.2 Requisitos de Segurança

Esta seção descreve os requisitos mínimos de segurança que devem ser atendidos pelos *tokens* criptográficos.

Os requisitos de segurança foram elaborados com base em:

- Requisitos de segurança FIPS 140-2 nível 2 [FIPS PUB 140-2];
- requisitos de algoritmos obrigatórios;
- requisitos de PIN e PUK;
- requisitos de identificação de hardware, software e *firmware*.

O padrão FIPS 140-2 abrange onze áreas de atuação relacionadas ao projeto e implementação de um módulo criptográfico. As áreas de atuação definidas pelo padrão FIPS 140-2 são apresentadas na Tabela 1[FIPS PUB 140-2].

Tabela 1. Áreas de atuação do padrão FIPS 140-2

Seção	Áreas de atuação do padrão FIPS 140-2
1	Especificação do módulo criptográfico
2	Portas e interfaces do módulo criptográfico
3	Papéis, serviços e autenticação
4	Modelo de estado finito
5	Segurança física
6	Ambiente operacional

Seção	Áreas de atuação do padrão FIPS 140-2
7	Gerenciamento de chaves criptográficas
8	Interferência e compatibilidade eletromagnética
9	Auto-testes
10	*Design assurance*
11	*Mitigação de outros ataques*

Das áreas de atuação definidas pelo padrão FIPS 140-2 e apresentadas na Tabela 1 apenas as 7 áreas seguintes foram consideradas na elaboração deste documento:

- Especificação do módulo criptográfico;
- papéis, serviços e autenticação;
- modelo de estado finito;
- segurança física;
- ambiente operacional;
- gerenciamento de chaves criptográficas;
- auto-testes.

Os demais requisitos de segurança (Algoritmos criptográficos obrigatórios, PIN e PUK, identificação de hardware, software e *firmware*) foram elaborados de forma a contextualizar *tokens* criptográficos e sua aplicação na ICP-Brasil.

A menos que seja explicitamente mencionado, o termo "módulo criptográfico" é equivalente ao termo " *token* criptográfico".

2.2.1 Delimitação do módulo criptográfico

DEFINIÇÃO: Um módulo criptográfico é composto por componentes de hardware, software e *firmware* que implementam funções ou processos criptográficos delimitados por uma fronteira criptográfica.

DEFINIÇÃO: A fronteira criptográfica de um cartão criptográfico ICP é o perímetro que estabelece os limites físicos dos circuitos integrados contidos no cartão.

2.2.2 Documentação técnica do módulo criptográfico

Existem requisitos de documentação técnica, descritos a seguir, que devem ser apresentados no processo de homologação para todos os componentes de hardware, software e *firmware* relacionados à segurança da operação do módulo criptográfico.

REQUISITO I.1: A documentação técnica deve descrever os componentes de hardware, software e *firmware* do módulo criptográfico, especificando a fronteira criptográfica que delimita tais componentes.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.01.01: Verificar se a documentação técnica inclui uma "lista de componentes principais" que descreve todos componentes de hardware, software e firmware do módulo criptográfico. Verificar se a "lista de componentes principais" inclui, mas não se limita aos seguintes tipos de componentes:

- Processadores, incluindo microprocessadores, processadores de sinal digital, processadores personalizados/dedicados, microcontroladores, ou quaisquer outros tipos de processadores;
- Circuitos integrados de memória ROM (*Read Only Memory*) para código executável de programas e dados [tal item pode incluir MPROM (*Mask-Programmed* ROM), PROM (*Programmable* ROM), EPROM (*Erasable* PROM), EEPROM (*Electrically Erasable* PROM) ou FLASH];
- Circuitos integrados de memória RAM (*Random Access Memory)* para armazenamento de dados temporários;
- Circuitos integrados semidedicado (*semi-custom*) de aplicação específica, tais como, *gate arrays*, *programmable logic arrays*, *field programmable gate arrays*, ou outros dispositivos lógicos programáveis;
- Circuitos integrados totalmente dedicados (*fully custom*) e de aplicação específica, incluindo quaisquer circuitos integrados criptográficos e dedicados;
- Outros elementos ativos de circuito eletrônico (a documentação não deve listar elementos passivos de circuito eletrônico, tais como, resistores *pull up/pull down* ou capacitores *bypass* se eles não desempenharem um papel significativo na segurança do módulo criptográfico e não estiverem na fronteira criptográfica [MCT-I]);
- Componentes de fornecimento de energia, incluindo alimentação (*power supply*), módulos de conversão de voltagem (por exemplo: módulos AC-DC ou DC-DC). transformadores, conectores de entrada de energia e conectores de saída de energia;
- Placa de circuito impresso ou outras superfícies de montagem de componentes;

- Encapsulamentos/Revestimentos, incluindo quaisquer portas de acesso removíveis ou coberturas/camadas;
- Conectores físicos para dispositivos externos ao módulo criptográfico, ou entre quaisquer submódulos independentes do módulo principal;
- Módulos de software/firmware que são modificáveis;
- Módulos de software/firmware que não são modificáveis;
- Outros tipos de componentes que não estão listados acima.

EN.I.01.02: Verificar se a documentação técnica especifica a fronteira criptográfica. A fronteira criptográfica deve incluir qualquer hardware ou software que insere, recebe, processa ou emite parâmetros de segurança importantes que poderiam conduzir ao comprometimento de informações sensíveis se não controlados adequadamente.

EN.I.01.03: Verificar se todos os componentes de hardware, software e firmware dentro da fronteira criptográfica estão incluídos na "lista de componentes principais", e que quaisquer componentes fora da fronteira criptográfica não estão listados como componentes do módulo criptográfico.

EN.I.01.04: Verificar se a documentação técnica mostra explicitamente e precisamente onde o perímetro físico da fronteira criptográfica está situado, incluindo detalhes sobre os seus componentes. Além disso, analisar se a documentação contém uma lista das portas conectadas a equipamentos externos, todos os fluxos de informação significativa e processamentos a serem desempenhados dentro da fronteira criptográfica, além de toda informação recebida e emitida.

EN.I.01.05: Verificar se a fronteira criptográfica é fisicamente contínua, de tal forma que não haja lacunas que poderiam permitir entrada, saída ou outro tipo de acesso não controlado ao módulo criptográfico. O projeto do módulo criptográfico deve também assegurar que não hajam interfaces não controladas para o interior ou para fora do módulo criptográfico que poderiam passar PCSs *(*Parâmetros Críticos de Segurança*)*, dados em texto legível, ou outras informações que se mal utilizadas ou utilizadas de forma inadequada poderiam conduzir a um comprometimento da segurança.

EN.I.01.06: Verificar se todos os componentes que estão identificados no diagrama de blocos pertencem à fronteira criptográfica, segundo **REQUISITO I.06**.

EN.I.01.07: Verificar se a documentação técnica descreve os componentes de software/firmware executados pelo módulo criptográfico, bem como seus serviços desempenhados, e os dispositivos de memória que armazenam dados e o código executável.

EN.I.01.08: Analisar a documentação técnica e identificar os componentes de hardware internos ou externos ao módulo criptográfico que interagem com o processador listado na "lista de componentes principais".

REQUISITO I.2: A documentação técnica deve descrever a configuração física do módulo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.02.01: Analisar a documentação técnica e verificar se a identificação do módulo criptográfico enquadra-se numa das seguintes definições, conforme padrão FIPS PUB 140-2, Seção 4.5: *single-chip module*, *multi-chip embedded module* ou *multi-chip standalone module.*

EN.I.02.02: Analisar a documentação técnica e verificar a disposição interna (*internal layout*) do módulo criptográfico por meio de desenhos técnicos, esboços ou diagramas de blocos que identifiquem cada bloco dos componentes de hardware.

EN.I.02.03: Analisar a documentação técnica e verificar as principais montagens/encapsulamentos físicos do módulo, e como são dispostas tais montagens/encapsulamentos no módulo criptográfico.

EN.I.02.04: Analisar a documentação técnica e verificar a descrição dos parâmetros físicos principais do módulo criptográfico, constando, no mínimo, dos seguintes itens:

- Forma de encapsulamento/revestimento e dimensões aproximadas, incluindo quaisquer interfaces de acesso ou coberturas/camadas;
- Dimensões, disposição (*layout*) e interconexões de placa(s) de circuito impresso;

- Localização da fonte de alimentação de energia, conversores de energia, e entradas e saídas de energia;
- Ativação de componentes interconectados por meio de condutores elétricos *(interconection wiring runs):* rotas e terminais;
- Arranjos de refrigeração, tais como, pratos de condução (*conduction plates)*, duto de refrigeração (*cooling airflow)*, trocadores de calor (*heat exchanger)*, haletas de refrigeração (*cooling fins)*, ventiladores (*fans)*, ou outros arranjos para a remoção de calor do módulo;
- Outros tipos de componentes não listados acima.

EN.I.02.05: Verificar se os itens descritos no **EN.I.02.04** estão em conformidade com as estruturas físicas contidas na "lista de componentes principais".

REQUISITO I.3: A documentação técnica deve descrever qualquer componente de hardware, software ou *firmware* que seja excluído dos requisitos de segurança apresentados neste documento e explicar a razão para tal exclusão.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.03.01: Verificar se a documentação técnica descreve os componentes excluídos dos requisitos de segurança definidos no Manual de Condutas Técnicas 3 - Volume I.

EN.I.03.02: Analisar a documentação técnica e identificar as razões e os argumentos apresentados pela PI para exclusão de componentes dos requisitos de segurança definidos no Manual de Condutas Técnicas 3 - Volume I. Verificar se as razões e argumentos apresentados para exclusão de componentes dos requisitos de segurança definidos no Manual de Condutas Técnicas 3 - Volume I são coerentes e precisos, não contendo pontos ambíguos e duvidosos.

EN.I.03.03: Verificar se a documentação técnica mostra que um componente, se apresentar funcionamento inadequado, não pode causar comprometimento de PCSs, dados em texto legível, ou outras informações que se mal utilizadas ou utilizadas de forma inadequada poderiam conduzir a um comprometimento da segurança.

EN.I.03.04: Verificar se quaisquer interfaces ou conexões físicas entre os componentes excluídos e o módulo criptográfico, não permitem divulgação não controlada de PCSs, dados em texto legível, ou outras informações que se mal utilizadas ou utilizadas de forma inadequada poderiam conduzir a um comprometimento da segurança.

EN.I.03.05: Verificar que componentes a serem excluídos dos requisitos do Manual de Condutas Técnicas 3 - Volume I estão também contidos na "lista de componentes principais".

REQUISITO I.4: A documentação técnica deve descrever as características elétricas, lógicas e físicas aplicáveis ao módulo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.04.01: Verificar se a documentação técnica atende ao **REQUISITO I.04.**

REQUISITO I.5: A documentação técnica deve listar todas as funções de segurança e operações criptográficas que são empregadas pelo módulo, assim como especificar todos os modos de operação suportados.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.05.01: Verificar se a documentação técnica fornecida descreve as funções de segurança (incluindo a lista de funções não aprovadas pela família de padrões FIPS), operações criptográficas e modos de operação suportados pelo módulo criptográfico.

REQUISITO I.6: A documentação técnica deve descrever o diagrama de blocos detalhando todos os componentes de hardware e de interconexão, incluindo:

- Microprocessadores;
- *buffers* de entrada e saída de dados;
- *buffers* com conteúdo de texto claro;
- *buffers* com conteúdo de texto cifrado;
- *buffers* de controle;
- memórias de armazenamento das chaves criptográficas;

- memórias de armazenamento dos componentes de software do módulo, tornando explícito onde foram implementados o SO (sistema operacional) e os algoritmos criptográficos;
- memória de trabalho ou operacional;
- memória de programa.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.06.01: Verificar se a documentação técnica contém um ou mais diagramas de blocos indicando os principais submódulos do módulo criptográfico. Neste caso, diagramas de blocos devem identificar, mas não estão limitados aos seguintes componentes:

- Microprocessadores ou quaisquer outros processadores presentes na "lista de componentes principais";
- *Buffer* (memória) que armazena dados de entrada ou saída considerados genéricos (exceto dados em texto plano e/ou cifrados ou informações de controle);
- *Buffer* (memória) de texto plano e/ou cifrado que armazena dados a serem cifrados ou decifrados;
- *Buffer* (memória) de controle que armazena informação de controle e estado que é inserida ou retirada do módulo criptográfico;
- Armazenamento de chaves criptográficas;
- Memória de trabalho ou operacional para processamento de informação;
- Memória de programa contendo o código executável de software ou firmware;
- Circuitos integrados (semi-) dedicados (por exemplo, circuitos integrados de aplicação específica, *gate arrays, field programmable gate arrays, programmable logic arrays* ou outros dispositivos lógicos programáveis);
- Outros tipos de componentes não listados acima.

EN.I.06.02: Verificar se a documentação técnica contém os diagramas de blocos que indicam os principais componentes de hardware, interconexões/interfaces internas e externas, e fluxos de dados com componentes internos e externos ao módulo criptográfico.

EN.I.06.03: Verificar se os diagramas de blocos identificam o tipo de informação transmitida nas interconexões com componentes internos e externos ao módulo criptográfico.

EN.I.06.04: Verificar se os diagramas de blocos identificam os componentes pertencentes à fronteira criptográfica do módulo criptográfico.

REQUISITO I.7: A documentação técnica deve descrever o projeto dos componentes de hardware, software e *firmware* do módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.07.01: Comparar a especificação do projeto de hardware, software e firmware, com a "lista de componentes principais" do módulo criptográfico.

EN.I.07.02: Verificar se há consistência entre o modelo de estado finito do módulo criptográfico e sua especificação de projeto.

EN.I.07.03: Verificar se a documentação técnica do projeto foi realizada utilizando linguagens de especificação de alto nível para software e firmware, e também esquemas para hardware.

REQUISITO I.8: A documentação técnica deve descrever todos os dados que são relacionados à segurança, descrevendo a forma e o local de armazenamento dos dados nos componentes de hardware. Dados relacionados à segurança incluem, mas podem não estar limitados a:

- Chave criptográfica em texto claro e cifrada ;
- dado de autenticação, como por exemplo, senha e PIN;
- parâmetros críticos de segurança (PCS).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.08.01: Verificar se a documentação técnica atende ao **REQUISITO I.08.**

REQUISITO I.9: A documentação técnica deve descrever a política de segurança adotada pelo módulo criptográfico. A política de segurança deve descrever as regras ou procedimentos que são derivados dos requisitos definidos neste documento, assim como as regras ou

procedimentos que foram derivados de quaisquer outros padrões ou requisitos adicionais impostos pelo fabricante.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.09.01: Examinar a política de segurança do módulo criptográfico, e verificar se está em conformidade com os requisitos especificados no apêndice C do padrão FIPS PUB 140-2.

EN.I.09.02: Verificar se a documentação técnica atende ao **REQUISITO I.09.**

2.2.3 Papéis, serviços e autenticação

REQUISITO I.10: O módulo criptográfico deve suportar o conceito de papel de acesso para associação com entidades usuárias externas e serviços oferecidos pelo módulo.

Nota: Este requisito é testado como parte do **REQUISITO I.11.**

2.2.3.1 Papéis de acesso

REQUISITO I.11: O módulo criptográfico deve suportar, no mínimo, os seguintes papéis de acesso:

- Usuário: Realização de serviços de segurança oferecidos pelo módulo após sua iniciação, incluindo operações criptográficas, geração de chaves criptográficas, o uso do sistema de arquivos, sobrescrita do valor de chaves criptográficas (*key zeroization*), etc;
- Oficial de segurança: Realização de serviços relacionados à iniciação do sistema de arquivo do módulo, gerenciamento do módulo, reiniciação do módulo, sobrescrita do valor de chaves criptográficas (*key zeroization*) e destruição do módulo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.11.01: Analisar a documentação técnica referente a este requisito, verificando que, pelo menos, um papel de acesso "Usuário" e um papel de acesso "Oficial de Segurança" são definidos no módulo criptográfico, juntamente com seus serviços associados.

EN.I.11.02: Assumir no módulo criptográfico um papel de acesso "Usuário", e depois realizar testes executando serviços associados ao papel de acesso assumido, verificando se há ou não conformidade com a documentação fornecida.

EN.I.11.03: Assumir no módulo criptográfico um papel de acesso "Oficial de Segurança", e depois realizar testes executando serviços associados ao papel de acesso assumido, verificando se há ou não conformidade com a documentação fornecida.

OBSERVAÇÃO: Uma entidade usuária externa não necessita assumir um papel de acesso para executar um serviço que não modifique, ou não substitua chaves criptográficas públicas ou que não afetem a segurança do módulo, das chaves criptográficas secretas e de PCSs, com relação à leitura, modificação, utilização ou substituição não autorizada. Exemplos de serviços que podem ser executados sem que a entidade usuária externa necessite assumir um papel de acesso, incluem:

- Informe de estado;
- auto-teste;
- leitura de certificado digital armazenado em EF (*Elementary Files*).

REQUISITO I.12: A documentação técnica deve descrever todos os papéis de acesso que são suportados pelo módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

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

OBSERVAÇÃO: Em um determinado momento, uma entidade usuária externa pode assumir um único papel. Porém, uma mesma entidade usuária externa, em diferentes momentos, pode assumir diferentes papéis.

2.2.3.2 Serviços

DEFINIÇÃO: O termo serviço faz referência a qualquer serviço, operação ou função que possa ser realizada pelo módulo criptográfico.

DEFINIÇÃO: Uma entrada de serviço representa qualquer entrada de dado ou controle que inicie ou realize um serviço, operação ou função específica. Uma saída de serviço representa qualquer saída de dado ou estado resultante da execução de um serviço, operação ou função iniciada por uma entrada de serviço. Toda entrada de serviço deve resultar em uma saída de serviço.

REQUISITO I.13: A documentação técnica deve descrever:

- Os serviços oferecidos pelo módulo criptográfico;
- para cada serviço oferecido pelo módulo criptográfico, suas entradas de serviço, suas correspondentes saídas de serviço e os papéis de acesso autorizados nos quais o serviço pode ser realizado;
- qualquer serviço fornecido pelo módulo criptográfico para o qual uma entidade usuária externa não necessita assumir um papel autorizado. Considerando estes serviços, deve ser esclarecido que não modifiquem ou substituam chaves criptográficas públicas e que não afetem a segurança do módulo, das chaves criptográficas secretas e dos PCSs, com relação à leitura, modificação, utilização ou substituição não autorizada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.13.01: Verificar se a documentação técnica atende ao **REQUISITO I.13.**

2.2.3.3 Identificação e autenticação de entidade usuária externa

Mecanismos de identificação e autenticação devem ser utilizados para identificar e autenticar uma entidade usuária externa no momento de acesso ao módulo criptográfico. Estando a entidade usuária externa devidamente identificada e autenticada é possível verificar se tal entidade está autorizada a executar um determinado serviço.

No caso do módulo criptográfico, escopo deste documento, ou seja, *token* criptográfico, podem ser utilizadas duas formas de identificação e autenticação de entidade usuária externa:

- Identificação e autenticação do papel de acesso da entidade;
- identificação e autenticação da entidade.

A forma mais usual e definida no padrão ISO 7816 é a identificação e autenticação do papel da entidade, sendo ela realizada através do PIN e PUK. A entidade usuária externa deve

informar ao módulo criptográfico o valor do PIN a fim de assumir o papel de usuário ou o valor do PUK para assumir o papel de oficial de segurança.

Dependendo do nível de segurança e do serviço a ser utilizado, o módulo criptográfico pode utilizar diferentes mecanismos de autenticação e controle de acesso.

DEFINIÇÃO: Mecanismos de identificação e autenticação da entidade usuária externa:

- Sem identificação e autenticação: Alguns serviços oferecidos pelo módulo criptográfico podem não requisitar identificação e autenticação da entidade usuária externa. Como exemplo é possível citar a leitura de *Elementary Files* contendo certificados digitais;
- sem autenticação: Os acessos são realizados sem autenticação;
- identificação e autenticação baseada em papel de acesso: O módulo criptográfico requisita à entidade usuária externa a seleção de um papel de acesso e sua autenticação neste papel. A seleção do papel pode ser explícita ou implícita. A entidade usuária externa pode, também, selecionar um ou mais papéis de acesso. O módulo criptográfico não necessita autenticar individualmente a identidade da entidade usuária externa. Se o módulo criptográfico permitir a uma entidade usuária externa alterar seu papel, então o módulo deve autenticar qualquer papel de acesso que não foi previamente autenticado. Por exemplo:
  - Identificação e autenticação baseada em PIN: O valor de PIN é utilizado para identificação e autenticação do papel de acesso usuário a ser assumido pela entidade usuária externa;
  - identificação e autenticação baseada em identidade: O módulo criptográfico requisita:

    a) que a entidade usuária externa seja individualmente identificada;

    b) que um ou mais papéis sejam, implicitamente ou explicitamente, selecionados pela entidade usuária externa (seleção de papéis);

    c) autenticar a identidade da entidade usuária externa e autorizar a entidade usuária externa a assumir o papel selecionado.

    Se o módulo criptográfico permitir a uma entidade usuária externa assumir um outro papel, então o módulo deve ou autenticar a entidade usuária externa previamente identificada ou verificar a autorização da entidade usuária externa em assumir o papel requisitado. Por exemplo:

- Identificação e autenticação baseada em nome de usuário e senha: A partir da identificação do usuário (por exemplo, um nome de usuário) é requisitada uma senha para autenticação desta identidade.

REQUISITO I.14: O módulo criptográfico deve empregar os mecanismos de identificação e autenticação baseado em papel de acesso ou baseado em identidade para controlar o acesso ao módulo criptográfico.

Nota: Este requisito é testado como parte do **REQUISITO I.11.**

OBSERVAÇÃO: Um módulo criptográfico pode permitir a uma entidade usuária externa identificada e autenticada executar vários serviços associados ao papel de acesso autorizado ou pode exigir uma identificação e autenticação separada para cada serviço ou diferentes conjuntos de serviços.

REQUISITO I.15: Quando o módulo criptográfico for desligado e na seqüência ligado novamente, os resultados das identificações e autenticações prévias não devem ser mantidos. Neste caso, o módulo criptográfico sempre deve requisitar que a entidade usuária externa seja novamente identificada e autenticada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.15.01: Verificar se a documentação técnica descreve os mecanismos e os critérios usados pelo módulo criptográfico para eliminar os resultados de autenticações prévias.

EN.I.15.02: Autenticar-se nos papéis suportados no módulo, e executar serviços associados. Em seguida, energizar e desenergizar o módulo, e tentar executar alguns serviços dos papéis assumidos anteriormente.
EN.I.15.03: Verificar se o módulo nega o acesso aos serviços e requer nova autenticação.

EN.I.15.04: Baseando-se nos **EN.I.15.02** e **EN.I.15.03**, verificar se há conformidade com o **REQUISITO I.15**.

Outras formas de identificação e autenticação podem ser utilizadas pelo módulo criptográfico, incluindo, mas não limitado a:

- Conhecimento ou posse de chave criptográfica ou equivalente;
- verificação de características pessoais, como por exemplo, biometria.

REQUISITO I.16: Dados de autenticação armazenados no interior do módulo criptográfico devem ser protegidos contra leitura, modificação, utilização e substituição não autorizada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.16.01: Verificar se a documentação técnica descreve como dados de autenticação armazenados no interior do módulo criptográfico são protegidos contra divulgação, modificação e substituição não autorizada.

EN.I.16.02: Tentar obter acesso aos dados de autenticação para os quais não está autorizado, usando métodos específicos. O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de alguma forma.

EN.I.16.03: Tentar modificar ou substituir dados de autenticação para os quais não está autorizado, usando métodos específicos. Verificar que o módulo não permite que dados de autenticação sejam modificados ou substituídos.

OBSERVAÇÃO: Se o módulo criptográfico não conter dados de autenticação necessários para autenticar a entidade usuária externa na primeira vez na qual é realizado o acesso ao módulo, então outros métodos, como por exemplo, controles no processo ou dados de autenticação padrão ("*default*"), devem ser usados para controlar o primeiro acesso ao módulo e iniciar os mecanismos de autenticação da entidade usuária externa.

REQUISITO I.17: A força ou robustez do mecanismo de autenticação deve estar em conformidade com as seguintes especificações:

- Para cada tentativa de uso do mecanismo de autenticação, a probabilidade deve ser menor do que 1 em 1.000.000, de que uma tentativa aleatória tenha sucesso, ou que uma aceitação falsa possa ocorrer (por exemplo, adivinhação de senha ou PIN, taxa de

erro de aceitação falsa de um parâmetro biométrico ou alguma combinação de métodos de autenticação).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.17.01: Analisar a documentação técnica, verificando, para cada mecanismo de autenticação suportado, se a probabilidade de uma tentativa aleatória tenha sucesso, ou que uma aceitação falsa possa ocorrer seja menor que 1 em 1.000.000.

EN.I.17.02: Para cada mecanismo de autenticação suportado, deve-se determinar o nível de exatidão de qualquer argumento fornecido via descrição analítica, verificando a existência de incertezas, pontos obscuros ou ambigüidades que possam comprometer o entendimento da documentação.

EN.I.17.03: Verificar por análise direta, se o dado de autenticação é obscurecido e que não há retorno visível durante a sua entrada.

EN.I.17.04: Verificar por análise direta, se mecanismo de realimentação não provê informações que poderiam ser usadas para advinhar ou determinar os dados de autenticação.

EN.I.17.05: Realizar os ensaios **EN.I.17.03** e **EN.I.17.04** para cada papel suportado pelo módulo criptográfico.

REQUISITO I.18: No contexto da CSP do *token* criptográfico, a força ou robustez do mecanismo de autenticação deve estar em conformidade com as seguintes especificações:

- A realimentação de dados de autenticação (*echo*) para uma entidade usuária externa deve ser obscura durante a autenticação (por exemplo, nenhuma exibição visível de caracteres deve haver no momento da inserção de um PIN);
- não devem haver métodos alternativos oferecidos a entidade usuária externa durante uma tentativa de autenticação que enfraqueçam a força ou robustez do mecanismo de autenticação.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.18.01: Verificar se a documentação técnica descreve os mecanismos de autenticação em conformidade com o **REQUISITO I.18.**

EN.I.18.02: Utilizando uma ferramenta específica que realiza chamadas pela CSP do módulo criptográfico, verificar por análise direta, se dados de autenticação são obscurecidos e que não existe retorno visível durante a sua entrada.

EN.I.18.03: Verificar por meio de análise direta dos mecanismos de autenticação, se mecanismos de realimentação não provêem informações que poderiam ser usadas para advinhar ou determinar os dados de autenticação da entidade usuária externa.

EN.I.18.04: Para cada mecanismo de autenticação suportado, deve-se determinar o nível de exatidão de qualquer argumento fornecido via descrição analítica, verificando a existência de incertezas, pontos obscuros ou ambigüidades que possam comprometer o entendimento da documentação.

EN.I.18.05: Verificar por meio de ferramenta específica que realiza chamadas via API, se existem métodos alternativos oferecidos a entidade usuária externa durante uma tentativa de autenticação que enfraqueçam a força ou robustez do mecanismo de autenticação.

REQUISITO I.19: A documentação técnica deve descrever:

- Os mecanismos de autenticação suportados pelo módulo criptográfico;
- os tipos de dados de autenticação que são requisitados pelo módulo para implementar os mecanismos de autenticação suportados;
- os métodos que são utilizados para realizar o controle de acesso ao módulo criptográfico no seu primeiro acesso e, em seguida, iniciar o mecanismo de autenticação;
- a força e robustez dos mecanismos de autenticação suportados pelo módulo e pela CSP do *token* criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.19.01: Verificar se a documentação técnica atende ao **REQUISITO I.19.**

2.2.4 Modelo de estado finito

A operação do módulo criptográfico deve ser descrita por meio de um modelo de estado finito (ou equivalente) representado por um diagrama de transição de estados e/ou uma tabela de transição de estados.

REQUISITO I.20: O módulo criptográfico deve incluir os seguintes estados operacionais e estados de erro:

- Estados de alimentação de energia: Estados para alimentação de energia primária, secundária ou backup. Estes estados podem diferenciar em função das fontes de energia que estão sendo aplicadas ao módulo criptográfico;
- estados do oficial de segurança: Estados nos quais os serviços do oficial de segurança são executados (por exemplo, iniciação e gerenciamento de chaves criptográficas);
- estados de entrada de chave ou PCSs: Estados para a inserção de chaves criptográficas e PCSs no módulo criptográfico;
- estados de usuário: Estados nos quais entidades usuárias externas no papel de acesso usuário executam serviços de segurança, realizam operações criptográficas ou desempenham outras funções;
- estados de auto-teste: Estados nos quais o módulo criptográfico realiza auto-testes;
- estados de erro: Estados quando o módulo criptográfico encontra um erro (por exemplo, falha em um auto-teste ou tentativa de cifrar quando chaves operacionais ou PCSs foram perdidos). Estados de erro poderiam incluir:

  a) “Erros rígidos”, os quais indicam um mal funcionamento do equipamento, podendo ser necessário executar serviços de manutenção ou reparo no módulo criptográfico;

  b) “Erros leves e recuperáveis”, os quais requerem apenas uma nova iniciação (*resetting*) do módulo criptográfico. A recuperação a partir de estados de erro deve ser possível, exceto para os casos em que ocorram os “Erros rígidos”.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.20.01: Analisar a documentação técnica e verificar se contém uma descrição do modelo de estado finito. Esta descrição deve conter a identificação e detalhamento de todos os estados do módulo e as respectivas transições de estados de acordo com o requisito.

OBSERVAÇÃO: O módulo criptográfico pode, ainda, utilizar outros estados, incluindo, mas não limitado a:

- Estados de manutenção: Estados para manutenção e prestação de serviços ao módulo criptográfico, incluindo testes de manutenção lógicos e físicos. Se o módulo criptográfico contém um papel de acesso de manutenção, então um estado de manutenção deve ser incluído.

REQUISITO I.21: A documentação do módulo criptográfico deve incluir o modelo de estado finito (ou equivalente), utilizando um diagrama de transição de estados e/ou uma tabela de transição de estados que representa a operação do módulo criptográfico descrevendo:

- Todos os estados de erro e operacionais do módulo criptográfico;
- as transições correspondentes de um estado para outro;
- os eventos de entrada, incluindo inserções de dados e controles, que causam transições de um estado para outro;
- os eventos de saída, incluindo condições internas do módulo criptográfico, saídas de dados, e saídas de estado resultantes de transições de um estado para outro.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.21.01: Analisar a documentação e verificar se contém uma descrição do modelo de estado finito. Esta descrição deve conter a identificação e detalhamento de todos os estados do módulo e as respectivas transições de estados. A descrição das transições de estados deve incluir condições internas do módulo, entradas de dados e controles que causam transições de um estado para outro, e saídas de dados e estados resultantes das transições de um estado para outro.

EN.I.21.02: Verificar se os diagramas de estado finito e as respectivas descrições estão consistentes com a documentação, no que diz respeito aos seguintes ítens:

- Interface de entrada de dados;
- Interface de saída de dados;
- Interface de entrada de controle;
- Interface de saída de estado;
- Papel do oficial de segurança;

- Papel do usuário;
- Outros papéis (se aplicável);
- Entrada de chaves (se aplicável);
- Mostrar estado do serviço;
- Auto-teste;
- Outros serviços autorizados, operações e funções (se aplicável);
- Estados de erro;
- Estados de contorno (se aplicável);
- Interface de manutenção (se aplicável);
- Papel de manutenção (se aplicável);
- Serviço de geração de chave (se aplicável);
- Serviço de exportação de chave (se aplicável);
- Estado de ociosidade (se aplicável);
- Estado de não iniciação (se aplicável).

EN.I.21.03: Verificar se todo estado identificado no diagrama de estado finito possui a respectiva identificação e descrição na documentação, e vice-versa.

EN.I.21.04: Verificar se a operação do módulo criptográfico está consistente com a descrição do diagrama de estado finito.

EN.I.21.05: Verificar, quando aplicável, se todos os estados de manutenção estão contidos no diagrama de estado finito.

EN.I.21.06: Verificar se existe uma cadeia de transições de um estado inicial de energização (*initial power-on state*) para cada estado no modelo, exceto para o próprio estado inicial de energização.

EN.I.21.07: Verificar se existe uma cadeia de transições de cada estado ativo do modelo para o estado de desativação (*power-off state*).

EN.I.21.08: Analisar a documentação e verificar se as ações do modelo de estado finito, como resultado de todas as possíveis entradas de dados e controles, estão bem definidas.

EN.I.21.09: Verificar se o módulo criptográfico suporta os seguintes estados operacionais e estados de erro:

- Estados de alimentação de energia;
- Estados do "Oficial de Segurança";
- Estados "Entrada de chave ou PCS";
- Estados de usuário;
- Estados de auto-teste.

2.2.5 Segurança física

O módulo criptográfico deve empregar controles de segurança física para restringir acessos físicos não autorizados ao seu conteúdo e, também, para evidenciar a leitura, modificação, utilização ou até mesmo a substituição não autorizada de componentes do módulo.
Quanto ao tipo de circuito, o módulo criptográfico pode ser classificado em mono-CI (Mono Circuito Integrado), multi-CI (Multi Circuito Integrado):

- Mono-CI: O único circuito integrado presente no módulo criptográfico deve ser protegido por um invólucro;
- multi-CI: Os vários circuitos integrados presentes no módulo criptográfico devem ser protegidos por um invólucro.

REQUISITO I.22: Os circuitos integrados presentes em um módulo criptográfico devem ser protegidos por um invólucro. O invólucro consiste de uma cobertura com revestimento que evidencie violações. Sua finalidade é deter a observação, sondagem ou manipulação do chip sem que haja a remoção do invólucro, provendo evidências sobre tentativas de violar ou remover os componentes protegidos.

Procedimentos de Ensaio para NSH 1, 2 e 3:
EN.I.22.01: Verificar se a documentação técnica descreve o invólucro que protege o módulo criptográfico.

EN.I.22.02: Inspecionar o módulo criptográfico por meio de equipamento específico, e verificar se seu invólucro cumpre a sua finalidade de deter a observação, sondagem ou

manipulação do módulo sem que haja a remoção do invólucro, provendo evidências sobre tentativas de violar ou remover os componentes protegidos.

REQUISITO I.23: A documentação técnica deve descrever qual a classificação do módulo criptográfico quanto ao tipo de circuito.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.23.01: Verificar se a documentação técnica atende ao **REQUISITO I.23.**

REQUISITO I.24: A documentação técnica deve descrever qual a composição dos materiais empregados na fabricação do invólucro que garante a segurança física do módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:
EN.I.24.01: Verificar se a documentação técnica atende ao **REQUISITO I.24.**

REQUISITO I.25: O invólucro que evidencia violações deve ser opaco no "*spectrum*" de luz visível.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.25.01: Verificar se a documentação técnica descreve a opacidade da cobertura/camada ou invólucro do módulo criptográfico.

EN.I.25.02: Inspecionar o módulo criptográfico por meio de equipamento específico, verificando a opacidade da cobertura/camada ou invólucro que evidencia violações físicas.

2.2.6 Ambiente operacional

O ambiente operacional de um módulo criptográfico faz referência aos componentes de software, *firmware* e hardware necessários para sua operação.
Um módulo criptográfico, quanto ao seu ambiente operacional, pode ser classificado em:

- Ambiente operacional de propósito geral: faz referência ao uso de um sistema operacional de propósito geral e comercial;
- ambiente operacional limitado: Ambiente operacional estático e não modificável, não baseado num sistema operacional de propósito geral para seu suporte;
- ambiente operacional modificável: Ambiente operacional passível de ser reconfigurado para adicionar, remover ou modificar funcionalidades. Ambientes operacionais são considerados modificáveis quando os componentes de software ou *firmware* podem ser modificados por operadores, ou então, quando operadores podem carregar e executar software ou *firmware* que não foi incluído como parte do processo de certificação do módulo.

Para módulos criptográficos do tipo *token* criptográfico de ambiente operacional limitado (estático não modificável) e monoaplicação não existem requisitos de segurança associados ao ambiente operacional.

2.2.7 Gerenciamento de chaves criptográficas

O gerenciamento de chaves criptográficas abrange o ciclo de vida completo das chaves criptográficas, seus componentes e PCSs empregados pelo módulo. Abrange a geração de números aleatórios, a geração de chaves, a atribuição de chaves, a importação e exportação de chaves, o armazenamento de chaves e a sobrescrita do valor da chave com zeros.

DEFINIÇÃO: Chave criptográfica cifrada faz referência a uma chave que é cifrada utilizando um algoritmo de segurança aprovado pela família de padrões FIPS.

DEFINIÇÃO: PCS cifrado faz referência a um PCS que é cifrado utilizando um algoritmo de segurança aprovado pela família de padrões FIPS.
OBSERVAÇÃO: Chaves criptográficas e PCSs cifrados utilizando um algoritmo de segurança não aprovado pela família de padrões FIPS serão considerados em formato de texto claro.

REQUISITO I.26: Chaves simétricas, chaves assimétricas privadas e PCSs devem estar protegidas dentro do módulo contra leitura, modificação, utilização e substituição não autorizada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.26.01: Analisar a documentação técnica referente a este requisito, verificando como chaves criptográficas e PCSs são protegidos contra divulgação, modificação e substituição não autorizada.

EN.I.26.02: Tentar obter acesso às chaves secretas, às chaves privadas e PCS para os quais não está autorizado, usando métodos específicos (por exemplo, invocando um comando de leitura ao arquivo que contém uma chave secreta). O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de outra forma.

EN.I.26.03: Tentar modificar ou substituir as chaves secretas, as chaves privadas e PCS para os quais não está autorizado, usando métodos específicos. Verificar que o módulo não permite que as chaves secretas, privadas e PCS utilizados por serviços criptográficos sejam modificados ou substituídos.

REQUISITO I.27: Chaves públicas devem estar protegidas dentro do módulo contra modificação e substituição não autorizada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.27.01: Analisar a documentação técnica referente a este requisito, verificando como chaves criptográficas e PCSs são protegidos contra divulgação, modificação e substituição não autorizada.

EN.I.27.02: Tentar obter acesso às chaves secretas, às chaves privadas e PCS para os quais não está autorizado, usando métodos específicos (por exemplo, invocando um comando de leitura ao arquivo que contém uma chave secreta). O módulo deve negar o acesso ou permitir somente o acesso aos dados cifrados ou protegidos de outra forma.

EN.I.27.03: Tentar modificar ou substituir as chaves secretas, as chaves privadas e PCS para os quais não está autorizado, usando métodos específicos. Verificar que o módulo não permite que as chaves secretas, privadas e PCS utilizados por serviços criptográficos sejam modificados ou substituídos.

REQUISITO I.28: A documentação técnica deve descrever todas as chaves criptográficas, seus componentes e PCSs empregados pelo módulo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.28.01: Verificar se a documentação técnica atende ao **REQUISITO I.28.**

REQUISITO I.29: A documentação técnica deve descrever quais métodos são usados pelo módulo criptográfico para proteger chaves simétricas, chaves assimétricas privadas e PCSs contra leitura, modificação, utilização e substituição não autorizada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.29.01: Verificar se a documentação técnica atende ao **REQUISITO I.29.**

REQUISITO I.30: A documentação técnica deve descrever quais métodos são usados pelo módulo criptográfico para proteger chaves públicas contra modificação e substituição não autorizada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.30.01: Verificar se a documentação técnica atende ao **REQUISITO I.30.**

2.2.7.1 Geradores de números aleatórios (*Random Number Generators* - RNG)

REQUISITO I.31: Algoritmos RNG determinísticos aprovados pela família de padrões FIPS devem ser usados pelo módulo criptográfico para geração de chaves ou para gerar vetores de iniciação (IV) definidos em algoritmos criptográficos (ver Figura 1).

Procedimentos de Ensaio para NSH 1:

EN.I.31.01: Analisar a documentação técnica referente a este requisito, verificando quais são os algoritmos RNG determinísticos usados pelo módulo criptográfico, e ainda, se tais

algoritmos são aprovados ou não pela família de padrões FIPS. Algoritmos aprovados são listados no FIPS 140-2 Anexo C.

EN.I.31.02: 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 RNG determinísticos suportados pelo módulo criptográfico. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se o comportamento estatístico dos algoritmos RNG determinísticos poderá ser executado nos NSHs 2 ou 3.

EN.I.31.03: 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 RNG determinístico implementado pelo módulo criptográfico, conforme listados no FIPS 140-2 Anexo C. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se o comportamento estatístico dos algoritmos RNG determinísticos poderá ser executado nos NSHs 2 ou 3.

Procedimentos de Ensaio para NSH 2:

EN.I.31.04: Verificar, por análise direta do código fonte dos algoritmos RNG determinísticos aprovados pela família de padrões FIPS, se tais algoritmos implementados estão em conformidade com a documentação.

Procedimentos de Ensaio para NSH 3:

EN.I.31.05: Verificar, por análise direta do código fonte do módulo criptográfico, se o algoritmo implementado RNG 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 I.32: Algoritmos RNG não aprovados pela família de padrões FIPS devem ser usados somente para gerar, sementes para RNG determinísticos aprovados ou vetores de iniciação (IV) de algoritmos criptográficos (ver Figura 1).

Procedimentos de Ensaio para NSH 1:

EN.I.32.01: Analisar a documentação técnica referente a este requisito, verificando quais são os algoritmos RNG não aprovados pela família de padrões FIPS usados pelo módulo criptográfico como por exemplo geradores tipo TRNG em hardware.

EN.I.32.02: 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 RNG não aprovados pela família de padrões FIPS suportados pelo módulo criptográfico. Caso não exista algum tipo de interface que permita a realização deste ensaio, será avaliado se o comportamento estatístico dos algoritmos RNG não aprovados poderá ser executado nos NSHs 2 ou 3.

Procedimentos de Ensaio para NSH 2:

EN.I.32.03: Verificar, por análise direta do código fonte dos algoritmos RNG não aprovados pela família de padrões FIPS, se tais algoritmos implementados estão em conformidade com a documentação.

Procedimentos de Ensaio para NSH 3:

EN.I.32.04: Verificar, por análise direta do código fonte do módulo criptográfico, se o algoritmo implementado RNG não aprovado pela família de padrões FIPS, é utilizado somente para geração de sementes para algoritmos RNG determinísticos aprovados pela família de padrões FIPS ou para geração de vetores de iniciação definidos em algoritmos criptográficos.

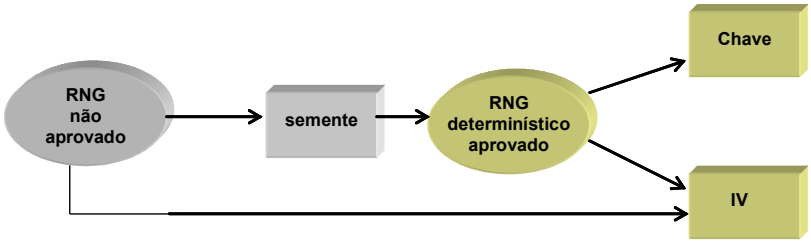

Figura 1. Geradores de números aleatórios

REQUISITO I.33: A documentação técnica deve descrever cada RNG empregado pelo módulo, seja ele aprovado ou não pelo padrão FIPS [FIPS 186-2, ANSI X9.31, ANSI X9.62-1998 e NIST SP 800-90].

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.33.01: Verificar se a documentação técnica atende ao **REQUISITO I.33.**

2.2.7.2 Geração de chaves criptográficas

REQUISITO I.34: O módulo 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 RNG, então o RNG utilizado também deve ser aprovado pela família de padrões FIPS.

Procedimentos de Ensaio para NSH 1:

EN.I.34.01: Analisar a documentação técnica referente a este requisito, verificando quais são os métodos de geração de chaves criptográficas usados pelo módulo, e ainda, se tais métodos são ou não aprovados pela família de padrões FIPS.

EN.I.34.02: 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 pelo módulo 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 poderá ser executada nos NSHs 2 ou 3.

Procedimentos de Ensaio para NSH 2:

EN.I.34.03: 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.I.34.04: 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 RNG, utilizem somente algoritmos RNG aprovados pela família de padrões FIPS .

REQUISITO I.35: O esforço para comprometer a segurança de um método de geração de chaves criptográficas, deve ser, no mínimo, igual ao esforço para determinar o valor da chave gerada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.35.01: Verificar se a documentação técnica descreve o esforço necessário para comprometer a segurança de um método de geração de chaves criptográficas.

EN.I.35.02: 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 I.36: Se uma semente for inserida no módulo criptográfico para servir como entrada durante o processo de geração de chaves criptográficas, então a entrada desta semente deve atender aos requisitos especificados na seção 2.2.7.4 (“Importação e exportação de chaves criptográficas”).

Nota: Este requisito é testado como parte da Seção 2.2.7.4**.**

REQUISITO I.37: A documentação técnica deve descrever cada um dos métodos de geração de chaves criptográficas empregados pelo módulo (aprovados ou não pela família de padrões FIPS).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.37.01: Verificar se a documentação técnica atende ao **REQUISITO I.37.**

2.2.7.3 Atribuição de chaves

DEFINIÇÃO: O processo ou protocolo de atribuição de chaves (*key establishment*) possibilita atribuir uma chave criptográfica simétrica compartilhada a parceiros legítimos. A atribuição de chaves pode ser realizada por um processo automático (protocolo de negociação de chaves ou protocolo de transporte de chaves), método manual ou uma combinação dos anteriores.

DEFINIÇÃO: Um método manual de atribuição de chaves é aquele no qual é utilizado um dispositivo de armazenamento para o transporte manual da chave.

DEFINIÇÃO: O processo ou protocolo de negociação de chaves (*key agreement*) possibilita atribuir uma chave criptográfica simétrica compartilhada aos parceiros legítimos em função de valores secretos escolhidos por cada um dos parceiros, de forma que nenhuma outra entidade possa determinar o valor da chave criptográfica. Exemplo de negociação de chaves é o algoritmo *Diffie-Hellman*.

DEFINIÇÃO: O processo ou protocolo de transporte de chaves (*key transport*) possibilita que uma chave criptográfica simétrica compartilhada seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.

REQUISITO I.38: Se métodos de atribuição de chaves são empregados pelo módulo criptográfico, então somente os métodos de atribuição de chaves aprovados pela família de padrões FIPS devem ser usados.

Procedimentos de Ensaio para NSH 1:

EN.I.38.01: Analisar a documentação técnica referente a este requisito, verificando quais são os algoritmos de atribuição de chaves presentes no módulo criptográfico, e ainda, se tais algoritmos constam no Anexo D do FIPS PUB 140-2.

Procedimentos de Ensaio para NSH 2:

EN.I.38.02: Verificar, por análise direta do código fonte dos métodos de atribuição de chaves, se tais métodos implementados no módulo criptográfico estão em conformidade com a documentação.

Procedimentos de Ensaio para NSH 3:

EN.I.38.03: Verificar, por análise direta do código fonte do módulo criptográfico, se somente métodos de atribuição de chaves aprovados pela família de padrões FIPS são usados.

REQUISITO I.39: Quando aplicável, a documentação deve descrever os métodos de atribuição de chaves empregados pelo módulo criptográfico (automático, manual ou combinação dos anteriores).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.39.01: Verificar se a documentação técnica atende ao **REQUISITO I.39.**

2.2.7.4 Importação e exportação de chaves criptográficas

Chaves criptográficas podem ser importadas ou exportadas de um módulo criptográfico usando um método manual ou um método automático.

REQUISITO I.40: Se o módulo criptográfico permitir a importação de chave criptográfica simétrica, chave criptográfica assimétrica privada ou PCSs, então as chaves criptográficas e PCSs devem ser cifrados utilizando algoritmos aprovados pela família de padrões FIPS.

Procedimentos de Ensaio para NSH 1:

EN.I.40.01: Verificar se a documentação técnica descreve como os processos de importação e exportação são realizados para chaves criptográficas simétricas ou assimétricas privadas.

EN.I.40.02: Verificar, por meio de ferramenta específica, se o processo de importação de chave assimétrica privada apresenta indícios de proteção conforme a documentação fornecida.

EN.I.40.03: Quando aplicável, verificar, por meio de ferramenta específica, se os processos de importação e exportação de chave simétrica apresentam indícios de proteção das chaves conforme a documentação fornecida. Caso não seja possível a realização deste ensaio, será avaliado se a verificação de proteção da chave simétrica nos processos de importação e exportação poderá ser executada nos NSHs 2 ou 3.

Procedimentos de Ensaio para NSH 2:

EN.I.40.04: Verificar, por análise direta do código fonte do componente de importação/exportação de chaves, se tal componente protege as chaves nos processos de importação e exportação pelo módulo criptográfico.

Procedimentos de Ensaio para NSH 3:

EN.I.40.05: Verificar, por análise direta do código fonte do módulo criptográfico, se somente algoritmos aprovados pela família de padrões FIPS são usados na proteção de chaves durante os processos de importação e exportação pelo módulo criptográfico.

OBSERVAÇÃO: Uma chave assimétrica pública pode ser importada ou exportada do módulo criptográfico em texto claro.

REQUISITO I.41: Não deve ser possível exportar uma chave criptográfica assimétrica privada do módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.41.01: Verificar se a documentação técnica descreve a impossibilidade de exportação de chaves criptográficas assimétricas privadas do módulo criptográfico.

EN.I.41.02: Verificar por meio de ferramenta específica se é possível exportar uma chave criptográfica assimétrica privada do módulo criptográfico.

REQUISITO I.42: O módulo criptográfico deve associar a chave importada ou exportada à entidade correta a qual a chave está vinculada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.42.01: Analisar se a documentação técnica descreve como o módulo criptográfico associa a chave importada ou exportada à sua entidade correta.

EN.I.42.02: Caso sejam aplicáveis as operações de exportação e importação de chaves, para cada chave presente no módulo criptográfico, primeiro exportar uma chave enquanto assume uma dada entidade por meio de ferramenta específica. Em seguida, assumir uma entidade diferente da primeira e tentar importar a chave exportada no módulo, verificando que a inserção não deve ser possível.

EN.I.42.03: Caso sejam aplicáveis as operações de exportação e importação de chaves, para cada chave presente no módulo criptográfico, primeiro importar uma chave enquanto assume uma dada entidade por meio de ferramenta específica. Em seguida, assumir uma entidade diferente da primeira e tentar exportar a chave importada no módulo, verificando que a exportação não deve ser possível.

REQUISITO I.43: A documentação técnica deve descrever os métodos de importação e exportação de chaves criptográficas simétricas, chaves criptográficas assimétricas privadas e PCSs empregados pelo módulo, os algoritmos criptográficos utilizados nos métodos de importação e exportação.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.43.01: Verificar se a documentação técnica atende ao **REQUISITO I.43.**

2.2.7.5 Armazenamento de chaves criptográficas

DEFINIÇÃO: Chaves criptográficas devem ser armazenadas dentro do módulo criptográfico em texto claro ou de forma cifrada.

REQUISITO I.44: Chaves assimétricas privadas e chaves simétricas não devem estar acessíveis por entidades usuárias externas e não autorizadas.

Nota: Este requisito é testado como parte do **REQUISITO I.27.**

REQUISITO I.45: Chaves assimétricas privadas e chaves simétricas, caso estejam armazenadas no módulo criptográfico na forma cifrada, devem utilizar algoritmos criptográficos aprovados pela família de padrões FIPS.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.45.01: Verificar se a documentação técnica descreve os métodos de armazenamento de chaves assimétricas privadas e chaves simétricas no módulo criptográfico.

REQUISITO I.46: O módulo criptográfico deve associar a cada chave armazenada (simétrica ou assimétrica) à sua respectiva entidade proprietária.
Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.46.01: Verificar se a documentação técnica descreve como o módulo criptográfico associa cada chave armazenada a sua respectiva entidade proprietária.

EN.I.46.02: Para cada chave K_i armazenada no módulo criptográfico, deve-se assumir a entidade proprietária desta chave por meio de ferramenta específica. Em seguida, deve-se assumir uma entidade diferente da primeira e tentar executar funções criptográficas com a chave K_i, verificando que esta execução não deve ser possível.

REQUISITO I.47: A documentação técnica deve descrever os métodos de armazenamento de chaves criptográficas empregados pelo módulo.
Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.47.01: Verificar se a documentação técnica atende ao **REQUISITO I.47**.

2.2.7.6 Sobrescrita do valor de chaves criptográficas

REQUISITO I.48: O módulo deve prover métodos para sobrescrever os valores de chaves criptográficas e PCSs.

Procedimentos de Ensaio para NSH 1 e 2:

EN.I.48.01: Analisar a documentação técnica referente a este requisito, verificando se os seguintes itens estão especificados:

- Técnicas de sobrescrita;
- Restrições de sobrescrita;
- Chaves criptográficas e PCSs que são sobrescritos;
- Análise da robustez das técnicas de sobrescrita perante o comprometimento de chaves e PCSs;
- Todas as chaves simétricas, chaves assimétricas privadas e PCSs são sobrescritos.

EN.I.48.02: 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.

EN.I.48.03: Executar a operação de sobrescrita em chaves armazenadas no módulo criptográfico. Após completar a operação de sobrescrita, verificar que não é possível obter acesso às chaves eliminadas.

EN.I.48.04: Executar a operação de sobrescrita em uma chave armazenada no módulo criptográfico. Após a conclusão desta operação de sobrescrita, verificar que a destruição foi realizada em um tempo que não é suficiente para comprometer a chave criptográfica eliminada.

Procedimentos de Ensaio para NSH 2:

EN.I.48.05: Verificar, por análise direta do código fonte do componente de sobrescrita de chaves, se o método de sobrescrita é adequado perante o comprometimento de chaves e PCSs.

Procedimentos de Ensaio para NSH 3:

EN.I.48.05: Verificar, por análise direta do código fonte do módulo criptográfico, se a ação de sobrescrita com zeros binários ocorre quando chaves simétricas, chaves assimétricas privadas e PCSs são eliminadas.

REQUISITO I.49: A documentação técnica deve descrever os métodos de sobrescrita dos valores de chaves criptográficas e PCSs que são empregados pelo módulo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.49.01: Verificar se a documentação técnica atende ao **REQUISITO I.49**.

2.2.8 Auto-testes

REQUISITO I.50: Para verificar o funcionamento apropriado do módulo criptográfico, duas categorias de auto-testes devem ser realizadas:

- Auto-testes de energia: tais testes devem ser executados quando o módulo é energizado (ou alimentado com energia elétrica);
- auto-testes condicionais: tais testes devem ser executados quando uma operação ou função de segurança for invocada.

Procedimentos de Ensaio para NSH 1:

EN.I.50.01: Analisar a documentação técnica que descreve os auto-testes do módulo criptográfico, verificando os respectivos estados de erro, os eventos que podem produzir tais estados, as ações necessárias para retirar os estados de erro, e ainda, se os seguintes testes estão incluídos:

- Testes de energia
    - Teste de algoritmo criptográfico;
    - Teste de integridade de software/firmware;
    - Teste de funções críticas;
    - Outros auto-testes que são executados na energização e sob demanda.
- Testes condicionais
    - Teste de consistência de par de chaves (*pairwise*), caso o módulo criptográfico gere chaves públicas e privadas;
    - Teste de carregamento do software/firmware;
    - Teste de entrada manual de chave;
    - Teste de gerador de números aleatórios contínuo;
    - Teste de contorno (*bypass*);

- Outros testes condicionais.

EN.I.50.02: Energizar o módulo criptográfico e analisar os auto-testes realizados, verificar se não há a necessidade de qualquer intervenção por parte de uma entidade usuária externa.

EN.I.50.03: Energizar o módulo criptográfico, e observar o indicador emitido na interface de saída de estado. Após a observação do indicador de estado, verificar se está ou não em conformidade com a documentação fornecida.

EN.I.50.04: Baseando-se nos procedimentos fornecidos pela PI, iniciar os auto-testes de energia sob demanda, verificar se está em conformidade com a documentação fornecida.

EN.I.50.05: Executar os seguintes auto-testes de energia: teste de algoritmo criptográfico, teste de integridade de software/firmware e teste de funções críticas.

EN.I.50.06: Executar os seguintes auto-testes condicionais: teste de consistência de paridade (*pairwise*), teste de carregamento do software/firmware, teste de entrada manual de chave, teste de gerador de números aleatórios contínuo e teste de contorno.

EN.I.50.07: Provocar os estados de erro dos auto-testes suportados pelo módulo criptográfico. Para cada estado de erro alcançado, executar as ações necessárias para retirar o módulo criptográfico do estado de erro alcançado, e depois verificar se está ou não em conformidade com a documentação fornecida.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.50.08: Para cada estado de erro dos auto-testes que não pôde ser alcançado, deve-se avaliar o código fonte do módulo criptográfico e a documentação do projeto para determinar se as ações necessárias para retirar o módulo criptográfico do estado de erro alcançado estão em conformidade com a documentação fornecida.

REQUISITO I.51: O módulo não deve realizar qualquer operação criptográfica enquanto o estado de erro provocado por falhas em um auto-teste persistir.

Procedimentos de Ensaio para NSH 1:

EN.I.51.01: Analisar a documentação técnica, sendo que as seguintes funções criptográficas devem estar incluídas na lista de funções inibidas quando o módulo criptográfico estiver num estado de erro:

- Cifrar;
- Decifrar;
- Geração segura de resumos criptográficos (*secure message hashing*);
- Verificação e criação de assinaturas digitais;
- Outras operações que necessitam do uso de criptografia.

EN.I.51.02: Provocar os estados de erro dos auto-testes suportados pelo módulo criptográfico 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.I.51.03: Verificar se quando o módulo criptográfico é conduzido a 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.I.51.04: Para cada estado de erro dos auto-testes que não pôde ser alcançado, avaliar o código fonte do módulo criptográfico 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 I.52: A documentação técnica do módulo criptográfico deve incluir descrições sobre:

- Os auto-testes realizados pelo módulo criptográfico dentro das categorias citadas no **REQUISITO I.50**;
- os estados de erro que o módulo criptográfico alcança quando um auto-teste falha;
- as condições e ações necessárias para retirar os estados de erro e reiniciar a operação normal do módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.52.01: Verificar se a documentação técnica atende ao **REQUISITO I.52.**

2.2.9 Algoritmos criptográficos obrigatórios

REQUISITO I.53: O módulo criptográfico deve suportar os seguintes sistemas criptográficos:

- Criptografia de dados:
  - DES (*Data Encryption Standard*) no modo CBC, apenas para uso legado (conforme padrão NIST FIPS PUB 46-3);
  - *Triple*-DES (3DES ou TDES) no modo CBC (conforme padrão NIST FIPS PUB 46-3);
  - RSA com tamanho mínimo de chaves de 1024 bits (conforme padrões NIST FIPS PUB 186-2 e PKCS #1 v. 2.1).
- Autenticação de entidades com criptografia de Chaves Públicas:
  - RSA com tamanho mínimo de chaves de 1024 bits (conforme padrões NIST FIPS PUB 186-2 e PKCS #1 v. 2.1).
- Resultado *Hash*:
  - SHA-1 (*Secure Hash Algorithm*) segundo padrão NIST FIPS PUB 180-2.

Procedimentos de Ensaio para NSH 1:

EN.I.53.01: Verificar se a documentação técnica descreve os sistemas criptográficos suportados pelo módulo.

EN.I.53.02: Executar testes de **criptografia de dados** verificando o suporte pelo módulo criptográfico dos algoritmos **DES e 3DES**. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências bibliográficas. 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 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.I.53.03: Executar testes de **criptografia de chave pública** verificando o suporte pelo módulo criptográfico do algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências bibliográficas. 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 assinaturas, que avalia a habilidade em gerar a assinatura correta que pode ser validada pela chave pública associada;
- Teste de verificação de assinaturas, que avalia a habilidade em reconhecer assinaturas válidas e inválidas.

EN.I.53.04: Executar testes de **resumo criptográfico de dados** verificando o suporte pelo módulo criptográfico do algoritmo SHA-1. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências bibliográficas. Os testes de **resumo criptográfico de dados** consistem em:

- Testes de mensagens curtas (*Short Message Test*), que avalia 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 avalia a exatidão na geração do resumo criptográfico para mensagens que contêm múltiplos blocos;
- Testes de mensagens geradas pseudo-aleatoriamente (*Pseudorandomly generated messages test*), que verifica a exatidão dos resumos criptográficos de dados para mensagens geradas pseudo-aleatoriamente.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.53.05: Executar testes de **criptografia de chave pública** verificando o suporte pelo módulo criptográfico do algoritmo RSA. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências bibliográficas. Os testes de **criptografia de chave pública** consistem em testar a geração de chaves, que avalia a habilidade de gerar os valores corretos dos componentes do algoritmo.

RECOMENDAÇÃO I.1: De forma opcional, é recomendado que o módulo criptográfico também possa suportar os seguintes sistemas criptográficos:

- Criptografia de dados:
  - AES (*Advanced Encryption Standard*) com tamanho mínimo de chaves de 128 bits (conforme padrão NIST FIPS PUB 197).
- Autenticação de entidades com criptografia de Chaves Públicas:
  - DSA (*Digital Signature Algorithm*) com tamanho mínimo de chaves de 512 bits (conforme padrão NIST FIPS PUB 186-2).
- Resultado *Hash* segundo o padrão NIST FIPS PUB 180-2:
  - SHA-224;
  - SHA-256;
  - SHA-384;
  - SHA-512.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.REC.I.01.01: Verificar se a documentação técnica descreve os sistemas criptográficos suportados pelo módulo.

EN.REC.I.01.02: Executar testes de **criptografia de dados** verificando o suporte pelo módulo criptográfico do algoritmo **AES**. Este ensaio deve estar baseado nos testes de validação publicados pelo NIST, conforme documentos listados na seção de referências bibliográficas. 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 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.REC.I.01.03: Verificar se a documentação técnica descreve algoritmos opcionais para geração de resumos criptográficos de dados.

EN.REC.I.01.04: Repetir o ensaio **EN.I.01.04** para os algoritmos **SHA-224, SHA-256**, **SHA-384** e **SHA-512**.

2.2.10 Requisitos de PIN e PUK

2.2.10.1 PIN

REQUISITO I.54: No módulo criptográfico, o uso da chave assimétrica privada deve ser habilitado apenas nos casos de identificação e autenticação bem sucedida do papel de acesso Usuário, ou seja, somente após a inserção correta do PIN por parte da entidade usuária externa.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.54.01: Verificar se a documentação técnica descreve quais papéis de acesso pode habilitar o uso da chave assimétrica privada.

EN.I.54.02: Autenticar-se com sucesso no módulo criptográfico utilizando o papel "Usuário". Logo após, com a chave assimétrica privada habilitada para uso, realizar operações criptográficas e verificar se tais operações foram concluídas com sucesso.

EN.I.54.03: Verificar se a chave assimétrica privada não está habilitada para uso nos dois casos seguintes:

- Falha na autenticação no módulo criptográfico para o papel de acesso "Usuário"; e

- Autenticação no módulo criptográfico com outros papéis de acesso diferentes de "Usuário".

REQUISITO I.55: O PIN que habilita acesso ao papel usuário deve ser escolhido, exclusivamente, pela entidade usuária externa do módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.55.01: Verificar se a documentação técnica descreve os métodos de escolha do PIN.

EN.I.55.02: Realizar, por meio de ferramenta específica, a autenticação do papel de acesso "Usuário", e verificar se o módulo criptográfico permite que o PIN seja trocado e escolhido exclusivamente pelo usuário.

2.2.10.2 Bloqueio do PIN

REQUISITO I.56: Por questões de segurança (contra ataques de adivinhação do PIN por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PIN do papel de acesso usuário após, no máximo, 5 tentativas mal sucedidas.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.56.01: Verificar se a documentação técnica descreve critérios de bloqueio de PIN.
EN.I.56.02: Provocar falhas de autenticação informando um PIN incorreto ao módulo criptográfico, verificando o atendimento quanto ao **REQUISITO I.56.**

2.2.10.3 Troca do PIN

REQUISITO I.57: Quando aplicável, o módulo criptográfico deve forçar que, no primeiro acesso, o proprietário altere o PIN padrão.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.57.01: Verificar se a documentação técnica descreve, quando aplicável, a obrigatoriedade de troca do PIN padrão no primeiro acesso ao módulo criptográfico.

EN.I.57.02: Com um módulo criptográfico em estado inicial, verificar que, no primeiro acesso, é forçado a trocar o PIN padrão.

REQUISITO I.58: O módulo criptográfico deve possibilitar a entidade usuária externa alterar o PIN do papel de acesso usuário, a qualquer momento, por sua própria iniciativa. Nesta situação, tal alteração deve ocorrer somente mediante uma inserção correta do PIN atual e duas inserções do novo PIN escolhido.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.58.01: Verificar se a documentação técnica descreve os métodos de troca do PIN.

EN.I.58.02: Iniciar uma operação de troca do PIN, verificando o atendimento quanto ao **REQUISITO I.58.**

2.2.10.4 Reinicialização do papel de acesso "Usuário"

REQUISITO I.59: O papel de acesso "Usuário", e conseqüentemente o valor do PIN associado, nunca deve ser reinicializado individualmente. Quando o papel de acesso "Usuário" for reinicializado, as chaves criptográficas associadas devem ser eliminadas.

Procedimentos de Ensaio para NSH 1:

EN.I.59.01: Verificar se a documentação técnica descreve os métodos de reinicialização do papel de acesso "Usuário".

EN.I.59.02: Reinicializar o módulo criptográfico de modo que o papel de acesso "Usuário" seja reinicializado, e verificar, por meio de ferramenta específica, se as chaves criptográficas associadas foram eliminadas.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.59.03: Verificar, por meio de inspeção direta do código fonte do módulo criptográfico, os métodos de reinicialização do papel de acesso "Usuário", e se tais métodos estão em conformidade com o **REQUISITO II.08** e documentação fornecida.

REQUISITO I.60: Para possibilitar a reutilização do módulo criptográfico pelo usuário, a reinicialização do papel de acesso "usuário" e conseqüentemente o valor do PIN e chaves criptográficas, deve ser realizada mediante inserção correta do PUK pela entidade usuária externa.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.60.01: Verificar se a documentação técnica descreve a possibilidade de reutilização do módulo criptográfico quando ocorrer a reinicialização do papel de acesso "Usuário".

EN.I.60.02: Reinicializar o papel de acesso "Usuário" do módulo criptográfico, e depois verificar se é possível sua reutilização com posterior escolha de novo PIN.

EN.I.60.03: Realizar operações criptográficas e verificar se foram completadas de forma bem sucedida utilizando o novo PIN escolhido.

2.2.10.5 PUK

DEFINIÇÃO: O PUK (PIN *Unlock Key*) é um código alfanumérico usado como chave para habilitar o desbloqueio e/ou alteração do PIN. Neste documento, o PUK será considerado como o PIN do oficial de segurança.

REQUISITO I.61: O módulo criptográfico deve permitir ao usuário, após informar corretamente o PUK, desbloquear e/ou trocar o PIN corrente.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.61.01: Verificar se a documentação técnica descreve as formas de desbloqueio e/ou troca do PIN corrente.

EN.I.61.02: Bloquear o PIN corrente e verificar se é possível desbloquear e/ou trocar por meio da inserção correta do PUK. Após tal procedimento, verificar se o PIN corrente foi desbloqueado e/ou trocado de forma bem sucedida realizando alguma operação criptográfica.

2.2.10.6 Bloqueio do PUK

REQUISITO I.62: Por questões de segurança (contra ataques de adivinhação do PUK por meio de sucessivas tentativas), o módulo criptográfico deve bloquear o PUK após, no máximo, 5 tentativas mal sucedidas.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.62.01: Verificar se a documentação técnica descreve os critérios de bloqueio do PUK.

EN.I.62.02: Provocar o bloqueio do PUK no módulo criptográfico, verificando o atendimento quanto ao **REQUISITO II.11.**

2.2.10.7 Troca do PUK

REQUISITO I.63: O módulo criptográfico deve possibilitar a alteração do PUK, a qualquer momento, por iniciativa da entidade usuária externa, sendo que tal alteração deve ocorrer somente mediante a inserção correta do PUK anterior. O PUK não pode ser alterado por outro modo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.63.01: Verificar se a documentação técnica descreve os métodos de alteração do PUK.

EN.I.63.02: Iniciar uma operação de troca do PUK, verificando o atendimento quanto ao **REQUISITO I.63.**

2.2.10.8 Cachê dos códigos PIN e PUK

O "Provedor de Serviços" (PS) pode realizar o cachê de código PIN somente em uma mesma sessão de aplicação.

Os requisitos técnicos abordados nesta seção são contextualizados na CSP do cartão criptográfico ICP.

REQUISITO I.64: O código PUK nunca deve ser mantido em cachê no Provedor de Serviços.

Procedimentos de Ensaio para NSH 1:

EN.I.64.01: Verificar se a documentação técnica descreve a não manutenção do código PUK em cache.

EN.I.64.02: Por meio de uma aplicação específica, executar a técnica de *dump* de memória no equipamento de ensaio, e depois verificar nos dados de memória coletados se há indícios do código PUK em cache.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.64.03: Verificar, por meio de inspeção direta do código fonte de todo software que manipula o PUK, se não há qualquer forma de armazenamento em cache do código PUK.

REQUISITO I.65: O Provedor de Serviços pode manter em cachê o código PIN desde que garanta a eliminação do PIN no cachê nas seguintes situações:

- Sempre que o módulo criptográfico for desconectado de sua interface;
- sempre que a aplicação associada for encerrada.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.65.01: Verificar se a documentação técnica descreve as situações nas quais o código PIN:

- é mantido em cache;
- deve ser eliminado do cache.

EN.I.65.02: Avaliando o cache do código PIN, deve-se realizar, por meio de uma aplicação específica, uma seqüência de operações criptográficas que necessite do uso do PIN e verificar se, após a primeira operação criptográfica, o PIN não é mais solicitado.

EN.I.65.03: Desconectar o módulo criptográfico, conectar novamente e verificar a solicitação do PIN antes da realização da primeira operação criptográfica.

EN.I.65.04: Por meio de uma aplicação específica, executar a técnica de *dump* de memória no equipamento de ensaio, e depois verificar nos dados de memória coletados se há indícios do código PIN em cachê.

EN.I.65.05: Encerrar a aplicação corrente, iniciar novamente e verificar a solicitação do PIN antes da realização da primeira operação criptográfica.

REQUISITO I.66: A eliminação do código PIN presente no cachê deve ser realizada com sobrescrita de seu valor.

Procedimentos de Ensaio para NSH 1:

EN.I.66.01: Verificar se a documentação técnica descreve os métodos de eliminação do código PIN presente no cache.

EN.I.66.02: Por meio de uma aplicação específica, executar a técnica de *dump* de memória no equipamento de ensaio, e depois verificar nos dados de memória coletados se há indícios da eliminação do código PIN em cache por sobrescrita.

Procedimentos de Ensaio para NSH 2 e 3:

EN.I.66.03: Verificar, por meio de inspeção direta do código fonte de todo software que trata do cache do PIN, se a eliminação do código PIN em cache é realizada por meio da técnica de sobrescrita.

RECOMENDAÇÃO I.2: Apesar de permitida, a funcionalidade de cachê deve ser evitada sempre que possível. Quando utilizada, é recomendada a implementação de controles adicionais, como por exemplo:

- Tempo de Vida (*Time To Live* - TTL): tempo de duração máxima do PIN no cachê;
- confirmação do uso da chave pelo usuário: o usuário deve ser notificado antes da utilização da chave privada, devendo o usuário ter a opção de concordar ou não (confirmar) com o uso da chave privada.

Procedimentos de Ensaio para NSH 1:

EN.REC.I.02.01: Verificar se a documentação técnica descreve controles adicionais de segurança que são empregados quando a funcionalidade do cache é utilizada.

EN.REC.I.02.02: Verificar, por meio de uma aplicação específica, se o tempo de duração máxima do PIN em cache está em conformidade com a documentação.

EN.REC.I.02.03: Quando a funcionalidade de cache for utilizada, verificar se é possível receber uma notificação por parte do sistema criptográfico sobre o uso da chave privada.

Procedimentos de Ensaio para NSH 2 e 3:

EN.REC.I.02.04: Quando aplicável, verificar, por meio de inspeção direta do código fonte de todo software que trata dos controles adicionais de cachê do PIN, se tais controles estão implementados de forma adequada e conforme documentação.

2.2.10.9 Qualidade dos códigos PIN e PUK

Os requisitos técnicos abordados nesta seção são contextualizados na CSP do cartão criptográfico ICP.

REQUISITO I.67: O Provedor de Serviços deve aplicar controles de qualidade no momento da definição dos códigos PIN e PUK pela entidade usuária externa. Deve implementar os seguintes controles:

- Tamanho mínimo de 4 a 8 caracteres;
- sensibilidade a letras maiúsculas e minúsculas do alfabeto português (*Case Sensitive*).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.67.01: Verificar se a documentação técnica descreve os controles de qualidade aplicados à definição dos códigos PIN e PUK.

EN.I.67.02: Realizar a troca do PIN, por meio de aplicação específica baseada no "Provedor de Serviços", e verificar por meio de comandos APDU se os controles de qualidade aplicados à definição do código PIN atendem ao **REQUISITO II.16**.

EN.I.67.03: Realizar a troca do PUK, por meio de aplicação específica baseada no "Provedor de Serviços", e verificar por meio de comandos APDU se os controles de qualidade aplicados à definição do código PUK atendem ao **REQUISITO II.16**.

2.2.11 Identificação de hardware, software e firmware

REQUISITO I.68: O *token* criptográfico deve possuir elementos que permitam a identificação das versões e revisões dos seguintes componentes do módulo criptográfico:

- Hardware;
- software;
- firmware.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.68.01: Verificar se a documentação atende ao **REQUISITO I.68.**

REQUISITO I.69: A documentação técnica do módulo criptográfico entregue para fins de homologação deve descrever as versões dos seguintes componentes:

- Hardware;
- software;
- firmware.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.I.69.01: Verificar se a documentação atende ao **REQUISITO I.69.**

2.3 Requisitos de interoperabilidade

REQUISITO II.1: *Tokens* criptográficos, devem atender aos requisitos de interoperabilidade ora estabelecidos, derivados e complementares aos padrões ISO/IEC 7816 e PS/SC versão 1.0, conforme descrito nos itens a seguir.

Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.3.**

2.3.1 Módulo criptográfico

O objetivo desta seção é detalhar o conjunto de requisitos técnicos necessários para propiciar a interoperabilidade de módulos criptográficos conectados a um computador.
A Figura 2 ilustra a arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC, por meio da qual aplicações podem invocar operações (criptográficas ou não) em módulos criptográficos, usando componentes do tipo SP (*Service Providers*). O componente Gerente de Recursos (*Resource Manager*) é responsável por controlar o acesso aos recursos.
Além disso, a Figura 2 também ilustra um mapeamento entre a arquitetura de interoperabilidade de cartões ISO 7816 e PC/SC e o conjunto de padrões ISO/IEC da família 7816.

Portanto, conforme indicado na Figura 2, o módulo criptográfico limita seu escopo em analisar um conjunto de comandos básicos de interoperabilidade definidos pelo padrão ISO/IEC 7816-4. A análise de tais comandos, como requisito inicial de interoperabilidade, propiciará ainda a verificação de conformidade aos seguintes aspectos do padrão ISO/IEC 7816-4:

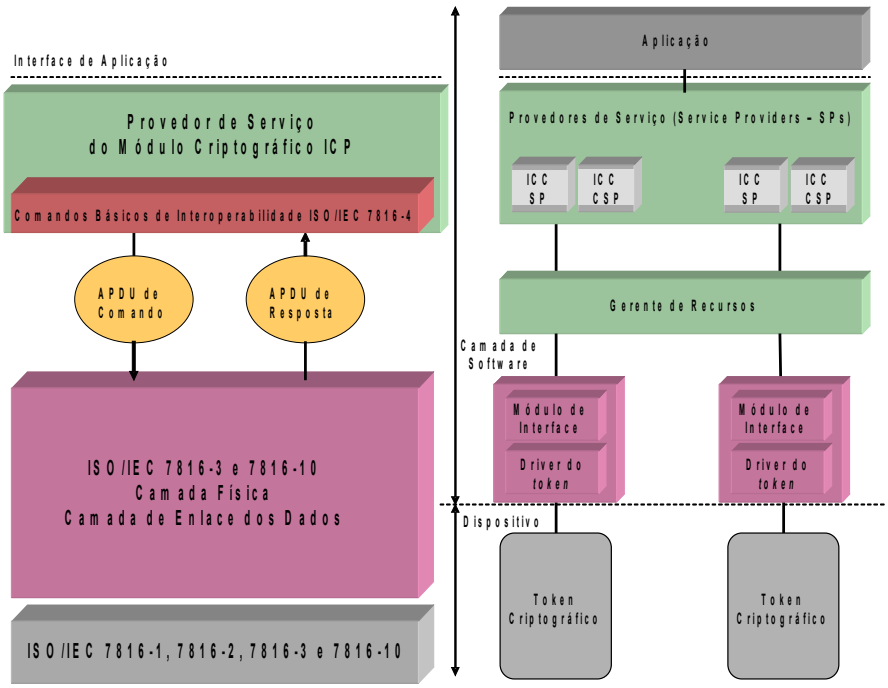

Figura 2. Arquitetura de interoperabilidade de *tokens* criptográficos ISO 7816 e PC/SC

- Conteúdo dos comandos e respostas (*Application Protocol Data Unit* - APDU) transmitidas ao módulo criptográfico e vice-versa;
- estrutura dos arquivos e dados usados no processamento dos comandos básicos de interoperabilidade;
- métodos de acesso aos arquivos e dados no módulo criptográfico.

Este documento não restringe a verificação dos comandos básicos de interoperabilidade em relação à plataforma e versão de sistema operacional, ou seja, os testes de conformidade com os comandos básicos de interoperabilidade poderão ser realizados em diferentes plataformas e versões de sistemas operacionais atualmente disponíveis (tais como, Microsoft Windows, Linux e UNIX).

2.3.1.1 Organização de arquivos e estrutura de dados

REQUISITO II.2: Um módulo criptográfico deve seguir as estruturas de dados de organização de arquivos conforme os requisitos e convenções definidas na seção 5.1 do padrão ISO/IEC 7816-4.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.02.01: Analisar a documentação técnica referente a este requisito, verificando se os seguintes itens estão em conformidade com a norma ISO/IEC 7816-4:

- Organização dos arquivos;
- Métodos de seleção de arquivos;
- Estruturas de arquivo elementar;
- Métodos de seleção de dados;
- Seleção de registros;
- Seleção de unidade de dados;
- Seleção de objeto de dados;
- Informação de controle de arquivo.

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO II.07**.

REQUISITO II.3: A documentação técnica deve descrever a organização de arquivos e estrutura de dados utilizada pelo módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.03.01: Verificar se a documentação técnica atende ao **REQUISITO II.3.**

2.3.1.2 Estrutura da mensagem de APDU

Uma aplicação necessita enviar um comando para ser processado pelo módulo criptográfico, o qual, por sua vez, retorna a respectiva resposta. Essa correspondência entre um comando emitido e sua respectiva resposta é denominada de "par comando-resposta".
Uma APDU (*application protocol data unit*) contém um comando ou uma resposta trocada com o módulo criptográfico.
Uma APDU de comando consiste de duas partes: um cabeçalho obrigatório de 4 bytes e um corpo de tamanho variável. Da mesma forma, uma APDU de resposta consiste de duas partes: um corpo de tamanho variável e um anexo obrigatório (*trailer*) de 2 bytes.

REQUISITO II.4: Um módulo criptográfico deve seguir uma estrutura de APDU (comando e resposta) conforme os requisitos e convenções definidas na seção 5.3 do padrão ISO/IEC 7816-4.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.04.01: Analisar a documentação técnica referente a este requisito, verificando se os seguintes itens estão em conformidade com a norma ISO/IEC 7816-4:

- APDU do tipo comando;
- Convenções de decodificação para parâmetros de comando APDU;
- APDU do tipo resposta.

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO II.07**.

REQUISITO II.5: A documentação técnica deve descrever a estrutura da mensagem APDU.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.05.01: Verificar se a documentação técnica atende ao **REQUISITO II.5.**

2.3.1.3 Comandos básicos de interoperabilidade

Com o intuito de buscar a interoperabilidade entre provedores de serviço, leitoras, módulos criptográficos e aplicações, este documento reconhece a iniciativa do padrão ISO/IEC 7816, e define a obrigatoriedade do atendimento a um conjunto mínimo de comandos.

REQUISITO II.7: Um módulo criptográfico deve suportar, no mínimo, o conjunto de comandos apresentados na Tabela 2.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.07.01: Analisar a documentação técnica referente a este requisito, verificando para cada comando básico suportado:

- Definição e escopo de uso;
- As condições de uso e segurança;
- Codificação da mensagem de comando APDU;

- Codificação da mensagem de resposta APDU;
- Condições de estado, informando os códigos retornados por APDU de resposta e as respectivas descrições destes códigos.

EN.II.07.02: Por meio de ferramenta específica, compor cada comando básico de interoperabilidade suportado pelo módulo criptográfico. Em seguida, tentar executar tais comandos e verificar se estão em conformidade com as funcionalidades previstas na Tabela 2:

- Estrutura de dados;
- Estrutura de APDU (comando e resposta);
- Codificação dos campos de dados das APDUs, cabeçalhos dos comandos e porções finais das respectivas respostas;
- Definição e escopo dos comandos;
- Condições de uso e segurança; e
- Condições de estado.

REQUISITO II.8: Caso um ou mais comandos descritos na Tabela 2 não sejam suportados pelo módulo criptográfico, a documentação técnica deve justificar a ausência.

Tabela 2. Conjunto mínimo de comandos básicos de interoperabilidade para módulos criptográficos

Comando	Definição e escopo	Exemplo (ISO 7816-4)
1	Comando para leitura de dados de um arquivo binário, iniciando a leitura de uma posição (offset) especificada por um parâmetro passado via comando.	READ BINARY
2	Comando para recuperar ou ler objetos de dados.	GET DATA
3	Comando para armazenar ou escrever objetos de dados.	PUT DATA
4	Comando para selecionar um arquivo.	SELECT FILE
5	Comando para comparar um segredo enviado via interface (PIN, por exemplo) com um valor de referência já armazenado no módulo criptográfico.	VERIFY

Comando	Definição e escopo	Exemplo (ISO 7816-4)
6	Comando para autenticar uma entidade externa perante um módulo criptográfico.	EXTERNAL AUTHENTICATE
7	Comando para requerer do módulo criptográfico um número randômico (desafio – "challenge") para ser usado posteriormente para fins de autenticação.	GET CHALLENGE

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.08.01: Verificar se a documentação técnica atende ao **REQUISITO II.8.**

REQUISITO II.9: A parte interessada deve prover os meios necessários em termos de informações e bibliotecas de software para que comandos básicos de interoperabilidade suportados possam ser verificados no módulo criptográfico.

Nota: requisito é testado como parte do **REQUISITO II.07**.

REQUISITO II.10: A documentação técnica deve descrever todos os comandos suportados pelo módulo criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.10.01: Verificar se a documentação técnica descreve comandos APDU proprietários suportados pelo *token* criptográfico assim como suas respectivas funcionalidades.

EN.II.10.02: Por meio de ferramenta específica executar cada comando proprietário descrito na documentação técnica e avaliar se suas respectivas funcionalidades estão condizentes com a documentação.

2.3.2 Conexão de *tokens* em computadores pessoais

Esta seção detalha os requisitos de interoperabilidade que devem ser atendidos por *tokens* criptográficos quando conectados em computadores pessoais (PC – *Personal Computers*). Tais requisitos foram derivados do padrão PC/SC versão 1.0, de dezembro de 1997, a saber:

- *Interoperability Specification for ICCs and Personal Computer Systems - Part 3*. "*Requirements for PC-Connected Interface Devices*";
- *Interoperability Specification for ICCs and Personal Computer Systems - Part 4*. "*IFD Design Considerations and Reference Design Information*".

Os requisitos de interoperabilidade necessários para um *token* estão concentrados em três componentes (veja Figura 3):

- Leitora virtual: dispositivo lógico que provê a interface com o módulo criptográfico;
- driver do *token*: corresponde a um driver instalado no PC que permite ao sistema operacional e outros componentes de software se comunicarem com o *token* (módulo criptográfico);
- módulo de Interface: corresponde à interface de programação hospedada em um PC que realiza interações entre o componente "Driver do *token*" e as camadas superiores.

Portanto, conforme ilustrado na Figura 3, esta seção restringe seu escopo em especificar requisitos de interoperabilidade que estão relacionados a:

- Leitora virtual;
- driver do *token*;
- módulo de interface;
- funcionalidades do módulo de interface.

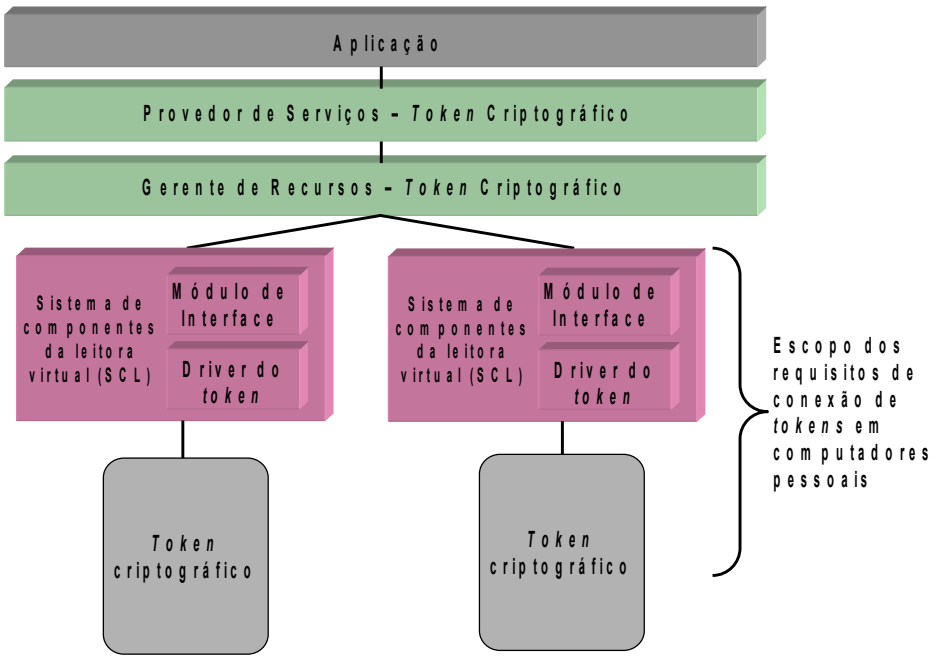

Figura 3. Componentes de *tokens* que devem atender aos requisitos de interoperabilidade especificados

2.3.2.1 Leitora virtual

REQUISITO II.11: O *token* se conecta a uma leitora virtual que é instalada no PC como um dispositivo virtual, a qual deve atender aos seguintes requisitos:

- Suportar comunicações de dados bidirecionais entre um *token* e um PC;
- incorporar as funcionalidades necessárias para suportar a interface disponível pelo componente "módulo de interface".

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.11.01: Verificar se a documentação técnica descreve os métodos de conexão entre a o *token* e um PC.

EN.II.11.02: Observar, por meio de ferramenta específica, a comunicação entre *token* criptográfico e PC, enviando comandos para o *token* e recebendo as respectivas respostas. Após observar as trocas de informações entre o *token* e o PC, verificar que a comunicação é bidirecional.

EN.II.11.03: Quanto às funcionalidades necessárias para suportar a interface disponível pelo componente "Módulo de Interface", este ensaio é verificado como parte das **Seções 2.3.2.3 e 2.3.2.4** deste documento.

2.3.2.2 Driver do *token*

REQUISITO II.12: Com relação ao canal de entrada e saída de dados (I/O) em um PC, pelo menos, a interface USB deve ser suportada pelo *token* e seu respectivo driver.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.12.01: Verificar se a documentação técnica descreve as interfaces suportadas pelo *token* e seu respectivo driver.

EN.II.12.02: Verificar, por meio da observação direta dos conectores e processo de instalação do driver, se o *token* suporta, pelo menos, a interface USB.

RECOMENDAÇÃO II.1: Considerando *tokens* criptográficos com interface USB, é recomendado, para fins de interoperabilidade, a implementação do padrão USB ICCD Revisão 1.0 [ICCD 1.0].

Procedimentos de Ensaio para NSH 1:

EN.II.19.01: Verificar se a documentação técnica descreve a compatibilidade do *token* criptográfico com o padrão USB ICCD Revisão 1.0.

EN.II.19.02: Por meio de ferramenta específica, estabelecer comunicação direta (em baixo nível) com o *token* criptográfico, e enviar instruções conforme o padrão USB ICCD Revisão 1.0. Uma vez que os dados das respostas a estas instruções foram obtidos, verificar a conformidade com o padrão USB ICCD Revisão 1.0.

Procedimentos de Ensaio para NSH 2 e 3:

EN.II.19.03: Verficar, por meio da análise direta do código fonte do driver do *token* criptográfico a conformidade com o padrão USB ICCD Revisão 1.0.

2.3.2.3 Módulo de interface

O módulo de interface corresponde a um software sendo executado em um PC que implementa uma interface padrão e independente tanto do hardware quanto do canal de I/O. Além disso, o módulo de interface também deve mapear as funcionalidades disponíveis pelo *token*.

REQUISITO II.13: A parte interessada possui a responsabilidade de criar os componentes "driver do *token*" e "módulo de interface", de tal forma que seja possível aos SPs (*Service Providers*) se comunicarem com um *token* criptográfico por meio da leitora virtual.

Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.3.2**.

REQUISITO II.14: Drivers de *tokens* criptográficos devem prover mecanismos de tratamento de erros.

Procedimentos de Ensaio para NSH 1:

EN.II.14.01: Analisar a documentação técnica referente a este requisito, e verificar se consta a descrição dos mecanismos de tratamento de erros relacionados ao driver do *token* criptográfico.

EN.II.14.02: Provocar erros relacionados ao driver do *token* criptográfico, e verificar se os mecanismos de tratamento de erros atuaram conforme documentação.

Procedimentos de Ensaio para NSH 2 e 3:

EN.II.14.03: Verficar, por meio da análise direta do código fonte do driver do *token* criptográfico, se os mecanismos de tratamento de erros estão implementadas conforme documentação.

2.3.2.4 Funcionalidades do módulo de interface

As funcionalidades descritas a seguir estão relacionadas aos requisitos de interoperabilidade, e devem estar visíveis por meio do componente "módulo de interface".

2.3.2.4.1 Funcionalidades obrigatórias

A - Características Operacionais

REQUISITO II.15: Em um dado instante, o módulo de interface deve suportar, no mínimo, uma conexão lógica e ativa entre uma aplicação e o *token*. Em outras palavras, o módulo de interface não necessita suportar múltiplas conexões ativas com uma aplicação. Entretanto, tal funcionalidade não deve impedir o gerenciamento de sessões conforme as características definidas pelo padrão ISO/IEC 7816-4.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.15.01: Verificar se a documentação técnica descreve o gerenciamento de sessões conforme as características definidas pelo padrão ISO/IEC 7816-4.
EN.II.15.02: Via API, estabelecer uma conexão lógica e ativa entre uma aplicação e o *token* criptográfico, conforme os passos descritos a seguir:

- Obter a lista de todas os *tokens* suportados pelo PC;
- Estabelecer uma conexão com um *token* escolhido.

EN.II.15.03: Baseando-se no ensaio **EN.II.15.02**, verificar que foi possível estabelecer uma conexão lógica com sucesso.

REQUISITO II.16: Se um módulo de interface suportar múltiplos *tokens*, ele deve apresentar uma conexão lógica independente para cada *token*. Além disso, neste caso, o módulo de interface deve também suportar uma funcionalidade que possibilite determinar a associação entre um dado *token* e sua respectiva conexão lógica.
A implementação de características relacionadas ao gerenciamento de sessões deve estar sob a responsabilidade do *token* criptográfico e seu respectivo provedor de serviços (SP – *Service Provider*).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.16.01: Verificar se a documentação técnica descreve o gerenciamento de múltiplos *tokens* pelo módulo de interface.

EN.II.16.02: Considerando múltiplos *tokens* conectados num PC, via API, estabelecer uma conexão lógica e ativa entre uma aplicação e cada *token* conectado. Em seguida, para as conexões lógicas estabelecidas com sucesso, verificar que tais conexões são independentes para cada *token*.

EN.II.16.03: Considerando múltiplos *tokens* conectadas a um PC, verificar se o módulo de interface permite, por meio de uma funcionalidade específica, associar uma conexão lógica estabelecida com um dado *token* conectado.

REQUISITO II.17: A documentação técnica do *token* deve descrever as características operacionais que estão implementadas no dispositivo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.17.01: Verificar se a documentação técnica atende ao **REQUISITO II.17.**

B – Enumeração das funcionalidades do *token*

REQUISITO II.18: O componente "Módulo de interface" deve prover uma interface que suporte a enumeração de funcionalidades (obrigatórias e opcionais). Tal interface deve estar disponível para requisição via SP do *token* criptográfico.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.18.01: Analisar a documentação técnica referente a este requisito, verificando as funcionalidades que podem ser enumeradas do módulo de interface.

EN.II.18.02: Via ferramenta específica, verificar se o módulo de interface permite, por meio de invocação de função em sua interface, enumerar as funcionalidades suportadas (obrigatórias e opcionais).

REQUISITO II.19: Em conformidade à codificação especificada pelo padrão PC/SC versão 1.0, parte 3, seção 3.1.2, tabela 3-1, no mínimo, uma invocação via SP deve retornar informações sobre:

- Fornecedor do *token*;
- comunicação;
- protocolos;
- gerenciamento de energia;
- características de garantia de segurança;
- características mecânicas;
- características específicas do fornecedor.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.19.01: Analisar a documentação técnica referente a este requisito, verificando as informações retornadas.

EN.II.19.02: Por meio de ferramenta específica, deve verificar se, no mínimo, as informações descritas no **REQUISITO II.19** são retornadas por invocação via Provedor de Serviços.

EN.II.19.03: Baseando-se no ensaio **EN.II.19.02**, verificar se as informações retornadas estão em conformidade com o padrão PC/SC versão 1.0, Parte 3, Seção 3.1.2 e Tabela 3-1.

REQUISITO II.20: A documentação técnica do *token* deve descrever todas as funcionalidades disponíveis no dispositivo, mostrando de forma clara a estrutura de dados utilizada (TLV, por exemplo).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.20.01: Verificar se a documentação técnica atende ao **REQUISITO II.20.**

REQUISITO II.21: A documentação técnica do *token* deve descrever as versões dos seguintes componentes:

- Hardware;
- software;
- firmware.

Procedimentos de Ensaio para NSH 1, 2 e 3:

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

REQUISITO II.22: A parte interessada deve prover os meios necessários para identificação pela entidade usuária externa das versões dos seguintes componentes do *token*:

- Hardware;
- software;
- firmware.

Procedimentos de Ensaio para NSH 1, 2 e 3:

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

2.3.2.4.2 Funcionalidades opcionais

Tokens podem implementar características que são específicas do fornecedor do dispositivo e cujas funcionalidades não foram definidas nesta especificação.

REQUISITO II.23: Características específicas do fornecedor do *token* devem ser isoladas de tal forma que não causem qualquer impacto nas funcionalidades definidas por este documento (Manual de Condutas Técnicas 3 – Volume I).

Nota: Este requisito não é testado separadamente e faz parte do **REQUISITO II.24**.

REQUISITO II.24: Características específicas do fornecedor do *token* devem ser isoladas de tal forma que não permitam que as funcionalidades definidas por este documento (Manual de Condutas Técnicas 3 – Volume I) sejam contornadas ou logradas.

Procedimentos de Ensaio para NSH 1:

EN.II.24.01: Verificar se a documentação técnica descreve detalhadamente as características específicas do fornecedor do *token*, assim como sua estrutura de dados e comandos.

EN.II.24.02: Por meio de aplicação específica, verificar o tráfego de informações entre o *token* e o PC, e verificar se as características específicas do fornecedor do *token* estão presentes.

Procedimentos de Ensaio para NSH 2:

EN.II.24.03: Basear-se nos resultados obtidos no ensaio **EN.II.24.02**, e com a análise do código fonte do driver da leitora, verificar como são tratadas as características específicas do fornecedor da leitora.

Procedimentos de Ensaio para NSH 3:

EN.II.24.04: Basear-se nos resultados obtidos no ensaio **EN.II.24.02**, e com a análise do código fonte do firmware do *token*, verificar o isolamento das características específicas do fornecedor do *token* e se estas oferecem qualquer risco de segurança para as funcionalidades definidas pelo Manual de Condutas Técnicas 3 – Volume I.

REQUISITO II.25: A documentação técnica do *token* deve descrever todas as características que são específicas do fornecedor e estejam implementadas no dispositivo.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.II.25.01: Verificar se a documentação técnica atende ao **REQUISITO II.25**.

2.4 Requisitos de Gerenciamento

REQUISITO III.1: O módulo criptográfico deve atender aos requisitos de gerenciamento ora estabelecidos, conforme descrito nos itens a seguir.

Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.4.**

2.4.1 Módulos Criptográficos

Os requisitos de gerenciamento fazem referência às funcionalidades que devem estar disponíveis ao proprietário do módulo criptográfico, permitindo executar operações de controle.

REQUISITO III.2: Funcionalidades de gerenciamento do módulo criptográfico devem estar disponíveis ao proprietário por meio de uma ferramenta específica ou utilitário. Tal utilitário deve ser provido pelo fornecedor do módulo criptográfico contendo, no mínimo, mas não limitado aos seguintes aspectos:

- Permitir a exportação de certificados digitais armazenados no módulo criptográfico;
- permitir a importação de certificados digitais para a área de armazenamento do módulo criptográfico;
- permitir a visualização de certificados digitais armazenados no módulo criptográfico;
- para cada certificado digital armazenado no módulo criptográfico, permitir que todos os campos contemplados pela ICP-Brasil sejam visualizados;

- permitir ao proprietário apagar chaves criptográficas e outros dados contidos no módulo criptográfico, segundo os procedimentos adequados de autenticação, caso seja necessário;
- permitir a troca do PIN por meio de confirmação e verificação, tanto do PIN atual, como por meio de duas inserções do novo PIN escolhido;
- permitir a eliminação do PIN somente mediante alerta e posterior confirmação do proprietário, conscientizando sobre o apagamento dos dados criptográficos associados;
- permitir a reutilização de módulos criptográficos.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.III.02.01: Verificar se a documentação técnica descreve as características do utilitário de gerenciamento do módulo criptográfico.

EN.III.02.02: Verificar se o utilitário de gerenciamento possui interface gráfica em idioma português do Brasil por meio de observação e inspeção direta na própria ferramenta.

EN.III.02.03: Usar um módulo criptográfico com certificado digital já armazenado, e depois via utilitário de gerenciamento executar os passos necessários para a exportação do certificado digital armazenado no módulo criptográfico. Após exportar o certificado digital, verificar se o processo foi bem sucedido comparando o certificado exportado com aquele armazenado no módulo criptográfico.

EN.III.02.04: Usar um módulo criptográfico, e depois via utilitário de gerenciamento executar os passos necessários para a importação de um certificado digital escolhido. Após importar o certificado digital para o módulo criptográfico, verificar se o processo foi bem sucedido comparando o certificado importado com o original.

EN.III.02.05: Obter acesso ao módulo criptográfico via utilitário de gerenciamento, escolher um certificado armazenado, e depois executar os passos necessários para a visualizar tal certificado. Logo após, finalizar este ensaio visualizando diretamente o certificado digital escolhido anteriormente.

EN.III.02.06: Obter acesso ao módulo criptográfico via utilitário de gerenciamento, escolher um certificado ICP-Brasil armazenado, e depois executar os passos necessários para a visualizar tal certificado. Logo após, finalizar este ensaio visualizando diretamente no certificado os campos contemplados pela ICP-Brasil.

EN.III.02.07: Usar um módulo com chaves criptográficas armazenadas, e depois via utilitário de gerenciamento executar os passos necessários para apagar as chaves ou outros dados contidos. Logo após, verificar por meio do utilitário de gerenciamento se as chaves criptográficas ou dados contidos que foram selecionados estão ausentes do módulo.

EN.III.02.08: Usar um módulo criptográfico com certificado digital armazenado, e depois via utilitário de gerenciamento executar os passos necessários para trocar o PIN corrente do usuário. Durante este processo, verificar que a troca do PIN foi realizada por meio de confirmação e verificação, tanto do PIN atual como por meio de duas inserções do novo PIN escolhido.

EN.III.02.09: Usar um módulo criptográfico com certificado digital armazenado, e depois via utilitário de gerenciamento executar os passos necessários para eliminar o PIN corrente do usuário. Durante este processo, verificar que a eliminação do PIN foi realizada somente mediante alerta e posterior confirmação por parte do proprietário, conscientizando-o sobre o apagamento dos dados criptográficos associados. Além disso, também verificar por meio do utilitário de gerenciamento se o certificado digital e as chaves criptográficas associadas ao PIN eliminado estão ausentes do módulo.

EN.III.02.10: Usar um módulo criptográfico, e depois via utilitário de gerenciamento executar as funcionalidades disponíveis para permitir a reutilização do módulo criptográfico. Logo após, verificar se é possível reutilizar o módulo criptográfico.

2.5 Requisitos funcionais

Os requisitos funcionais dizem respeito à avaliação de funções relacionadas à arquitetura do módulo criptográfico que podem ser invocadas por aplicações de usuários por meio de uma interface de alto nível denominada de API (*Application Programming Interface*).

REQUISITO IV.1: O módulo criptográfico deve atender aos requisitos funcionais ora estabelecidos, conforme descrito nos itens a seguir. No escopo deste documento, pelo menos uma das seguintes API serão consideradas para análise dos requisitos funcionais:

- Microsoft CryptoAPI;
- PKCS#11;
- JCE.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.IV.01.01: Verificar se a documentação técnica descreve as APIs que devem ser consideradas na análise dos requisitos funcionais.

Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.5.**

REQUISITO IV.2: No mínimo, os requisitos funcionais devem estar disponíveis por invocação, via API, em uma das seguintes plataformas de sistemas operacionais:

- Linux kernel 2.4 ou versões superiores;
- Microsoft Windows 2000 / XP ou versões superiores.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.IV.02.01: Verificar se a documentação técnica descreve as plataformas de sistemas operacionais que devem ser consideradas na análise dos requisitos funcionais.
Nota: Este requisito não é testado separadamente e faz parte da **Seção 2.5.**

2.5.1 Gerenciamento de chaves criptográficas

REQUISITO IV.3: Os seguintes requisitos funcionais de gerenciamento de chaves criptográficas devem estar disponíveis por invocação via API do sistema operacional:

- Gerar chave criptográfica assimétrica de forma randômica no módulo criptográfico;
- destruir chave criptográfica assimétrica com sobrescrita de valores;
- recuperar parâmetros sobre uma determinada chave criptográfica assimétrica, tais como:

- algoritmo;
- expoente público (RSA);
- módulo (RSA);
- tamanho da chave;
- permissões.

Procedimentos de Ensaio para NSH 1:

EN.IV.03.01: Analisar se a documentação técnica descreve os requisitos funcionais de gerenciamento de chaves criptográficas.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta de software ou utilitário desenvolvido pelo LEA, baseando-se nas APIs e nas plataformas de sistemas operacionais indicadas na documentação técnica apresentada para os **REQUISITOS IV.1 e IV.2** deste documento.

EN.IV.03.02: Gerar chaves criptográficas assimétricas de forma aleatória no módulo criptográfico. Após a geração, verificar se a chave gerada está presente no módulo criptográfico e executar operações criptográficas que validem as chaves assimétricas.

EN.IV.03.03: Escolher uma determinada chave criptográfica assimétrica e depois recuperar seus parâmetros associados. Após a recuperação, verificar que os parâmetros obtidos correspondem à chave selecionada.

Procedimentos de Ensaio para NSH 2 e 3:

EN.IV.03.04: Verificar, por meio de inspeção direta do código fonte do módulo criptográfico, se a destruição de chaves criptográficas assimétricas é realizada por meio da técnica de sobrescrita de valores.

2.5.2 Exportação e importação de chaves criptográficas

REQUISITO IV.4: Os seguintes requisitos funcionais de exportação e importação devem estar disponíveis por invocação via API do sistema operacional:

- Exportar chave criptográfica assimétrica pública do módulo criptográfico;
- exportar certificado digital do módulo criptográfico;
- exportar cadeia de certificação do módulo criptográfico;
- importar/exportar cadeia de certificação em/de módulo criptográfico;
- importar certificado digital para o módulo criptográfico segundo padrão X.509 versão 3;
- importar cadeia de certificação para o módulo criptográfico;
- permitir gravação no módulo criptográfico de certificados digitais compatíveis às normas ICP-Brasil e que usam a recomendação ITU-T X.509 versão 3 (conforme perfil estabelecido na RFC 3280).

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.IV.04.01: Analisar se a documentação técnica descreve os requisitos de exportação e importação.

Nota: Os ensaios referentes a esta seção serão realizados por meio de uma ferramenta de software ou utilitário desenvolvido pelo LEA, baseando-se nas APIs e nas plataformas de sistemas operacionais indicadas na documentação técnica apresentada para os **REQUISITOS IV.1 e IV.2** deste documento.

EN.IV.04.02: Exportar a chave criptográfica assimétrica pública do módulo criptográfico. Após a exportação, verificar se a chave foi exportada e executar operações criptográficas que validem a chave.

EN.IV.04.03: Exportar certificado digital do módulo criptográfico segundo formato PKCS#7. Após a exportação, verificar se o certificado foi exportado no formato PKCS#7, e se tal certificado corresponde àquele selecionado durante a operação de exportação.

EN.IV.04.04: Exportar cadeia de certificação do módulo criptográfico. Após a exportação, verificar se a cadeia de certificação exportada é válida e corresponde àquela selecionada durante a operação de exportação.

EN.IV.04.05: Importar/exportar cadeia de certificação para/do módulo criptográfico. Após a importação/exportação, verificar se a cadeia de certificação importada/exportada é válida e corresponde àquela selecionada durante a operação de exportação.

EN.IV.04.06: Importar certificado digital para o módulo criptográfico segundo padrões X.509 versão 3 e PKCS#7. Após a importação, verificar se o certificado foi importado nos padrões requisitados, e se tal certificado corresponde àquele selecionado durante a operação de importação.

EN.IV.04.07: Importar cadeia de certificação para o módulo criptográfico. Após a importação, verificar se a cadeia de certificação é válida e corresponde àquela selecionada durante a operação de importação.

2.5.3 Requisitos de armazenamento

REQUISITO IV.5: O módulo criptográfico deve possuir capacidade de armazenamento para certificados digitais de, no mínimo, 16 Kbytes.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.IV.05.01: Analisar se a documentação técnica descreve a capacidade de armazenamento do módulo criptográfico reservada para certificados digitais.

EN.IV.05.02: Por meio de aplicação específica (por exemplo, utilitário de gerenciamento), gravar certificados digitais de tamanhos conhecidos na área de armazenamento do módulo criptográfico, totalizando um volume de dados escritos maior que 16Kbytes. Após a gravação, verificar que foi possível a gravação de, pelo menos, 16Kbytes de memória contendo certificados digitais na área de armazenamento do módulo.

2.6 Requisitos de documentação

Os requisitos de documentação dizem respeito aos documentos e suas características que devem acompanhar o objeto de homologação (*token* criptográfico) na sua forma comercial.

REQUISITO V.1: O responsável deve fornecer, no mínimo, as seguintes informações, em idioma português do Brasil, na documentação que acompanha o objeto de homologação na sua forma comercial:

- Utilização;
- instalação dos CSPs;
- instalação e uso da ferramenta de gerenciamento;
- especificações técnicas;
- plataformas de sistemas operacionais compatíveis;
- guia de desenvolvimento;
- bibliotecas de software disponíveis.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.V.01.01: Verificar se a documentação que acompanha o produto atende ao **REQUISITO V.1**.

REQUISITO V.2: Toda documentação relacionada ao software deve informar as plataformas de sistemas operacionais suportadas e os requisitos de ambiente operacional necessários para sua operação.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.V.02.01: Verificar se a documentação que acompanha o produto atende ao **REQUISITO V.2**.

REQUISITO V.3: Todo software deve:

- Possuir ou possibilitar a configuração da sua interface gráfica em idioma português do Brasil;
- possuir tópicos de ajuda em idioma português do Brasil;
- permitir a visualização da versão do software e o nome de seu responsável.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.V.03.01: Verificar se os softwares que acompanham o produto atendem ao **REQUISITO V.3**.

REQUISITO V.4: As versões dos componentes de software devem estar descritas à entidade usuária externa na documentação que acompanha o produto.

Procedimentos de Ensaio para NSH 1, 2 e 3:

EN.V.04.01: Verificar se os softwares que acompanham o produto atendem ao **REQUISITO V.4**.

3 Referências bibliográficas

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

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

[ICCD 1.0] UNIVERSAL SERIAL BUS. ***Specification for USB Integrated Circuit(s) Card Devices.*** *Revision 1.0.* April, 2005.

[FIPS 186-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: *Digital Signature Standard (DSS).*** FIPS PUB 186-2. Washington. US Government Printing Office: Jan. 27, 2000.

[FIPS PUB 140-2] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). **Federal Information Processing Standards Publication: Security Requirements for Cryptographic Modules.** FIPS PUB 140-2. Washington. US Government Printing Office: May 25, 2001.

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

[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. Brasília. ICP-Brasil: 2007.

[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 da ICP-Brasil.** DOC ICP-10.02. ICP-Brasil: 2007.

[IN 03/2007 – ITI] INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO. **Instrução normativa 03/2007: Padrões e procedimentos técnicos a serem observados nos processos de homologação de cartões inteligentes (*smart cards*), leitoras de cartões inteligentes e *tokens* criptográficos no âmbito da ICP-Brasil.** DOC-ICP-10.03. Brasília. ICP-Brasil: 2007.

[ISO/IEC 7816-2] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 2: Dimensions and location of the contacts.** Reference Number: 7816-2. Genève, Switzerland: ISO/IEC. 1999(E).

[ISO/IEC 7816-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols.** Reference Number: 7816-3. Genève, Switzerland: ISO/IEC. 1997(E).

[ISO/IEC 7816-3] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification cards – Integrated circuit(s) cards with contacts – Part 3: Electronic signals and transmission protocols - AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1,8 V.** Reference Number: 7816-3. Genève, Switzerland, ISO/IEC: 1997/Amd. 1:2002(E).

[ISO/IEC 7816-4] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange.** Reference Number: 7816-4. Genève, Switzerland, ISO/IEC : 1995(E).

[ISO/IEC 7816-5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 5: Numbering system and registration procedure for application identifiers.** Reference Number: 7816-5. Genève, Switzerland, ISO/IEC: 1994(E).

[ISO/IEC 7816-6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 6: Interindustry data elements for interchange.** Reference Number: 7816-6. Genève, Switzerland, ISO/IEC: 2004(E).

[ISO/IEC 7816-7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 7: Interindustry commands for Structured Card Query Language (SCQL).** Reference Number: 7816-7. Genève, Switzerland, ISO/IEC: 1999(E).

[ISO/IEC 7816-8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 8: Commands for security operations.** Reference Number: 7816-8. Genève, Switzerland, ISO/IEC: 2004(E).

[ISO/IEC 7816-9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION / INTERNATIONAL ELECTROTECHNICAL COMMISSION. **Identification Cards – Integrated circuit(s) cards with contacts – Part 9: Commands for card management.** Reference Number: 7816-9. Genève, Switzerland, ISO/IEC: 2004(E).

[NIST SP 800-90] DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), INFORMATION TECHNOLOGY LABORATORY (ITL). ***Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised).*** Special Publication 800-90. Washington. US Government Printing Office: March, 2007.

[PC/SC 1.0 Part 2] PC/SC WORKGROUP. **Interoperability Specification for ICCs and Personal Computer Systems – Part 2. Interface Requirements for Compatible IC Cards and Readers.** Version 1.0. PC/SC Specification: Dec, 1997.

[PC/SC 1.0 Part 3] PC/SC WORKGROUP. **Interoperability Specification for ICCs and Personal Computer Systems – Part 3. Requirements for PC-Connected Interface Devices.** Version 1.0. PC/SC Specification: Dec, 1997.

[RSA PKCS#11] RSA LABORATORIES – PKCS#11: CRYPTOGRAPHIC TOKEN INTERFACE STANDARD. RSA Security Inc. Version 2.20. June, 2004.

[USB 2.0] UNIVERSAL SERIAL BUS REVISION 2.0 SPECIFICATION – USB-IF.

[RESOLUÇÃO 41 – ICP-BRASIL] COMITÊ GESTOR DA ICP-BRASIL. RESOLUÇÃO N° 41, DE 18 DE ABRIL DE 2006 – REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADOS NA ICP-BRASIL. ICP-BRASIL: Infraestrutura de Chaves Públicas Brasileira. 18 de Abril de 2006.

ANEXO I

Requisitos para a Avaliação de Manutenção

REQUISITO	Quantidade de ensaios
REQUISITO I.10	0
REQUISITO I.11	3
REQUISITO I.14	0
REQUISITO I.15	4
REQUISITO I.16	3
REQUISITO I.17	5
REQUISITO I.20	1
REQUISITO I.22	2
REQUISITO I.25	2
REQUISITO I.26	3
REQUISITO I.27	3
REQUISITO I.31	5
REQUISITO I.32	4
REQUISITO I.34	4
REQUISITO I.35	2
REQUISITO I.36	0
REQUISITO I.38	3
REQUISITO I.40	5
REQUISITO I.41	2
REQUISITO I.42	3
REQUISITO I.44	0
REQUISITO I.45	1
REQUISITO I.46	2
REQUISITO I.48	6
REQUISITO I.50	8
REQUISITO I.51	4
REQUISITO I.53	5
REQUISITO I.54	3

REQUISITO	Quantidade de ensaios
REQUISITO I.55	2
REQUISITO I.56	2
REQUISITO I.57	2
REQUISITO I.58	1
REQUISITO I.59	3
REQUISITO I.60	3
REQUISITO I.61	2
REQUISITO I.62	2
REQUISITO I.63	2
REQUISITO I.68	1
REQUISITO II.4	1
REQUISITO II.12	2
REQUISITO II.15	3
REQUISITO II.16	3
REQUISITO II.18	2
REQUISITO II.22	1
REQUISITO II.23	0
REQUISITO II.24	4
REQUISITO IV.3	4
REQUISITO IV.4	7