Anexo IV – Especificações Técnicas - Segurança

URNA ELETRÔNICA – UE2022

Sumário

A. Aspectos Gerais

A.1. **Arquitetura de Segurança da UE**

1. A arquitetura de segurança da Urna Eletrônica (UE) deverá incluir os seguintes dispositivos: (1) Módulo de Segurança Embarcado (MSE); (2) Módulo de Segurança do Teclado do Eleitor (MSTE); (3) Módulo de Segurança da Impressora de Relatórios (MSIR) (4) Módulo de Segurança do Leitor Biométrico (MSLB); (5) Módulo de Segurança Genérico (MSG);

1.1. O Módulo de Segurança Genérico (MSG) consistirá em um modelo conceitual de dispositivo periférico seguro, que poderá ser adquirido em momento posterior ao da aquisição da UE2022. Portanto, a implementação do *hardware* e *firmware*s de segurança da UE2022 deverá prever a conexão, no futuro, de novos periféricos.

1.2. O Módulo de Segurança Genérico (MSG) não será objeto deste Projeto Básico, ressalvado o disposto no item 1.1;

1.3. O Módulo de Segurança do Leitor Biométrico (MSLB):

1.3.1. Deverá se comunicar com a UCP (Unidade Central de Processamento) da placa-mãe apenas por meio de um canal seguro (autenticado e cifrado), estabelecido a cada vez que a urna é iniciada;

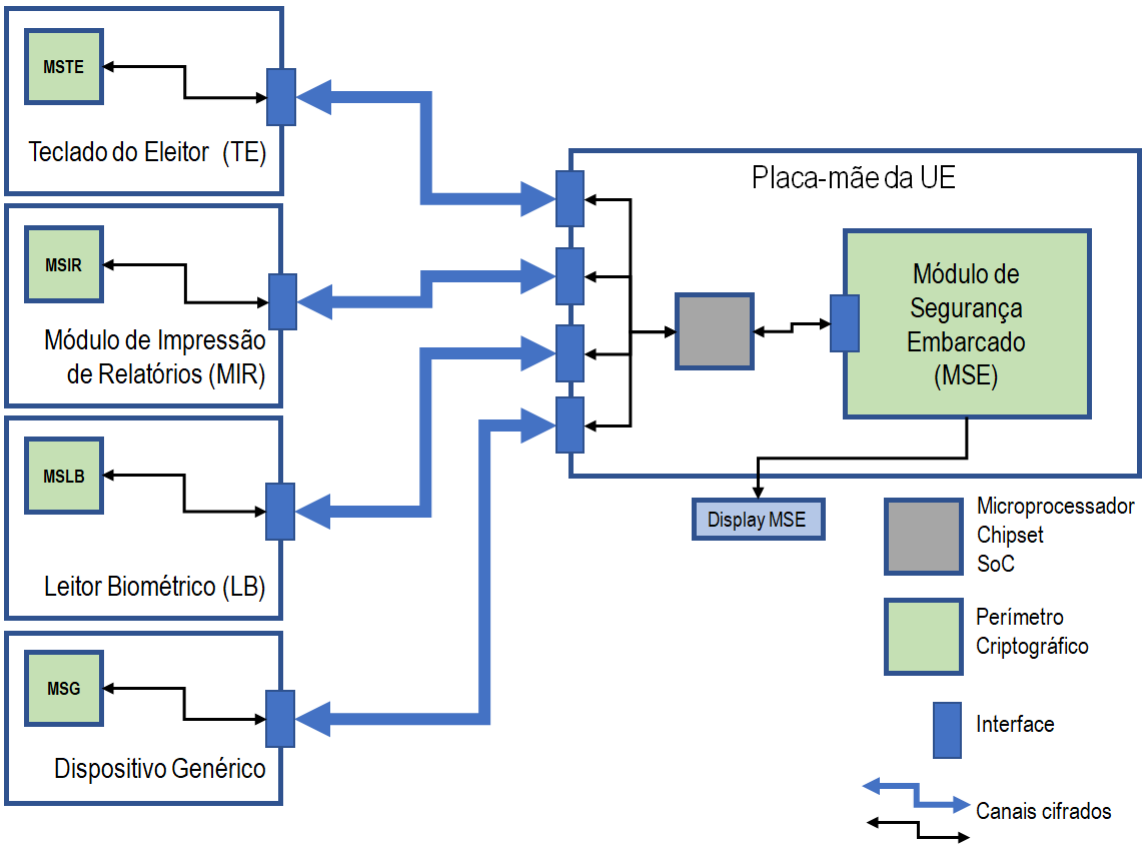

Figura 1 - Arquitetura de segurança da comunicação entre os dispositivos seguros da UE

2. O perímetro criptográfico consistirá numa fronteira explicitamente definida, que estabelece os limites físicos do respectivo módulo criptográfico.

2.1. Qualquer perímetro criptográfico deverá ter seu fornecimento de energia elétrica obrigatoriamente originado das fontes de alimentação da urna, sendo vedado o uso de bateria interna dentro do perímetro criptográfico e/ou uso de bateria adicional ou específica.

3. Toda comunicação entre a UCP (Unidade Central de Processamento) da UE e cada um de seus dispositivos periféricos (Teclado do Eleitor, Módulo de Impressão de Relatórios, Leitor Biométrico e o Dispositivo Genérico) deverá ser realizada estabelecendo-se canais seguros de comunicação, que utilizem os módulos criptográficos próprios de cada periférico, usando o Módulo de Segurança Embarcado (MSE).

4. Um módulo criptográfico deverá conter, no mínimo, e salvo disposição em contrário neste Projeto Básico:

4.1. um microprocessador (ou microcontrolador);

4.2. memória não-volátil;

4.3. memória não-regravável;

4.4. memória volátil;

4.5. as unidades de memória citadas nos itens 4.2, 4.3 e 4.4, não deverão ter acesso físico externamente ao perímetro criptográfico;

4.6. gerador de números realmente aleatórios (TRNG);

4.6.1. com projeto completo e fonte de aleatoriedade auditados pelo TSE, para os casos do MSE e MSTE;

4.6.2. embutido em chip específico, em conformidade com as normas NIST SP 800-90A/B/C, para o MSLB, MSIR e MSG;

4.7. *firmware*s.

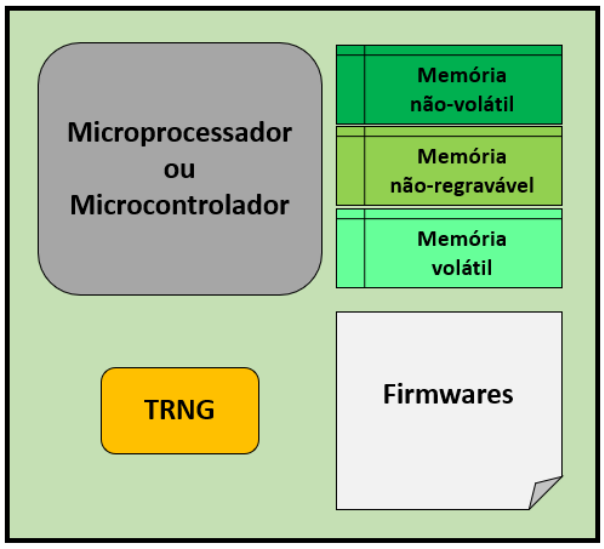

Figura 2 - Componentes mínimos de um módulo criptográfico

A.2. **O Módulo de Segurança Embarcado (MSE)**

5. O Módulo de Segurança Embarcado (MSE) consistirá num sistema computacional confinado a perímetros físicos restritos, embarcado em um sistema computacional hospedeiro, que em conjunto com um *firmware*, implementará funções criptográficas e/ou processos, inclusive algoritmos criptográficos e geração de chaves criptográficas.

6. A Contratada deverá implementar solução baseada em microprocessador (ou microcontrolador), que deverá estar soldado na placa-mãe, não sendo permitida uma solução conectada por cabos e/ou conectores;

7. O MSE deverá ser utilizado na carga do sistema operacional das UEs.

7.1. A carga do sistema operacional nas UEs deverá se basear em soluções de carga usuais do mercado de computadores pessoais, adicionados dos meios necessários para prover, nas UEs, autenticação na execução de seus *firmwares*, *loaders*, sistemas operacionais e aplicativos.

7.2. O *loader* do sistema operacional deverá:

7.2.1. Residir em mídia não-volátil com sistema de arquivos ou particionamento;

7.2.2. Fazer parte da cadeia de confiança e ter sua autenticidade e integridade comprováveis;

7.2.3. Ser distinguível entre os elementos dessa cadeia de confiança (MSE, *Firmware* da Placa-mãe, e *Kernel*);

8. O MSE terá como características básicas:

8.1. Funcionar como única raiz de confiança, implementada em *hardware*, de uma pilha de inicialização segura que não poderá ser desabilitada;

8.2. Ser dedicado às funções criptográficas de:

8.2.1. assinatura e verificação com primitivas de chaves assimétricas;

8.2.2. cifração e decifração com primitivas de chaves simétricas e assimétricas;

8.2.3. resumo digital;

8.2.4. autenticação com chaves assimétricas;

8.3. Possuir funções para geração, armazenamento e uso seguro de chaves criptográficas;

8.4. Possibilitar a autenticação de dispositivos seguros conectados à urna;

8.5. Prover método seguro e auditável de atualização de seu próprio *firmware*;

8.6. Prover método seguro para provar o conteúdo completo de seu próprio *firmware*;

8.7. Permitir o bloqueio das funcionalidades do *hardware* da urna;

9. Estarão obrigatoriamente inclusos no conceito de PCS (Parâmetros Críticos de Segurança), para as Urnas Eletrônicas, os seguintes itens de *hardware*:

9.1. Dispositivos que lidam com materiais de chaves em claro (microprocessador/microcontrolador);

9.2. Geradores de números aleatórios e suas fontes de entropia (TRNG);

9.3. Dispositivos de guarda de chaves (memória);

9.4. Eventuais controles lógicos ou circuitos que sejam críticos à inicialização segura da urna;

10. A solução proposta pela Contratada deverá ser aceita pela equipe técnica do TSE.

A.3. **Nomenclatura para os Fluxos de Inicialização**

11. As urnas poderão utilizar as seguintes abordagens para implementar o *software* básico:

11.1. BIOS, boot*loader*, *Kernel* do UENUX;

11.1.1. Para efeito de compatibilidade com a nomenclatura utilizada nesse anexo, entende-se o BIOS como o "*Firmware* da placa-mãe", o boot*loader* como o "*Loader* do *Kernel*" e o *Kernel* do UENUX pelo mesmo nome;

11.2. Conforme a versão 1.7[1] da especificação UEFI (*Unified Extensible Firmware Interface*) *Platform Initialization* (PI):

11.2.1. SEC: fase "*Security*";

11.2.2. PEI: fase "*Pre-EFI Initalization*";

11.2.3. DXE: fase "*Driver Execution Dispatcher*";

11.2.4. BDS: fase "*Boot Device Selection*";

11.2.5. OSL: fase "*OS Loader*";

11.2.6. RT: fase "*Runtime*";

11.2.7. AL: fase "*Afterlife*;

11.2.8. Para efeito de compatibilidade com a nomenclatura utilizada neste anexo, entende-se as fases SEC, PEI, DXE e parte da fase BDS compreendidas como o "*Firmware* da placa-mãe", parte da fase BDS e a fase OSL como "*Loader* do *Kernel*" e o RT como "*Kernel* do UENUX";

11.2.9. Não será permitido o salvamento de estados de execução que não possam ser autenticados por parâmetros críticos de segurança de propriedade do TSE;

11.2.10. A fase AL poderá ser tratada de maneira assíncrona, por sistema computacional que venha a controlar a fonte de energia, desde que sob autorização do TSE;

11.2.11. Não será permitido o uso de abordagem que utilize "BIOS legado" (*BIOS legacy*) implementado em UEFI;

11.2.12. Qualquer partição de sistema utilizada por uma cadeia de validação UEFI deverá ter sua integridade e autenticidade validadas, antes de sua utilização.

B. Requisitos de Especificação do MSE

B.4. **Microprocessadores**

12. O(s) microprocessador(es) do MSE deverão ter desempenho suficiente para realizar tarefas de assinatura e verificação.

12.1. Para efeito de aferição, o microprocessador (microcontrolador) proposto para o MSE deverá executar o algoritmo E-521 (OID Ed521: 1.3.6.1.4.1.44588.2.1) implementado na biblioteca libE521, a ser fornecida pelo TSE.

12.2. Os tempos máximos a serem atingidos deverão ser:

12.2.1. Tempo de assinatura EdDSA não determinístico (com hash interno) de um bloco maior ou igual a 1 Kbytes em até 1.000 milissegundos;

12.2.2. Tempo de verificação da assinatura EdDSA (com hash interno) de um bloco maior ou igual a 1 Kbytes em até 1.200 milissegundos;

12.2.3. Tempo de cifração simétrica AES-CTR (128 bits) de um bloco de pelo menos 5 MBytes, em menos de 5 segundos;

12.2.4. Tempo de decifração simétrica AES-CTR (128 bits) de um bloco de pelo menos 5 MBytes, em menos de 5 segundos;

[1] http://www.uefi.org/specifications

13. O microprocessador principal da placa-mãe deverá dispor de subconjuntos de instruções SSE3 e AES;

14. Os tempos registrados no item 12.2 deverão consistir das respectivas operações criptográficas e eventuais sobrecargas causadas pela comunicação de dados e/ou implementações exigidas nos protocolos implementados pela solução apresentada pela Licitante/Contratada. Tais tempos serão verificados através dos testes de desempenho do Anexo Ia – Modelo de Engenharia;

B.5. **Armazenamento**

15. Deverá ser previsto o armazenamento de 12 certificados digitais, sendo 8 certificados para autenticação com o mecanismo (EdDSA) descrito no item 34 e 4 certificados para sigilo, com o mecanismo descrito no item 33. O TSE fornecerá todos os certificados;

16. Deverá ser previsto o armazenamento de 8 pares de chaves assimétricas, sendo 1 para o processo fabril e de manutenção das urnas, 3 pares de chaves para assinatura digital e 4 pares de chaves para sigilo. A urna eletrônica deverá gerar os pares de chaves para assinatura e sigilo, exceto aquele par de chaves de sigilo indicado no item 17;

17. Um dos 4 pares de chaves de sigilo deverá ser igual para todas as urnas. Esse par de chaves será utilizado para cifração e decifração, e sua geração obedecerá ao processo definido pelo TSE e informado após a assinatura do contrato;

18. Deverá ser previsto espaço para o armazenamento equivalente a 5 certificados digitais, referentes aos modos de operação (Oficial, Simulado, Desenvolvimento, Inicializador e Manutenção);

19. Deverá ser previsto o armazenamento de uma assinatura digital, com o mecanismo (EdDSA) descrito no item 34, referente à assinatura utilizada para autenticar o *Firmware* da placa-mãe com a chave de nível 0;

20. A Contratada deverá prever espaço de armazenamento suficiente para até mais 2 (dois) níveis acima do nível mais alto da estrutura de chaves ilustrada na Figura 3, para atendimento a possível vinculação com autoridades certificadoras ICP Brasil;

21. Deverá ser previsto espaço para armazenamento de um identificador único, não regravável e gravado durante a fabricação, de no mínimo 64 bits de tamanho, que será denominado **número interno da urna**.

21.1. A faixa de números e eventual regra de formação dos números internos será fornecida pelo TSE e a Contratada deverá entregar, posteriormente, o identificador de cada equipamento relacionado ao número de patrimônio;

22. Deverá ser previsto espaço para o armazenamento equivalente a, pelo menos, 20 pares de chaves assimétricas RSA 2048, que poderão ser geradas pela própria urna eletrônica e/ou implantadas em processo a ser definido pelo TSE.

23. A Contratada deverá reservar espaço em *hardware* para as bibliotecas criptográficas a serem fornecidas pelo TSE;

23.1. Tais bibliotecas exigirão, no mínimo, 64KBytes de espaço em memória não-volátil (para armazenar o binário do *firmware*) e 32KBytes de espaço em memória volátil (para tempo de execução);

24. Além desse espaço de memória, deverão ser consideradas as necessidades das implementações de mecanismos de verificação de autenticidade e integridade do *firmware*, durante o processo de atualização, bem como das implementações da API para atendimento dos serviços de segurança exigidos, para cada módulo criptográfico;

24.1. Para que seja possível evoluir os *firmware*s e conexões das urnas eletrônicas, ao longo de sua vida útil, devem ser previstos espaços de armazenamento não utilizados, tanto para conter o próprio *firmware*, quanto para sua execução e ainda para eventuais chaves e certificados que vierem a ser utilizados.

B.6. **Especificação**

25. A Contratada deverá fornecer:

25.1. documentação específica de todas as portas físicas, interfaces lógicas e caminhos de dados definidos como de entrada e saída do respectivo módulo criptográfico;

25.2. documentação específica dos controles lógicos e manuais do perímetro criptográfico;

25.3. documentação específica de todos os indicadores de estados lógicos e físicos do perímetro criptográfico;

25.4. documentação específica das características elétricas, lógicas e físicas aplicáveis ao perímetro criptográfico;

25.5. documentação específica que:

25.5.1. liste todas as funções de segurança e operações criptográficas que são empregadas pelo perímetro criptográfico;

25.5.2. indique todos os modos de operação suportados, para cada função de segurança/operação criptográfica listada no item 25.5.1 acima;

25.6. documentação contendo diagramas de blocos detalhando todos os principais componentes de *hardware* e de interconexão, incluindo:

25.6.1. Microprocessadores;

25.6.2. Buffers de entrada e saída;

25.6.3. Buffers com conteúdo de texto em claro;

25.6.4. Buffers com conteúdo de texto cifrado;

25.6.5. Buffers de controle;

25.6.6. Memórias de armazenamento das chaves criptográficas;

25.6.7. Memórias de armazenamento dos componentes de *software* do respectivo módulo criptográfico, tornando explícito onde foram implementados o Sistema Operacional e os algoritmos criptográficos;

25.6.8. Memória de trabalho ou operacional;

25.6.9. Memória de programa;

25.6.10. Quaisquer outros componentes não listados acima e que façam parte da solução.

25.7. documentação específica do projeto dos componentes de *hardware*, *software* e *firmware* do respectivo módulo criptográfico. Linguagens de especificação de alto nível para *software* e *firmware*, além de esquemas para *hardware*, devem ser usados para documentar o projeto;

25.8. documentação específica de todos os dados que são relacionados à segurança, demonstrando como e onde são armazenados tais dados nos componentes de *hardware*. Dados relacionados à segurança incluem, mas podem não estar limitados a:

25.8.1. Chaves criptográficas secretas e privadas em texto em claro e cifradas;

25.8.2. Dados de autenticação, como por exemplo, senhas e PIN;

25.8.3. Parâmetro Crítico de Segurança - PCS;

25.8.4. Outras informações protegidas e de caráter sigiloso (por exemplo, dados de auditoria e eventos de auditoria), cuja divulgação ou modificação possa comprometer a segurança do perímetro criptográfico.

25.9. documentação específica da política de segurança adotada pelos módulos criptográficos. A política de segurança deve conter explicitamente regras e/ou procedimentos derivados de quaisquer outros padrões ou requisitos adicionais impostos pela Contratada;

C. Requisitos de Portas e Interfaces do MSE

26. Deverão ser documentadas todas as interfaces lógicas e físicas presentes no perímetro criptográfico;

27. O perímetro criptográfico deverá assegurar que o fluxo de informação e acesso físico sejam realizados apenas pelas portas físicas e interfaces lógicas relacionadas na documentação referida no item 26;

28. Todo dado que entrar no perímetro criptográfico via respectiva interface de entrada deverá seguir somente pelo caminho de entrada definido para essa finalidade. Da mesma forma, todo dado que sair do perímetro criptográfico via respectiva interface de saída deverá seguir somente pelo caminho de saída definido para essa finalidade;

29. Todo caminho de saída de dados deverá ser logicamente desconectado dos circuitos e processos durante a geração, entrada ou destruição (preenchimento com zeros “0” binários) de chaves criptográficas;

29.1. As portas físicas e interfaces lógicas para a entrada e saída de componentes de chaves criptográficas, dados de autenticação e PCS, deverão ser fisicamente e logicamente separadas de qualquer outra porta e interface do perímetro criptográfico.

29.2. Componentes de chaves criptográficas, dados de autenticação e outros PCSs, deverão entrar ou sair diretamente do perímetro criptográfico (via caminho confiado ou cabo diretamente ligado).

D. Requisitos de Papéis, Serviços e Autenticação

D.7. **Serviços**

30. Deverá ser permitida a troca das chaves criptográficas, em qualquer etapa do ciclo de vida da urna, por um processo seguro a ser definido entre o TSE e a Contratada;

31. Cifração e decifração simétricas;

32. Geração de chaves assimétricas;

33. Cifração e decifração assimétrica (ECIES, com chaves de pelo menos 521 bits);

33.1. Conforme padrão SECG SEC 1 (sem a XOR para cifração) ou IEEE 1363a;

34. Assinatura digital e verificação;

34.1. EdDSA com chaves de pelo menos 521 bits;

34.2. RSA com chaves de tamanho de 2048 e de 4096 bits;

35. Algoritmo de resumo digital:

35.1. SHA-1;

35.2. Família SHA-2, inclusive SHA-256, SHA-384 e SHA-512;

35.3. Família SHA-3, inclusive Shake256;

36. Algoritmos de autenticação com chave:

36.1. HMAC com Família SHA-2;

36.2. MAC com SIPHASH;

37. Gerador de número aleatório em *hardware*, conforme definido nos itens 93 e 94;

38. Gerador de número aleatório PRNG.

39. Mostrar e/ou disponibilizar o resultado do estado corrente do módulo criptográfico;

39.1. Os estados serão baseados no Modelo de Estado Finito, com requisitos definidos na Seção E;

40. Atualizar *firmware*s dos dispositivos listados no item 1 e subitens, permitindo a atualização completa dos *firmware*s de todos os dispositivos ou individualmente, para cada dispositivo e cada *firmware*, conforme definido no item 58.

40.1. Os módulos criptográficos deverão ter implementados, em seus *firmware*s, funcionalidade que forneça prova de conteúdo por meio de técnica criptográfica que não possa ser falseada por *firmware* não autêntico.

40.1.1. A prova de conteúdo não deverá envolver espaço de memória que contenha as chaves privadas, mas deverá envolver espaços livres da memória que armazena o *firmware* criptográfico dos módulos criptográficos.

40.2. Os métodos para a prova de conteúdo na atualização dos *firmware*s serão tratados em reunião inicial com a Contratada;

41. Executar os autotestes especificados na seção J;

42. Realizar no mínimo uma operação de uma função de segurança aprovada pelo TSE num modo criptográfico de operação (por exemplo, utilizando o algoritmo criptográfico simétrico no modo de operação CBC).

43. As bibliotecas criptográficas previstas nos itens 31, 32, 33, 34, 35, 36, 38 consistirão de implementações proprietárias e serão fornecidas pela Contratada (exceto aqueles que explicitamente definidos como fornecidos pelo TSE na seção O);

43.1. Todas as operações que exigirem uso de fonte de aleatoriedade real (física), deverão utilizar os serviços do item 37;

43.2. Todos os demais serviços e funcionalidades descritas neste e nos demais anexos a este Projeto Básico deverão ser implementados pela Contratada, que deverá se responsabilizar pelo funcionamento completo da urna eletrônica;

43.3. Adicionalmente, o TSE fornecerá a especificação das interfaces e informações que considerar necessárias, cabendo à Contratada a integração das mesmas ao *hardware* ofertado;

44. Os serviços 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41 e 42 se referem a todos os módulos criptográficos listados no item 1;

D.8. **Autenticação**

45. Dados de autenticação armazenados no perímetro criptográfico deverão ser protegidos contra divulgação, modificação e substituição não autorizada;

E. Requisitos do Modelo de Estado Finito

46. A operação dos módulos criptográficos da UE deverá ser especificada através de um modelo de estado finito (ou equivalente), representado por um diagrama de transição de estados e/ou uma tabela de transição de estados.

46.1. Cada módulo criptográfico, inclusive aqueles indicados no item 1, deverão ter seus respectivos Modelos de Estado Finito.

46.2. O diagrama de transição de estados e/ou a tabela de transição de estados deverá incluir:

46.2.1. Todos os estados operacionais e estados de erro de cada módulo criptográfico;

46.2.2. As transições de um estado ao outro;

46.2.3. Os eventos de entrada que causarem transições de um estado para outro;

46.2.4. Os eventos de saída resultantes das transições de um estado para outro.

46.3. O módulo criptográfico deverá incluir os seguintes estados operacionais e estados de erro:

46.3.1. Estados de alimentação de energia: estados para alimentação de energia primária, secundária ou *backup*. Esses estados poderão se diferenciar em função das fontes de energia que estão sendo aplicadas ao módulo criptográfico;

46.3.2. Estados “Entrada de chave ou PCS”: Estados para a inserção de chaves criptográficas e PCS no módulo criptográfico;

46.3.3. Estados de usuário: Estados nos quais os usuários autorizados obterão serviços de segurança, realizarão operações criptográficas ou desempenharão outras funções;

46.3.4. Estados de autoteste: Estados nos quais o módulo criptográfico realizará autotestes;

46.3.5. Estados de erro: Estados quando o módulo criptográfico encontrará um erro (por exemplo, falha em um autoteste ou tentativa de criptografar quando chaves operacionais ou PCSs foram perdidos). Estados de erro poderão incluir:

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

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

46.3.6. Um módulo criptográfico poderá, ainda, utilizar outros estados, incluindo, mas não limitado a:

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 contiver um papel de acesso de manutenção, então um estado de manutenção deverá ser incluído.

46.4. Não será aceito qualquer tipo de estado de desvio (*by-pass*).

46.5. A documentação de cada módulo criptográfico deverá incluir uma representação do modelo de estado finito (ou equivalente), utilizando um diagrama de transição de estados e/ou uma tabela de transição de estados que deverá especificar:

46.5.1. Todos os estados de erro e operacionais do módulo criptográfico;

46.5.2. As transições correspondentes de um estado para outro;

46.5.3. Os eventos de entrada, incluídas as inserções de dados e controles que causarem transições de um estado para outro;

46.5.4. Os eventos de saída, incluídas condições internas do módulo criptográfico, saídas de dados e saídas de estado resultantes de transições de um estado para outro.

F. Requisitos do Nível de Segurança Física

47. O dispositivo de segurança deverá ser crítico para o funcionamento da solução, ou seja, qualquer violação ou remoção de um dos seus componentes de *hardware* ou de *software* deverá impedir o funcionamento da urna eletrônica;

48. Todas as memórias voláteis e não voláteis, para dados e programas do dispositivo microcontrolador/microprocessador dos dispositivos listados no item 1, deverão ser embarcadas e não poderão ser acessíveis externamente para leitura, por nenhum tipo de interface (GPIO, Serial, JTAG etc);

48.1. Para realização de testes ou em determinadas etapas do processo fabril, deverá ser possível o uso de interfaces para leitura/gravação em memórias internas, porém apenas depois de acordado entre o TSE e a Contratada;

49. Poderá haver mais de um perímetro criptográfico na UE;

50. Os perímetros criptográficos das urnas eletrônicas, cujos TRNGs não estiverem embarcados em um circuito integrado, deverão estar protegidos por resina, com as seguintes características:

50.1. espessura mínima de 5 mm;

50.2. grau mínimo de dureza de 80 SHORE-D, que dificulte e evidencie tentativas de violação dos dispositivos;

50.3. Temperatura de transição vítrea acima do ponto de fusão do material a ser empregado para emoldurar a resina (e.g. plástico);

50.4. A resina deverá ser totalmente opaca ao espectro de luz visível e a raios-X, devendo ser empregada, se necessário, substância adicional;

50.5. Deverá haver alguma solução para impedir o funcionamento, caso haja algum acesso físico pela face inferior da placa de circuito impresso de um perímetro criptográfico;

51. Portas, tampas ou interfaces de acesso para manutenção, quando presentes no perímetro criptográfico, deverão ser protegidas com sensores que detectem o acesso a estas portas. A ativação de tais sensores deverá iniciar instantaneamente no perímetro criptográfico um processo de destruição de informações críticas armazenadas em sua memória, como por exemplo, chaves criptográficas ou parâmetros críticos de segurança;

52. Se o perímetro criptográfico possuir orifícios ou fendas para ventilação, estas deverão ser construídas de forma a prevenir qualquer tipo de sondagem ou observação indevida do interior deste perímetro;

53. Quaisquer ligações entre componentes do perímetro criptográfico e elementos externos que possam resultar em possíveis ataques à correta execução dos serviços do perímetro criptográfico e verificação da cadeia de segurança deverão ser protegidas (ex: trilhas internas), sendo que a solução sugerida pela Contratada deverá ser aprovada pelo TSE;

53.1. Todas as ligações entre o MSE e a CPU deverão ser inacessíveis externamente (ex: por trilhas internas entre componentes BGA), salvo aprovação contrária do TSE;

54. A documentação técnica do respectivo módulo criptográfico deverá especificar todos os componentes de *hardware*, *software*, *firmware* que estarão contidos dentro da fronteira criptográfica e protegidos pelos mecanismos de segurança física, além da fronteira criptográfica que delimitará tais componentes;

55. A documentação técnica do respectivo módulo criptográfico deverá especificar quais mecanismos de segurança física estão implementados neste perímetro e seus respectivos componentes;

56. Quando aplicável, a documentação técnica do respectivo módulo criptográfico deverá descrever as interfaces de acesso para manutenção e os mecanismos de destruição de chaves criptográficas simétricas e assimétricas privadas e PCSs, que serão ativados quando a interface de acesso para manutenção for utilizada;

G. Requisitos do Ambiente Operacional

57. O uso de dispositivo de memória externa ao microcontrolador/microprocessador somente será permitido para armazenamento de dados não voláteis e se:

57.1. Todo o conteúdo armazenado no dispositivo externo for embalado criptograficamente (cifrado, autenticado, com garantia de proteção contra ataques de repetição);

57.2. As chaves utilizadas na embalagem do conteúdo da memória externa estiverem armazenadas exclusivamente na memória interna do microcontrolador;

57.3. Os algoritmos criptográficos empregados forem aprovados pelo TSE.

58. Deverá ser permitida a atualização do *firmware* de cada um dos dispositivos relacionados à solução de segurança da urna eletrônica, listados no item 1.

58.1. Essa atualização deverá ser realizada por procedimento de IAP (*In Application Programming*), no qual o próprio dispositivo realiza a sua atualização de *firmware*.

58.2. O dispositivo somente realizará a sua atualização, mediante assinatura digital feita pelo TSE, contra certificado constante no próprio *firmware*, garantindo-se a integridade e autenticidade do novo *firmware*.

58.3. Essa atualização deverá ser realizada sem a necessidade de abertura do gabinete da urna eletrônica;

58.4. O processo de atualização deverá:

58.4.1. Possibilitar a prova do conteúdo gravado a partir da comparação com o conteúdo a ser gravado;

58.4.2. Impedir que a atualização chegue a qualquer estado inalcançável, ou seja, que a urna sempre possa ser reiniciada em estado operacional;

58.4.3. Permitir o acompanhamento do estágio em que se encontra durante a atualização;

58.4.4. Manter registros de eventos (logs) das últimas 10 (dez) atualizações ocorridas;

a) Tais registros de eventos deverão ser mantidos em área de memória persistente do respectivo dispositivo de segurança;

b) Tais registros de eventos deverão ser recuperáveis;

c) Deverá ser possível autenticar tais registros de eventos;

59. Quando os componentes de *software* e *firmware* forem carregados para dentro do perímetro criptográfico, deverá ser utilizado um método de autenticação aprovado pelo TSE. Esse método de autenticação deverá ser utilizado para todos os componentes de *software* e *firmware* validados.

60. Todo componente de *software*/*firmware* que vier a ser carregado, de fora para dentro do perímetro criptográfico deverá ser testado:

60.1. Para aferir a integridade de sua amostra original:

60.1.1. Se a amostra original não estiver íntegra, de acordo com o teste de integridade, a amostra original do *software*/*firmware* não deverá ser carregada;

60.2. Para aferir o sucesso da operação de carga:

60.2.1. Depois de completamente carregado, o conteúdo gravado deverá ser comparado com a amostra original;

60.2.2. Caso o conteúdo carregado seja diferente da amostra original, deverá ser indicado um erro;

60.2.3. O processo de carga não deverá permitir que haja qualquer estado inalcançável, ou seja, o processo de carga deverá garantir que a urna sempre possa ser reiniciada em estado operacional;

61. Qualquer código de detecção de erro que venha a ser utilizado em algum teste, deverá ter, no mínimo, 16 bits de tamanho;

61.1. Caso não seja possível verificar o código de detecção de erro, o respectivo teste que o utiliza deverá falhar;

62. Todos os dispositivos de *hardware* que representem ou lidem com PCSs (Parâmetros Críticos de Segurança) deverão estar contidos conceitualmente em um perímetro criptográfico sujeito aos seguintes requisitos:

62.1. PCSs somente poderão adentrar ou deixar o perímetro criptográfico de forma cifrada e com verificação de integridade e autenticidade, por meio de assinaturas digitais;

63. O perímetro criptográfico deverá incluir os seguintes estados operacionais e estados de erro:

63.1. Estados de alimentação de energia:

63.1.1. Estados para alimentação de energia primária, secundária ou *backup*. Esses estados poderão se diferenciar em função das fontes de energia que estiverem sendo aplicadas ao perímetro criptográfico;

63.1.2. Estados nos quais serviços são realizados, como, por exemplo, inicialização e gerenciamento de chaves criptográficas;

63.2. Estados “Entrada de chave ou de Parâmetro Crítico de Segurança (PCS)”:

63.2.1. Estados para a inserção de chaves criptográficas e PCS no perímetro criptográfico;

63.3. Estados de autoteste:

63.3.1. Estados nos quais serão realizados autotestes no perímetro criptográfico;

63.4. Estados de erro:

63.4.1. “Erros críticos”: indicarão um mal funcionamento da urna, podendo ser necessário executar serviços de manutenção da urna;

63.4.2. “Erros leves e recuperáveis”: exigirão apenas uma nova inicialização do perímetro criptográfico.

G.9. **Requisitos operacionais para o Processo Produtivo e Manutenção**

64. Será definido pelo TSE, em conjunto com a Contratada, um processo específico para segurança no processo de gravação dos *firmware*s dos dispositivos seguros listados no item 1;

65. Este processo será baseado na estrutura de produção do *hardware* definida pela Contratada, e envolverá o desenvolvimento de versões de *firmware* para utilização em locais diversos do local de integração final da urna eletrônica;

65.1. Um diagrama de blocos sobre o processo de segurança para gravação dos *firmware*s e geração de chaves deverá ser entregue pela contratada juntamente com o Relatório do Modelo de Qualificação

66. Estas versões de *firmware* não deverão incluir a lógica de negócio e os algoritmos criptográficos especificados neste Anexo. Incluirão funções de autoteste, verificação de hash, verificação de assinatura

digital e outras, garantindo a integridade do conteúdo gravado e a integridade e autenticidade dos *firmware*s que serão gravados posteriormente;

67. Deverá ser desenvolvido mecanismo que garanta a integridade do *firmware* gravado nos dispositivos seguros antes que a placa-mãe seja inserida no processo de integração final da urna eletrônica;

68. Após a gravação da versão final de *firmware*, todos os refugos e restos de produção que contenham os dispositivos seguros especificados neste Anexo deverão ser entregues ao TSE após o processo produtivo;

69. Será estabelecido pelo TSE, e implementado pela Contratada, um processo de controle das placas que contenham os dispositivos seguros, permitindo seu rastreamento durante toda a produção e prestação de serviços de manutenção e garantia.

H. Requisitos de Gerenciamento das Chaves Criptográficas

70. A hierarquia de chaves e certificados digitais das urnas modelo 2022 está descrita na Figura 3.

70.1. A Contratada deverá implementar, no MSE, todo o *firmware* e bibliotecas que deem suporte às operações com essa estrutura de chaves e certificados digitais;

71. A estrutura dos certificados armazenados no dispositivo de segurança possuirá 3 níveis (Nível 0, Nível 1 e Nível 2) e 5 modos (Oficial, Simulado, Desenvolvimento, Inicializador e Manutenção), sendo esses modos aplicáveis apenas aos Níveis 1 e 2;

72. Os modos Oficial, Simulado e Desenvolvimento são modos de Eleição e, após as verificações necessárias, deverão permitir o funcionamento pleno da urna, conforme item 143.2;

73. Os modos Inicializador e Manutenção deverão permitir apenas o funcionamento restrito, conforme item 143.1;

74. Ao iniciar em um modo, o MSE não deverá permitir o acesso a informações exclusivas dos demais modos;

74.1. Todos os certificados digitais de todos os níveis deverão estar disponíveis via API, assim como a recuperação de campos específicos destes, exceto no modo Manutenção;

74.2. As chaves especiais (veja Figura 3) e respectivo Certificado de Sigilo também deverão estar disponíveis em qualquer modo, exceto o modo Manutenção;

74.3. Todos os parâmetros acessíveis no modo Manutenção deverão ser aprovados pelo TSE e, em caso de necessidade de manutenção, o TSE poderá aprovar o acesso a parâmetros públicos, incluindo dados de certificados;

75. No momento da inicialização do dispositivo de segurança, este deverá:

75.1. Receber o certificado digital da ICP Brasil “Autoridade Certificadora Raiz Brasileira v7” e os certificados digitais do TSE “AC URNA v2”, “AC UE2022” e “Inicializador”, e a assinatura do “*Firmware* da placa-mãe”, assinado pela chave privada correspondente à chave pública do certificado “Inicializador”.

75.2. A inserção destes certificados e da assinatura do *Firmware* da placa-mãe no dispositivo de segurança somente será realizada mediante confirmação de autenticidade e integridade, por meio de verificação de assinatura digital com uma chave pública de um certificado fornecido pelo TSE e armazenado no código do *firmware* do dispositivo de segurança (*hardcoded*);

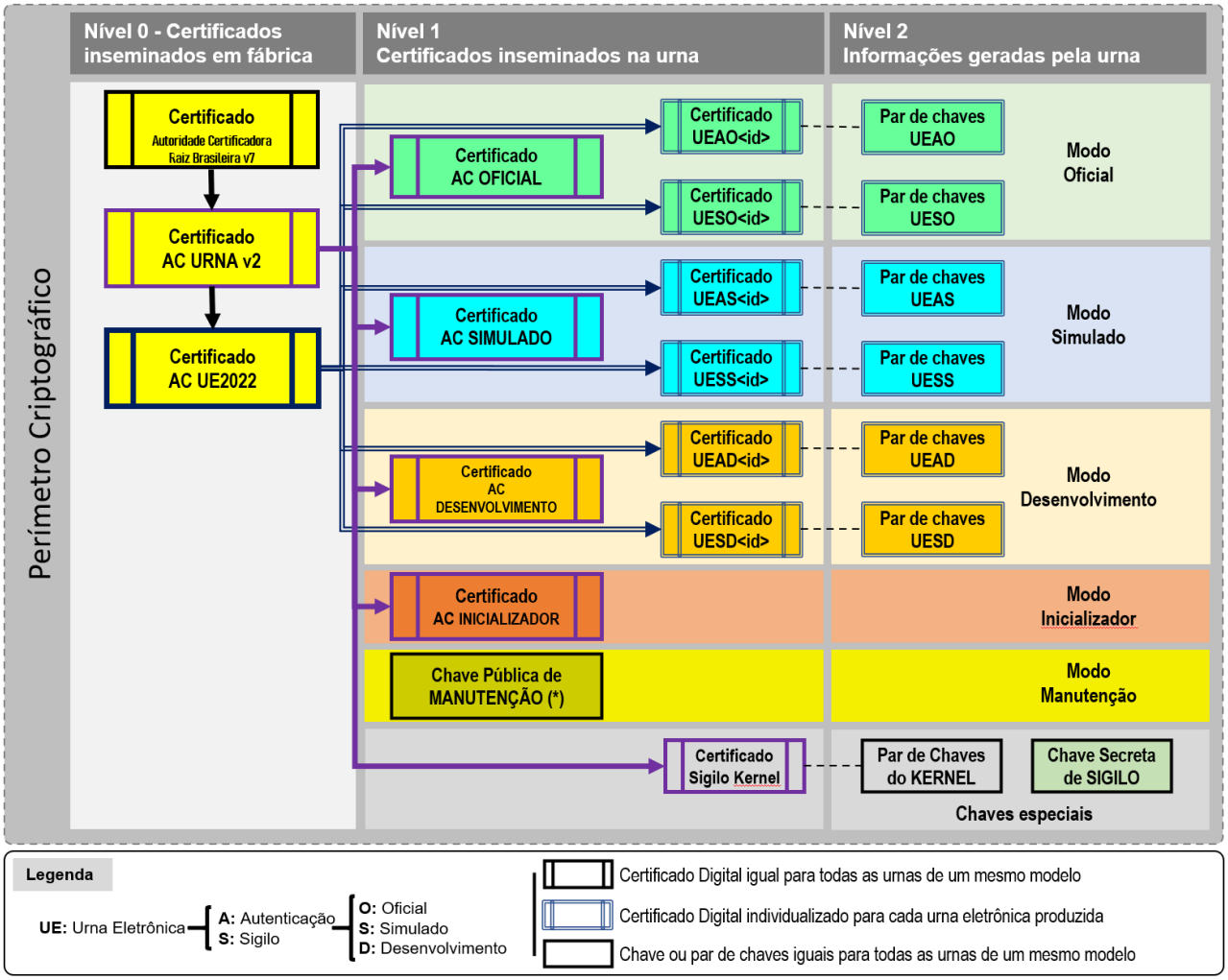

Figura 3 - Estrutura de chaves assimétricas da Justiça Eleitoral

76. Após o processo descrito no item 75, o dispositivo de segurança deverá gerar 6 (seis) pares de chaves relativos aos modos de eleição do dispositivo de segurança. As chaves privadas deverão ser mantidas em modo privado e as chaves públicas deverão ser exportadas em forma de requisição de certificado (CSR, compatível com o padrão X509v3), para que possam ser certificadas pela Justiça Eleitoral. O gerador TRNG do MSE (item 93) deverá ser utilizado para a geração destas chaves;

76.1. A exportação de chaves públicas na forma de requisição de certificado (CSR, compatível com o padrão X509v3) também poderá ocorrer em procedimento de atualização, em momento definido de acordo com a necessidade e conveniência do TSE, em momento diferente do processo descrito no item 75;

77. Estes certificados, juntamente com os demais certificados e chaves gerados pelo TSE, serão inseridos no dispositivo de segurança da UE2022 conforme estrutura definida na Figura 3.

78. Chaves secretas, chaves assimétricas privadas e PCSs deverão estar protegidas, dentro do perímetro criptográfico, contra divulgação, modificação e substituição não autorizadas;

79. Chaves assimétricas públicas deverão estar protegidas dentro do perímetro contra modificação e substituição não autorizadas;

80. Quando geradas internamente ao perímetro criptográfico, chaves criptográficas deverão ser, obrigatoriamente, configuradas com um dos seguintes atributos: exportável ou não exportável;

81. O sistema deverá impedir o acesso, por meio de outros processos, às chaves privadas e secretas, PCS e valores intermediários de geração de chaves enquanto o perímetro criptográfico estiver em execução;

82. Uma chave criptográfica simétrica ou assimétrica privada quando importada ou exportada do perímetro criptográfico deverá ser cifrada utilizando algoritmo aprovado pelo TSE;

83. Uma chave pública poderá ser importada ou exportada do perímetro criptográfico;

84. Deverá ser possível configurar, no perímetro criptográfico, com atributo "não exportável", uma chave criptográfica assimétrica privada, para fins de assinatura digital. Tão logo seja gerada tal chave, deverá ser definido tal atributo como "não exportável" e ser impossível alterá-lo para "exportável";

85. Deverá ser possível configurar, no perímetro criptográfico, com atributo "não exportável", uma chave criptográfica simétrica e/ou assimétrica privada, para fins de sigilo. Tão logo tenha sido gerada tal chave, deverá ser definido tal atributo como "não exportável" e ser impossível alterá-lo para "exportável";

86. Chaves criptográficas deverão ser armazenadas dentro do perímetro criptográfico em claro ou cifradas;

87. Chaves assimétricas privadas e simétricas secretas não deverão ser acessíveis;

88. Se as chaves (públicas e privadas) forem utilizadas para realizar um método de transporte de chaves, a chave pública deverá cifrar uma sequência bem conhecida. O conteúdo cifrado deverá ser comparado a essa sequência. Se essas duas sequências forem iguais o teste deverá falhar. Se as sequências forem diferentes, a chave privada deverá ser utilizada para decifrar o cifrado, e o resultado deverá ser comparado à sequência conhecida. Se as duas sequências forem diferentes, o teste deverá falhar. Quando componentes de *software* e *firmware* forem carregados externamente para dentro do perímetro criptográfico, este teste deverá ser executado;

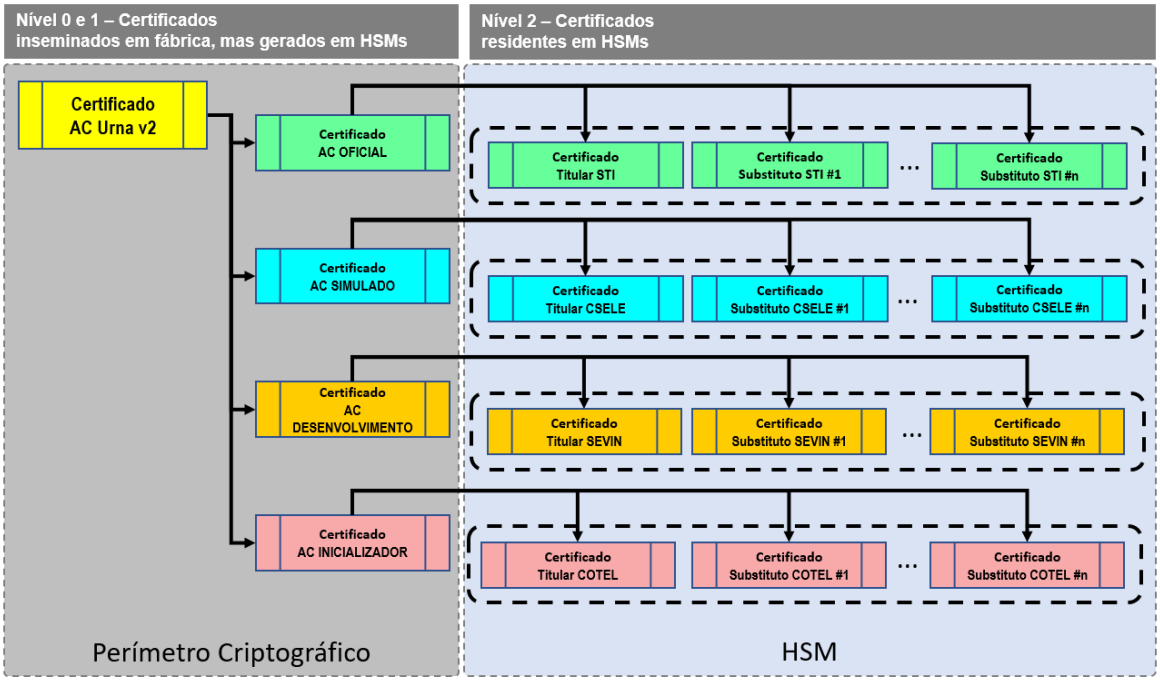

Figura 4 – Estrutura de chaves para autenticação de *softwares* básicos

89. Uma hierarquia de chaves provenientes de módulos criptográficos externos deve ser implantada durante o processo produtivo das UE2022, para que possam ser utilizas por seus *softwares* e aplicações para autenticar *softwares* básicos tais como *Kernel*, *Loader* do *Kernel*, *Firmwares* da Placa-mãe e *Drivers*. Essa hierarquia está ilustrada na Figura 4 e os certificados a serem implantados no MSE são o AC Oficial, AC Simulado, AC Desenvolvimento e AC Inicializador (os mesmos ilustrados na Figura 3). Eles correspondem a perfis de ocupantes dos cargos responsáveis pelos artefatos a serem autenticados;

89.1. Os *softwares* básicos serão assinados pelos certificados de Nível 2, não implantados no MSE. As validações da autenticidade dos *softwares* básicos serão realizadas pelos certificados de Nível 0 e 1 implantados previamente no MSE.

H.10. **Importação e Exportação de Chaves Criptográficas**

90. A documentação deverá especificar os métodos de importação e/ou de exportação de chaves criptográficas empregados pelo perímetro criptográfico;

H.11. **Geradores de Números Aleatórios**

91. Se cada chamada de um gerador de números aleatórios produzir menos que 16 bits, os primeiros *n* bits gerados depois da energização, inicialização ou reset (para algum *n* > 15) não serão utilizados, mas armazenados para comparação com os próximos *n* bits gerados. Cada subsequência gerada, de *n* bits, deverá ser comparada com os *n* bits previamente gerados. O teste deverá falhar se quaisquer das sequências comparadas de *n* bits forem iguais;

92. O algoritmo RNG aprovado pelo TSE deve ser usado somente para gerar um único inicializador para geração da chave assimétrica comum a todas as urnas eletrônicas, apenas nesse caso;

93. Cada um dos módulos criptográficos presentes no MSE e MSTE deverá conter um gerador de número realmente aleatório implementado em *hardware* (TRNG – *True Random Number Generator*). Cada um desses TRNGs deverá:

93.1. Possuir fonte de ruído redundante;

93.2. Possuir fonte de entropia própria implementada em *hardware*;

93.3. Possuir teste contínuo da fonte de entropia;

93.4. Possuir controle contínuo de qualidade;

93.5. Possuir autoteste, da saída dos valores aleatórios, para indicar;

93.5.1. se o TRNG está energizado;

93.5.2. se o TRNG está apresentando valores inadequados (constantes ou restritos a um intervalo muito pequeno);

93.6. Estar em conformidade com o preconizado no documento AIS 31, PTG.2, em sua versão 2.0;

93.7. Não apresentar desconformidade com os testes estatísticos NIST e *Diehard*;

93.8. Não estar embutido em circuito integrado;

93.9. Possuir Interface de Aplicação (API) que permita acesso aos valores gerados, bem como aos indicadores de qualidade. Os códigos-fonte dessa API deverão ser entregues ao TSE de forma que possam ser submetidos para futuras auditorias as quais as urnas eletrônicas forem submetidas;

93.10. Disponibilizar projeto (esquema elétrico, B.O.M., *firmwares* e respectivos códigos-fonte) ao TSE, de forma que possa ser entregue para futuras auditorias as quais as urnas eletrônicas forem submetidas;

93.10.1. Quando submetido a auditorias, deverá ser possível comprovar, por inspeção visual em amostra sem resina, que o circuito implementado (real) corresponde ao circuito que consta no esquema elétrico (projetado);

93.11. Ter projeto aceito pela equipe técnica do TSE.

94. Cada um dos módulos criptográficos presentes no MSLB e MSIR deverá conter um gerador de número aleatório implementado em *hardware*. Cada um desses geradores de números aleatórios deverá:

94.1. Atender as recomendações contidas nos documentos:

94.1.1. NIST 800-90A – *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*

94.1.2. NIST 800-90B – *Recommendation for the Entropy Sources Used for Random Bit Generation*

94.1.3. NIST 800-90C – *Recommendations for Random Bit Generator (RBG) Constructions*

94.2. Possuir fonte de entropia própria implementada em *hardware*;

94.3. Possuir teste contínuo da fonte de entropia;

94.4. Possuir controle contínuo de qualidade;

94.5. Possuir autoteste, da saída dos valores aleatórios, para indicar;

94.5.1. se o gerador de números aleatórios está energizado;

94.5.2. se o gerador de números aleatórios está apresentando valores inadequados (constantes ou restritos a um intervalo muito pequeno);

94.6. Possuir Interface de Aplicação (API) que permita acesso aos valores gerados, bem como aos indicadores de qualidade. Os códigos-fonte dessa API deverão ser entregues ao TSE de forma que possam ser submetidos para futuras auditorias as quais as urnas eletrônicas forem submetidas;

94.7. Disponibilizar projeto (esquema elétrico, B.O.M., *firmware*s e respectivos códigos-fonte) ao TSE, de forma que possa ser entregue para futuras auditorias às quais as urnas eletrônicas sejam submetidas;

94.8. Ter especificação aceita pela equipe técnica do TSE.

I. Requisitos de Interferência e Compatibilidade Eletromagnética

95. O dispositivo contido no perímetro criptográfico será protegido contra ataques de emanações eletromagnéticas, de acordo com as normas IEC 61.000-6-3 (relativo à emissão) e IEC 61.000-6-1 (relativo à imunidade). Dentro dessas normas, a urna eletrônica deverá ser avaliada e classificada no nível: Classe B;

96. O dispositivo contido no perímetro criptográfico não deverá gerar emanações eletromagnéticas que permitam, mesmo que parcialmente, a extração ou determinação probabilística de qualquer PCS (Parâmetro Crítico de Segurança), considerando a metodologia de medição estipulada no item 95.

97. A UE2022 deverá ser protegida contra ataques e análises de radiações eletromagnéticas emanadas e conduzidas. Em especial a UE2022 deverá:

97.1. Impossibilitar que um adversário situado a uma distância de 0,5 metro da cabina de votação, mesmo que utilize equipamentos especializados, seja capaz de violar o sigilo do voto, ainda que estatisticamente;

97.2. Ter o Terminal do Mesário (TM), o Terminal do Eleitor (TE), o Módulo Impressor de Relatórios (MIR), os módulos criptográficos listados no item 1 e o Display da urna eletrônica construídos de forma a impedir que emanações eletromagnéticas capturadas de fora da cabina de votação ou emanadas para fora da cabina de votação sejam capazes de:

97.2.1. violar, mesmo que estatisticamente, o sigilo do voto;

97.2.2. interferir ou alterar as características especificadas da urna eletrônica;

97.2.3. ferir qualquer princípio, garantido por legislação, relacionado ao voto.

98. A Contratada deverá apresentar documentação comprovando conformidade da UE2022 às normas de EMI/EMC para equipamentos de tecnologia da informação compatíveis com as normas reconhecidas internacionalmente (IEC CISPR 22 E 24, FCC CFR 47);

99. A Contratada deverá apresentar documentação constando o nome do laboratório responsável onde foi obtida para a Urna Eletrônica a certificação de conformidade EMI/EMC para equipamentos de tecnologia da informação;

J. Requisitos de Autotestes

100. Para verificar o funcionamento apropriado do perímetro criptográfico, duas categorias de autotestes devem ser realizadas:

100.1.1. autotestes de energização, a serem executados quando o perímetro é energizado (ou alimentado com energia elétrica);

100.1.2. autotestes condicionais, a serem executados quando uma operação ou função de segurança aplicável é solicitada.

101. Se o perímetro criptográfico falhar durante um autoteste, ele deverá ser conduzido a um estado de erro e emitir um indicador de erro com mensagem adequada pelo Display do MSE e pelo Led da Cadeia de Segurança.

102. O perímetro criptográfico não deverá realizar qualquer operação criptográfica enquanto persistir o estado de erro provocado por falhas em um autoteste;

103. Os testes de energização serão executados pelo perímetro criptográfico, assim que a urna eletrônica for energizada;

104. Os testes de energização deverão ser executados automaticamente e sem exigir a intervenção de qualquer operador. O módulo criptográfico deverá realizar testes dos algoritmos criptográficos do tipo “resposta conhecida” para todas as funções criptográficas (cifração/decifração, assinatura digital/verificação e geração de números aleatórios);

105. A documentação deverá listar todos os testes de funções criptográficas do tipo “resposta conhecida”;

106. A documentação do respectivo módulo criptográfico deverá especificar os seguintes itens:

106.1. Os autotestes realizados pelo respectivo módulo criptográfico;

106.2. O estado de erro que o respectivo módulo criptográfico puder entrar quando um autoteste falha;

106.3. As condições e ações necessárias para sair dos estados de erro e reiniciar a operação normal do respectivo módulo criptográfico (por exemplo, isto pode incluir a manutenção ou retorno da urna à Contratada para fins de reparo);

106.4. Testes da integridade de *software* e *firmware*;

106.5. Testes de funções críticas;

106.6. Outros testes realizados na energização ou sob demanda.

K. Requisitos de Garantia do Projeto

107. Todos os códigos-fonte de *firmware*s e APIs que tiverem papel determinante na segurança computacional do hardware e software da urna deverão ser abertos ao TSE, que por sua vez, poderá torná-los disponíveis aos interessados em auditar as urnas eletrônicas;

107.1. O código-fonte em *assembly* que não tiver código-fonte em linguagem de alto nível correspondente deverá vir acompanhado do pseudocódigo correspondente, em linguagem natural e documentado;

107.2. O código-fonte do *firmware* da placa-mãe deverá ser compilável de forma repetível, por meio de um ambiente computacional que gere códigos binários a partir dos códigos-fonte. Ou seja, o conjunto de códigos-fonte do *firmware* da placa-mãe, caso não sofra alterações, deverá, sempre, por meio do referido ambiente computacional, gerar códigos binários idênticos;

107.3. Exercem papel determinante na segurança computacional do *hardware* e *software* da urna os *firmwares* e APIs que estiverem envolvidos na geração, ou no uso, ou na destruição de parâmetros criptográficos que tenham alguma relação com o processo eleitoral, ou ainda com a segurança computacional da própria urna;

108. Todos os protocolos, esquemas e algoritmos criptográficos a serem utilizados deverão ser aprovados pelo TSE.

109. A documentação da Contratada deverá descrever o sistema de gerenciamento de configuração para o respectivo módulo criptográfico, com detalhamento sobre os componentes do respectivo módulo criptográfico;

110. A documentação deverá listar os procedimentos específicos de instalação segura e inicialização do perímetro criptográfico;

111. A documentação deverá especificar a relação entre o projeto dos componentes de *hardware*, o *software* e o *firmware* do respectivo módulo criptográfico;

112. O documento “Guia do Administrador” deverá especificar:

112.1. Funções administrativas, eventos de segurança, parâmetros de segurança, portas físicas e as interfaces lógicas do respectivo módulo criptográfico;

112.2. Procedimentos de como administrar o respectivo módulo criptográfico de modo seguro;

112.3. Suposições relacionadas ao comportamento do usuário que são relevantes à operação segura do respectivo módulo criptográfico.

113. O documento “Guia do Usuário” deverá especificar:

113.1. As funções, portas físicas e interfaces lógicas de segurança disponíveis para o usuário do respectivo módulo criptográfico;

113.2. Todas as responsabilidades do usuário necessárias para a operação segura do respectivo módulo criptográfico.

114. Se o respectivo módulo criptográfico contiver componentes de *software* ou *firmware*, a documentação deverá especificar o código-fonte com comentários que esclareçam a correspondência dos componentes do respectivo módulo criptográfico;

115. Se o respectivo módulo criptográfico contiver apenas componentes de *hardware*, a documentação deverá listar tais componentes, apresentando os esquemas elétricos e/ou a linguagem de baixo nível;

116. A documentação deverá descrever a especificação das portas externas e interfaces do respectivo módulo criptográfico e o propósito dessas interfaces;

117. Todos os circuitos geradores de números aleatórios (TRNG) deverão passar por testes que atestem a conformidade com o item 93.

117.1. Esses testes deverão ser condição para aprovação do Modelo de Qualificação e deverão ocorrer após a entrega dos equipamentos citados no item 118, em bancada com energia, espaço e tempo disponíveis para que permaneçam em execução por, pelo menos, 7 (sete) dias corridos.

117.2. O local onde tal bancada será instalada deverá ser definido pelo TSE;

117.3. Tais testes, chamados de Testes do TRNG, se iniciarão logo após as entregas dos equipamentos citados no item 118.

117.3.1. Caso ocorram insucessos na realização dos testes, a Contratada poderá implementar as correções até atingir a conformidade com o item 93, desde que a citada conformidade seja atingida até a aprovação do Modelo de Qualificação.

118. Para dar cabo dos testes do item 117, deverão ser disponibilizados:

118.1. Uma placa-mãe, com a resina aplicada (item 50), da UE2022 com o MSE contendo o circuito TRNG a ser testado;

118.2. Uma placa de cada um dos periféricos contendo os módulos de segurança listados no item 1, com TRNG e com a resina aplicada (item 50), quando aplicável.

118.3. *Softwares e firmware*s específicos para a coleta das massas de valores aleatórios de cada um dos dispositivos TRNG dos itens 118.1 e 118.2.

118.3.1. Tais *firmware*s deverão ser carregados nos respectivos dispositivos de maneira segura, conforme preconiza o item 67;

118.3.2. Os códigos-fonte desses *softwares* e *firmware*s deverão ser previamente entregues ao TSE, para que possam ser analisados, antes de serem testados. Deverá ser possível verificar se os códigos-fonte entregues e analisados correspondem àqueles que estão em execução;

118.3.3. As massas de valores aleatórios a serem geradas deverão possibilitar a verificação da origem (do dispositivo periférico ou MSE que a originou), bem como da ordem na qual foi gerada. O tamanho em bytes também deverá estar disponível.

119. Cada dispositivo listado no item 1 deverá dispor de 5 kits de desenvolvimento de *firmware*, a ser entregue conforme Cronograma de Eventos do Anexo I – Descrição de Produtos e Serviços UE2022.

119.1. Tais kits deverão permitir o desenvolvimento de *firmware*s para cada módulo criptográfico listado no item 1, em bancada, pela equipe técnica do TSE.

119.2. Tais kits poderão ser únicos para um ou mais conjuntos de dispositivos do item 1 ou então distintos, para cada um deles, conforme aplicável.

119.3. Cada um dos kits deverá ter a possibilidade de conexão com um computador hospedeiro PC (Windows ou Linux), executando um *software* que permita o desenvolvimento de *firmware*s para cada um dos módulos criptográficos listados no item 1. Esse *software* será fornecido ao TSE, e, deverá, minimamente:

119.3.1. Compilar códigos em linguagens de baixo e alto nível;

119.3.2. Gerar código realocável;

119.3.3. Ligar códigos para gerar executáveis binários;

119.3.4. Dispor de ambiente IDE (*Interactive Development Environment*);

119.3.5. Possuir monitoramento de *hardware*;

119.3.6. Possuir monitoramento da execução da aplicação;

119.3.7. Geração eficiente de código;

119.3.8. Otimização de código quanto a tempo e espaço;

119.3.9. Caso seja proprietário, o *software* deverá ser licenciado, para cada um dos kits, ao TSE;

119.4. A Contratada deverá realizar treinamento para expor à área técnica do TSE o processo de desenvolvimento de *software*s embarcados, *firmwares* e *drivers* usando os referidos kits de desenvolvimento;

119.4.1. A carga horária deverá prever o treinamento de 8 pessoas, com pelo menos 24 horas por pessoa (total de 192 horas);

119.4.2. O treinamento deverá ser obrigatoriamente presencial;

119.4.3. O treinamento deverá ser realizado em um período de 3 (três) dias úteis consecutivos;

119.4.4. O treinamento deverá ser iniciado conforme indicado no Cronograma de Eventos (Anexo I);

119.4.5. O treinamento deverá ser realizado nas instalações do TSE e dispor, para uso durante todo o tempo da capacitação, para cada pessoa: um kit de desenvolvimento, um PC (já instalado no TSE) com o *software* do referido kit de desenvolvimento, uma gravadora de *firmware*s para as memórias onde serão gravados os *firmwares*, conforme especificado pela Contratada, na Proposta;

119.4.6. O treinamento deverá tornar os servidores da área técnica do TSE capazes de compilar, ligar, usar o ambiente do IDE, compreender as ferramentas de monitoramento, usar as ferramentas para geração de código eficiente e otimizado por tempo/espaço, gravar e descarregar *firmware*s.

L. Requisitos de Mitigação a Ataques

120. Todas as chaves criptográficas e PCSs, dados de autenticação, entradas de controle e saídas de status deverão ser comunicadas por meio de um mecanismo confiável que utilize portas físicas de E/S dedicadas ou caminho confiável;

121. O uso das chaves privadas da urna eletrônica deverá ser restrito ao *hardware* de segurança e ao modo na qual o *loader* do *Kernel* do UENUX foi verificado, ou seja, caso este tenha sido verificado na fase de desenvolvimento, o dispositivo deverá permitir apenas o uso da chave privada de desenvolvimento, e assim respectivamente.

122. A documentação técnica do respectivo módulo criptográfico deverá especificar quais os tipos de ataques classificados como não invasivos serão mitigados por este respectivo módulo;

123. A documentação técnica do respectivo módulo criptográfico deverá especificar quais outros tipos de ataques serão mitigados por este respectivo módulo;

L.12. Comunicação segura entre periféricos e o terminal do eleitor

124. A Contratada deverá prover solução com autenticação segura para estabelecer canais seguros de comunicação entre a placa-mãe da UE e:

124.1. o leitor de impressão digital;

124.2. o teclado do eleitor (TE);

124.3. o módulo impressor de relatórios (MIR);

124.4. dois dispositivos genéricos (DG).

125. Os canais de comunicação dos itens 124.1 e 124.2 deverão ser cifrados e autenticados.

125.1. Para o canal seguro do item 124.2, a criptografia utilizada deverá gerar um conjunto de dados diferente a cada tecla pressionada, inclusive se pressionada a mesma tecla repetidamente;

126. A decifração e a autenticação dos dados provenientes dos dispositivos periféricos do item 124 deverão ser realizadas pelo MSE, em *hardware*, com chave específica e protegida pelo dispositivo;

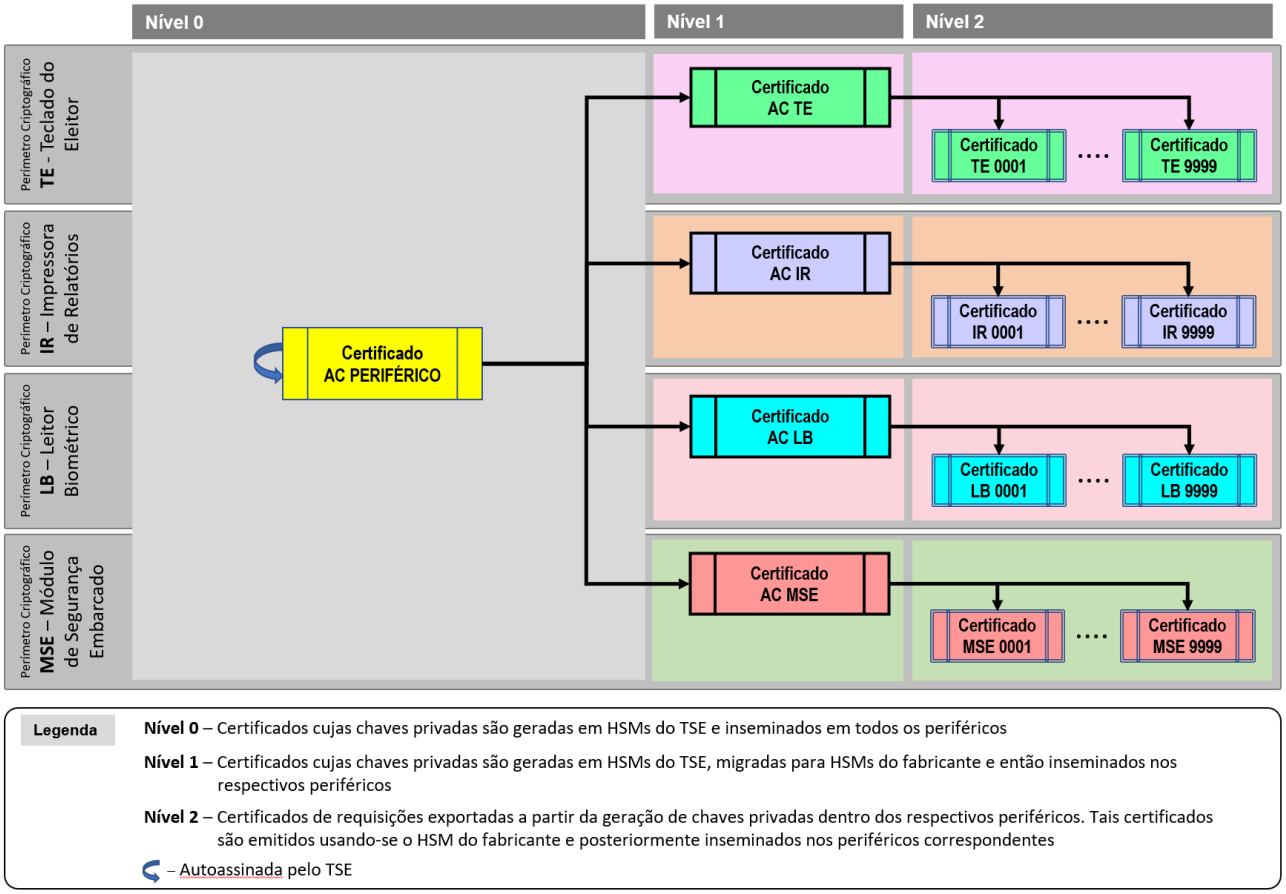

Figura 5 – Estrutura de chaves de periféricos

127. A chave utilizada para estabelecer a sessão segura deverá fazer parte de uma hierarquia de chaves públicas (Figura 5). Os certificados dessa hierarquia deverão ser implantados em cada um dos módulos listados no item 1;

127.1. As chaves de cada periférico produzido deverão ser diferentes, geradas no próprio perímetro criptográfico e autenticadas por uma hierarquia de chaves públicas. Essa hierarquia será gerada pelo TSE e entregue à Contratada para ser migrada em HSMs próprios da Contratada;

127.1.1. A critério do TSE, a hierarquia poderá ser gerada pela própria Contratada;

127.2. Os certificados correspondentes às requisições geradas nos periféricos deverão ser emitidos pela Contratada durante o processo produtivo, assim como a gestões para acesso, publicação e revogação dos certificados e requisições desses periféricos;

127.3. A critério do TSE, serão estabelecidos protocolos de auditoria para garantir que essa hierarquia entregue está sendo utilizada em todos os periféricos produzidos;

127.4. Os padrões criptográficos utilizados na hierarquia deverão estar listados na seção O. Eventual necessidade de padrão criptográfico fora daquela lista deverá ser analisada pela equipe técnica do TSE;

128. A solução proposta pela Contratada deverá ser aceita pela equipe técnica do TSE.

M. Requisitos de Gerenciamento do MSE

129. Se a Contratada dispuser de utilitários de gerenciamento e diagnósticos de problemas, então deverá tornar a respectiva documentação detalhada sobre esses utilitários disponível ao TSE.

M.13. **Cadeia de Segurança**

130. O *Firmware* da placa-mãe deverá permitir a inicialização da UE2022 pela Mídia de Aplicação (MA) ou pela Memória Interna (MI);

131. Não deverá ser possível gravar o *Loader* do *Kernel* no *Firmware* da placa-mãe da UE2022. A tarefa do *Firmware* da placa-mãe deverá ser a de carregar e dar partida no *Loader* do *Kernel*, de acordo com as definições a serem repassadas pelo TSE. Tais definições incluirão, por exemplo, os procedimentos para realizar verificação de assinatura digital (criptografia assimétrica) do *Loader* do *Kernel*, entre outros;

132. Todas as sinalizações de *hardware* especificadas neste Projeto Básico deverão ser implementadas de maneira assíncrona, ou seja, a aplicação deverá ser notificada das alterações de estado ocorridas no *hardware* pelo *driver* do dispositivo, sem a necessidade de consultas (*polling*) ao *driver*;

133. Ao ser energizada, o primeiro dispositivo a ser executado será o MSE, que executará a autenticação (verificação de assinatura digital) do *Firmware* da placa-mãe de forma ativa, não exigindo qualquer forma de intervenção da CPU da placa-mãe, com as seguintes características:

133.1. O *Firmware* da placa-mãe não poderá ser executado enquanto não houver sua validação completa e bem sucedida pelo MSE;

133.2. O MSE deverá autenticar, por meio de API, o *Firmware* da placa-mãe, assinado por uma chave hierarquicamente inferior ao certificado "AC Inicializador", utilizando a hierarquia imediatamente superior, ou seja, o próprio certificado "AC Inicializador" implantado no MSE, conforme exigido no item 89.

133.2.1. A chave privada utilizada na assinatura do *Firmware* da placa-mãe corresponde a um certificado hierarquicamente inferior, residente em módulo criptográfico externo (HSM), conforme ilustra a Figura 4.

133.2.2. A assinatura do *Firmware* da placa-mãe e o certificado correspondente de hierarquia inferior do "AC Inicializador" deve ter sido também previamente implantada no MSE;

133.3. O processador deverá estar desligado (desenergizado) ou em modo reset, até que a validação completa e bem sucedida do MSE sobre o *Firmware* da placa-mãe esteja concluída, observado, especialmente, o item 137.1;

133.4. O acesso às interfaces USB e mídias deverá estar desabilitado até que a validação completa e bem sucedida sobre o *Firmware* da placa-mãe esteja concluída, observado, especialmente, o item 137.1;

133.5. Após a verificação do *Firmware* da placa-mãe ser bem sucedida e finalizada, o controle poderá ser entregue a esse *Firmware* e o processador poderá ser ligado/liberado;

133.6. A leitura, verificação e entrega para execução do *Firmware* da placa-mãe corresponde à etapa 1 descrita na Figura 6;

133.7. O tempo total entre a urna ser ligada e o início da execução do *Firmware* da placa-mãe (correspondente à etapa 1, conforme ilustrado na Figura 6), não poderá exceder 1,0s;

134. O dispositivo deverá fornecer interface de aplicação (API) para que o *Firmware* da placa-mãe valide o *Loader* do *Kernel* do UENUX por meio de verificação de assinatura digital;

134.1. O MSE deverá ser utilizado, por meio de API, para autenticar o *Loader* do *Kernel* do UENUX, assinado por uma das chaves hierarquicamente inferiores aos certificados "AC Oficial", "AC Simulado" ou "AC Desenvolvimento", utilizando a hierarquia imediatamente superior, ou seja, um dos próprios certificados "AC Oficial", "AC Simulado" ou "AC Desenvolvimento" implantados no MSE conforme exige o item 89;

134.1.1. As chaves privadas utilizadas nas respectivas assinaturas do *Loader* do *Kernel* do UENUX correspondem a certificados hierarquicamente inferiores, residentes em módulo criptográfico externo (HSM), conforme ilustra a Figura 4.

135. O dispositivo deverá fornecer interface de aplicação (API) para que o *Loader* do *Kernel* valide o *Kernel* do UENUX por meio de verificação de assinatura digital;

135.1. O MSE deverá ser utilizado, por meio de API, para autenticar o *Kernel* do UENUX, assinado por uma das chaves hierarquicamente inferiores aos certificados "AC Oficial", "AC Simulado" ou "AC Desenvolvimento", utilizando a hierarquia imediatamente superior, ou seja, um dos próprios certificados "AC Oficial", "AC Simulado" ou "AC Desenvolvimento" implantados no MSE conforme exige o item 89;

135.1.1. As chaves privadas utilizadas nas respectivas assinaturas do *Kernel* do UENUX correspondem a certificados hierarquicamente inferiores, residentes em módulo criptográfico externo (HSM), conforme ilustra a Figura 4.

136. As interfaces entre o dispositivo, o *Firmware* da placa-mãe, o *Loader* do *Kernel*, e o *Kernel* do UENUX deverão ser aprovadas pelo TSE;

137. Caso a autenticação do *Firmware* da placa-mãe, do *Loader* do *Kernel* ou dos dispositivos de *hardware* não tenha sido completada com sucesso, o dispositivo de segurança se encarregará de bloquear o funcionamento da urna eletrônica;

137.1. Não deverá haver microcontroladores ou outros dispositivos externos ao perímetro criptográfico que, se atacados, permitam a continuidade do funcionamento da urna eletrônica, caso a autenticação descrita no item 137 não tenha sido completada com sucesso.

138. Na autenticação do *Firmware* da placa-mãe (e Extensão de BIOS, caso exista no projeto) deverá ser verificada a assinatura digital de todo o conteúdo da memória que contiver o *Firmware* da placa-mãe (seja esse *Firmware* da placa-mãe correspondente ao BIOS ou de etapas do UEFI gravadas em *firmware*), com as seguintes características:

138.1. Ao iniciar a autenticação do *Firmware* da placa-mãe, o Led da Cadeia de Segurança deverá ser aceso com a cor VERDE, piscando em 8 Hz;

138.2. O certificado digital do nível 0 "Inicializador" utilizado para a verificação do *Firmware* da placa-mãe (e Extensão do BIOS, caso exista) deverá estar guardado dentro do perímetro criptográfico do MSE;

138.3. Caso o *Firmware* da placa-mãe (incluindo a Extensão de BIOS, caso exista) não seja autêntico, a urna deverá ter o seu funcionamento impedido e acender o Led da Cadeia Segurança do TE (Terminal do Eleitor) com a cor VERDE, piscando em 2 Hz**.**

138.4. Não será considerado, para fins de verificação, o espaço variável do *Firmware* da placa-mãe (caso seja utilizado o BIOS, a NVRAM *Non-Volatile Random Access Memory*)*;*

139. Deverá autenticar o *Loader* do *Kernel* por meio de assinatura digital de todo o seu conteúdo.

139.1. A assinatura digital do *Loader* do *Kernel* e o certificado de hierarquia inferior correspondente ("AC Oficial", "AC Simulado" ou "AC Desenvolvimento") à chave utilizada para assinatura deverão estar guardados dentro da Mídia de Aplicação (MA)/Memória Interna (MI).

139.2. A verificação da assinatura digital do *Loader* do *Kernel* deverá ser realizada, pelo dispositivo de segurança (MSE), com uso de uma das chaves relacionadas aos seguintes certificados (Figura 3): AC Urna e "Inicializador" (nível 0), Oficial, Simulado e Desenvolvimento (nível 1) ou pela chave de Manutenção.

139.3. Caso o *Loader* do *Kernel* não seja autêntico, a urna deverá ter o seu funcionamento impedido e acender a cor AMARELA no Led da Cadeia Segurança do TE, piscando em 2 Hz;

139.4. Ao iniciar a autenticação do *Loader* do *Kernel*, o Led da Cadeia de Segurança deverá ser aceso na cor AMARELA, piscando em 8 Hz;

140. A autenticação do *Kernel* do UENUX, quando configurada para ser realizada pelo dispositivo de segurança, deverá seguir o mesmo critério descrito no item 139, ou seja, utilizando a mesma chave que validou o *Loader* do *Kernel*.

140.1. Após a carga do *Kernel* do UENUX, caso o sistema não seja autêntico, a urna eletrônica deverá ter o seu funcionamento impedido depois de 4 minutos a partir do início da execução do *Loader* do *Kernel* e acenderá a cor VERMELHA no Led da Cadeia de Segurança do TE, piscando em 2 Hz;

140.2. Ao iniciar a autenticação do *Kernel* do UENUX, o Led da Cadeia de Segurança deverá ser aceso na cor VERMELHA, piscando em 8 Hz;

141. Quando a autenticação do *Kernel* do UENUX ocorrer com um certificado de nível 1, deverá ser feita uma autenticação do dispositivo de segurança (MSE), conforme ilustra a Figura 6. Essa autenticação corresponderá a um protocolo de desafio-resposta executado por uma aplicação em nível de usuário. Em resumo, a autenticação deverá ser implementada da seguinte forma:

141.1. a aplicação autenticadora acenderá o Led da Cadeia de Segurança na cor AMARELA, piscando em 4 Hz;

141.2. a aplicação autenticadora requisitará os certificados da urna ao MSE;

141.3. o dispositivo de segurança MSE enviará os certificados da urna para a aplicação autenticadora;

141.4. a aplicação autenticadora comparará os certificados recebidos, após a requisição do passo do item 141.2, com sua cópia local do certificado AC Urna;

141.5. a aplicação autenticadora gerará 16 bytes aleatórios;

141.6. o dispositivo de segurança MSE assinará o dado gerado do item 141.5, com o componente de chave privada do certificado nível 2;

141.7. o dispositivo de segurança MSE enviará a assinatura realizada no item 141.6 para a aplicação autenticadora e libera o MSE para uso;

141.8. a aplicação autenticadora verificará a assinatura com o certificado nível 2 enviado pelo MSE, no passo do item 141.3;

141.9. caso a verificação do passo do item 141.8 seja bem sucedida:

141.9.1. liberará a placa-mãe para uso;

141.9.2. caso o certificado de nível 2 utilizado no passo do item 141.8 tenha sido o Oficial, acenderá o Led da Cadeia de Segurança do TE com a cor VERDE, continuamente, sem piscar;

141.9.3. caso o certificado de nível 2 utilizado no passo do item 141.8 tenha sido diferente do Oficial, acenderá o Led da Cadeia de Segurança do TE com a cor VERMELHA, continuamente, sem piscar;

141.10. caso a verificação do passo do item 141.8 seja mal sucedida:

141.10.1. impedirá o uso da placa-mãe;

141.10.2. impedirá o funcionamento dos teclados do TE e do TM;

141.10.3. acenderá o Led da Cadeia de Segurança do TE com a cor VERMELHA, piscando em 1 Hz;

142. uma versão mais detalhada do processo de autenticação será repassada para a Contratada.

143. O estado inicial dos módulos TE (Terminal do Eleitor) e TM (Terminal do Mesário) deverá ser bloqueado. O desbloqueio só poderá ser realizado pelo *Kernel* do UENUX e deverá atender às seguintes regras de funcionamento:

143.1. Funcionamento restrito: somente as teclas BRANCO e CORRIGE, do TE ficarão liberadas. Isso ocorrerá quando os itens 139 e 140 forem atendidos utilizando-se apenas uma chave do nível 0, modo Manutenção ou modo Inicializador;

143.2. Funcionamento pleno: o teclado do TE e do TM deverá operar normalmente, ou seja, todas as teclas devem ser reconhecidas. Isso ocorrerá quando os itens 139 e 140 forem atendidos utilizando-se uma chave do nível 1;

144. Quando a autenticação pela chave de manutenção for utilizada, o Led da Cadeia de Segurança do TE deverá acender na cor AMARELA, continuamente. Somente as chaves de autenticação do TSE poderão permitir que a urna eletrônica possa operar sem restrições;

145. O TSE poderá solicitar modificações na forma de sinalização e nas mensagens retornadas ao usuário durante a autenticação dos dispositivos de segurança, devendo estas serem formalizadas na avaliação do Modelo de Qualificação.

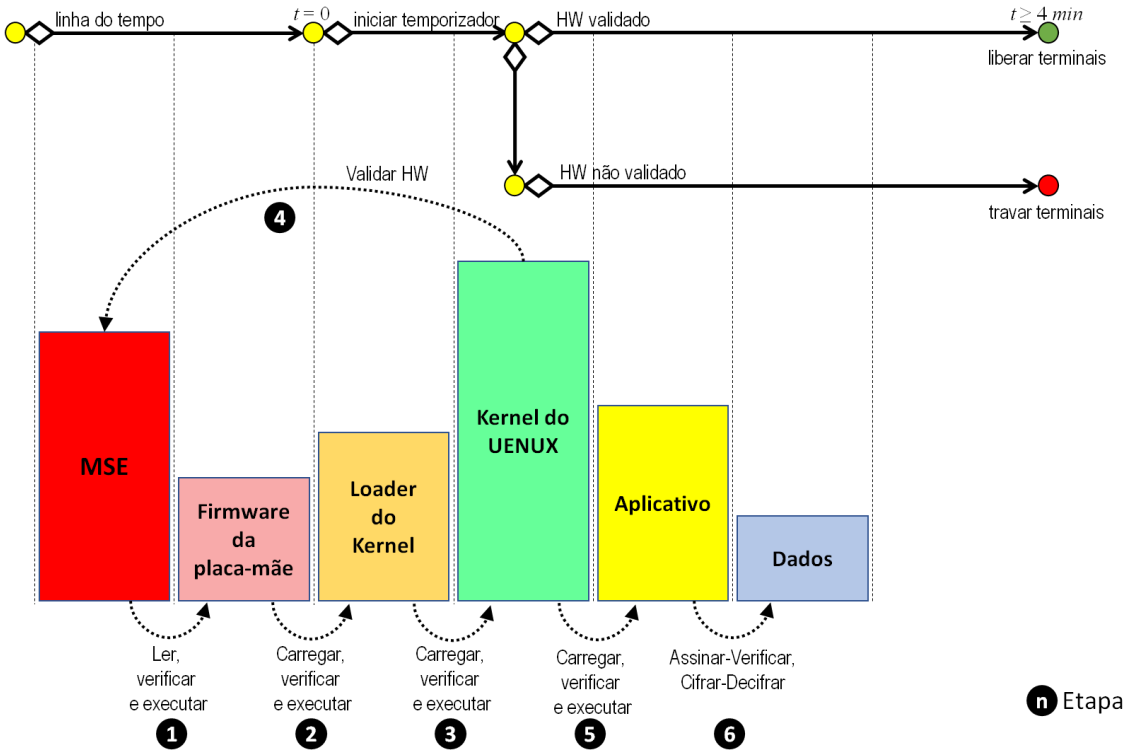

Figura 6 - Cadeia de Segurança

M.14. **Logs e registros**

146. O sistema deverá prover mecanismo para registrar qualquer tipo das seguintes operações nos dados criptográficos e PCSs:

146.1. modificação,

146.2. acesso,

146.3. apagamento e

146.4. adição;

N. Requisitos de Interoperabilidade

N.15. Características da API (Application Programmable Interface)

147. A API deverá:

147.1. Disponibilizar aos aplicativos o acesso estruturado a todos os recursos da UE2022, como mostrar uma informação textual e gráfica, armazenar, recuperar, imprimir e transmitir as informações tratadas e geradas na UE2022;

147.2. Permitir que o desenvolvimento de aplicativos da urna seja baseado somente nas interfaces especificadas nas APIs.

148. Todos os dispositivos da urna eletrônica devem utilizar estruturas internas do *kernel*.

148.1. Quando da inexistência de definições específicas, deverá seguir padrões de mercado: ISO 15435/1999, ISO 9945-1/2002 [IEE 1003.1-2001], WOSA, Motif, PKCS#11 v2.30 ou superior.

149. Os ajustes no Relógio Interno, posteriores àquele realizado em fábrica, somente poderão ser realizados via *software*. O BIOS não deverá permitir o ajuste de data e hora pelo setup.

150. Assinatura e Criptografia: Interface para assinatura digital, criptografia simétrica e assimétrica para arquivos, PKCS#11 v2.30 ou superior.

151. Não utilizar tecnologia tida como obsoleta tanto pelo mercado como pelo meio acadêmico.

N.16. Sustentação

152. A biblioteca criptográfica (com funções assimétricas de curvas elípticas) irá permitir utilização de quaisquer curvas de quaisquer tamanhos. Os parâmetros das curvas, inclusive seus tamanhos, serão argumentos de entrada dessa biblioteca;

153. Não será fornecido à Contratada o código-fonte das bibliotecas criptográficas. Somente serão fornecidos os binários compilados pelo TSE em máquina de sua propriedade.

154. A critério do TSE, qualquer algoritmo acima poderá ser excluído ou substituído;

155. A Contratada será responsável pela realização de testes das bibliotecas fornecidas pelo TSE quando da integração ao seu *hardware*, não podendo, após o fornecimento das urnas eletrônicas, alegar defeitos nas mesmas para se isentar da prestação da garantia técnica prevista neste edital;

N.17. Características do *Firmware*

156. Todos os componentes do perímetro criptográfico deverão ser implementados por uma linguagem de alto nível, exceto se o uso de uma linguagem de baixo nível (ex.: *Assembly*) for tido como essencial em relação ao desempenho e seu uso for expressamente autorizado pelo TSE. Neste caso, quando um código em *assembly* for implementado, o código-fonte correspondente a esse *assembly* deverá ser entregue ao TSE;

O. Algoritmos Criptográficos Obrigatórios

157. O módulo criptográfico deverá suportar, no mínimo, as seguintes funções criptográficas, que serão fornecidas na forma de API, pela Contratada (exceto aqueles que explicitamente definidos como fornecidos pelo TSE):

157.1. Criptografia de Dados:

157.1.1. Cifração e decifração simétricas AES-CTR com tamanho de chave de no mínimo 256 bits (conforme padrão NIST FIPS PUB 197);

157.1.2. Cifração e decifração assimétricas ECIES com chaves de no mínimo 521 bits (conforme padrão SECG SEC 1 (sem a XOR para cifração) ou IEEE 1363a) – fornecido pelo TSE;

157.2. Autenticação de Entidades com Criptografia de Chave Pública:

157.2.1. EdDSA com chaves de pelo menos 521 bits - fornecido pelo TSE;

157.2.2. RSA com chaves de tamanho entre 2048 e 4096 bits (conforme padrão ANSI X9.31 e PKCS#1 v1.5);

157.3. Resumo Digital Criptográfico de Dados

157.3.1. SHA-1 (conforme padrão NIST FIPS PUB 180-2);

157.3.2. Família SHA-2, inclusive SHA-256, SHA-384 e SHA-512 (conforme padrão NIST FIPS PUB 180-4);

157.3.3. Família SHA-3, inclusive Shake256 (conforme padrão NIST FIPS 202);

157.4. Funções para Autenticação e Verificação de Integridade

157.4.1. CBC-MAC baseado nos algoritmos AES (conforme padrão NIST PUB 800-38B);

157.4.2. HMAC baseado nos algoritmos de resumo criptográficos implementados (conforme padrão NIST FIPS PUB 198);

157.4.3. MAC com SIPHASH (conforme implementação de Aumasson & Bernstein – *SipHash: a fast short-input PRF* ou biblioteca indicada pelo TSE);

157.4.4. CMAC baseado nos algoritmos AES (conforme padrão NIST PUB 800-38B);

157.4.5. CCM-MAC baseado nos algoritmos AES (conforme padrão NIST PUB 800-38C);

157.4.6. EAX-MAC[2] baseado nos algoritmos AES.

157.5. A sintaxe de comandos da API será entregue à Contratada, pelo TSE;

157.6. Outros algoritmos propostos deverão ser submetidos ao TSE para aprovação;

P. Requisitos de Documentação

158. Os requisitos do perímetro criptográfico serão baseados em um subconjunto de itens contidos no Manual de Condutas Técnicas 7 - Volume I, versão 1.0 (MCT-7), publicado pela Estrutura de Chaves Públicas Brasileira – ICP-Brasil, os quais o TSE entende como requisitos mínimos para o projeto da Urna Eletrônica. Os textos referentes aos requisitos foram alterados com o objetivo de ajustá-los às necessidades do projeto da Urna Eletrônica;

159. A Contratada deverá entregar documentação completa da solução ao TSE, abrangendo todos os módulos de segurança: MSE e os módulos criptográficos dos periféricos. Nos próximos itens, a palavra "documentação" se referirá à documentação de todos os módulos criptográficos da UE2022.

160. A documentação deverá especificar todas as chaves criptográficas, seus componentes e PCSs empregados pelo perímetro criptográfico;

161. A documentação deverá especificar quais métodos serão usados pelo respectivo módulo criptográfico, para proteger chaves públicas e secretas, chaves privadas, programas e *firmwares*, e PCSs, contra divulgação, modificação e substituição não autorizada;

[2] BELLARE, M.; ROGAWAY, P.; WAGNER, D. – The EAX Mode Operation (A Two-Pass Authenticated-Encryption Scheme Optimized for Simplicity and Efficiency. In: *LNCS 3017 – Proceedings of the Fast Software Encryption 2004*, p389-407, 2004 (disponível em https://web.cs.ucdavis.edu/~rogaway/papers/eax.pdf)

162. A Contratada deverá fornecer documentação específica de qualquer componente de *hardware*, *software* ou *firmware* que esteja excluído dos requisitos de segurança apresentados neste documento e explicar a razão para tal exclusão;

163. A documentação deverá especificar o ambiente de desenvolvimento utilizado para implementar o respectivo módulo criptográfico;

164. A documentação sobre o armazenamento e a proteção de dados em claro, de *softwares* e *firmwares*, de chaves criptográficas, dos PCSs e dos dados de autenticação deverá estar muito bem detalhada;

165. A documentação deverá especificar o método de RNG, detalhando passo a passo;

166. A documentação deverá especificar os métodos de armazenamento de chaves criptográficas empregados no respectivo módulo criptográfico;

167. A documentação deverá especificar o código-fonte com comentários que esclareçam a correspondência dos componentes do respectivo módulo criptográfico;

168. A documentação do perímetro criptográfico deverá especificar:

168.1. Os mecanismos de autenticação suportados pelo perímetro criptográfico;

168.2. Os tipos de dados de autenticação que serão requisitados pelo perímetro para implementar os mecanismos de autenticação suportados;

168.3. Os métodos autorizados que serão utilizados para realizar o controle de acesso ao perímetro criptográfico no seu primeiro acesso e, em seguida, inicializar o mecanismo de autenticação.

169. A Contratada deverá fornecer documentação técnica completa de projeto e de produto da Urna Eletrônica e de cada módulo criptográfico;

170. Toda a documentação prevista neste Anexo deverá ser entregue ao TSE até a entrega do Modelo de Produção – MP.

P.18. **Manuais**

171. A Contratada deverá fornecer:

171.1. **Manual de Instalação**, especificando a arquitetura da Urna Eletrônica na qual é suportada a instalação de cada módulo criptográfico;

171.2. **Manual de Configuração**, detalhando as ferramentas e recursos disponíveis para a configuração de cada módulo criptográfico na Urna Eletrônica onde o mesmo será implantado;

171.3. **Manual de Operador**, detalhando as ferramentas e recursos disponíveis de cada módulo criptográfico;

171.4. **Manual de Administrador** (*Security* Officer), detalhando as ferramentas e recursos disponíveis somente aos administradores de cada módulo criptográfico;

171.5. **Manual de desenvolvedor** detalhando a(s) API(s) proprietária(s) para desenvolvimento de aplicações utilizando o perímetro criptográfico;

171.6. **Manual de Integração** de cada módulo criptográfico com a(s) API(s) de mercado para desenvolvimento de sistemas integrados;

171.7. **Manual de Importação de Chaves** para dentro de cada módulo criptográfico, detalhando a aplicabilidade do uso de outros *hardwares* externos ao respectivo módulo.

Q. Requisitos Gerais

Q.19. Requisitos Gerais de Desenvolvimento

172. O projeto de desenvolvimento do *hardware* criptográfico, incluindo suas interfaces com outros módulos e dispositivos será feito de modo interativo, sendo a solução para os requisitos validada e aprovada pelo TSE;

Q.20. Requisitos Gerais de Segurança

173. A versão de produção dos *firmware*s deverá ser compilada com a presença de técnicos do TSE, com os seguintes requisitos mínimos:

173.1. As respectivas ferramentas de compilação deverão ser disponibilizadas, em licença definitiva, incluindo eventuais bibliotecas de terceiros, para que o TSE possa atualizar e recompilar o *firmware* fornecido pela Contratada;

173.2. A Contratada deverá disponibilizar documentação de instalação do ambiente e geração do *firmware* reproduzindo as mesmas condições do ambiente de geração da versão de produção;

173.3. Quaisquer atualizações de versão e correções durante o período da garantia do *Software* ficará por conta da Contratada e, após este período, deverá haver apenas a geração de nova versão com a correção;

Q.21. Requisitos do Display do MSE

174. O Display do MSE deverá mostrar mensagens específicas de sucesso e modo de inicialização, em todas as fases durante a cadeia de segurança.

174.1. No mínimo, deverão ser mostradas mensagens de todas as fases onde há indicação diferenciada pelo Led da Cadeia de Segurança descritos neste Anexo, assim como quaisquer mensagens de erro correspondentes nessas fases;

174.2. A Contratada, durante o desenvolvimento da segurança em *hardware*, deverá sugerir as mensagens de sucesso e erro a serem apresentadas no Display do MSE, relacionadas a todo o fluxo de inicialização da urna e utilização dos serviços do MSE e demais dispositivos de segurança, as quais serão aprovadas pelo TSE;

Q.22. Requisitos de Certificação

175. O perímetro criptográfico do MSE deverá ser homologado ICP-Brasil, atendendo, no mínimo, aos requisitos necessários para a geração de certificados tipo A4 e S4 (sob a hierarquia da raiz da cadeia V7 da ICP-Brasil – E-521) com Nível de Segurança de Homologação 3 – NSH3;

175.1. A homologação será por conta da Contratada e deverá utilizar laboratórios acreditados no âmbito do Sistema Brasileiro de Avaliação de Conformidade – SBAC do INMETRO e Organizações Certificadoras de Produtos para esta finalidade;

175.2. Como referência, deverá ser utilizado o Manual de Condutas Técnicas – 03 do ITI ou outro conjunto de requisitos equivalente a este Anexo deste Projeto Básico;

R. Verificação dos requisitos de Segurança

176. Os requisitos deste Anexo IV ao Projeto Básico serão verificados durante a licitação nos testes de segurança descritos no Anexo Ia;

177. Os demais requisitos serão aferidos pelo TSE durante o desenvolvimento do projeto da UE2022, de acordo com o item 172, sempre com o objetivo de conferir efetividade das implementações de segurança conforme os propósitos de cada item, resultando em um *hardware* adequadamente seguro.