Anexo IV – Especificações Técnicas - Segurança

URNA ELETRÔNICA – UE2020

Sumário

A. Aspectos Gerais

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

1. A segurança da Urna Eletrônica (UE) deve 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) consiste de um modelo conceitual de dispositivo periférico seguro, que poderá ser adquirido em momento posterior ao da aquisição da UE2020. Portanto, a implementação do hardware e firmwares de segurança da UE2020 deverá prever a conexão, no futuro, de novos periféricos.

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

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

1.3.1. Deve 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;

2. O perímetro criptográfico consiste de uma fronteira explicitamente definida, que estabelece os limites físicos do respectivo módulo criptográfico.

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) deve ser realizada estabelecendo-se canais seguros de comunicação, que utilizem módulos criptográficos próprios de cada periférico e do Módulo de Segurança Embarcado (MSE).

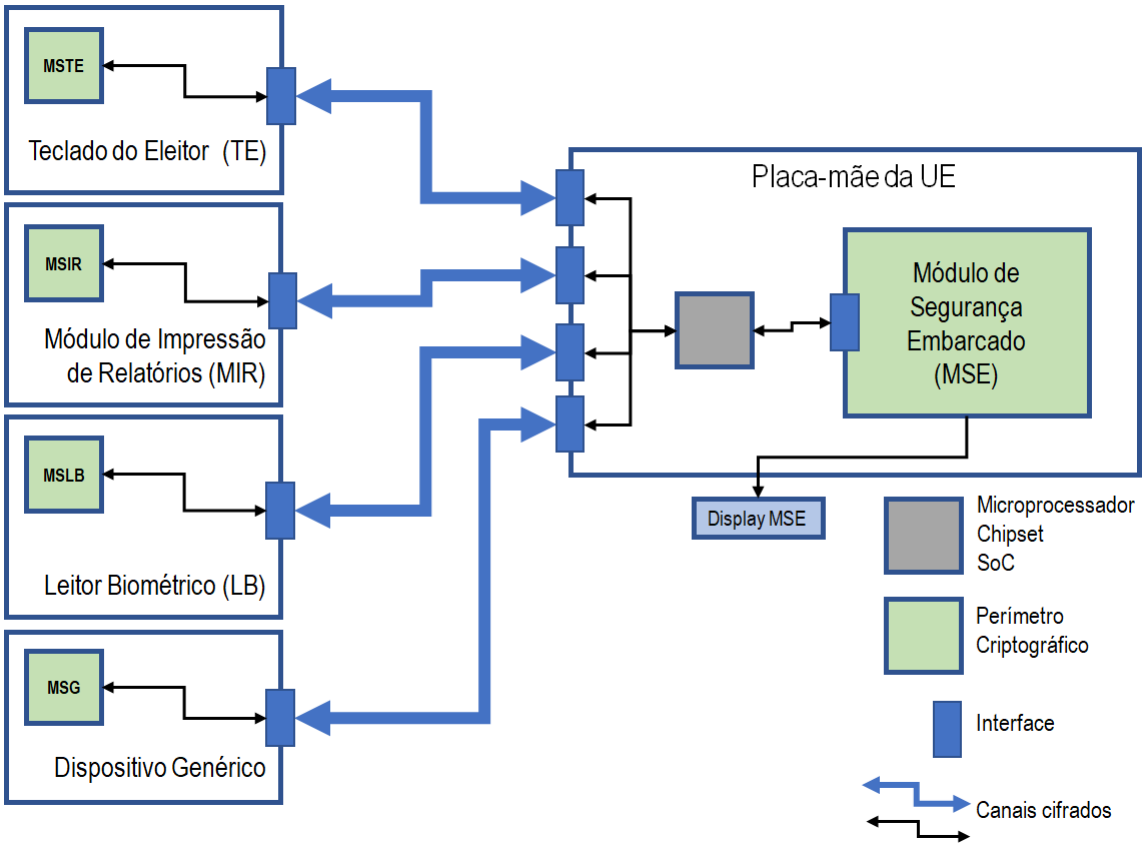

Figura 1 - Arquitetura de segurança da comunicação entre os dispositivos seguros da UE

4. Um módulo criptográfico contém, no mínimo, 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. cada uma das unidades de memória, dos itens 4.2, 4.3 e 4.4, não deve 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. firmwares.

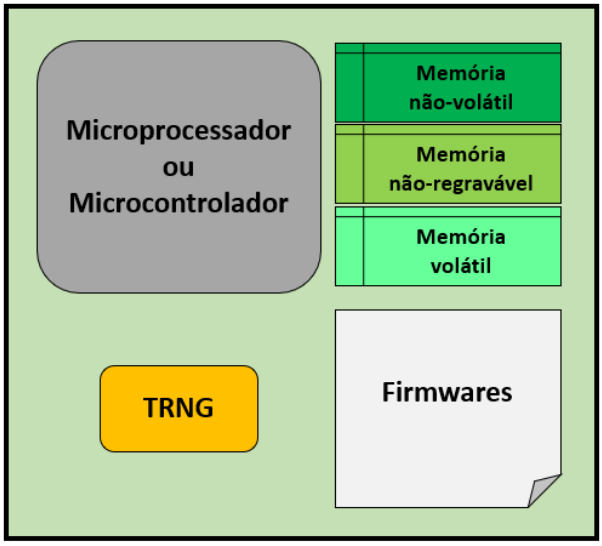

Figura 2 - Componentes mínimos de um módulo criptográfico

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

5. O Módulo de Segurança Embarcado (MSE) consiste de um sistema computacional confinado a perímetros físicos restritos, embarcado em um sistema computacional hospedeiro, que em conjunto com um firmware, implementa 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 deve ser utilizado na carga do sistema operacional das UEs.

7.1. A carga do sistema operacional nas UEs deve 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 tem 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. Estão 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, bootloader, 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 bootloader como o “Loader do Kernel” e o Kernel do UENUX pelo mesmo nome;

11.2. Conforme especificação da versão 2.7[1] do UEFI (Unified Extensible Firmware Interface):

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. TSL: fase “Transient System Load”;

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 TSL 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 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;

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

11.2.12. Qualquer partição de sistema utilizada por uma cadeia de validação UEFI deve 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 devem ter desempenho suficiente para realizar tarefas de assinatura e verificação.

12.1. Para efeito de aferição, o microprocessador (microcontrolador) proposto do MSE deverá executar o algoritmo P-521 (secp521r1) da implementação de referência da biblioteca BearSSL (versão 0.5)[2].

12.2. Os tempos máximos a serem atingidos são:

12.2.1. Tempo de assinatura ECDSA (com algoritmo hash SHA512) de um bloco maior ou igual a 1 Kbytes em até 1 milissegundos;

12.2.2. Tempo de verificação da assinatura ECDSA (com algoritmo hash SHA512) 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;

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

14. Os tempos registrados no item 12 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 pela realização dos testes de desempenho do Anexo Ia;

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 43 e 4 certificados para sigilo, com o mecanismo descrito no item 42. 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 processo definido pelo TSE e informado após a assinatura do contrato;

18. Deverá ser previsto espaço para o armazenamento equivalente a 5 (cinco) 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 43, referente à assinatura utilizada para autenticar o firmware da placa-mãe com a chave de nível 0;

[2] https://bearssl.org/#download-and-installation

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 fornecer, 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 exigem, 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 firmwares 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 deve fornecer documentação específica de todas as portas físicas, interfaces lógicas e caminhos de dados definidos como de entrada e saída do respectivo módulo criptográfico;

26. A Contratada deve fornecer documentação específica dos controles lógicos e manuais do perímetro criptográfico;

27. A Contratada deve fornecer documentação específica de todos os indicadores de estados lógicos e físicos do perímetro criptográfico;

28. A Contratada deve fornecer documentação específica das características elétricas, lógicas e físicas aplicáveis ao perímetro criptográfico;

29. A Contratada deve fornecer documentação específica que:

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

29.2. especificar todos os modos de operação suportados, para cada função de segurança/operação criptográfica listada no item 29.1 acima;

30. A Contratada deve fornecer documentação contendo diagramas de blocos detalhando todos os principais componentes de *hardware* e de interconexão, incluindo:

30.1. Microprocessadores;

30.2. Buffers de entrada e saída;

30.3. Buffers com conteúdo de texto em claro;

30.4. Buffers com conteúdo de texto cifrado;

30.5. Buffers de controle;

30.6. Memórias de armazenamento das chaves criptográficas;

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

30.8. Memória de trabalho ou operacional;

30.9. Memória de programa;

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

31. A Contratada deve fornecer 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;

32. A Contratada deve fornecer 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:

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

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

32.3. Parâmetro Crítico de Segurança - PCS;

32.4. 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.

33. A Contratada deve fornecer 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

34. O fornecimento da energia elétrica do perímetro criptográfico deve obrigatoriamente provir 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 para o MSE;

35. Devem ser documentadas todas as interfaces lógicas e físicas presentes no perímetro criptográfico;

36. O perímetro criptográfico deve assegurar que o fluxo de informação e acesso físico sejam realizados apenas pelas portas físicas e interfaces lógicas relacionadas na documentação referida no item 35;

37. Todo dado que entra no perímetro criptográfico via respectiva interface de entrada deve seguir somente pelo caminho de entrada definido para essa finalidade. Da mesma forma, todo dado que sai do perímetro criptográfico via respectiva interface de saída deve seguir somente pelo caminho de saída definido para essa finalidade;

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

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

38.2. Componentes de chaves criptográficas, dados de autenticação e outras PCS, devem entrar ou sair diretamente do perímetro criptográfico (via caminho confiado ou cabo diretamente ligado).

D. Requisitos de Papéis, Serviços e Autenticação

D.7. **Serviços**

39. 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;

40. Cifração e decifração simétricas;

41. Geração de chaves assimétricas;

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

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

43. Assinatura digital e verificação;

43.1. EdDSA com chaves de pelo menos 521 bits;

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

44. Algoritmo de resumo digital:

44.1. SHA-1;

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

44.3. Família SHA-3, inclusive Shake256;

45. Algoritmos de autenticação com chave:

45.1. HMAC com Família SHA-2;

45.2. MAC com SIPHASH;

46. Gerador de número aleatório em hardware, conforme definido nos itens 101 e 102;

47. Gerador de número aleatório PRNG.

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

48.1. Os estados serão baseados no Modelo de Estado Finito, com requisitos definidos no item E e subitens;

49. Atualizar firmwares dos dispositivos listados no item 1 e subitens, permitindo a atualização completa dos firmwares de todos os dispositivos ou individualmente, para cada dispositivo e cada firmware, conforme definido no item 67.

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

49.1.1. 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.

49.2. Os métodos para a prova de conteúdo na atualização dos firmwares serão tratados em reunião inicial com a Contratada;

50. Executar os auto-testes especificados na seção J;

51. 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).

52. As bibliotecas criptográficas previstas nos itens 40, 41, 42, 43, 44, 45, 47 consistirão de implementações proprietárias e serão fornecidas pelo TSE.

52.1. Todas as operações que exigirem uso de fonte de aleatoriedade real (física), devem utilizar os serviços do item 46;

52.2. 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;

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

53. Os serviços 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51 se referem a todos os módulos criptográficos listados no item 1;

D.8. **Autenticação**

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

E. Requisitos do Modelo de Estado Finito

55. A operação dos módulos criptográficos da UE deve 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.

55.1. Cada módulo criptográfico, o que inclui o MSE e os módulos criptográficos dos periféricos indicados no item 1, devem ter seus respectivos Modelos de Estado Finito.

55.2. O diagrama de transição de estados e/ou a tabela de transição de estados deve incluir:

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

55.2.2. As transições de um estado ao outro;

55.2.3. Os eventos de entrada que causam transições de um estado para outro;

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

55.3. O módulo criptográfico deve incluir os seguintes estados operacionais e estados de erro:

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

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

55.3.3. Estados de usuário: Estados nos quais os usuários autorizados obtêm serviços de segurança, realizam operações criptográficas ou desempenham outras funções;

55.3.4. Estados de auto-teste: Estados nos quais o módulo criptográfico realiza auto-testes;

55.3.5. Estados de erro: Estados quando o módulo criptográfico encontra um erro (por exemplo, falha em um auto-teste ou tentativa de criptografar quando chaves operacionais ou PCS foram perdidos). Estados de erro poderiam incluir: a) “Erros críticos”, 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 inicialização (*resetting*) do módulo criptográfico. A recuperação a partir de estados de erro deve ser possível, exceto para os casos em que ocorram os “Erros críticos”.

55.3.6. Um módulo criptográfico pode, 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 deve ser incluído.

55.4. Não será aceito qualquer tipo de estados de desvio (*by-pass*).

55.5. A documentação de cada módulo criptográfico deve 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 deve especificar:

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

55.5.2. As transições correspondentes de um estado para outro;

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

55.5.4. 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

56. 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;

57. 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);

57.1. 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;

58. Pode haver mais de um perímetro criptográfico na UE;

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

59.1. espessura mínima de 5 mm;

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

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

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

59.5. 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;

60. Portas, tampas ou interfaces de acesso para manutenção, quando presentes no perímetro criptográfico, devem ser protegidas com sensores que detectam o acesso a estas portas. A ativação de tais sensores deve 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;

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

62. 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 devem ser protegidas (ex: trilhas internas), sendo que a solução sugerida pela Contratada deverá ser aprovada pelo TSE;

62.1. 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;

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

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

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

G. Requisitos do Ambiente Operacional

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

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

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

66.3. Os algoritmos criptográficos empregados forem aprovados pelo TSE.

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

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

67.2. 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*.

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

67.4. O processo de atualização deve:

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

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

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

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

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

b) Tais registros de eventos devem ser recuperáveis;

c) Deve ser possível autenticar tais registros de eventos;

68. 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 componentes de *software* e *firmware* validados.

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

69.1. Para aferir a integridade de sua amostra original:

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

69.2. Para aferir o sucesso da operação de carga:

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

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

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

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

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

71. Todos os dispositivos de hardware que representam ou lidam com PCSs (Parâmetros Críticos de Segurança) devem estar contidos conceitualmente em um perímetro criptográfico sujeito aos seguintes requisitos:

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

72. O perímetro criptográfico deve incluir os seguintes estados operacionais e estados de erro:

72.1. Estados de alimentação de energia:

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

72.2. Estados nos quais serviços são realizados

72.2.1. por exemplo, inicialização e gerenciamento de chaves criptográficas;

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

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

72.4. Estados de auto-teste:

72.4.1. Estados nos quais são realizados auto-testes no perímetro criptográfico;

72.5. Estados de erro:

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

72.5.2. “Erros leves e recuperáveis”: exigem apenas uma nova inicialização do perímetro criptográfico.

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

73. Será definido pelo TSE, em conjunto com a Contratada, um processo específico para segurança no processo de gravação dos firmwares dos dispositivos seguros listados no item A.1.1;

74. 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;

75. Estas versões de firmware não deverão incluir a lógica de negócio e os algoritmos criptográficos especificados neste Anexo. Incluirão funções de auto-teste, verificação de Hash, verificação de assinatura digital e outras, garantindo a integridade do conteúdo gravado e a integridade e autenticidade dos firmwares que serão gravados posteriormente;

76. 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;

77. 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;

78. 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

79. A hierarquia de chaves e certificados digitais das urnas modelo 2009 a 2020 está descrita na Figura 3.

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

80. A estrutura dos certificados armazenados no dispositivo de segurança possui 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;

81. Os modos Oficial, Simulado e Desenvolvimento são modos de Eleição e, após as verificações necessárias, deverão permitir o funcionamento pleno da urna, conforme item 151.2;

82. Os modos Inicializador e Manutenção devem permitir apenas o funcionamento restrito, conforme item 151.1;

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

83.1. 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;

83.2. As chaves especiais (veja Figura 3) e respectivo certificado de sigilo também deverão estar disponíveis em qualquer modo, exceto o modo manutenção;

83.3. 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;

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

84.1. receber os certificados digitais do TSE "AC Urna" e "Inicializador", e a assinatura do "*Firmware* da placa-mãe", assinado pela chave privada correspondente à chave pública do certificado "Inicializador".

84.2. 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*);

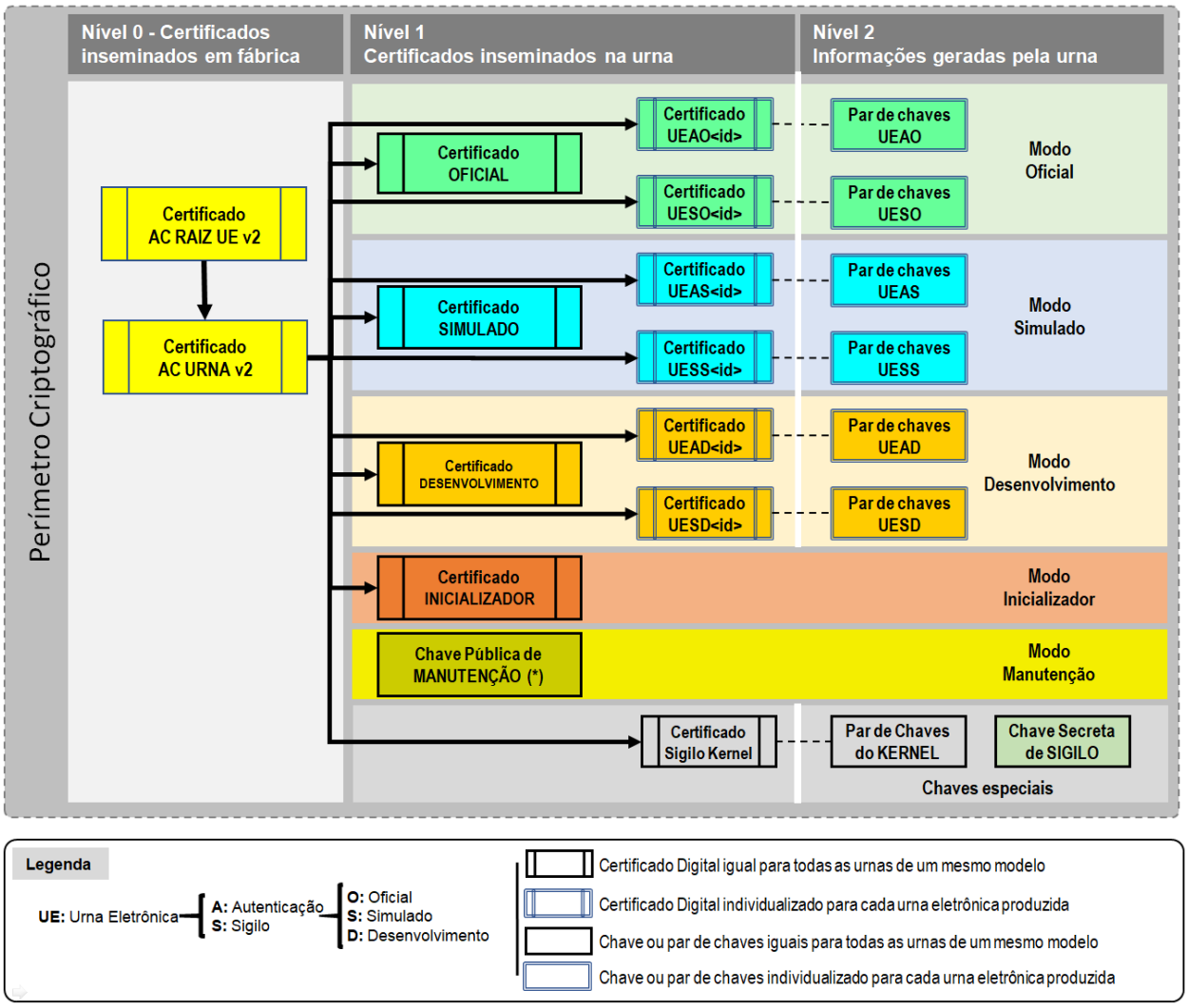

Figura 3 - Estrutura de chaves assimétricas da Justiça Eleitoral

85. Após o processo descrito no item 84, 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 101) deverá ser utilizado para a geração destas chaves;

85.1. 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 84;

86. Estes certificados, juntamente com os demais certificados e chaves gerados pelo TSE, serão inseridos no dispositivo de segurança da UE2020 conforme estrutura definida na Figura 3.

87. Chaves secretas, chaves assimétricas privadas e PCSs devem estar protegidas, dentro do perímetro criptográfico, contra divulgação, modificação e substituição não autorizada;

88. Chaves assimétricas públicas devem estar protegidas dentro do perímetro contra modificação e substituição não autorizada;

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

90. O sistema deve 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;

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

92. Uma chave pública pode ser importada ou exportada do perímetro criptográfico;

93. Deve 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, deve ser definido tal atributo como “não exportável” e não deverá ser possível alterar seu valor para “exportável”;

94. Deve 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, deve ser definido tal atributo como “não exportável” e não deverá ser possível alterar seu valor para “exportável”;

95. Chaves criptográficas devem ser armazenadas dentro do perímetro criptográfico em claro ou cifradas;

96. Chaves assimétricas privadas e simétricas secretas não devem ser acessíveis;

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

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

98. A documentação deve especificar os métodos de importação e ou de exportação de chaves criptográficas empregados pelo perímetro criptográfico;

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

99. 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, deve ser

comparada com os *n* bits previamente gerados. O teste deve falhar se quaisquer das sequências comparadas de *n* bits forem iguais;

100. 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;

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

101.1. Possuir fonte de ruído redundante;

101.2. Possuir fonte de entropia própria implementada em hardware;

101.3. Possuir teste contínuo da fonte de entropia;

101.4. Possuir controle contínuo de qualidade;

101.5. Possuir auto-teste, da saída dos valores aleatórios, para indicar;

101.5.1. se o TRNG está energizado;

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

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

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

101.8. Não estar embutido em circuito integrado;

101.9. 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;

101.10. 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;

101.10.1. 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);

101.11. Ter projeto aceito pela equipe técnica do TSE.

102. Cada um dos módulos criptográficos presentes no MSLB, MSIR e MSG deve conter um gerador de número aleatório implementado em hardware. Cada um desses geradores de números aleatórios deve:

102.1. Atender as recomendações contidas nos documentos:

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

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

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

102.2. Possuir fonte de entropia própria implementada em hardware;

102.3. Possuir teste contínuo da fonte de entropia;

102.4. Possuir controle contínuo de qualidade;

102.5. Possuir auto-teste, da saída dos valores aleatórios, para indicar;

102.5.1. se o gerador de números aleatórios está energizado;

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

102.6. 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;

102.7. 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;

102.8. Ter especificação aceita pela equipe técnica do TSE.

I. Requisitos de Interferência e Compatibilidade Eletromagnética

103. 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;

104. O dispositivo contido no perímetro criptográfico não deve 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 103.

105. A UE deve ser protegida contra ataques e análises de radiações eletromagnéticas emanadas e conduzidas. Em especial a UE deve:

105.1. 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;

105.2. 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 devem ser 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:

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

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

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

106. A Contratada deverá apresentar documentação comprovando conformidade da Urna Eletrônica 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);

107. 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 Auto-testes

108. Para verificar o funcionamento apropriado do perímetro criptográfico, duas categorias de auto-testes devem ser realizadas:

108.1. auto-testes de energização:

108.1.1. tais testes devem ser executados quando o perímetro é energizado (ou alimentado com energia elétrica);

108.2. auto-testes condicionais:

108.2.1. tais testes devem ser executados quando uma operação ou função de segurança aplicável é solicitada.

109. Se o perímetro criptográfico falhar durante um auto-teste, o perímetro criptográfico deve 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.

110. O perímetro criptográfico não deve realizar qualquer operação criptográfica enquanto persistir o estado de erro provocado por falhas em um auto-teste;

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

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

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

114. A documentação do respectivo módulo criptográfico deve especificar os seguintes itens:

114.1. Os auto-testes realizados pelo respectivo módulo criptográfico;

114.2. O estado de erro que o respectivo módulo criptográfico puder entrar quando um auto-teste falha;

114.3. 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);

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

114.5. Testes de funções críticas;

114.6. Outros testes realizados na energização ou sob demanda.

K. Requisitos de Garantia do Projeto

115. Todos os códigos-fonte de firmwares e APIs devem ser abertos ao TSE, que por sua vez, deve poder torná-los disponíveis aos interessados em auditar as urnas eletrônicas;

115.1. O código-fonte em assembly que não tiver código-fonte em linguagem de alto nível correspondente deve vir acompanhado do pseudo-código correspondente, em linguagem natural e documentado;

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

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

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

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

120. O documento "Guia do Administrador" deve especificar:

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

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

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

121. O documento "Guia do Usuário" deve especificar:

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

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

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

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

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

125. Todos os circuitos geradores de números aleatórios (TRNG) deverão passar por testes que atestem a conformidade com o item 101.

125.1. Esses testes deverão ser condição para aprovação do Modelo de Qualificação e deverão ocorrer após a entrega dos equipamentos citados no item 126, em bancada com energia, espaço e tempo disponíveis para que permaneçam em execução por, pelo menos, 7 (sete) dias corridos.

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

125.3. Tais testes, chamados de Testes do TRNG, se iniciarão logo após as entregas dos equipamentos citados no item 126.

125.3.1. Caso ocorram insucessos na realização dos testes, a Contratada poderá implementar as correções até atingir a conformidade com o item 101, desde que a citada conformidade seja atingida até a aprovação do Modelo de Qualificação.

126. Para dar cabo dos testes do item 125, deverão ser disponibilizados:

126.1. Uma placa-mãe, com a resina aplicada (item 59), da UE2020 com o MSE contendo o circuito TRNG a ser testado;

126.2. Uma placa de cada um dos periféricos contendo os módulos de segurança listados no item 1, com TRNG e também com a resina aplicada (item 59), quando aplicável.

126.3. Firmwares específicos para a coleta das massas de valores aleatórios de cada um dos dispositivos TRNG dos itens 126.1 e 126.2.

126.3.1. Tais firmwares deverão ser carregados nos respectivos dispositivos de maneira segura, conforme preconiza o item 76;

126.3.2. Os códigos-fonte desses firmwares 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;

126.3.3. As massas de valores aleatórios geradas devem 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.

127. 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 UE2020.

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

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

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

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

127.3.2. Gerar código realocável;

127.3.3. Ligar códigos para gerar executáveis binários;

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

127.3.5. Monitoramento de hardware;

127.3.6. Monitoramento da execução da aplicação;

127.3.7. Geração eficiente de código;

127.3.8. Otimização de código quanto a tempo e espaço;

127.3.9. Caso seja proprietário, o software deve ser licenciado, para cada um dos kits, ao TSE;

127.4. A Contratada deverá expor, para a área técnica do TSE, o processo de desenvolvimento de softwares embarcados, *firmwares* e *drivers* usando os referidos kits de desenvolvimento;

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

127.4.2. O treinamento deve ser obrigatoriamente presencial;

127.4.3. O treinamento deve ser realizado em um período de 3 (um) dias úteis consecutivos;

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

127.4.5. O treinamento deve 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 firmwares para as memórias onde serão gravados os *firmwares*, conforme especificado pela Contratada, na Proposta;

127.4.6. O treinamento deve 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 firmwares.

L. Requisitos de Mitigação a Ataques

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

129. 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.

130. A documentação técnica do respectivo módulo criptográfico deve especificar quais os tipos de ataques classificados como não invasivos são mitigados por este respectivo módulo;

131. A documentação técnica do respectivo módulo criptográfico deve especificar quais outros tipos de ataques são mitigados por este respectivo módulo;

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

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

132.1. o leitor de impressão digital;

132.2. o teclado do eleitor (TE);

132.3. o módulo impressor de relatórios (MIR);

132.4. um dispositivo genérico (DG).

133. Os canais de comunicação dos itens 132.1 e 132.2 devem ser cifrados e autenticados.

133.1. Para o canal seguro do item 132.2, a criptografia utilizada deve gerar um conjunto de dados diferente a cada tecla pressionada, inclusive se pressionada a mesma tecla repetidamente;

134. A decifração e a autenticação dos dados provenientes dos dispositivos periféricos do item 132 deverão ser realizadas pelo MSE, em hardware, com chave específica e protegida pelo dispositivo;

135. A chave utilizada para estabelecer a sessão segura deverá ser assinada por um certificado da hierarquia de chaves (Figura 3), que deverá ser implantado em cada um dos módulos listados no item 1;

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

M. Requisitos de Gerenciamento do MSE

137. Se a Contratada dispuser de utilitários de gerenciamento e diagnósticos de problemas, então deve tornar a respectiva documentação detalhada sobre esses utilitários disponíveis ao TSE.

M.13. **Cadeia de Segurança**

138. O *Firmware* da placa-mãe deverá permitir a inicialização da UE2020 pela Mídia de Aplicação (MA) ou pela Memória Interna (MI);

139. Não deve ser possível gravar o *Loader* do Kernel no Firmware da placa-mãe da UE2020. 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;

140. 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;

141. 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 seguintes características:

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

141.2. 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 145.1;

141.3. 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 145.1;

141.4. 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;

141.5. A leitura, verificação e entrega para execução do firmware da placa-mãe corresponde à etapa 1 descrita na Figura 4;

141.6. 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 4), não pode exceder 1,0s;

142. 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;

143. 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;

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

145. 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;

145.1. Não deverá haver microcontroladores ou outros dispositivos externos ao perímetro criptográfico que, se atacado, permita a continuidade do funcionamento da urna eletrônica, caso a autenticação descrita no item 145 não tenha sido completada com sucesso.

146. 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:

146.1. 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;

146.2. 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;

146.3. 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.

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

147. Deverá autenticar o Loader do Kernel por meio de assinatura digital de todo o seu conteúdo. A assinatura digital do Loader do Kernel deverá estar guardada dentro da Mídia de Aplicação (MA)/Memória Interna (MI). 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. 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;

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

148. A autenticação do Kernel do UENUX, quando configurada para ser realizada pelo dispositivo de segurança, deve seguir o mesmo critério descrito no item 147, ou seja, utilizando a mesma chave que validou o Loader do Kernel. 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;

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

149. 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 4. Essa autenticação corresponde a um protocolo de desafio-resposta executado por uma aplicação em nível de usuário. Em resumo, a autenticação deverá ser implementada da seguinte forma:

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

149.2. a aplicação autenticadora requisita os certificados da urna ao MSE;

149.3. o dispositivo de segurança MSE envia os certificados da urna para a aplicação autenticadora;

149.4. a aplicação autenticadora compara os certificados recebidos, após a requisição do passo do item 149.2, com sua cópia local do certificado AC Urna;

149.5. a aplicação autenticadora gera 16 bytes aleatórios;

149.6. o dispositivo de segurança MSE assina o dado gerado do item 149.5, com o componente de chave privada do certificado nível 2;

149.7. o dispositivo de segurança MSE envia a assinatura realizada no item 149.6 para a aplicação autenticadora e libera o MSE para uso;

149.8. a aplicação autenticadora verifica a assinatura com o certificado nível 2 enviado pelo MSE, no passo do item 149.3;

149.9. caso a verificação do passo do item 149.8 for bem sucedida:

149.9.1. libera a placa-mãe para uso

149.9.2. caso o certificado de nível 2 utilizado no passo do item 149.8 tenha sido o Oficial, acende o Led da Cadeia de Segurança do TE com a cor VERDE, continuamente, sem piscar;

149.9.3. caso o certificado de nível 2 utilizado no passo do item 149.8 tenha sido diferente do Oficial, acende o Led da Cadeia de Segurança do TE com a cor VERMELHA, continuamente, sem piscar;

149.10. caso a verificação do passo do item 149.8 for mal sucedida:

149.10.1. impede o uso da placa-mãe;

149.10.2. impede o funcionamento dos teclados do TE e do TM;

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

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

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

151.1. Funcionamento restrito: somente as teclas BRANCO e CORRIGE, do TE ficarão liberadas. Isso ocorrerá quando os itens 147 e 148 forem atendidos utilizando-se apenas uma chave do nível 0, modo Manutenção ou modo Inicializador;

151.2. 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 147 e 148 forem atendidos utilizando-se uma chave do nível 1;

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

153. 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.

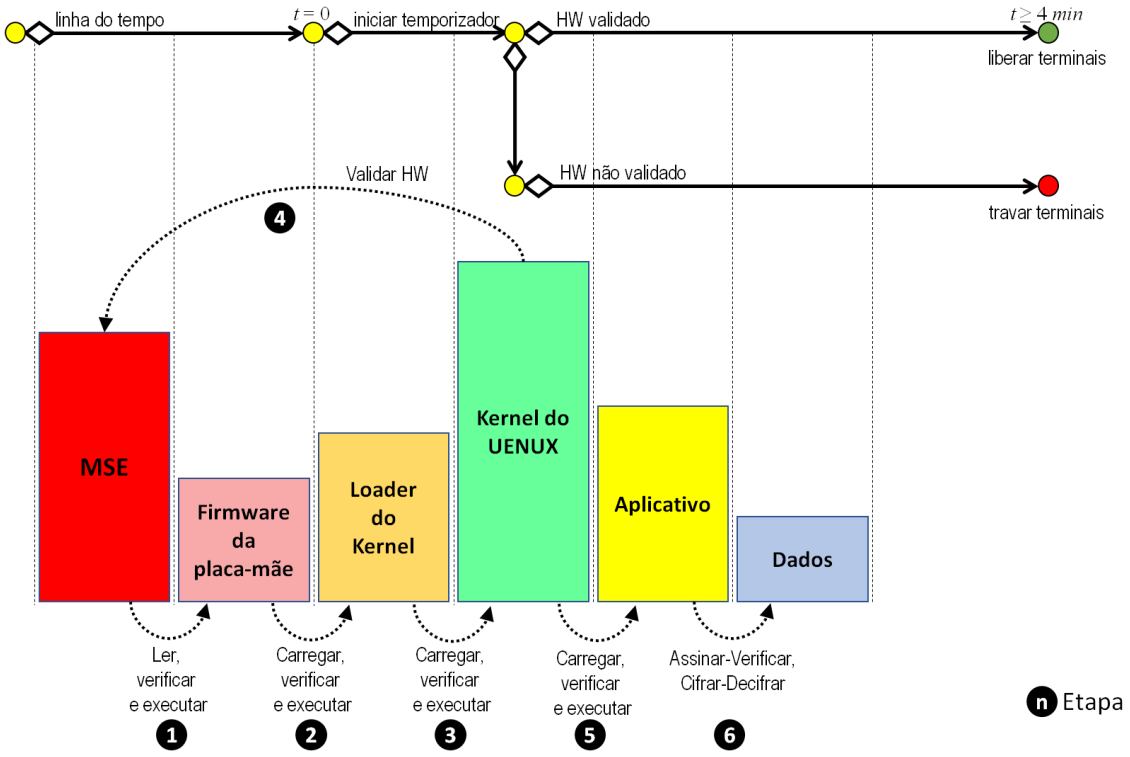

Figura 4 - Cadeia de Segurança

M.14. **Logs e registros**

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

154.1. modificação,

154.2. acesso,

154.3. apagamento e

154.4. adição;

N. Requisitos de Interoperabilidade

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

155. Disponibilizar aos aplicativos o acesso estruturado a todos os recursos da UE2020, como mostrar uma informação textual e gráfica, armazenar, recuperar, imprimir e transmitir as informações tratadas e geradas na UE2020;

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

157. Todos os dispositivos da urna eletrônica devem utilizar estruturas internas do kernel;

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

159. Relógio Interno:

159.1. Os ajustes posteriores àquele realizado em fábrica somente poderão ser realizados via software. O BIOS não deverá permitir o ajuste de data e hora pelo setup.

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

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

N.16. **Sustentação**

162. 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;

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

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

165. A Contratada é 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**

166. Todos os componentes do perímetro criptográfico devem 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 deve ser entregue ao TSE;

O. Algoritmos Criptográficos Obrigatórios

167. O módulo criptográfico deve suportar, no mínimo, as seguintes funções criptográficas, que serão fornecidas na forma de API, pelo TSE:

167.1. Criptografia de Dados:

167.1.1. Cifração e decifração simétricas AES-CTR com tamanho de chave de no mínimo 256 bits, nos modos de operação ECB e CBC (conforme padrão NIST FIPS PUB 197);

167.1.2. 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);

167.2. Autenticação de Entidades com Criptografia de Chave Pública:

167.2.1. EdDSA com chaves de pelo menos 521 bits (a ser fornecida pelo TSE);

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

167.3. Resumo Digital Criptográfico de Dados

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

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

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

167.4. Funções para Autenticação e Verificação de Integridade

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

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

167.4.3. MAC com SIPHASH (conforme implementação de Aumasson & Bernstein – *SipHash: a fast short-input PRF*);

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

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

167.7. Outros algoritmos propostos serão submetidos ao TSE para aprovação;

P. Requisitos de Documentação

168. Os requisitos do perímetro criptográfico são 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;

169. A Contratada deve 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 refere à documentação de todos os módulos criptográficos da UE2020.

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

171. A documentação deve especificar quais métodos são 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;

172. A Contratada deve 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;

173. A documentação deve especificar o ambiente de desenvolvimento utilizado para implementar o respectivo módulo criptográfico;

174. 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 deve estar muito bem detalhada;

175. A documentação deve especificar o método de RNG, detalhado passo a passo;A documentação deve especificar os métodos de armazenamento de chaves criptográficas empregados no respectivo módulo criptográfico;

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

177. A documentação do perímetro criptográfico deve especificar:

177.1. Os mecanismos de autenticação suportados pelo perímetro criptográfico;

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

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

178. A Contratada deve fornecer documentação técnica de projeto e de produto, completa, da Urna Eletrônica, e de cada módulo criptográfico;

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

P.18. **Manuais**

180. A Contratada deve fornecer:

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

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

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

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

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

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

180.7. **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

181. 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

182. A versão de produção dos firmwares deverá ser compilada com a presença de técnicos do TSE, com os seguintes requisitos mínimos:

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

182.2. 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;

182.3. 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

183. O Display do MSE deverá mostrar mensagens específicas de sucesso e modo de inicialização em todas as fases durante a cadeia de segurança, no mínimo para todas as fases onde há indicação diferenciada pelo Led da Cadeia de Segurança descritos neste Anexo e quaisquer mensagens de erro correspondentes nessas fases;

183.1. 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

184. O perímetro criptográfico do MSE deverá ser homologado ICP-Brasil, atendendo, no mínimo, os 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;

184.1. 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;

184.2. 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

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

186. Os demais requisitos serão aferidos pelo TSE durante o desenvolvimento do projeto da UE2020, de acordo com o item 181, sempre com o objetivo de conferir efetividade das implementações de segurança conforme os propósitos de cada item, resultando em um hardware adequadamente seguro.