Anexo Ia – Testes Complementares para Avaliação do Modelo de Engenharia

URNA ELETRÔNICA – UE2020

Sumário

A. Introdução

1. Este anexo descreve as condições estabelecidas para os testes complementares para avaliação do Modelo de Engenharia da UE2020 (ME-UE2020).

B. Teste de Carga e Autonomia

B.1. **Teste de Carga**

2. Cada licitante deverá utilizar sua bateria entregue junto com o ME e cujo modelo foi ofertado na proposta técnica, descarregada.

3. Para comprovar que a bateria está descarregada, as licitantes deverão instalar a bateria nos seus respectivos ME-UE2020 e ligá-los, cabendo ao TSE observar o acendimento do respectivo LED de indicação de bateria em nível crítico do Terminal do Eleitor. Após este procedimento o ME-UE2020 será desligado;

4. A carga da bateria será realizada com o ME-UE2020 desligado e conectado à rede de energia elétrica AC;

5. A bateria será carregada até atingir sua carga máxima (100%), conforme tempo informado na proposta técnica. Atingido este tempo, a bateria interna será retirada do ME-UE2020, devidamente identificada e lacrada pela equipe do TSE, na presença dos licitantes. Esta será a bateria a ser utilizada no Teste de Autonomia (B.2).

B.2. **Teste de Autonomia**

6. Para execução do Teste de Autonomia, a urna deverá ser inicializada e todas as funcionalidades necessárias para realização dos testes a seguir.

7. A bateria interna para o Teste de Autonomia será a mesma carregada durante o Teste de Carga, a qual será reinstalada no ME-UE2020 para início do teste;

8. Não será permitida a substituição da bateria interna depois de iniciado o Teste de Autonomia;

9. O TSE fornecerá às licitantes a bobina de papel térmico modelo Termoscript KPH70 da Oji Papéis, que será utilizada no teste de autonomia;

10. A instalação da bateria interna e da bobina será realizada com a urna desligada e desconectada da alimentação AC. Após a instalação, será ligada a urna, momento em que se iniciará a contagem do tempo do Teste de Autonomia;

11. Assim que carregado o sistema, a urna deverá imprimir três documentos (*Teste de impressão de documentos longos*):

11.1. Documento com 1.750 linhas numeradas e totalmente preenchidas por caracteres “A” no restante do espaço de impressão horizontal (ex. Linha1: “1AAA...”, Linha1750: “1750AAA...”), utilizando a fonte de tamanho normal especificada no Anexo II, bem como o tempo de impressão;

11.2. Documento com 3.500 linhas numeradas e totalmente preenchidas por caracteres “A” no restante do espaço de impressão horizontal (ex. Linha1: “1AAA...”, Linha3500: “3500AAA...”), utilizando a fonte de tamanho reduzido especificada no Anexo II;

11.3. Documento contendo a impressão de um Brasão das Armas de República de tamanho 4 x 4 cm, em até 3 (três) segundos;

11.3.1. O TSE disponibilizará a imagem do Brasão.

11.4. Documento com 10 linhas, totalmente preenchidas por caracteres “A”, e com um quadrado totalmente preenchido, conforme alínea 13.2.3.e), com tempo de impressão de 3(três) segundos medido a partir da confirmação do teclado do TE;

11.5. Os tempos para impressão estabelecidos incluem a operação de corte final do papel.

12. O teste de autonomia deverá ter interface que emula as principais funcionalidades de um Terminal de urnas de modelos anteriores, com um teclado virtual e incluindo a simulação de LEDs de Bateria Interna, Aguarde e Liberado, com as respectivas cores, conforme Figura 1;

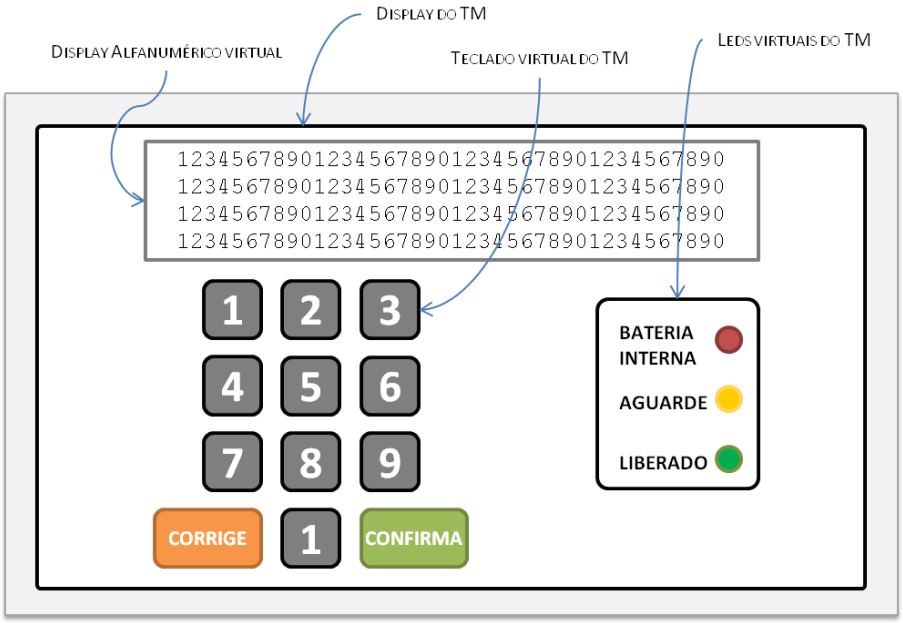


Figura 1 – Teclado e LEDs virtuais do Terminal do Mesário

13. A partir deste ponto, a urna deverá executar os seguintes procedimentos a cada minuto, até o término do teste de autonomia:

13.1. De 0 (zero) até 20 (vinte) segundos, com tolerância de 05 (cinco) segundos para mais ou para menos:

13.1.1. Apresentar o horário da urna em tempo real no formato HH:MM:SS no display alfanumérico virtual do TM;

13.1.2. Receber um número qualquer de 10 (dez) dígitos (digitado por um usuário), contendo todos os dígitos entre 0 (zero) e 9 (nove), através do teclado virtual no display do TM e apresentá-lo no display alfanumérico virtual, juntamente com a informação do item 13.1.1. Este número deverá ser gravado na Memória de Resultado e na Mídia USB externa, numa pasta denominada “DIGITOSTM”.

13.1.3. Capturar uma impressão digital e apresentá-la no display do TM durante um tempo mínimo de 02 (dois) segundos, em um retângulo com mesmas proporções do leitor ofertado e mostrando toda a imagem capturada.

a) Este retângulo deverá ter pelo menos 70% da altura da área visível do display do TM, conforme Figura 2;

b) A imagem capturada deverá ser gravada na Memória de Resultado e na Mídia USB externa, numa pasta denominada “DIGITAISTM”;

Figura 2 – Imagem da impressão digital capturada

13.1.4. Manter a representação de LEDs virtuais no display do TM os leds AGUARDE e LIBERADO do TM ligados e o led virtual BATERIA INTERNA piscando;

13.1.5. Durante esse período, o Terminal do Eleitor poderá estar desligado.

13.2. De 20 (vinte) até 60 (sessenta) segundos, com tolerância de 05 (cinco) segundos para mais ou para menos:

13.2.1. Apresentar durante todo o intervalo do item 13.1.2, alternando a cada 10 (dez) segundos, com tolerância de 02 (dois) segundos para mais ou para menos, as telas abaixo, com as seguintes especificações:

a) TELA 1: Apresentar no display do TE:

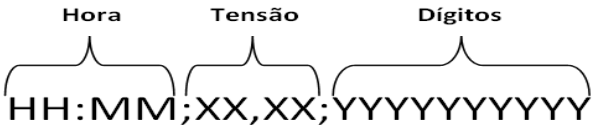
a.1) em tempo real, o horário da urna no formato HH:MM:SS.

a.2) atualizando a cada apresentação da TELA 1, a tensão da bateria interna no formato decimal "XX,XX Volts".

a.3) um número aleatório de 10 dígitos gerado, pelo ME-UE2020, a cada apresentação da tela.

a.4) A altura da fonte utilizada para apresentação das informações deverá ser no mínimo 30% da altura do display, na cor azul, e o restante do display deverá apresentar a cor branca.

a.5) A cada apresentação, essas informações deverão ser gravadas na Memória de Resultado e na Mídia USB externa, numa pasta denominada "DISPLAYTE", no seguinte formato:



b) TELA 2: Receber um número qualquer de 10 (dez) dígitos (digitado pelo usuário), contendo todos os dígitos entre 0 (zero) e 9 (nove), através do teclado do TE e apresentá-lo no display, utilizando a fonte de tamanho normal especificada no Anexo II, a cada tecla digitada. Este número deverá ser gravado na Memória de Resultado e na Mídia USB externa, numa pasta denominada "DIGITOSTE";

c) TELA 3: Apresentar no display do TE uma imagem de resolução 1024 x 600, formato JPEG, a ser fornecida pelo TSE;

d) TELA 4: Receber um número aleatório de 10 (dez) dígitos dígitos (digitado pelo usuário), contendo todos os dígitos entre 0 (zero) e 9 (nove), através do teclado do TE e apresentá-lo no display, utilizando a fonte de tamanho normal especificada no Anexo II, a cada tecla digitada. Esse número deverá ser gravado na Memória de Resultado e na Mídia USB externa, numa pasta denominada "DIGITOSTE".

13.2.2. Durante o período do item 13.2, o Terminal do Mesário poderá estar desligado.

13.2.3. Imprimir um documento com:

a) O horário da impressão no formato HH:MM;

b) A tensão da bateria interna no formato decimal "XX,XX Volts";

c) Um número qualquer (sorteado a cada impressão) de 10 dígitos e seu HASH (SHA-512) no formato hexadecimal (128 caracteres);

d) Um número sequencial para contagem de documentos impressos;

e) Um quadrado totalmente preenchido, na cor preta, com área mínima de 1,0 cm², com aferição da área feita da seguinte forma:

e.1) Medição com paquímetro em mm (divisão do nônio de 0,02mm) das dimensões vertical e horizontal do quadrado, considerando duas casas decimais ;

e.2) Conversão para cm de cada medida;

e.3) Multiplicação das medidas para encontrar área;

e.4) Arredondamento para uma casa decimal conforme ABNT NBR 5891:2014;

e.5) Exemplo 1 (aprovado): altura = 9,72mm; largura = 9,84mm $\rightarrow$ altura = 0,972cm; largura = 0,984cm $\rightarrow$ altura $\times$ largura = 0,956448 cm^2 $\rightarrow$ Arrendondamento para 1 casa decimal = 1,0cm^2;

e.6) Exemplo 2 (reprovado): altura = 9,64mm; largura = 9,84mm $\rightarrow$ altura = 0,964cm; largura = 0,984cm $\rightarrow$ altura $\times$ largura = 0,94999 cm^2 $\rightarrow$ Arrendondamento para 1 casa decimal = 0,9cm^2;

e.7) a CAT fará medição em três documentos impressos, à sua escolha, durante todo o teste de autonomia;

e.8) Caso algum documento não atinja 1cm^2 conforme regras acima, a licitante poderá abrir manutenção para corrigir a impressão dos documentos;

e.9) Caso o problema de área persista o problema, a licitante será penalizada com 3 (três) PM (períodos de manutenção), além daqueles eventualmente utilizados para resolver o problema;

e.10) Quadrados com área menor que 0,8cm^2 não corrigidos pela licitante por manutenção do ME implicarão reprovação do Modelo de Engenharia;

f) O leiaute da impressão deve seguir o modelo abaixo:

g) O documento deverá ser cortado ao término da impressão;

h) As fontes utilizadas deverão ser do tamanho normal, incluindo espaçamento entre linhas, conforme relatório impresso no teste do item 11.1;

13.2.4. A cada hora de teste serão selecionadas aleatoriamente 03 (três) amostras do documento do item 13.2.3 para medição da densidade óptica de impressão no quadrado e verificação do HASH do número aleatório impresso.

a) A medida será efetuada com o Densitômetro Óptico, e os valores medidos de cada documento devem ser no mínimo 1,12 e a média das três medições no mínimo 1,17.

a.1) O Densitômetro a ser utilizado será da marca X-Rite, modelo Exact Basic, com as seguintes configurações:

13.2.4.a.1.1. Botão VT: desativado

13.2.4.a.1.2. Condição de Medição: M0.

13.2.4.a.1.3. Status da Densidade: ISO Status T.

13.2.4.a.1.4. Base Branca de Densidade: Absoluta.

13.2.4.a.1.5. Precisão da Densidade: Alta (x.xxx).

13.2.4.a.1.6. Todas as Densidades: CMYK.

13.2.4.a.1.7. Densidade / VT: Chapada – Auto.

13.2.4.a.1.8. Valor Tonal: Murray-Davies.

b) A conferência do HASH será realizada pela geração do HASH do número impresso em um software, verificando nas amostras selecionadas se o mesmo está igual ao da impressão. Em no mínimo uma das amostras, o HASH impresso deve ser igual ao HASH gerado no software.

14. As licitantes deverão possuir técnicos em número suficiente para realizar as atividades previstas nos itens 13.1.2, 13.1.3 e 13.1.4 (digitação e captura de digitais) durante todo o teste de autonomia. Caso a equipe do TSE julgue conveniente, esta poderá operar o modelo de engenharia durante todo ou parte do teste.

15. A medida do tempo de autonomia se inicia desde quando o ME-UE2020 é ligado até o momento da primeira ocorrência de qualquer uma das seguintes situações:

15.1. Indicação de bateria interna em nível crítico, feita pelo respectivo led do TE;

15.2. Não impressão do documento do item 13.2.3, por motivos que não sejam caracterizados como falha do módulo impressor ou do ME-UE2020;

15.3. Intervenção no ME-UE2020 que caracterize “auxílio” à bateria interna.

16. Todas as interrupções durante o teste gerarão parada de contagem do tempo do Teste de Autonomia, bem como a retirada da bateria interna;

17. A contagem será retomada apenas após o fim da interrupção, quando o ME-UE2020 retornar ao estado operacional imediatamente subsequente ao da parada, momento em que será novamente inserida a bateria;

18. Os casos de parada, por motivos de manutenção, serão tratados conforme regras descritas no Anexo I, que trata sobre as normas para Avaliação do ME-UE2020.

C. Testes de Segurança

19. Os requisitos de segurança exigidos para o ME-UE2020 fazem parte do conjunto de funcionalidades que serão aferidas no teste do dispositivo de segurança e autenticação especificado no Anexo IV;

20. As licitantes deverão realizar os testes com algoritmos de criptografia da biblioteca BearSSL, conforme indica o Anexo IV. O TSE não irá fornecê-los nesta etapa;

21. O teste especificado verificará o encadeamento de segurança para autenticação do Firmware da placa-mãe, Loader do Kernel e do Kernel de Teste;

21.1. O “Kernel de Teste” se refere ao Kernel versão 4.9, disponível em https://mirrors.edge.kernel.org/pub/linux/kernel/v4.x/linux-4.9.1.tar.gz.

22. Para estes testes, a Licitante deverá utilizar uma Mídia de Aplicação (MA) que contenha um aplicativo, desenvolvido por ela, que capture teclas do Teclado do TE e as apresente no Display do TE. Nesta mídia, o Sistema Operacional (inclusive o Kernel de Teste) e os aplicativos, e somente estes, deverão estar contidos numa única partição;

23. A Licitante deverá disponibilizar, para estes testes, placas-mãe com as seguintes características:

23.1. uma placa sem o chip que contém o processador principal;

23.2. uma placa com o chip que contém o processador principal (placa original do ME-UE2020 ou substituída em período de manutenção);

23.3. os chips que contiverem o Firmware da placa-mãe, em todas as placas-mãe, devem ser soqueteados;

23.4. todas as placas-mãe com o perímetro criptográfico sem resina e com conector que permita a leitura/gravação de informação em memória interna não-volátil e endereçável pela unidade de processamento do MSE (ex: JTAG);

23.5. todas as placas-mãe devem ser idênticas, ou seja, originadas do mesmo projeto e desenho;

24. A Licitante deverá fornecer equipamento externo à placa-mãe, para leitura/gravação da memória do Firmware da placa-mãe;

25. A Licitante deverá fornecer equipamento que, a partir de interface USB de um computador conectada ao respectivo conector do MSE, permita a leitura/gravação de memória não-volátil do chip que contiver a unidade de processamento do MSE. Essa memória não-volátil deverá, além de ser interna ao chip, ser endereçável pela sua unidade de processamento;

26. A Licitante deverá fornecer um ou mais computadores que executem os softwares que leiam/gravem em memórias não-voláteis;

27. A Licitante deverá fornecer todas as mídias que serão utilizadas, nestes testes, como Mídia Interna (MI), como Mídia de Aplicação (MA), inclusive aqueles testes que necessitarão de cópias idênticas;

28. A equipe do TSE irá calcular o HASH da partição que contenha o Sistema Operacional e os aplicativos, garantindo que esta seja a mesma em todas as etapas dos testes (exceto na alteração para verificação do Kernel de Teste).

Classe	REQUISITO	PROCEDIMENTO DE TESTE
1	a) Atender ao Teste de Compilação Repetível do Firmware da placa-mãe	Executar o Teste de Compilação Repetível da placa-mãe
1	b)Atender ao Teste de Verificação do Firmware da placa-mãe	Executar o Teste de Verificação do Firmware da placa-mãe
1	c)Atender ao Teste de Verificação do Loader do Kernel	Executar o Teste de Verificação do Loader do Kernel
1	d)Atender ao Teste de Verificação do kernel de Teste	Executar o Teste de Verificação do Kernel de Teste

C.1. **Teste de Compilação Repetível do Firmware da placa-mãe**

29. Para este teste, deverá ser apresentado, pela Licitante, um ambiente computacional (hardware e software) no qual seja possível:

29.1. Visualizar o código-fonte do Firmware da placa-mãe;

29.2. Construir o(s) código(s) binário(s) do Firmware da placa-mãe e que serão utilizados nos testes do item C.2;

29.3. Comprovar que o código-binário do Firmware da placa-mãe construído pelo ambiente computacional corresponda ao código-fonte que estiver sendo visualizado;

30. A equipe da Licitante apresentará o referido ambiente computacional mostrando, para a equipe do TSE, as principais partes do código-fonte do Firmware da placa-mãe;

31. A equipe da Licitante construirá, diante da equipe do TSE, uma versão do código binário do Firmware da placa-mãe, demonstrando os mecanismos existentes para comprovar que o código-fonte exibido corresponde ao código binário gerado;

32. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo secp521r1 e assinará digitalmente o arquivo do código binário do Firmware da placa-mãe gerado no passo 31, com a chave criada pelo TSE e com hash SHA-512. A referida assinatura digital deverá ser registrada para posterior conferência;

33. A equipe da Licitante, sob supervisão da equipe do TSE, realizará uma alteração totalmente reversível e então, usando o ambiente computacional apresentado no passo 30, reconstruirá o código binário do Firmware da placa-mãe, a partir da versão alterada;

34. A equipe da Licitante, sob supervisão da equipe do TSE, reverterá a alteração realizada no passo 33 e então, usando o ambiente computacional apresentado no passo 30, reconstruirá o código binário do Firmware da placa-mãe, a partir da versão com a alteração revertida;

35. A equipe do TSE deverá verificar se a assinatura digital do passo 32 corresponde ao arquivo binário do Firmware da placa-mãe gerado no passo 34. A verificação deve confirmar que o código binário gerado no passo 31 **é igual** ao código binário gerado no passo 34;

C.2. **Teste de Verificação do Firmware da placa-mãe**

36. Para este teste, será utilizada a placa sem o chip que contém o processador principal da placa-mãe (item 23.1);

37. A equipe da Licitante retirará o chip onde se encontra o Firmware da placa-mãe e o colocará em equipamento de leitura/gravação externa (a ser providenciado pela Licitante) para leitura em um computador (também da Licitante);

38. A equipe da Licitante realizará a leitura completa do Firmware da placa-mãe (*dump* completo, incluindo espaço livre do chip, excluindo eventual espaço NVRAM) e o armazenará em um em um arquivo de computador;

39. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo secp521r1 e assinará digitalmente o arquivo de *dump* do Firmware da placa-mãe, com a chave criada pelo TSE e com hash SHA-512, em um PC. A referida assinatura digital deverá ser registrada para posterior conferência;

40. A equipe da Licitante recolocará o chip contendo o Firmware da placa-mãe, em seu respectivo soquete, no ME-UE2020;

41. A equipe da Licitante conectará o equipamento leitor/gravador no MSE (item 25) para que, usando um computador (item 26), implante, em memória não-volátil do microcontrolador do MSE, a parte privada do par de chaves gerado pelo TSE no passo 39;

42. A equipe da Licitante desconectará o equipamento leitor/gravador do MSE;

43. A equipe do TSE posicionará uma câmera de vídeo em frente ao display do MSE e iniciará a gravação de um vídeo;

44. A equipe da Licitante deverá ligar o ME-UE2020 e o firmware contido no MSE deverá assinar um conteúdo equivalente a 64 (sessenta e quatro) bytes com o valor hexadecimal “AA” com a chave implantada no passo 41 (com hash SHA-512). Os primeiros 5 (cinco) dígitos dessa assinatura deverão ser concatenados com os seus 5 (cinco) últimos dígitos e então exibidos no display do MSE;

45. Logo em seguida, o firmware contido no MSE deverá assinar o Firmware da placa-mãe com a chave implantada no passo 41 (com hash SHA-512). Os primeiros 5 (cinco) dígitos dessa assinatura deverão ser concatenados com os seus 5 (cinco) últimos dígitos e então exibidos no display do MSE;

46. A equipe do TSE interromperá a gravação do vídeo, iniciada no passo 43;

47. A equipe do TSE deverá conferir e registrar o resultado exibido no display do MSE. Esse resultado exibido deve ser **totalmente coincidente** com os respectivos dígitos da assinatura realizada pela equipe do TSE, no passo 39;

48. A equipe do TSE deverá alterar uma ou mais posições do arquivo de *dump* do Firmware da placa-mãe;

49. O chip contendo o Firmware da placa-mãe deverá ser novamente retirado do ME-UE2020, pela equipe da Licitante, e recolocado no equipamento de gravação/leitura externa.

50. A equipe da Licitante, deverá proceder a gravação do *dump* do Firmware da placa-mãe, alterado pela equipe do TSE, no seu respectivo chip;

51. A equipe da Licitante deverá recolocar o chip do Firmware da placa-mãe em seu respectivo soquete;

52. A equipe da Licitante ligará o ME-UE2020 e então o firmware do MSE deverá assinar o Firmware da placa-mãe com a chave implantada no passo 41 (com hash SHA-512). Os 5 (cinco) dígitos mais significativos dessa assinatura deverão ser concatenados com os 5 (cinco) dígitos menos significativos dessa assinatura e então exibidos no display do MSE;

53. A equipe do TSE deverá conferir e registrar o resultado exibido no display do MSE. Esse resultado exibido **não pode ser coincidente** com os respectivos dígitos da assinatura realizada pela equipe do TSE, no passo 39;

54. A equipe do TSE, em um computador, assinará digitalmente o arquivo de *dump* do Firmware da placa-mãe, alterado no passo 48, com a chave criada pelo TSE, no passo 39, e com hash SHA-512;

55. A equipe da Licitante deverá repetir o passo 52;

56. A equipe do TSE deverá conferir e registrar o resultado exibido no display do MSE. Esse resultado exibido deve ser **totalmente coincidente** com os respectivos dígitos da assinatura realizada pela equipe do TSE, no passo 54;

57. A equipe do TSE, usando o vídeo gravado no passo 46, deverá calcular e registrar a diferença de tempo entre a exibição do resultado do passo 45 e a exibição do resultado do passo 44. Essa medida de tempo será utilizada para detectar eventuais discrepâncias anômalas, conforme o item 103.

C.3. **Teste de Verificação do Loader do Kernel**

58. Para este teste, será utilizada a placa com o chip que contém o processador principal da placa-mãe (item 23.2);

59. A equipe da Licitante deverá executar um procedimento para que os parâmetros de inicialização do ME-UE2020 assumam a sua configuração *default*, no que se refere à ordem de inicialização dos dispositivos;

60. A equipe da Licitante deverá retirar qualquer mídia que porventura esteja inserida no conector da Mídia de Aplicação (MA) do ME-UE2020;

61. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo secp521r1;

62. A equipe da Licitante deverá apresentar 2 (dois) arquivos: um que será utilizado para gravar o Loader do Kernel na Mídia de Carga (MC) e outro que será utilizado para gravar o Sistema Operacional na Mídia de Carga (MC);

63. A equipe do TSE assinará digitalmente o arquivo do Loader do Kernel, com a chave criada pelo TSE e com hash SHA-512, em um PC;

64. Usando o arquivo do Loader do Kernel assinado no passo 63, a equipe da Licitante deverá gerar uma Mídia de Carga (MC), isto é, com Loader do Kernel e Sistema Operacional (com Kernel de Teste);

65. A equipe da Licitante deverá fazer uma cópia idêntica da Mídia de Carga (MC) utilizada no passo 64;

66. A equipe da Licitante conectará o equipamento leitor/gravador no MSE (item 25) para que, usando um computador (item 26), implante, em memória não-volátil do microcontrolador do MSE, a parte privada do par de chaves gerado pelo TSE no passo 61;

67. A equipe da Licitante desconectará o equipamento leitor/gravador do MSE;

68. A equipe do TSE posicionará uma câmera de vídeo em frente ao display do MSE e iniciará a gravação de um vídeo;

69. A equipe da Licitante deverá ligar o ME-UE2020 e o firmware contido no MSE deverá assinar um conteúdo equivalente a 64 (sessenta e quatro) bytes com o valor hexadecimal “AA” com a chave implantada no passo 66 (com hash SHA-512). Os primeiros 5 (cinco) dígitos dessa assinatura deverão ser concatenados com os seus 5 (cinco) últimos dígitos e então exibidos no display do MSE;

70. Logo em seguida, o Firmware da placa-mãe, utilizando o MSE, deverá assinar o Loader do Kernel com a chave implantada no passo 66, e a equipe do TSE deverá verificar:

70.1. Se no display do MSE, estão exibidos os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital e se esses **são idênticos** aos respectivos dígitos da assinatura gerada no passo 63;

70.2. Se o respectivo Sistema Operacional foi completamente carregado;

71. A equipe do TSE interromperá a gravação do vídeo, iniciada no passo 68;

72. A equipe da Licitante deverá limpar toda a Memória Interna (MI) do ME-UE2020 utilizando comando do Sistema Operacional carregado no passo 70;

73. A equipe da Licitante deverá desligar o ME-UE2020, retirar a Mídia de Carga (MC) do conector da Mídia de Aplicação (MA) e inseri-la em uma interface USB de um PC e, conforme definição da equipe do TSE, alterar alguma informação de um ou mais setores onde estão gravados o Loader do Kernel, na Mídia de Carga (MC);

74. A equipe da Licitante deverá retirar a Mídia de Carga (MC) alterada da interface USB do PC e inseri-la no conector da Mídia de Aplicação (MA) da urna;

74.1. A equipe da Licitante deverá reiniciar o ME-UE2020 com a Mídia de Carga (MC) alterada e a equipe do TSE deverá conferir se o Firmware da placa-mãe, utilizando o MSE, assinou o Loader do Kernel, verificando se no display do MSE, estão exibidos os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital e se esses **não são idênticos** aos respectivos dígitos da assinatura gerada no passo 63;

75. A equipe da Licitante deverá desligar o ME-UE2020 e repetir o procedimento do passo 59;

76. A equipe da Licitante deverá iniciar o ME-UE2020 e nenhuma carga de Sistema Operacional deverá ocorrer e o display do MSE deverá apresentar a mensagem “LOADER DO KERNEL. AUSENTE”;

77. A equipe da Licitante deverá desligar a urna e repetir o procedimento do passo 59;

78. A equipe da Licitante deverá inserir, no respectivo conector do ME-UE2020, a cópia idêntica da Mídia de Carga (MC) com o Loader do Kernel assinado (gerada no passo 65), iniciar o ME-UE2020 e a equipe do TSE deverá conferir se o Firmware da placa-mãe, utilizando o MSE, assinou o Loader do Kernel, verificando:

78.1. Se no display do MSE, estão exibidos os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital e se esses **são idênticos** aos respectivos dígitos da assinatura gerada no passo 63;

78.2. Se o respectivo Sistema Operacional foi completamente carregado.

79. A equipe do TSE, usando o vídeo gravado no passo 71, deverá calcular e registrar a diferença de tempo entre a exibição do resultado do passo 69 e a exibição do resultado do passo 70.1. Essa medida de tempo será utilizada para detectar eventuais discrepâncias anômalas, conforme o item 103.

C.4. **Teste de Verificação do Kernel de Teste**

80. Para este teste, será utilizada a placa com o chip que contém o processador principal da placa-mãe (item 23.2);

81. A equipe da Licitante deverá executar um procedimento para que os parâmetros de inicialização do ME-UE2020 assumam a sua configuração *default*, no que se refere à ordem de inicialização dos dispositivos;

82. A equipe da Licitante deverá retirar qualquer mídia que porventura esteja inserida no conector da Mídia de Aplicação (MA) do ME-UE2020;

83. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo secp521r1;

84. A equipe da Licitante deverá apresentar 2 (dois) arquivos: um que será utilizado para gravar o Loader do Kernel na Mídia de Carga (MC) e outro que será utilizado para gravar o Sistema Operacional (com o Kernel de Teste) na Mídia de Carga (MC);

85. A equipe do TSE assinará digitalmente o arquivo do Kernel de Teste, com a chave criada pelo TSE e com hash SHA-512, em um PC;

86. Usando o arquivo do Kernel de Teste assinado no passo anterior, a equipe da Licitante deverá gerar uma Mídia de Carga (MC), isto é, com o Loader do Kernel e com o Sistema Operacional (com o Kernel de Teste assinado);

87. A equipe da Licitante deverá fazer uma cópia idêntica da Mídia de Carga (MC) utilizada no passo 86;

88. A equipe da Licitante conectará o equipamento leitor/gravador no MSE (item 25) para que, usando um computador (item 26), implante, em memória não-volátil do microcontrolador do MSE, a parte privada do par de chaves gerado pelo TSE no passo 83;

89. A equipe da Licitante desconectará o equipamento leitor/gravador do MSE;

90. A equipe da Licitante deverá inserir, no respectivo conector do ME-UE2020, a Mídia de Carga (MC) com o Kernel de Teste assinado;

91. A equipe do TSE posicionará uma câmera de vídeo em frente ao display do MSE e iniciará a gravação de um vídeo;

92. A equipe da Licitante deverá ligar o ME-UE2020 e o firmware contido no MSE deverá assinar um conteúdo equivalente a 64 (sessenta e quatro) bytes com o valor hexadecimal “AA” com a chave implantada no passo 88 (com hash SHA-512). Os primeiros 5 (cinco) dígitos dessa assinatura deverão ser concatenados com os seus 5 (cinco) últimos dígitos e então exibidos no display do MSE;

93. Logo em seguida, o Loader do Kernel, utilizando o MSE, deverá assinar o Kernel com a chave implantada no passo 88, e a equipe do TSE deverá verificar:

93.1. Se no display do MSE, estão exibidos os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital e se esses **são idênticos** aos respectivos dígitos da assinatura gerada no passo 85;

93.2. Se o respectivo Sistema Operacional foi completamente carregado.

94. A equipe do TSE interromperá a gravação do vídeo, iniciada no passo 91;

95. A equipe da Licitante deverá limpar toda a Memória Interna (MI) do ME-UE2020 utilizando comando do Sistema Operacional carregado no passo anterior;

96. A equipe da Licitante deverá desligar a ME-UE2020, retirar a Mídia de Carga (MC) do conector da Mídia de Aplicação (MA), inseri-la em uma interface USB de um PC e, conforme definição da equipe do TSE, alterar alguma informação de um ou mais setores onde está gravado o Kernel de Teste, na Mídia de Carga (MC);

97. A equipe da Licitante deverá retirar a Mídia de Carga (MC) alterada da interface USB do PC e inseri-la no conector da Mídia de Aplicação (MA) da urna;

97.1. A equipe da Licitante deverá reiniciar o ME-UE2020 com a Mídia de Carga (MC) alterada no ME-UE2020 e a equipe do TSE deverá conferir se o Loader do Kernel, utilizando o MSE, assinou o Kernel de Teste, verificando se no display do MSE, estão exibidos os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital e se esses **não são idênticos** aos respectivos dígitos da assinatura gerada no passo 85;

98. A equipe da Licitante deverá desligar o ME-UE2020 e repetir o procedimento do passo 81;

99. A equipe da Licitante deverá iniciar o ME-UE2020 e nenhuma carga de Sistema Operacional deverá ocorrer e o display do MSE deverá apresentar a mensagem “KERNEL. AUSENTE”;

100. A equipe da Licitante deverá desligar o ME-UE2020 e repetir o procedimento do passo 81;

101. A equipe da Licitante deverá inserir, no respectivo conector do ME-UE2020, a cópia idêntica da Mídia de Carga (MC) com o Kernel de Teste assinado (gerada no passo 87), iniciar a urna e a equipe do TSE deverá conferir se o Loader do Kernel, utilizando o MSE, assinou o Kernel de Teste, verificando:

101.1. Se no display do MSE, estão exibidos os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital e se esses **são idênticos** aos respectivos dígitos da assinatura gerada no passo 85;

101.2. Se o respectivo Sistema Operacional foi completamente carregado.

102. A equipe do TSE, usando o vídeo gravado no passo 94, deverá calcular e registrar a diferença de tempo entre a exibição do resultado do passo 92 e a exibição do resultado do passo 93.1. Essa medida de tempo será utilizada para detectar eventuais discrepâncias anômalas, conforme o item 103.

103. Caso forem observadas discrepâncias anômalas entre as medidas de tempo de assinatura do Firmware da placa-mãe (passo 57), do Loader do Kernel (passo 79) e do Kernel de Teste (passo 102), poderão ser solicitadas diligências por parte da equipe do TSE, para apurar suas causas;

103.1. Ocorreria “discrepância anômala” caso, por exemplo, a execução de assinatura de binário maior for mais rápida que a execução de assinatura de binário menor;

D. Testes de desempenho

D.1. **Tempo de inicialização do sistema operacional**

104. O objetivo deste teste é obter o tempo de inicialização do kernel do sistema operacional;

105. Para a execução deste teste serão usados:

105.1. Versão do Kernel Linux 4.9, conforme indicado no item C.21.1;

105.2. A ferramenta `systemd-analyze` disponível na versão do sistema operacional acima para obter o tempo de inicialização do sistema dividido em tempo para inicialização do Kernel e tempo para inicialização do espaço do usuário (*userspace*).

105.3. O tempo que será considerado será o tempo obtido para inicialização do kernel;

105.4. A configuração padrão da ferramenta `systemd-analyze` será usada;

106. O Kernel Linux 4.9 será gravado pelo Tribunal Superior Eleitoral em uma mídia USB;

107. Para realização deste teste o MSE deverá estar configurado para não realizar a autenticação do kernel;

108. Para realização deste teste o loader do Kernel deverá estar configurado para não realizar a autenticação do kernel;

109. O Modelo de Engenharia (ME) da licitante deve, após as etapas de inicialização predecessoras necessárias, conforme descrito no Anexo IV, ser inicializado a partir de uma mídia USB citado no item 106;

110. Após inicializado o sistema operacional, será executada a ferramenta `systemd-analyze` para obtenção do tempo de inicialização do Kernel;

111. O ME será desligado e ligado novamente por três vezes para obtenção de três tempos de inicialização do kernel;

112. É vedado o salvamento de estados do kernel entre as inicializações do sistema operacional, cada inicialização deve ser realizada “a frio”;

113. Será calculado o tempo médio de inicialização do kernel;

114. O tempo médio para inicialização do kernel deverá ser menor ou igual que 2 segundos.

D.2. **Tempo de cifração de blocos de dados**

115. Para a realização deste teste, o ME-UE2020 deverá utilizar a placa-mãe sem o chip que contém o processador principal da placa-mãe (item C.23.1);

116. Para efeito de aferição, o MSE deverá executar o algoritmo AES-CTR de 128 bits da implementação de referência da biblioteca BearSSL (versão 0.5);

117. A equipe do TSE gerará uma chave simétrica;

118. A equipe do TSE gerará um bloco de valores aleatórios de 5MBytes;

119. A equipe da Licitante conectará o equipamento leitor/gravador no MSE (item C.25) para que, usando um computador (item C.26), implante, em memória não-volátil do microcontrolador do MSE, a chave secreta gerada no passo 117 e o bloco de valores aleatórios gerados no passo 118. A equipe da Licitante definirá a posição de memória onde será inicialmente alocado o referido bloco;

120. A equipe da Licitante desconectará o equipamento leitor/gravador do MSE;

121. A equipe da Licitante reiniciará o ME-UE2020 e o firmware do MSE deverá executar 250 (duzentos e cinquenta) interações, em um procedimento interativo de cifração AES-CTR de 128 bits com a chave implantada no passo 119, do bloco de valores aleatórios implantados no mesmo passo;

122. A cada interação, o bloco de valores aleatórios deverá ser alterado de forma que os 10 (dez) primeiros bytes da cifração realizada ocupem, na mesma ordem, os 10 (dez) últimos bytes do mesmo bloco.

122.1. A cada 25 (vinte e cinco) interações, deverão ser exibidos, no display do TSE, os 5 (cinco) primeiros bytes do bloco de valores aleatórios concatenados com os 5 (cinco) últimos bytes do mesmo bloco, que deverá permanecer no display, até as próximas 25 (vinte e cinco) interações;

123. Para registrar o tempo total, deverá ser utilizada uma câmera de vídeo para registrar o display do MSE, bem como um cronômetro. Em caso de discrepância entre os resultados obtidos com os dois métodos, será utilizado aquele obtido com a câmera de vídeo. O resultado final desse teste é o tempo médio da assinatura do bloco de dados, ou seja, o tempo total obtido com o método descrito, dividido por 250 (duzentos e cinquenta), que corresponde ao número de interações;

124. O TSE analisará o vídeo, para verificar a correspondência entre as partes das cifrações exibidas no display do MSE, registradas em vídeo, e as cifrações geradas em processo interativo idêntico executado anteriormente;

125. O tempo médio para realizar a cifração deverá ser **menor que 5 segundos** e os valores verificados no passo 124 deverão ser **totalmente coincidentes**.

D.3. **Tempo para assinatura de blocos de dados**

126. Para a realização deste teste, o ME-UE2020 deverá utilizar a placa-mãe sem o chip que contém o processador principal da placa-mãe (item C.23.1);

127. Para efeito de aferição, o MSE deverá executar o algoritmo P-521 (secp521r1) da implementação de referência da biblioteca BearSSL (versão 0.5);

128. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo secp521r1;

129. A equipe do TSE gerará um bloco de valores aleatórios de 1KBytes;

130. A equipe da Licitante conectará o equipamento leitor/gravador no MSE (item C.25) para que, usando um computador (item C.26), implante, em memória não-volátil do microcontrolador do MSE, a parte privada do par de chaves gerado pelo TSE no passo 128 e o bloco de valores aleatórios gerados no passo 129. A equipe da Licitante definirá a posição de memória onde será inicialmente alocado o referido bloco;

131. A equipe da Licitante desconectará o equipamento leitor/gravador do MSE;

132. A equipe da Licitante reiniciará o ME-UE2020 e o firmware do MSE deverá executar 1.000 (hum mil) interações, em um procedimento interativo de assinaturas ECDSA com a chave implantada no passo 130, com hash SHA-512, do bloco de valores aleatórios implantados no mesmo passo;

133. A cada interação, o bloco de valores aleatórios deverá ser alterado de forma que os 10 (dez) primeiros bytes da assinatura obtida ocupem, na mesma ordem, os 10 (dez) primeiros bytes do bloco de valores aleatórios.

133.1. A cada 100 (cem) interações, deverão ser exibidos, no display do TSE, os 5 (cinco) primeiros dígitos da assinatura digital concatenados com os 5 (cinco) últimos dígitos da assinatura digital, que deverá permanecer no display, até as próximas 100 (cem) interações;

134. Para registrar o tempo total, deverá ser utilizada uma câmera de vídeo para registrar o display do MSE, bem como um cronômetro. Em caso de discrepância entre os resultados obtidos com os dois métodos, será utilizado aquele obtido com a câmera de vídeo. O resultado final desse teste é o tempo médio da assinatura do bloco de dados, ou seja, o tempo total obtido com o método descrito, dividido por 1.000 (hum mil), que corresponde ao número de interações;

135. O TSE irá analisar o vídeo, para verificar a correspondência entre as partes das assinaturas exibidas no display do MSE, registradas em vídeo, e as assinaturas geradas em processo interativo idêntico executado anteriormente;

136. O tempo médio para realizar as assinaturas deverá ser **menor que 1 segundo** e os valores verificados no passo 135 deverão ser **totalmente coincidentes**.

D.4. **Teste de latência do Touch Screen do Terminal do Mesário**

137. Posicionar câmera para filmagem do ato de apertar a tecla virtual do TM da UE2020, de maneira que haja visualização concomitante da superfície do touch screen e do feedback visual da tecla virtual.

138. Tal posicionamento será feito com a ajuda de um espelho, conforme Figura 3;

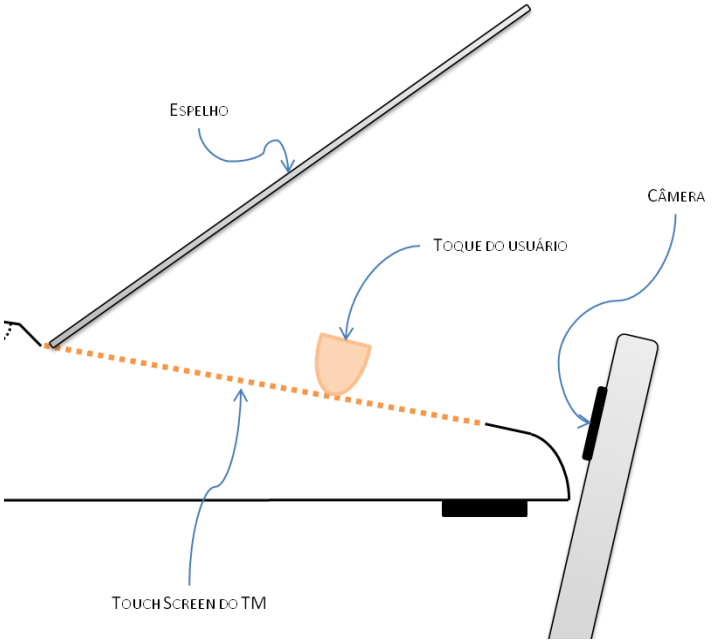


Figura 3 – Esquema ilustrativo do teste da latência do TM

139. O usuário apertará a tecla e, ao retirar o dedo (release), serão contados quantos frames serão necessários até que apareça o feedback visual no Terminal do Mesário;

140. Para fins de aferição serão contados frames completos, inclusive o primeiro frame em que não há mais contato físico do dedo do usuário com a superfície do touch screen do TM e, e incluindo o frame correspondente à manifestação visual correspondente ao caractere da digitada no display do TM;

141. A câmera e a filmagem utilizadas no teste deverão ter, pelo menos, 60 frames por segundo;

142. A velocidade do vídeo será utilizada para cálculo em milissegundos de cada frame da filmagem (`tFrame`);

143. Com o vídeo obtido, será contada a quantidade de frames conforme item 140 (`dVimg`) , e será realizado o cálculo do tempo relacionado entre o momento da digitação e a visualização do número da tecla no display (`lTecla`), a partir da fórmula abaixo:

`dVimg X tFrame = lTecla`

onde:

`dVimg` → Nº de frames da digitação até o surgimento da imagem no display

`tFrame` → tempo para apresentação de um frame

144. `lTecla` → latência para visualização do tempo da tecla no display;

145. O teste será aprovado, caso `lTecla` atinja, no máximo, 200ms.