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 as 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;

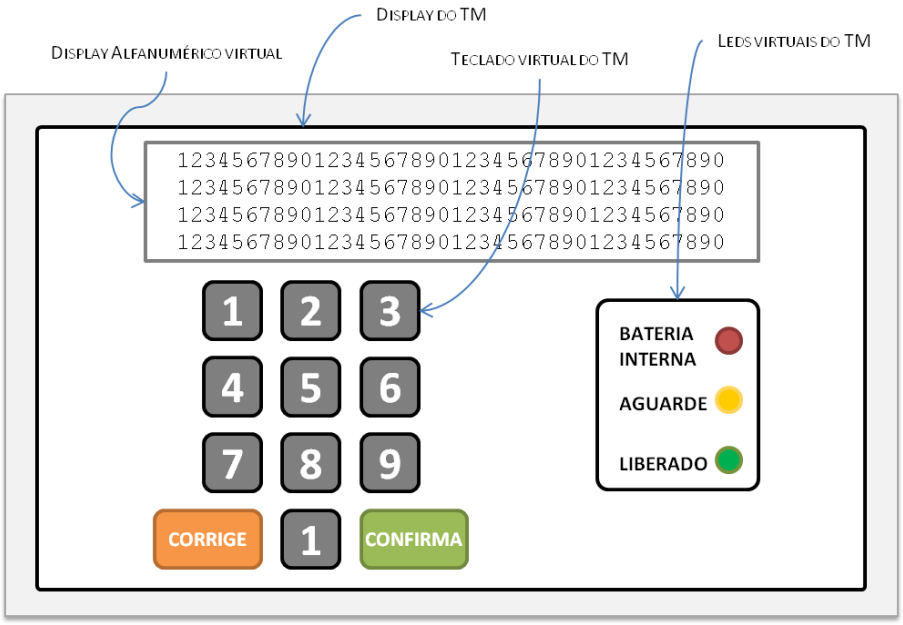


Figura 1 – Teclado e LEDs virtuais do Terminal do Mesário

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 13.2, 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:

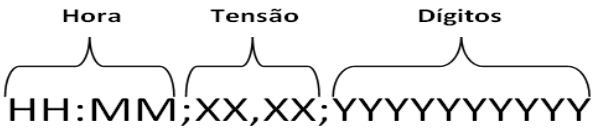
a.1) em tempo real, o horário da urna no formato HH:MM:SS.

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;

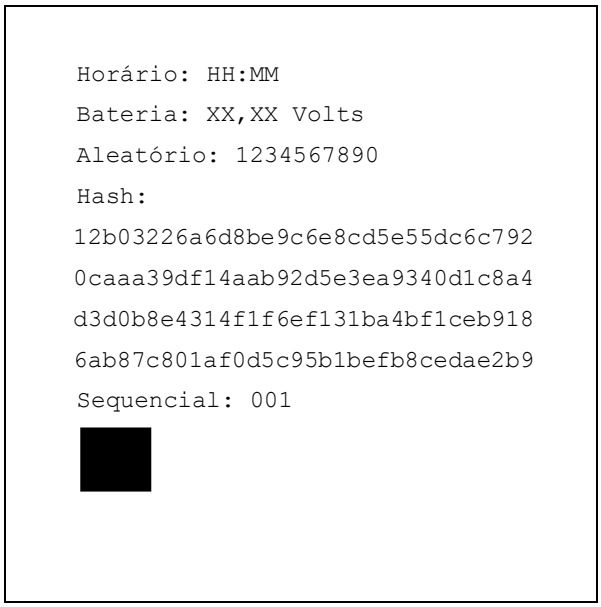
e.7) a CAT fará medição em três documentos impressos, à sua escolha, durante todo o teste de autonomia;

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, 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 nos testes do dispositivo de segurança e autenticação especificado no Anexo IV e os constantes na tabela abaixo:

Classe	REQUISITO	PROCEDIMENTO DE TESTE
1	a) Atender ao Teste de Compilação Repetível do Firmware da placa-mãe	Executar o Teste de Compilação Repetível do Firmware da placa-mãe (seção C.1)
1	b) Atender ao Teste de Verificação do Firmware da placa-mãe	Executar o Teste de Verificação do Firmware da placa-mãe (seção C.2)
1	c) Atender ao Teste de Verificação do Loader do Kernel	Executar o Teste de Verificação do Loader do Kernel (seção C.3)
1	d) Atender ao Teste de Verificação do Kernel de Teste	Executar o Teste de Verificação do Kernel de Teste (seção C.4)

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. Os testes especificados verificarão a capacidade de implementar o encadeamento de segurança para autenticação do Firmware da placa-mãe, Loader do Kernel e do Kernel de Teste, por meio da execução dos testes das seções C.2 - Teste de Verificação do Firmware da placa-mãe, C.3 - Teste de Verificação do Loader do Kernel e C.4 - Teste de Verificação do Kernel de Teste, além da preparação e demonstração da capacidade de compilação repetível do firmware, conforme o teste da seção C.1 - Teste de Compilação Repetível do Firmware da placa-mãe;

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) com os arquivos necessários para cada teste. Nesta mídia, o Loader do Kernel, o Sistema Operacional (incluindo o Kernel de Teste), e os aplicativos (ex: dd para apagar dados da Mídia Interna) deverão estar contidos numa única partição;

22.1. Para a execução de determinados comandos, poderá ser utilizado teclado USB externo, a ser providenciado pela licitante;

22.2. A visualização dos comandos com o sistema operacional carregado deverá ser feita no display do TE;

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) e Mídia de Aplicação (MA), inclusive aqueles testes que necessitarão de cópias idênticas;

28. Para os comandos de geração de chaves privadas, chaves públicas, assinatura e verificação nos testes das seções C.1, C.2, C.3, C.4 e D.3 serão utilizados os comandos abaixo:

28.1. Será utilizado o seguinte comando com a ferramenta OpenSSL (versão 1.1.1) para geração da chave privada usando o algoritmo secp521r1:

```
openssl ecparam -name secp521r1 -genkey -param_enc explicit -out chaveprivada.pem
```

28.2. Será utilizado o seguinte comando para cálculo da chave pública usando o algoritmo secp521r1 a partir da chave privada gerada:

```
openssl ec -in chaveprivada.pem -pubout -out chavepublica.pem
```

28.3. Será utilizado o seguinte comando para gerar a assinatura com hash SHA-512 de um arquivo:

```
openssl dgst -sha512 -sign chaveprivada.pem -out arqassinatura arquivo.bin
```

28.4. Será utilizado o seguinte comando para verificar a assinatura de um arquivo:

```
openssl dgst -sha512 -verify chavepublica.pem -signature arqassinatura arquivo.bin
```

28.5. Os textos em itálico nos comandos acima são nomes variáveis, escolhidos pela CAT;

28.6. O par de chaves em cada um dos testes poderá ser reutilizado em todos os testes, ou a CAT poderá, a seu critério, gerar novos pares de chaves a cada novo teste e/ou para cada licitante;

28.7. A CAT, a seu critério, poderá calcular *hashs* dos arquivos envolvidos no teste para registro;

29. Nos testes das seções C.2, C.3,C.4 e D.3, o resultado a ser mostrado no Display do MSE deverá estar de acordo com as regras a seguir:

29.1. Os primeiros 5 (cinco) *nibbles*, em sua representação hexadecimal (“0” a “F”), do componente R da assinatura gerada no respectivo passo, deverão ser concatenados aos 5 (cinco) últimos *nibbles* do componente S da assinatura gerada;

29.2. As assinaturas mostradas no Display do MSE deverão ser feitas com SHA-512;

29.3. **Exemplo** em hexadecimal de arquivo de assinatura gerado pelo comando do item 28.3:

```
30 81 87 02 41 64 BF F0  DF 8D 87 D4 77 C3 B7 5C
1F 9F 6D DE C3 BD 16 56  3F B5 EB 3B F3 14 4A 59
49 34 01 D1 CC 07 7D 76  B6 BC C2 64 8F 00 09 BC
A0 C7 0F E2 80 1B CA E4  3F FD 84 CF C2 41 DF B9
32 F2 D3 30 58 45 02 42  00 ED 97 53 60 D7 C4 D5
62 81 5D 34 34 4B 7E 51  0F 1F 95 C2 CE 5B 24 AD
77 CE 95 80 B3 C9 2E A1  91 8C D9 CC 68 C1 CF 2A
B7 8F B4 03 77 0E 58 BE  52 14 36 78 EC 9A 3E B6

E0 59 2F 09 12 12 26 B9  92 E6
```

29.4. O `asn1parse` do `openssl` para o arquivo de exemplo do item 29.3 é:

```
0:d=0  hl=3 l= 135 cons: SEQUENCE
3:d=1  hl=2 l=  65 prim: INTEGER
:64BFF0DF8D87D477C3B75C1F9F6DDEC3BD16563FB5EB3BF3144A59493401D1CC077D76B6BCC2648F0009BCA0C70FE2801BC
AE43FFD84CFC241DFB932F2D3305845
C.    70:d=1  hl=2 l=  66 prim: INTEGER
:ED975360D7C4D562815D34344B7E510F1F95C2CE5B24AD77CE9580B3C92EA1918CD9CC68C1CF2AB78FB403770E58BE52143
678EC9A3EB6E0592F09121226B992E6
```

29.5. Para a assinatura gerada no exemplo do item 29.3, o valor a ser apresentado display do MSE é "**64BFF992E6**"

30. Caso forem observadas discrepâncias anômalas entre as medidas de tempo de assinatura do Firmware da placa-mãe (passo 51), do Loader do Kernel (passo 68) e do Kernel de Teste (passo 85), poderão ser solicitadas diligências por parte da equipe do TSE, para apurar suas causas;

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

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

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

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

31.2. Construir o(s) código(s) binário(s) do Firmware da placa-mãe e que será(ão) utilizado(s) nos testes do item C.2;

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

32. 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;

33. A equipe da Licitante construirá, por meio de compilação e 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;

34. A equipe do TSE gerará um par de chaves assimétricas e assinará digitalmente o arquivo do código binário do Firmware da placa-mãe gerado no passo 33, com a chave privada criada pelo TSE. A referida assinatura digital deverá ser registrada para posterior conferência;

35. A equipe da Licitante, conforme definição da equipe do TSE, realizará, no código-fonte, uma alteração totalmente reversível e então, usando o ambiente computacional apresentado no passo 32, reconstruirá o código binário do Firmware da placa-mãe, a partir da versão alterada;

36. A equipe da Licitante, sob supervisão da equipe do TSE, reverterá a alteração realizada no passo 35 e então, usando o ambiente computacional apresentado no passo 32, reconstruirá, por meio de nova compilação, o código binário do Firmware da placa-mãe, a partir da versão com a alteração revertida;

37. A equipe do TSE deverá verificar se a assinatura digital do passo 34 corresponde ao arquivo binário do Firmware da placa-mãe gerado no passo 36. A verificação deve confirmar que o código binário gerado no passo 33 **é igual** ao código binário gerado no passo 36, além de ser diferente da versão gerada no passo 35;

37.1. Serão verificados os arquivos de firmware gerados nos passos 33, 35 e 36, sendo que arquivo de assinatura empregado na verificação de assinatura será o gerado no passo 34;

38. O Teste C.1 será considerado **atendido** caso a verificação do item 37 for bem sucedida para as verificações dos binários gerados nos passos 33 e 36, e mal sucedida na verificação do binário gerado no passo 35;

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

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

40. 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);

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

42. A equipe do TSE preservará o arquivo de *dump* do Firmware da placa-mãe (excluindo eventual espaço NVRAM);

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

44. 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 (item 25) do microcontrolador do MSE, chave privada gerada anteriormente pelo TSE;

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

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

47. 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 44.

47.1. O resultado da assinatura gerada deverá ser exibido no Display do MSE conforme formato e regras definidas no item 29;

47.2. A assinatura gerada, em formato DER (binário ASN.1) deverá ser gravada em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26);

48. Logo em seguida, o firmware contido no MSE deverá assinar o Firmware da placa-mãe (excluindo eventual espaço NVRAM) com a chave implantada no passo 44.

48.1. O resultado da assinatura gerada deverá ser exibido no Display do MSE conforme formato e regras definidas no item 29;

48.2. A assinatura gerada, em formato DER (binário ASN.1) deverá ser gravada em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26);

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

50. As assinaturas geradas nos itens 47.2 e 48.2 serão recuperadas em arquivos por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26) e serão utilizados para verificação de assinatura digital dos arquivos de 64 (sessenta e quatro) bytes com o valor hexadecimal "AA" e do arquivo dump do Firmware da placa-mãe, com a chave pública gerada pelo TSE.

50.1. O TSE também verificará no vídeo se os resultados exibidos são **totalmente coincidentes** com os *nibbles* das respectivas assinaturas recuperadas em arquivo, conforme formato e regras definidas no item 29;

51. A equipe do TSE, usando o vídeo gravado no passo 49, deverá calcular e registrar a diferença de tempo entre a exibição do resultado do passo 48 e a exibição do resultado do passo 47. Essa medida de tempo será utilizada para detectar eventuais discrepâncias anômalas, conforme o item 30.

52. A mensagem de um passo deverá ser mantida no display do MSE até que haja necessidade de apresentação de outra mensagem.

53. O Teste C.2 será considerado **atendido** caso:

53.1. Os resultados das verificações pela equipe do TSE no passo 50 forem bem sucedidos;

53.2. Os resultados das verificações pela equipe do TSE no passo 50.1 forem bem sucedidos;

53.3. Não forem constatadas discrepâncias anômalas na diferença de tempo calculada no passo 51.

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

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

55. 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 (Mídia de Carga precede outras mídias);

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

57. A equipe da Licitante deverá apresentar 2 (dois) arquivos: o Loader do Kernel na Mídia de Carga (MC) e o arquivo de imagem do Kernel de Teste, que serão utilizados para os testes que utilizam a Mídia de Carga (MC);

57.1. Caso o Loader do Kernel tenha mais de um arquivo, as assinaturas e verificações serão feitas com base no arquivo principal (aquele que efetivamente faz a carga do Sistema Operacional);

58. A equipe do TSE preservará o arquivo do Loader do Kernel;

59. Usando o arquivo do Loader do Kernel preservado no passo 58, a equipe da Licitante deverá gerar uma Mídia de Carga (MC), isto é, com Loader do Kernel e Sistema Operacional (com Kernel de Teste);

60. 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, chave privada gerada anteriormente pelo TSE;

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

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

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

64. 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 60.

64.1. O resultado da assinatura gerada deverá ser exibido no Display do MSE conforme formato e regras definidas no item 29;

64.2. A assinatura gerada, em formato DER (binário ASN.1) deverá ser gravada em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26);

65. Logo em seguida, o Firmware da placa-mãe, utilizando o MSE, deverá assinar o Loader do Kernel com a chave implantada no passo 60;

65.1. O resultado da assinatura gerada deverá ser exibido no Display do MSE conforme formato e regras definidas no item 29;

65.2. A assinatura gerada, em formato DER (binário ASN.1) deverá ser gravada em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26);

66. A equipe do TSE interromperá a gravação do vídeo, iniciada no passo 63;

67. As assinaturas geradas nos itens 64.2 e 65.2 serão recuperadas em arquivos por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26) e serão utilizados para verificação de assinatura digital dos arquivos de 64 (sessenta e quatro) bytes com o valor hexadecimal "AA" e do arquivo do Loader do Kernel preservado no passo 59, com a chave pública gerada pelo TSE;

67.1. O TSE também verificará no vídeo se os resultados exibidos são **totalmente coincidentes** com os respectivos *nibbles* das respectivas assinaturas recuperadas em arquivo, conforme formato e regras definidas no item 29, além de verificar se o respectivo Sistema Operacional foi completamente carregado;

68. A equipe do TSE, usando o vídeo gravado no passo 66, deverá calcular e registrar a diferença de tempo entre a exibição do resultado do passo 65 e a exibição do resultado do passo 64. Essa medida de tempo será utilizada para detectar eventuais discrepâncias anômalas, conforme o item 30.

69. A mensagem de um passo deverá ser mantida no display do MSE até que haja necessidade de apresentação de outra mensagem.

70. O Teste C.3 será considerado **atendido** caso:

70.1. Os resultados das verificações pela equipe do TSE no passo 67 forem bem sucedidos;

70.2. Os resultados das verificações pela equipe do TSE no passo 67.1 forem bem sucedidos;

70.3. Não forem constatadas discrepâncias anômalas na diferença de tempo calculada no passo 68.

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

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

72. 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 (Mídia de Carga precede outras mídias);

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

74. A equipe da Licitante deverá apresentar 2 (dois) arquivos: o Loader do Kernel na Mídia de Carga (MC) e o arquivo de imagem do Kernel de Teste, que serão utilizados para os testes que utilizam a Mídia de Carga (MC);

75. A equipe do TSE preservará o arquivo do Kernel de Teste;

76. Usando o arquivo do Kernel de Teste preservado no passo 75, 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);

77. 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, chave privada gerada anteriormente pelo TSE;

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

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

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

81. 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 77 (com hash SHA 512).

81.1. O resultado da assinatura gerada deverá ser exibido no Display do MSE conforme formato e regras definidas no item 29;

81.2. A assinatura gerada, em formato DER (binário ASN.1) deverá ser gravada em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26);

82. Logo em seguida, o Loader do Kernel, utilizando o MSE, deverá assinar o Kernel com a chave implantada no passo 77;

82.1. O resultado da assinatura gerada deverá ser exibido no Display do MSE conforme formato e regras definidas no item 29;

82.2. A assinatura gerada, em formato DER (binário ASN.1) deverá ser gravada em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26);

83. A equipe do TSE interromperá a gravação do vídeo, iniciada no passo 80;

84. As assinaturas geradas nos itens 81.2 e 82.2 serão recuperadas em arquivos por meio do equipamento leitor/gravador no MSE (item 25), com o auxílio de um computador (item 26) e serão utilizados para verificação de assinatura digital dos arquivos de 64 (sessenta e quatro) bytes com o valor hexadecimal “AA” e do arquivo do Kernel de Teste preservado no passo 75, com a chave pública gerada pelo TSE

84.1. O TSE também verificará no vídeo se os resultados exibidos são **totalmente coincidentes** com os respectivos *nibbles* das respectivas assinaturas recuperadas em arquivo, conforme formato e regras definidas no item 29, além de verificar se o respectivo Sistema Operacional foi completamente carregado;

85. A equipe do TSE, usando o vídeo gravado no passo 83, deverá calcular e registrar a diferença de tempo entre a exibição do resultado do passo 82 e a exibição do resultado do passo 81. Essa medida de tempo será utilizada para detectar eventuais discrepâncias anômalas, conforme o item 30.

86. A mensagem de um passo deverá ser mantida no display do MSE até que haja necessidade de apresentação de outra mensagem.

87. O Teste C.4 será considerado **atendido** caso:

87.1. Os resultados das verificações pela equipe do TSE no passo 84 forem bem sucedidos;

87.2. Os resultados das verificações pela equipe do TSE no passo 84.1 forem bem sucedidos;

87.3. Não forem constatadas discrepâncias anômalas na diferença de tempo calculada no passo 85.

D. Testes de desempenho

D.1. Tempo de inicialização do sistema operacional

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

89. Para a execução deste teste serão usados:

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

89.2. 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*).

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

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

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

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

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

93. 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 citada no item 90;

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

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

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

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

98. O Teste D.1 será considerado **atendido** caso o tempo médio para inicialização do kernel for **menor ou igual a 2 segundos**.

D.2. Tempo de cifração de blocos de dados

99. 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 23.1);

100. Para efeito de aferição, o MSE deverá executar o algoritmo AES-CTR de 128 bits da implementação de referência da biblioteca BearSSL, conforme versão indicada no Anexo IV;

101. A equipe do TSE gerará uma chave simétrica e eventual vetor de inicialização (IV);

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

103. 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 interna ao microcontrolador do MSE, a chave secreta e eventual vetor de inicialização gerados no passo 101 e implante em memória não-volátil endereçável pelo microcontrolador do MSE, o bloco de valores aleatórios gerados no passo 102. A equipe da Licitante definirá a posição de memória onde será inicialmente alocado o referido bloco;

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

105. A equipe da Licitante reiniciará o ME-UE2020 e o firmware do MSE deverá executar 250 (duzentos e cinquenta) iterações, em um procedimento interativo de cifração AES-CTR de 128 bits com a chave implantada no passo 103, do bloco de valores aleatórios implantados no mesmo passo;

106. A cada iteração, 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.

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

106.2. A concatenação e a posição dos *nibbles*, além da exibição no Display do MSE, deverão seguir as regras do item 29.

107. 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 iterações;

108. 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;

109. A mensagem de um passo deverá ser mantida no display do MSE até que haja necessidade de apresentação de outra mensagem.

110. O Teste D.2 será considerado **atendido** caso:

110.1. O tempo médio para realizar a cifração for **menor que 5 segundos;**

110.2. Os valores verificados no passo 108 forem **totalmente coincidentes**.

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

111. 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 23.1);

112. Para efeito de aferição, o MSE deverá executar o algoritmo P-521 (secp521r1) da implementação de referência da biblioteca BearSSL, conforme versão indicada no Anexo IV;

113. A equipe do TSE gerará um par de chaves assimétricas usando o algoritmo secp521r1, conforme comandos dos itens 28.1 e 28.2;

114. A equipe do TSE gerará um bloco de valores aleatórios de 1024 Bytes;

115. 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 113 e o bloco de valores aleatórios gerados no passo 114. A equipe da Licitante definirá a posição de memória onde será inicialmente alocado o referido bloco;

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

117. A equipe da Licitante reiniciará o ME-UE2020 e o firmware do MSE deverá executar 1.000 (hum mil) iterações, em um procedimento iterativo de assinaturas ECDSA com a chave implantada no passo 115, com hash SHA-512, do bloco de valores aleatórios implantados no mesmo passo;

118. A cada iteração, 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.

118.1. O resultado da assinatura do bloco de valores aleatórios (modificado conforme item 118) deverá ser exibido no Display do MSE, a cada 25 (vinte e cinco) iterações, incluindo a exibição da primeira iteração, conforme formato e regras definidas no item 29;

118.2. A cada uma das 1000 (hum mil) iterações, o ME da licitante deverá gravar a assinatura gerada, em formato DER (binário ASN.1), concatenada com os 10 (dez) primeiros bytes do respectivo bloco de valores aleatórios assinado, em espaço de memória não-volátil acessível por meio do equipamento leitor/gravador no MSE (item C.25), com o auxílio de um computador (item C.26);

118.3. Após o final dos testes, o espaço de memória utilizado para armazenamento das informações geradas no item 118.2 deverá ser gravado em um arquivo no computador (item C.26), com a utilização do equipamento leitor/gravador no MSE (item C.25) (se necessário o ME poderá ser reiniciado);

118.4. O arquivo deverá conter, pelo menos, as informações geradas no item 118.2 referentes às últimas 51 (cinquenta e uma) iterações (950ª iteração até a 1000ª iteração);

119. Para registrar o tempo total, deverá ser utilizada uma câmera de vídeo para registrar o display do MSE ao lado de um cronômetro. 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, a partir da exibição da primeira iteração, até a 1000ª iteração;

119.1. O tempo total apurado será dividido por 999 (novecentos e noventa e nove);

119.2. A câmera de vídeo iniciará a gravação antes do passo 117;

120. O TSE irá analisar o vídeo, para verificar a correspondência entre as partes das assinaturas exibidas no display do MSE, relativas às 51 (cinquenta e uma) iterações finais registradas em vídeo, e as respectivas assinaturas geradas e recuperadas no arquivo do item 118.3;

120.1. A partir dos 51 (cinquenta e um) registros de 10 (dez) bytes iniciais dos blocos de valores aleatórios, o TSE irá reconstruir os 51 (cinquenta e um) blocos correspondentes, considerando o valor aleatório do bloco inicial (item 114);

120.2. Em seguida, utilizando as 51 (cinquenta e uma) assinaturas finais recuperadas em arquivo no passo do item 118.3, o TSE efetuará a verificação de assinatura de cada bloco correspondente reconstruído;

121. A mensagem de um passo deverá ser mantida no display do MSE até que haja necessidade de apresentação de outra mensagem.

122. O Teste D.3 será considerado **atendido** caso:

122.1. O tempo médio para realizar cada assinatura for **menor que 1 segundo;**

122.2. Todas as verificações das assinaturas do passo 120.2 forem bem sucedidas.

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

123. 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.

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

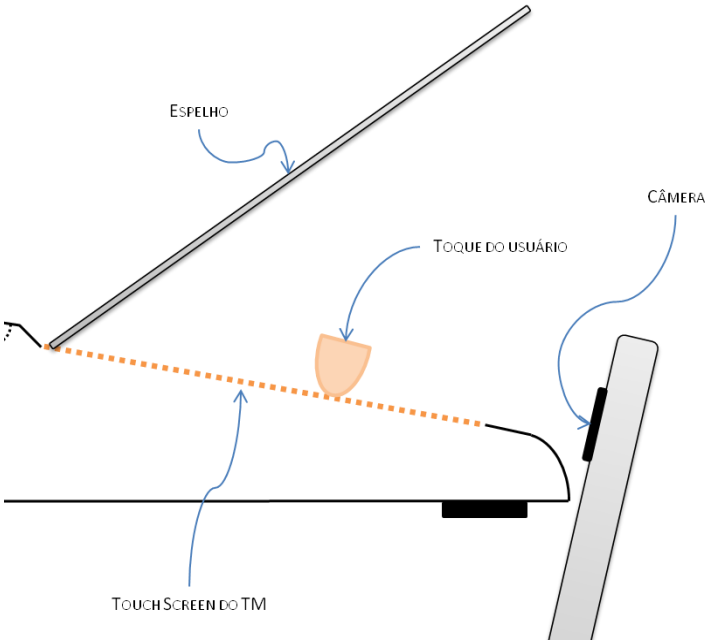


Figura 3 – Esquema ilustrativo do teste da latência do TM

125. 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;

126. 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;

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

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

129. Com o vídeo obtido, será contada a quantidade de frames conforme item 126 (`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

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

131. O Teste D.4 será considerado **atendido** caso `lTecla` atinja, no máximo, 200ms.