Universidade Federal de Minas Gerais
Departamento de Ciência da Computação
DCC603 - Engenharia de Software – 2019/2

Alunos: Bernardo Augusto de Oliveira Senna
Breno Tanure Prata
Frederico Ribeiro Queiroz
Icaro Kened Torres Neto
Victor Hugo Nascimento Costa Val

Documento de Projeto Arquitetural
Sistema de Urna Eletrônica (UE)

Sumário

A. Aspectos Gerais

A.1. Arquitetura de Segurança da Urna Eletrônica

1. A segurança da Urna Eletrônica (UE) inclui os seguintes dispositivos:
   - Módulo de Segurança Embarcado (MSE)
   - Módulo de Segurança do Teclado do Eleitor (MSTE)
   - Módulo de Segurança da Impressora de Relatórios (MSIR)
   - Módulo de Segurança do Leitor Biométrico (MSLB)
   - 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 a aquisição da UE. Portanto, a implementação do hardware e firmwares de segurança deverá dar suporte a conexão de novos periféricos.

   1.2. O Módulo de Segurança do Leitor Biométrico (MSLB) se comunica com a Unidade Central de Processamento (UCP) da placa mãe da UE apenas por meio de um único canal seguro, estabelecido quando a urna é iniciada.

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

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

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

4. 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.

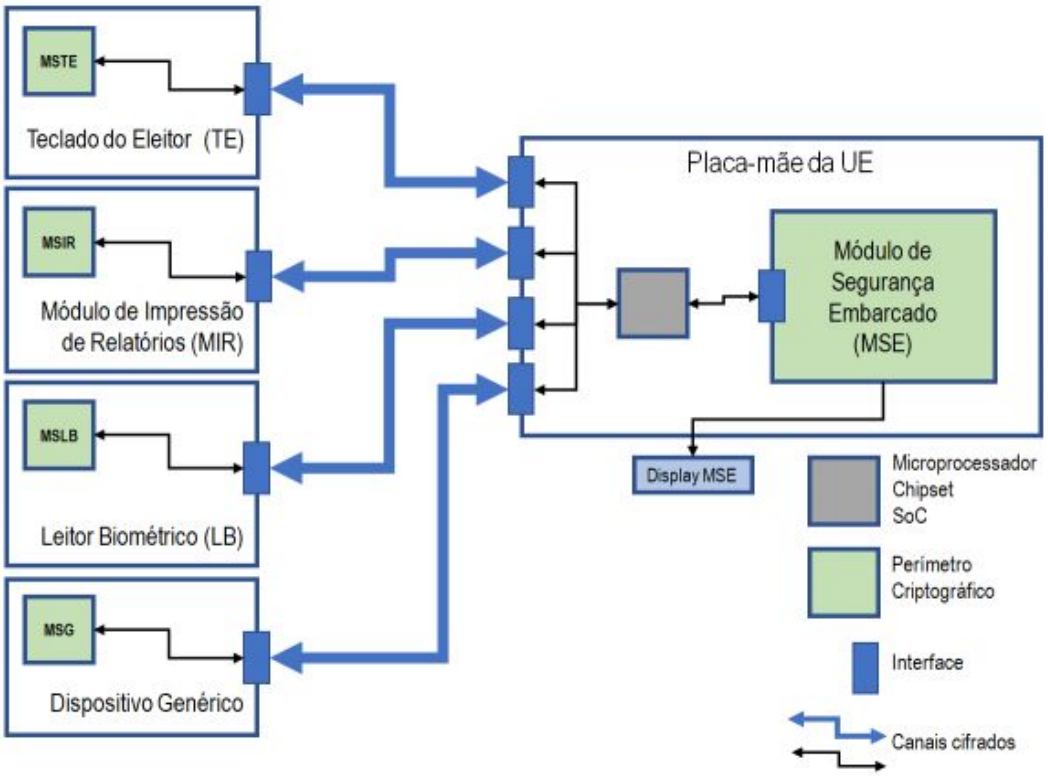

Figura 1 - Arquitetura de segurança da comunicação entre os dispositivos da UE

5. A solução será implementada baseada em um microprocessador, que estará soldado na placa-mãe, não sendo permitida uma solução conectada por cabos e/ou conectores.

6. O MSE será utilizado na carga do sistema operacional das UEs.

    6.1. A carga do sistema operacional nas UEs se baseia 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, módulos e aplicativos.

7. O MSE tem como características básicas:

    7.1. Funcionar como única raiz de confiança, implementada em hardware, de um pilha de inicialização segura que não poderá ser desabilitada.

7.2. Ser dedicado às seguintes funções criptográficas:

7.2.1. assinatura e verificação com primitivas de chaves assimétricas;
7.2.2. cifração e decifração com primitivas de chaves simétricas e assimétricas;
7.2.3. resumo digital;
7.2.4. autenticação com chaves assimétricas;

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

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

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

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

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

B. Arquitetura de Segurança Física

8. Qualquer violação ou remoção de um dos componentes de hardware ou de software automaticamente impedirá o funcionamento de todos os componentes da UE.

9. A parte traseira da placa-mãe é protegida por um *backplate* metálico, para impedir acesso físico ao circuito pela face inferior da UE.

10. Todos os orifícios e fendas para ventilação são construídas de forma a prevenir qualquer tipo de sondagem ou observação indevida do interior do perímetro criptográfico.

C. Modelo de Cenário do Sistema

11. O Diagrama a seguir mostra a organização e a dependência dentro de um conjunto de componentes externos à UE. Nele há 3 componentes principais: o eleitor, a urna e o fiscal eleitoral.

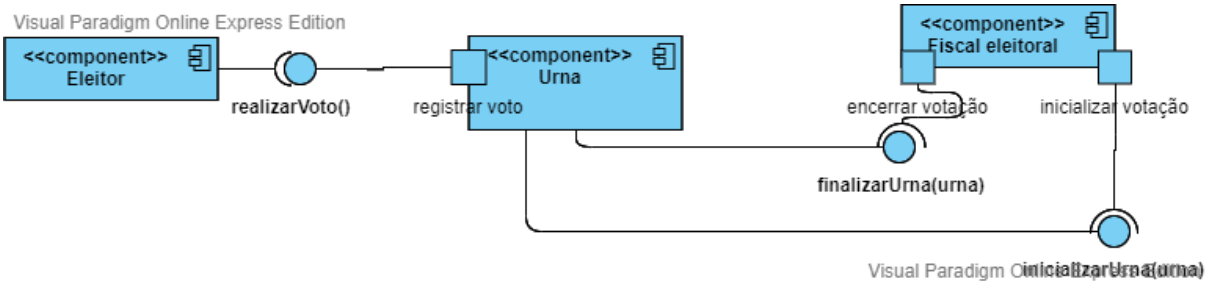

Figura 2 - Diagrama de Componentes modelando o cenário de registro de voto