Teste Público de Segurança da Urna – 2023

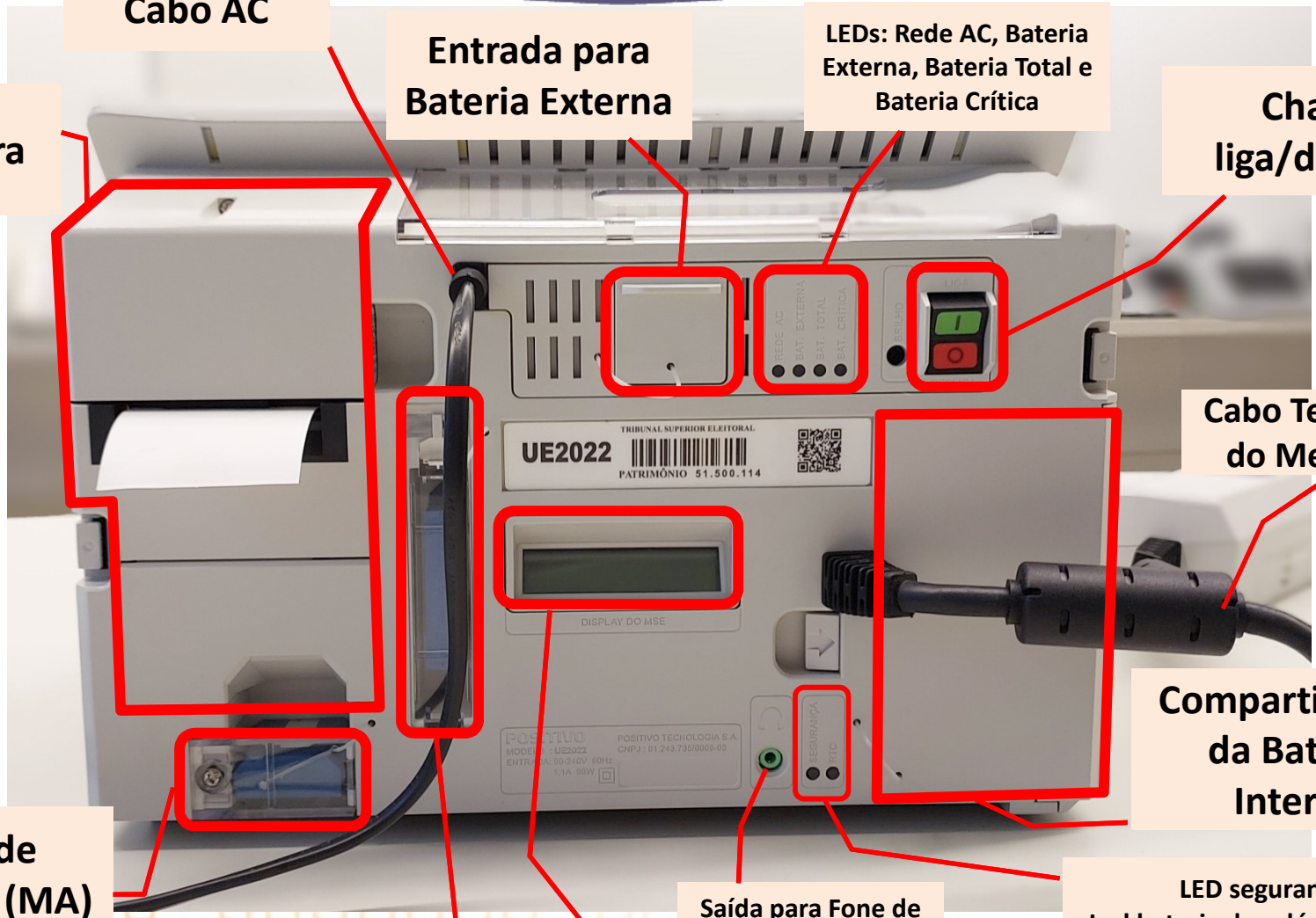
Hardware da Urna Eletrônica
(Modelos UE2020/UE2022)

Coordenadoria de Tecnologia Eleitoral – Cotel

Tribunal Superior Eleitoral
Secretaria de Tecnologia da Informação – STI

As Urnas Eletrônicas 2020 e 2022

As Urnas Eletrônicas 2020 e 2022



Cabo AC

Entrada para Bateria Externa

LEDs: Rede AC, Bateria Externa, Bateria Total e Bateria Crítica

Chave liga/desliga

Impressora

Cabo Terminal do Mesário

Compartimento da Bateria Interna

Mídia de Aplicação (MA) ou Mídia Externa

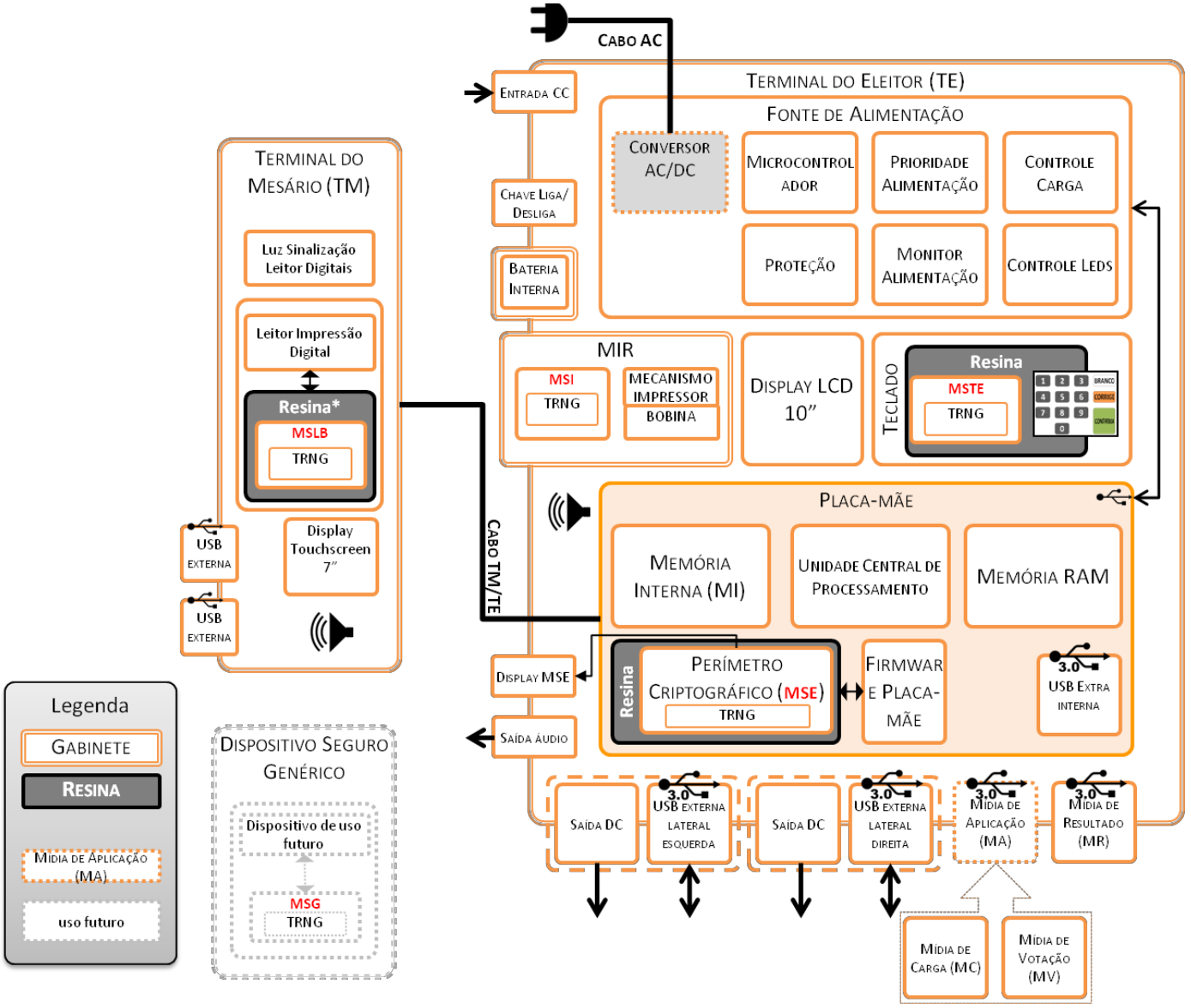
Saída para Fone de Ouvido

LED segurança
Led bateria do relógio interno (RTC – *Real Time Clock*)

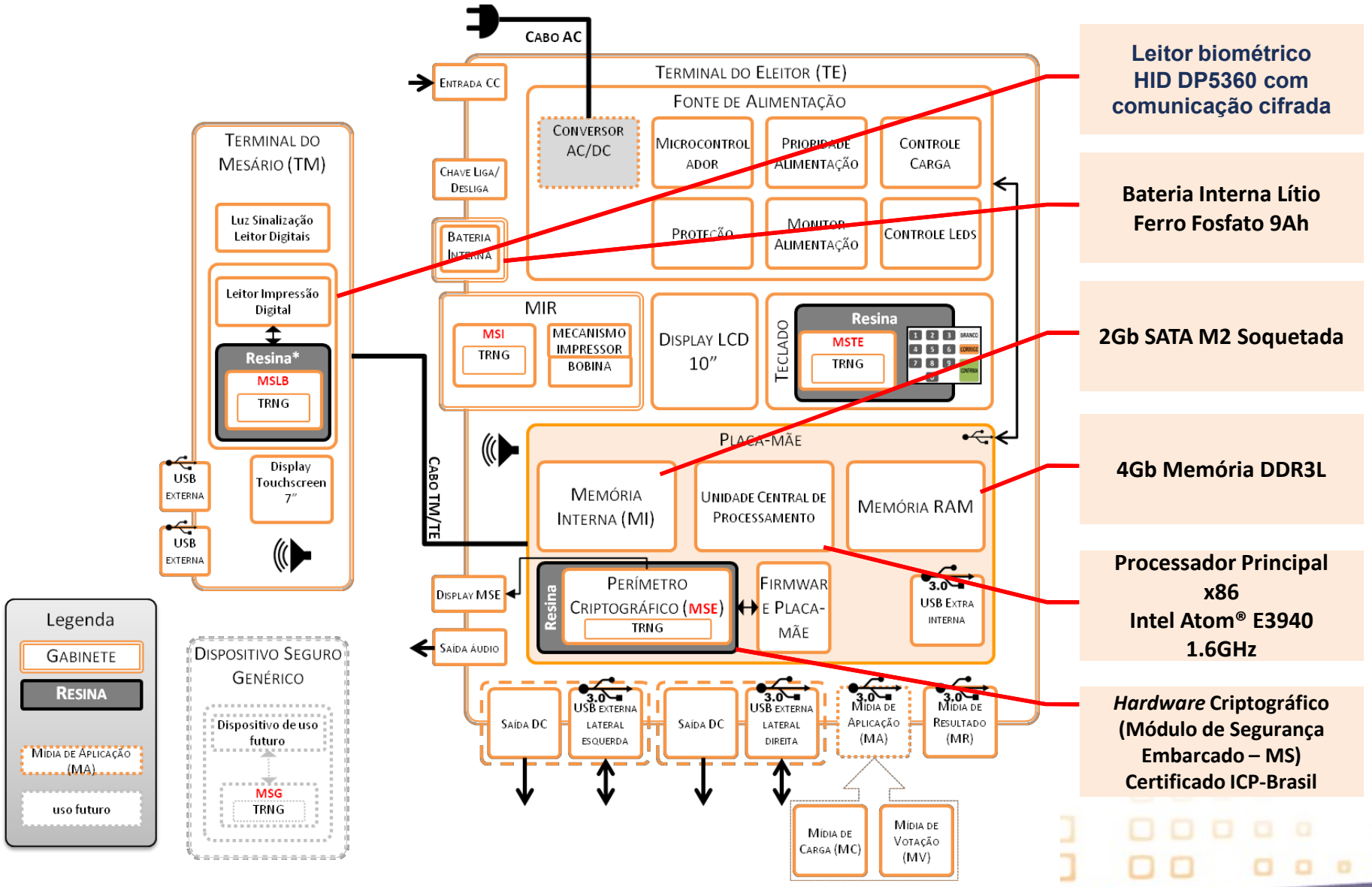
Mídia de Resultado (MR)

Display do Módulo de Segurança Embarcado (MSE)

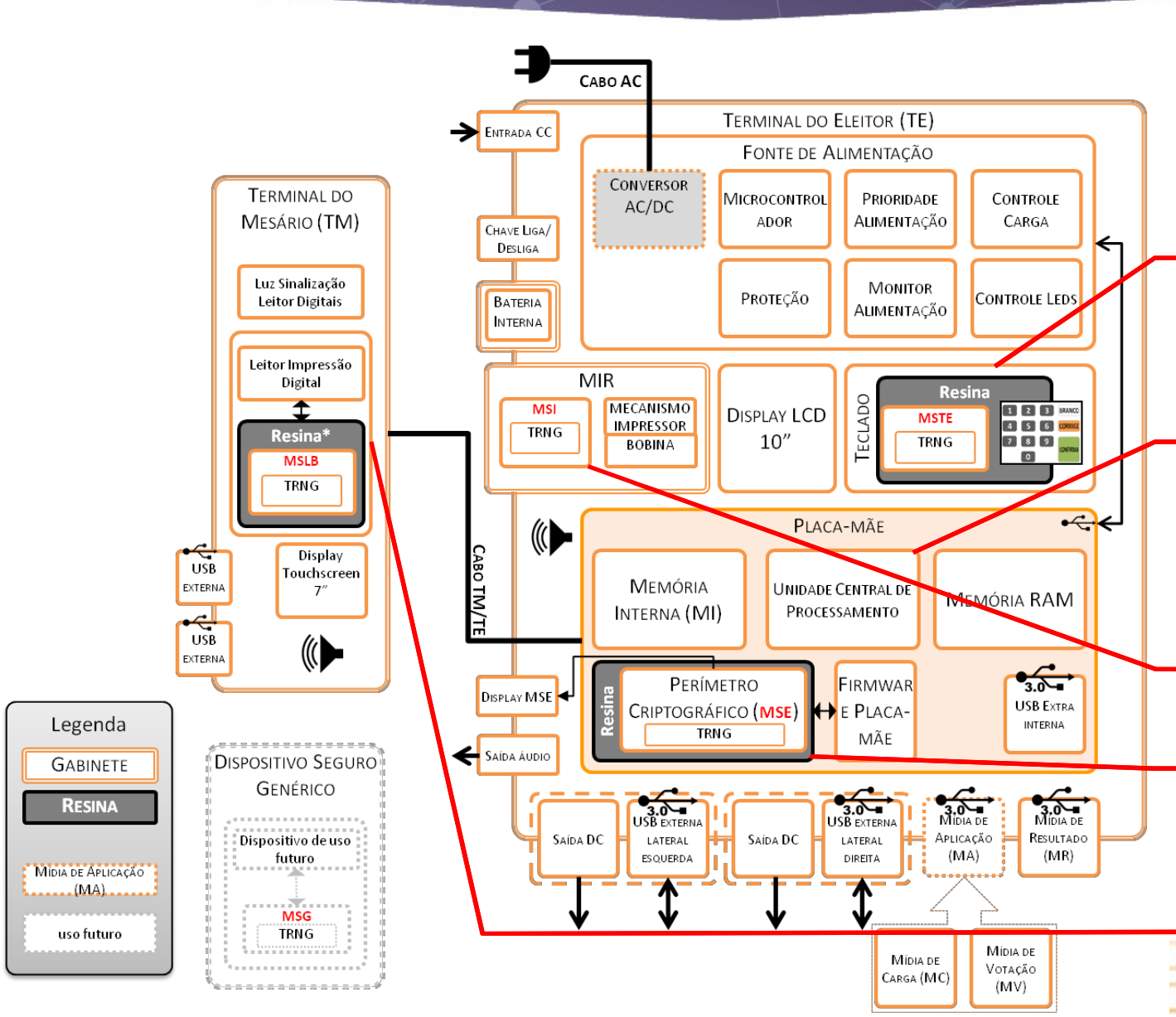
Arquitetura Geral das UE2020 e UE2022



Arquitetura Geral das UE2020 e UE2022



Arquitetura da Segurança das UE2020 e UE2022



A urna possui 5 processadores

Teclado cifrado
Módulo de Segurança do Teclado do Eleitor (MSTE)
Plataforma ARM

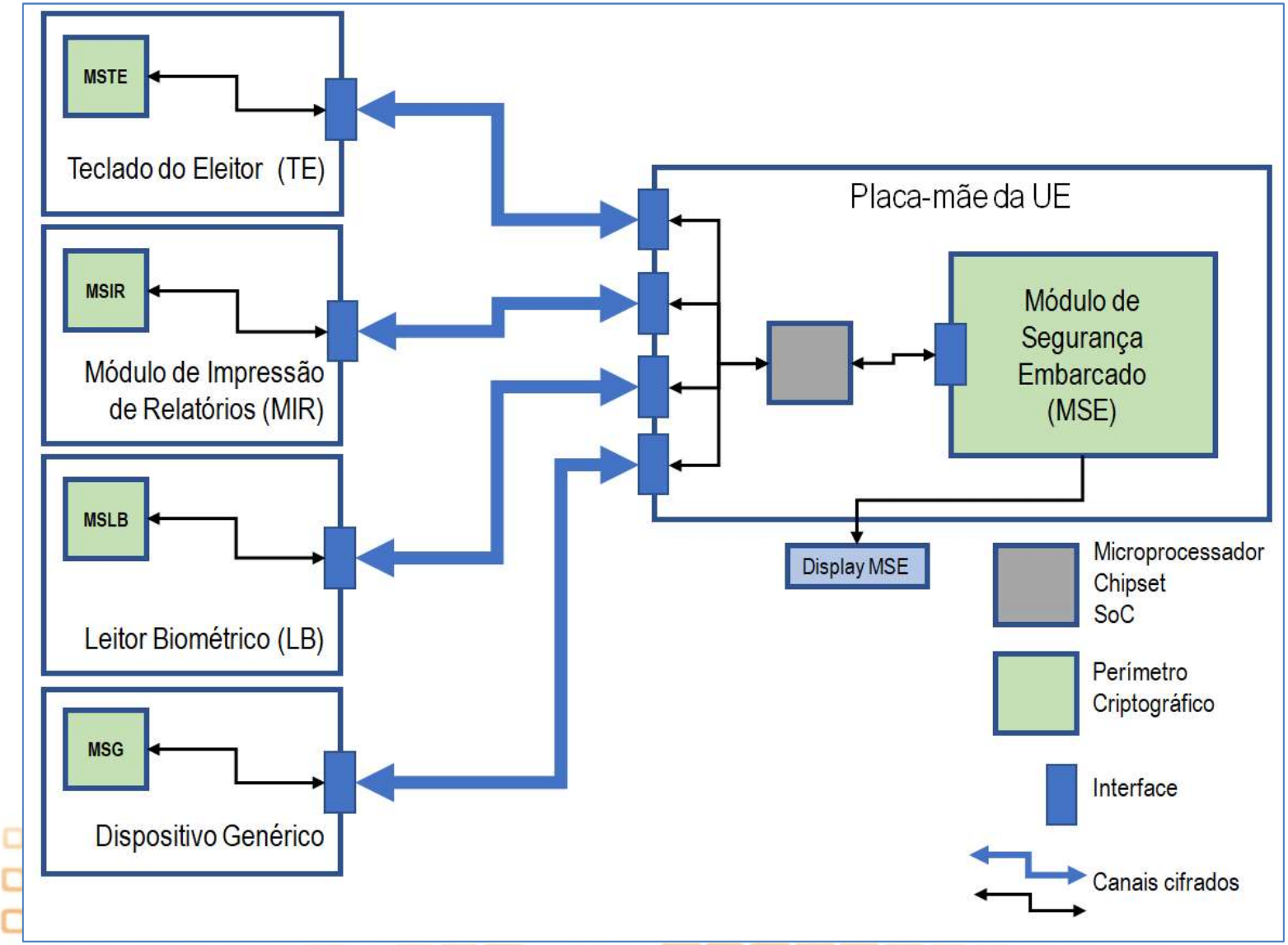
Processador principal
Plataforma x86

Impressora Segura
Módulo de Segurança da Impressora de Relatórios (MSIR)
Plataforma ARM

Módulo de Segurança Embarcado (MSE)
Plataforma ARM

Leitor Biométrico Cifrado
Módulo de Segurança do Leitor Biométrico (MSLB)
Plataforma ARM

Arquitetura da Segurança das UE2020 e UE2022



O Módulo de Segurança Embarcado (MSE)

A partir do modelo UE2009, as urnas utilizam uma arquitetura denominada T-DRE, criada pelo TSE e por pesquisadores da Unicamp.

T-DRE significa *Trusted Direct Recording Electronic.*

Hoje a arquitetura conta com cinco processadores: um x86 e quatro ARM em perímetros criptográficos.

Nas UE2009 a UE2015, o MSE era chamado de MSD – Main Security Device

T-DRE: a hardware trusted computing base for direct recording electronic vote machines

Twenty-Sixth Annual Computer Security Applications Conference, ACSAC 2010, Austin, Texas, USA, 6-10 December 2010

Principais Funções do MSE

Autenticação segura durante o *boot*

BIOS/UEFI antes da energização do processador x86;

Bootloader na partição EFI;

Kernel do UENUX (incluindo sua decifração).

Autenticação do *boot* em 5 perfis distintos

Autenticação da mídia assinada digitalmente em um dos cinco modos: Oficial, Simulado, Desenvolvimento, Manutenção e Inicializador.

Assinatura digital com não repúdio em três perfis, conforme inicialização

Certificação do perímetro criptográfico, conforme normas ICP-Brasil;

Algoritmos e circuitos elaborados para garantir a geração e segurança no uso das chaves privadas.

Provimento de serviços criptográficos simétricos e assimétricos

Fornecimento ao sistema de uma série de primitivas criptográficas simétricas, além de cifração e assinatura digital.

Fonte de números aleatórios (TRNG – *True Random Number Generator*)

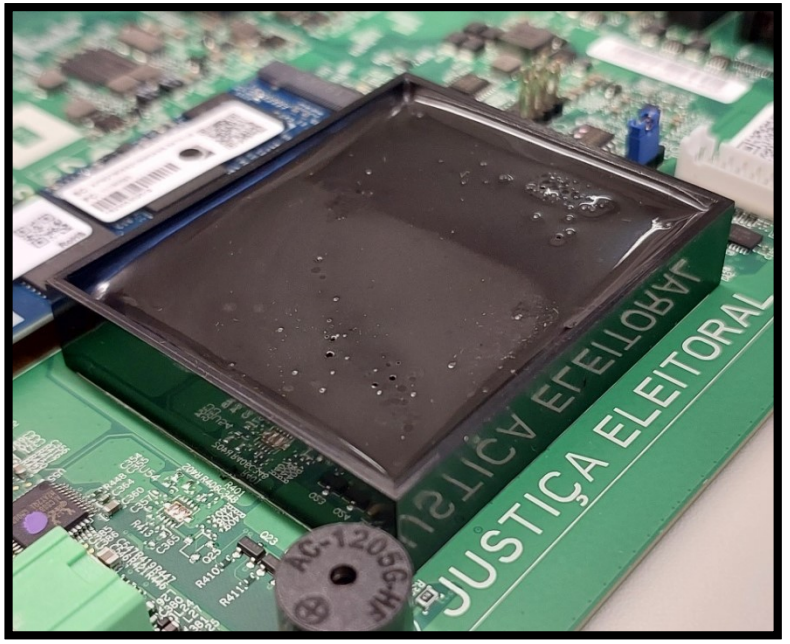
Circuito construído de modo a gerar valores verdadeiramente aleatórios, usados na geração de chaves e em outros usos.

Perfis operacionais do MSE

- Perfis operacionais
  - **Desenvolvimento** – Utilizado para executar *softwares* que se encontram em desenvolvimento
  - **Simulado** – Utilizado para testar *softwares* em fase distinta, sem que seja a versão oficial
  - **Oficial** – Utilizado para as eleições oficiais (LED de segurança acende verde)

Perfis Operacionais do MSE

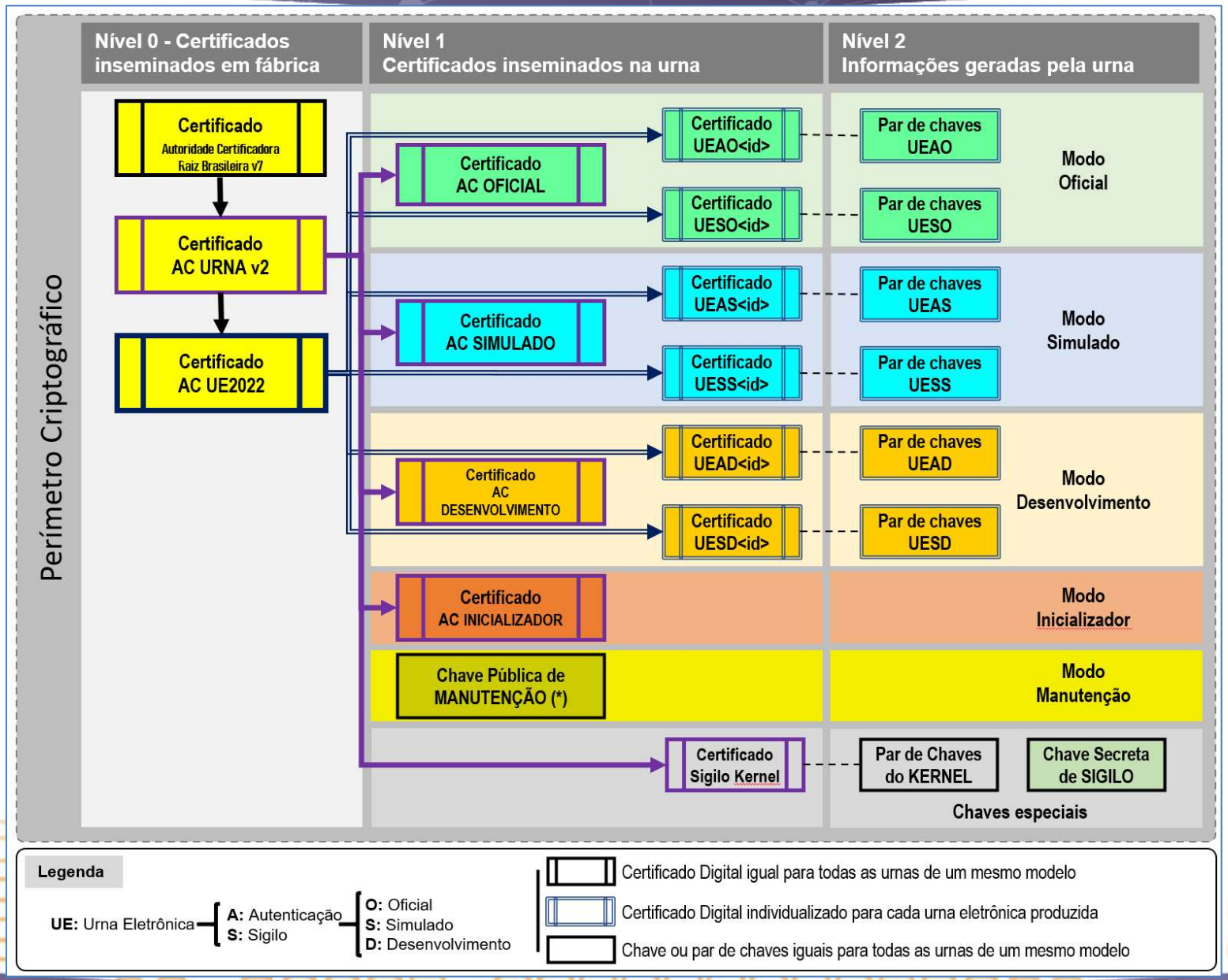
- Perfis operacionais
  - **Desenvolvimento** – Utilizado para executar *softwares* que se encontram em desenvolvimento
  - **Simulado** – Utilizado para testar *softwares* em fase distinta, sem que seja a versão oficial
  - **Oficial** – Utilizado para as eleições oficiais (LED de segurança acende verde)
- Somente esses três perfis permitem a assinatura digital pelo MSE
- Cada perfil utiliza seu próprio par de chaves (de assinatura e outro de cifração), sendo vedado pelo próprio MSE usar as chaves de perfil distinto do assinado na mídia



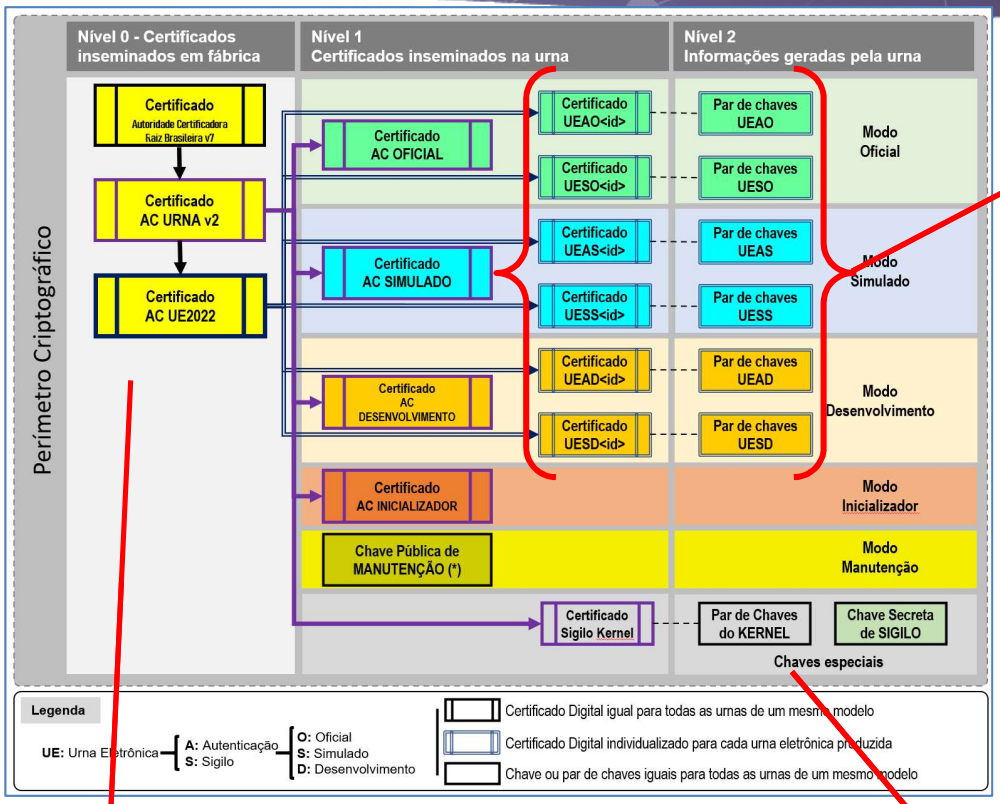
Perfis específicos do MSE

- Perfil Inicializador
  - Permite o *download* seguro de outro *firmware* para o MSE, MSTE, MSLB, MSIR
  - Permite a inserção dos certificados digitais correspondentes
- Perfil Manutenção
  - Permite execução de *software* do fabricante para teste da urna
- **ATENÇÃO: os perfis Inicializador e Manutenção NÃO permitem:**
  - O uso de pares de chave de assinatura e cifração da urna; e
  - O uso completo do Teclado do Eleitor – Apenas teclas BRANCO e CORRIGE são permitidas, além de teste sequencial do teclado.

Arquitetura da Segurança da UE2020/UE2022



Arquitetura da Segurança da UE2020/UE2022



Cada urna possui 3 pares de chaves para assinatura e 3 de cifração, com seus respectivos:

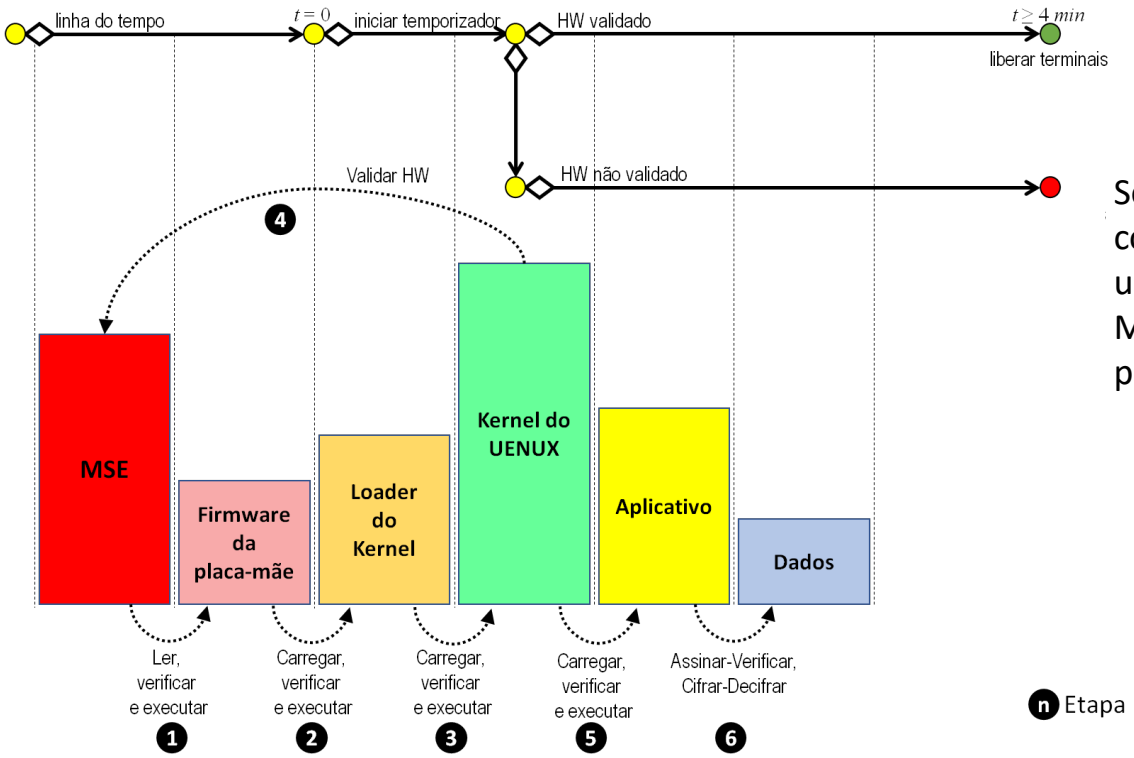
UEAO<nro interno> – Assinatura Oficial
UESO<nro interno> – Sigilo Oficial
UEAS<nro interno> – Assinatura Simulado
UESS<nro interno> – Sigilo Simulado
UEAD<nro interno> – Assinatura Desenvolvimento
UESD<nro interno> – Sigilo Desenvolvimento

- *As urnas UE2020 e UE2022 utilizam o algoritmo de curvas elípticas de Edwards E521*
- *O esquema de assinatura digital é o EdDSA – Edwards-curve Digital Signature Algorithm*

- **Todas as urnas UE2020 e UE2022 são subordinadas a uma Autoridade Certificadora: AC UE2020 e AC UE2022, respectivamente**
- **Essas duas ACs são subordinadas à AC URNA v2**

- **Há um par de chaves igual para todas as urnas que auxilia na guarda segura da chave simétrica que cifra o Kernel do UENUX**

Cadeia de Segurança da Urna Eletrônica

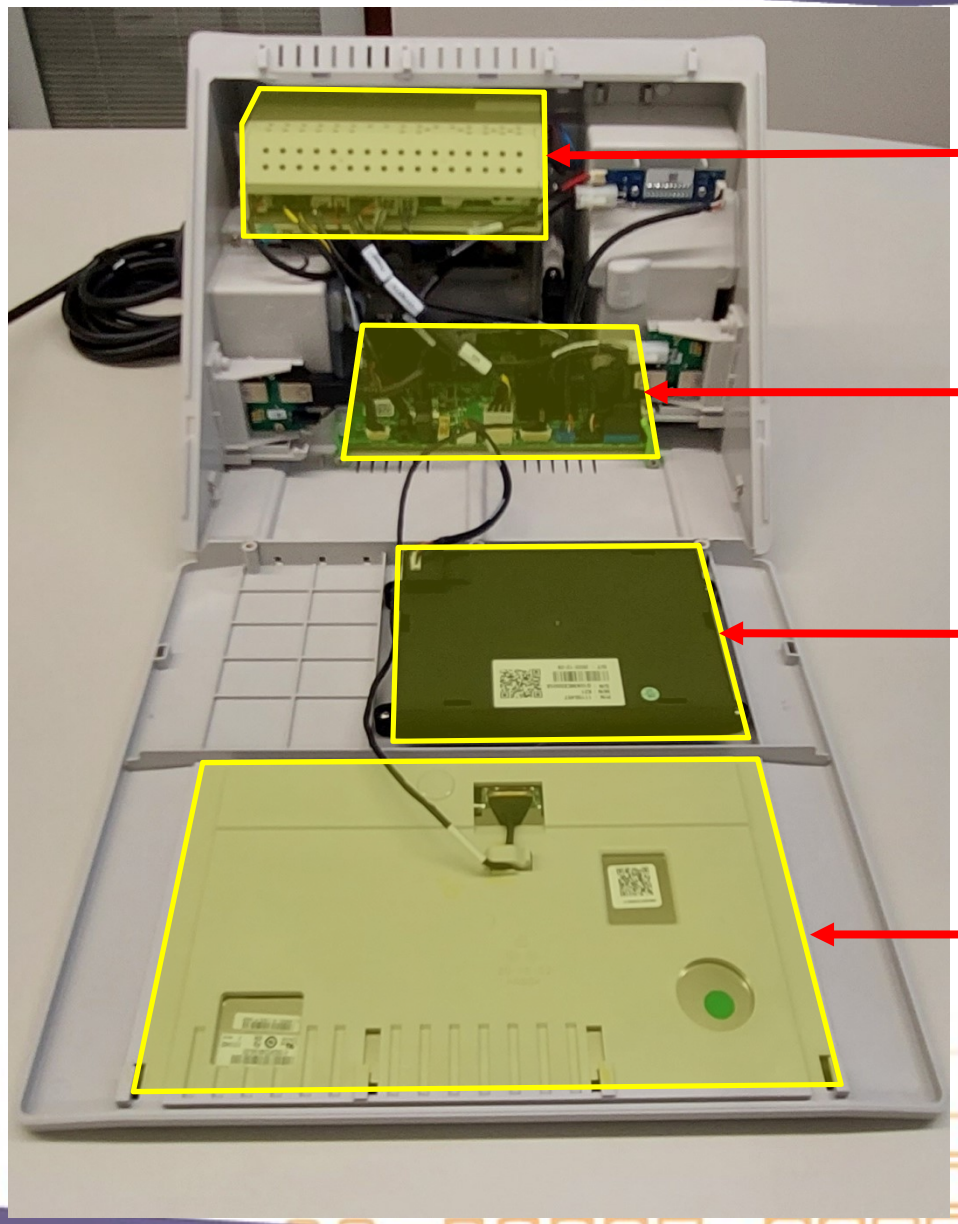


Se tudo não ocorrer corretamente dentro de um limite de tempo, o MSE desliga a energia do processador x86 da urna

1. O MSE valida conteúdo da versão única para o modelo da BIOS/UEFI
2. Com o auxílio do MSE, o Loader é validado em um dos perfis de boot
3. Com o auxílio do MSE, o Kernel do UENUX é validado e decifrado
4. O UENUX faz um desafio criptográfico para assegurar que está em uma urna eletrônica
5. O UENUX valida a execução de aplicativos pela respectivas assinaturas
6. A partir de um SCUE/GAP validado pelo UENUX, os demais arquivos da urna são validados quanto à sua integridade e autenticidade

A UE2020 e UE2022 internamente

Vista interna – Terminal do Eleitor



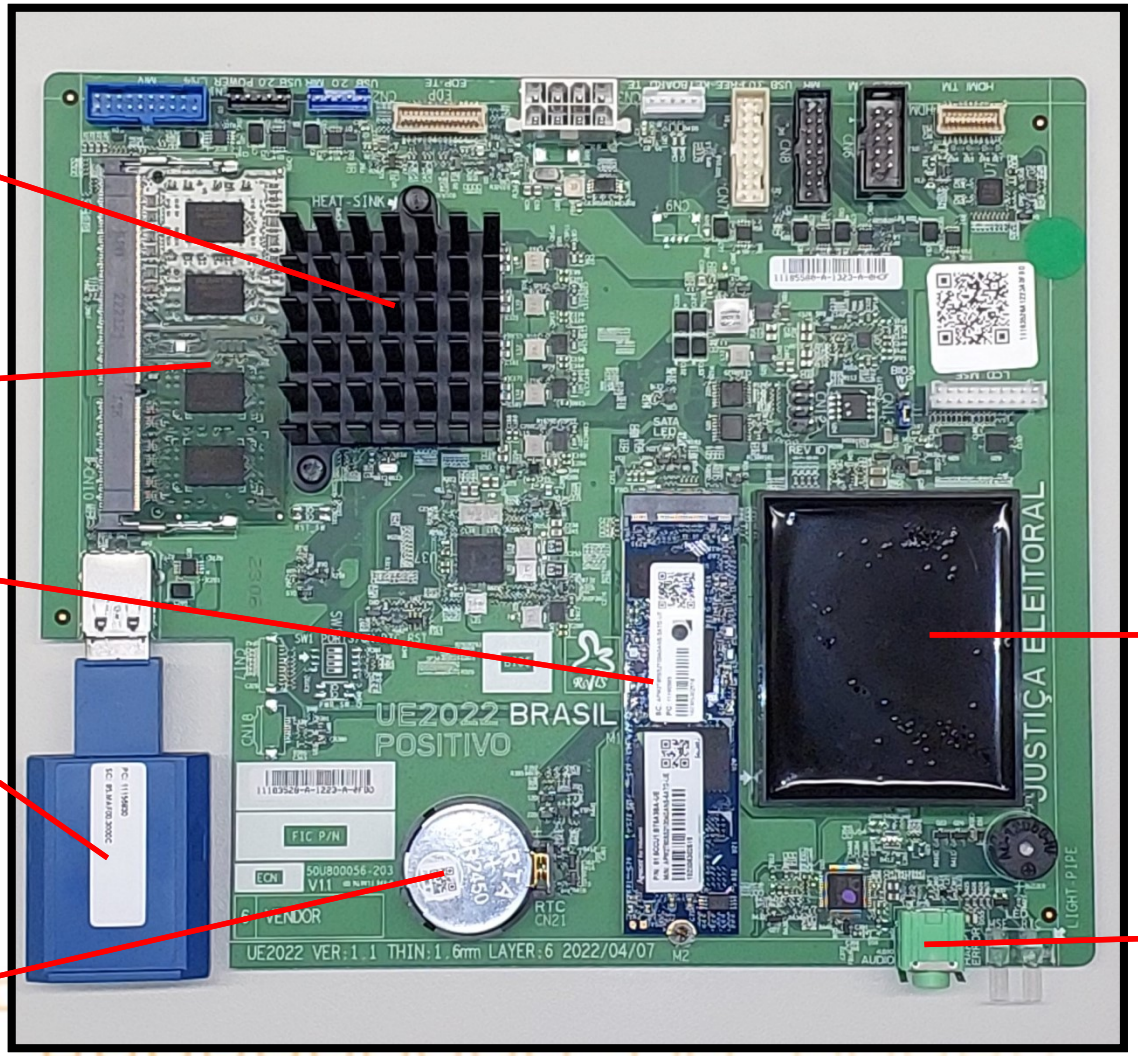
Fonte de Alimentação

Placa-mãe

Teclado do Terminal do Eleitor

Tela do Terminal do Eleitor

Placa-mãe UE2020 e UE2022



Processador x86

Memória RAM DDR3

Mídia de Interna (SSD)

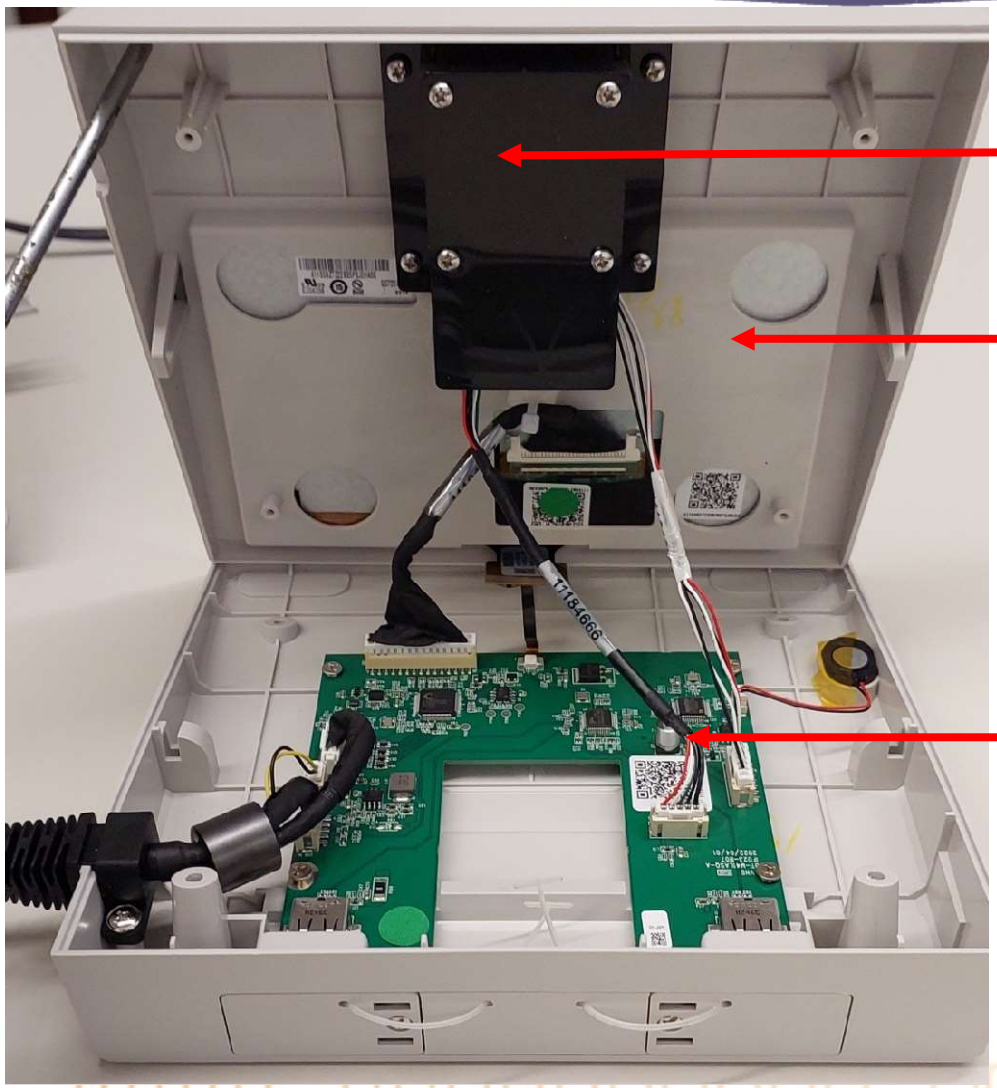
Mídia de Aplicação

Bateria Relógio Interno

MSE

Saída para Fone de Ouvido

Terminal do Mesário

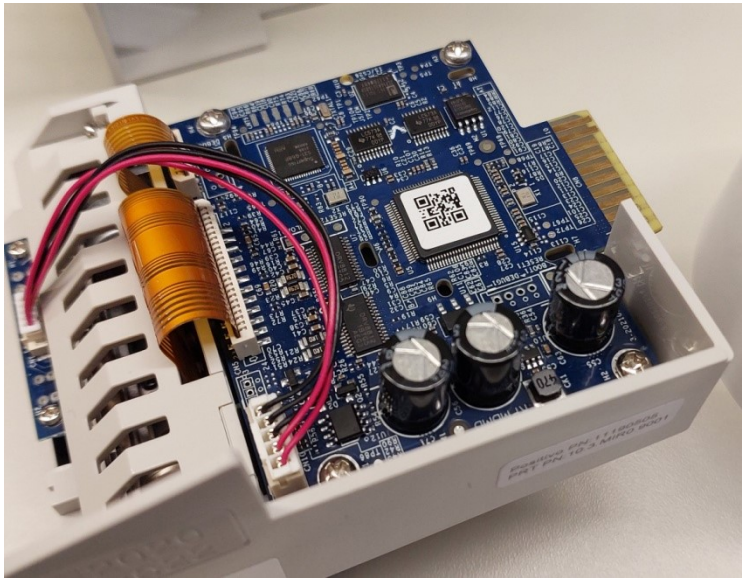


Leitor Biométrico

Tela do TM com *touchscreen*

Placa Controladora

Módulo Impressor de Relatórios



Coordenadoria de Tecnologia Eleitoral – Cotel

cotel@tse.jus.br