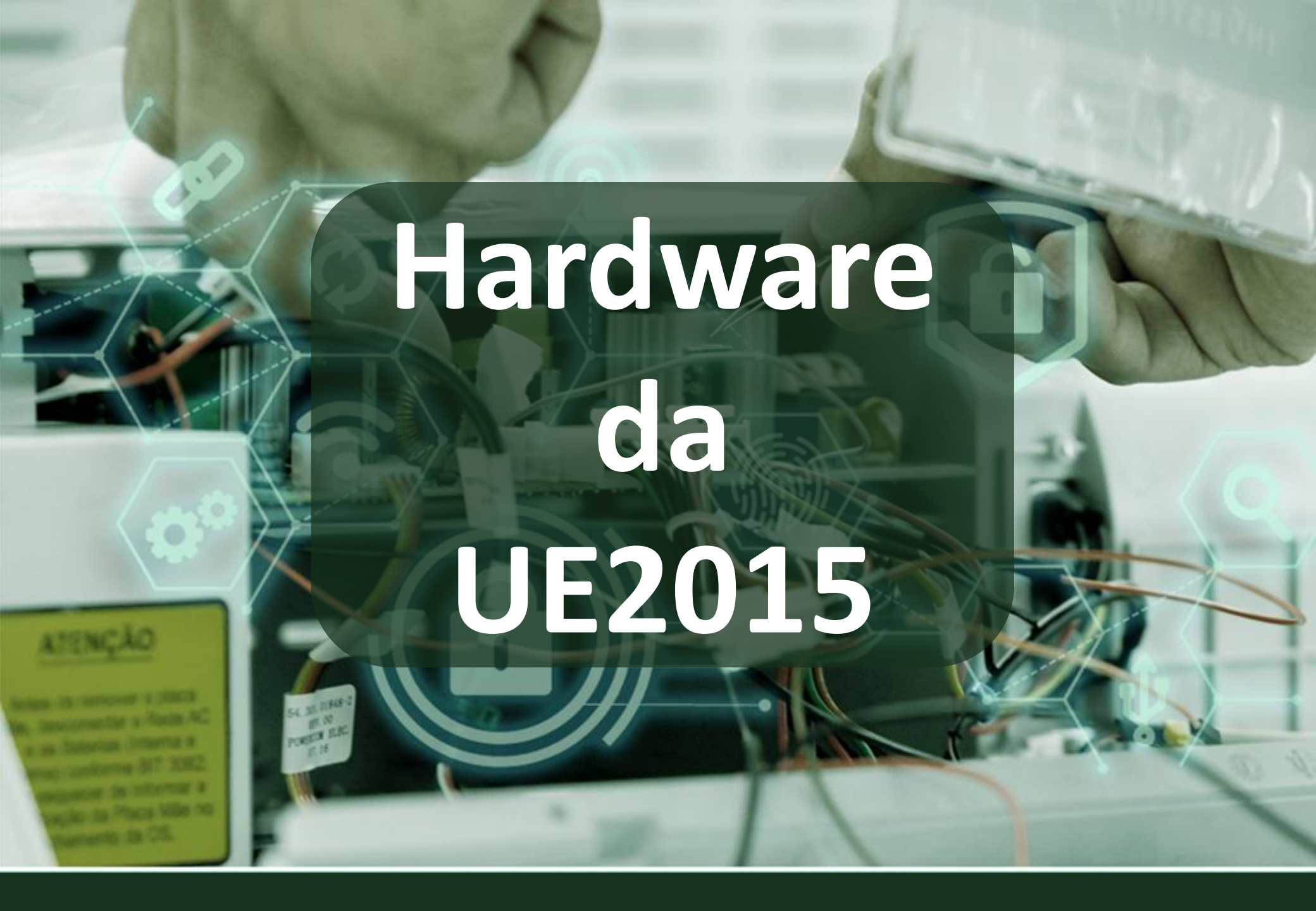


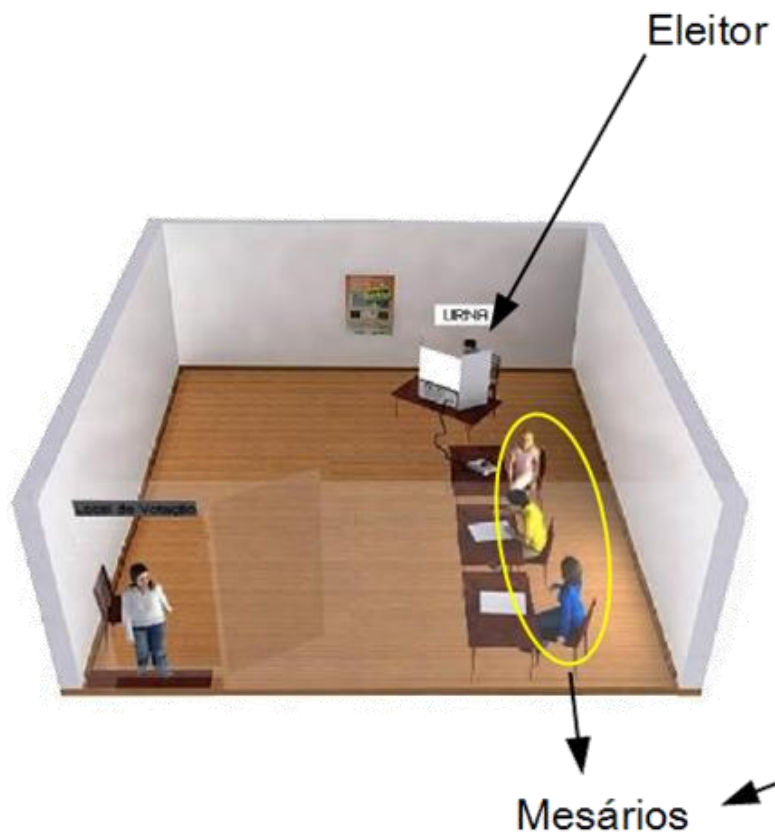
The background image shows a person's hands working on a computer. On the left, a yellow warning label with the word 'ATENÇÃO' is visible. In the center, a person is holding a transparent plastic case, likely for a hard drive. The image is overlaid with a dark green semi-transparent rectangle containing the title text. Various light green tech icons, including a padlock, gears, a magnifying glass, a USB symbol, and a Wi-Fi symbol, are scattered around the central text area.

Hardware da UE2015

Objetivos

- **Apresentar aos participantes do TPS2021:**
 - A urna eletrônica que será utilizada no evento – modelo UE2015
 - A arquitetura do hardware da UE2015, com foco nos aspectos de segurança
 - O encadeamento de segurança das urnas eletrônicas
- Há informações adicionais depois do último slide, para servirem como:
 - Referência rápida das partes da UE2015
 - nomenclatura utilizada pela JE (facilitar a comunicação)
 - Um guia para facilitar a abertura da UE2015

Seção Eleitoral



A Urna Eletrônica UE2015



A Urna Eletrônica UE2015



TERMINAL DO ELEITOR - TE



A Urna Eletrônica UE2015



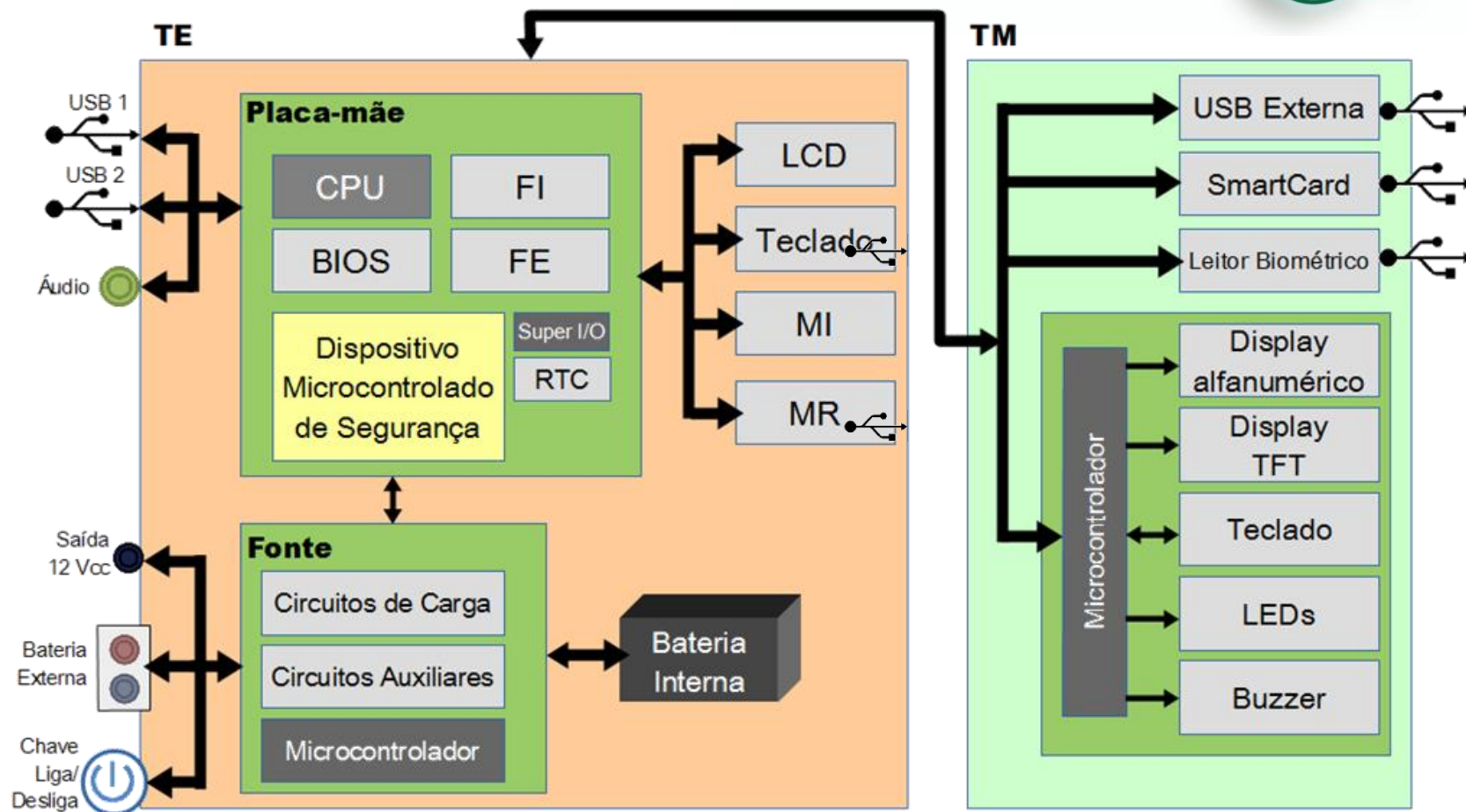
**TERMINAL DO MESÁRIO
TM**

UE2015 – especificações

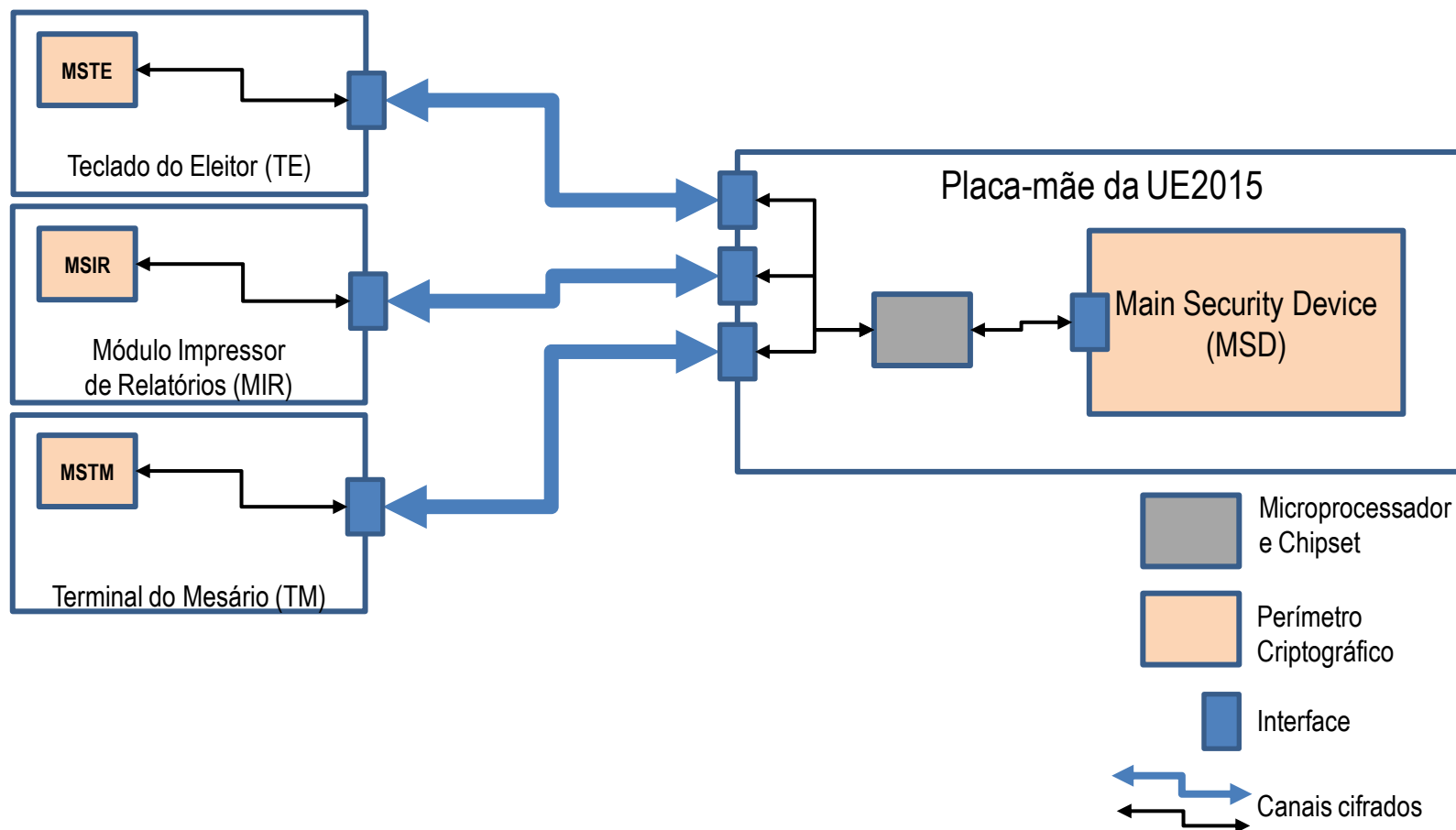


Placa-mãe	Proprietária da Diebold Nixdorf
CPU	Intel Atom Z510P 1,10 GHz
Fonte	Microcontrolada
Display	LCD Policromático 10,1" HannStar (1280 x 768)
Bateria	UNICOPA (Unipower) Chumbo-ácido – 12V - 7,0Ah – UP1270
Impressora	Térmica Mecaf
Display alfanumérico do TM	4 linhas por 40 colunas
Display gráfico do TM	TFT 240x320 – 2.4" – DLC
Leitor de Impressões Digitais	Futronic FS-81HS
Leitor de SmartCard	Argos Mini II
CompactFlashes – <i>Flash Card</i>	Apacer 512MB
USBs externas do TE	2
USBs externas do TM	1
Fabricante	Diebold Nixdorf

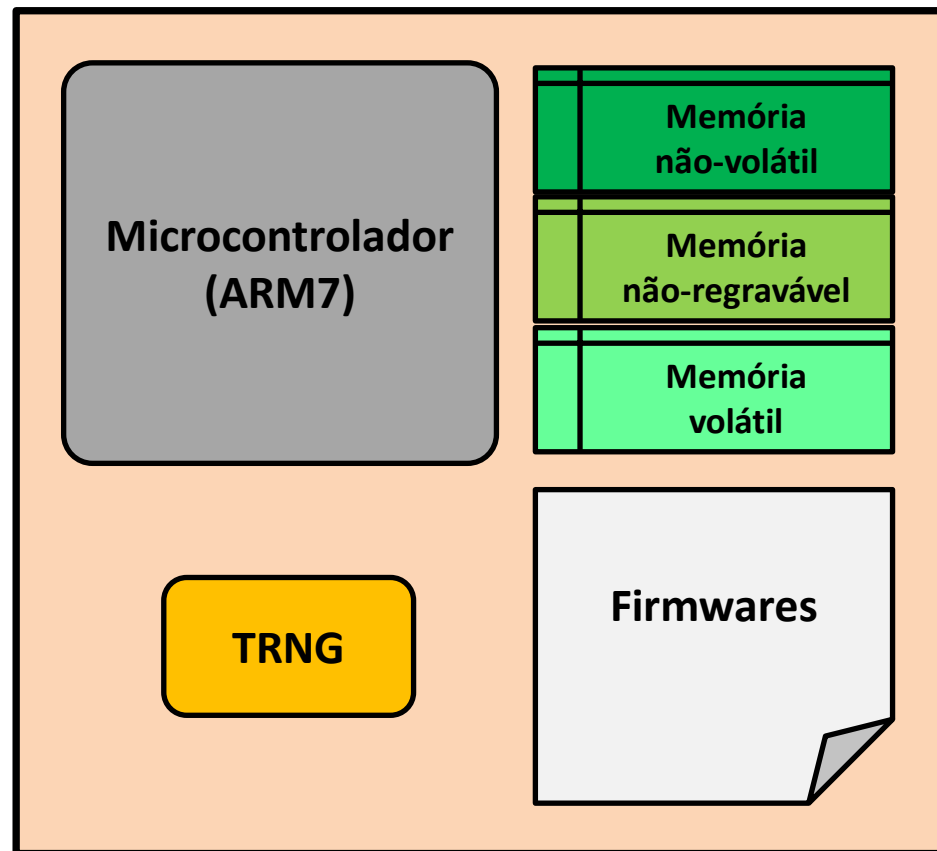
Arquitetura do *hardware* da UE2015



Módulos de segurança em *hardware*



Componentes dos módulos de segurança em *hardware*



Características dos firmwares do MSD



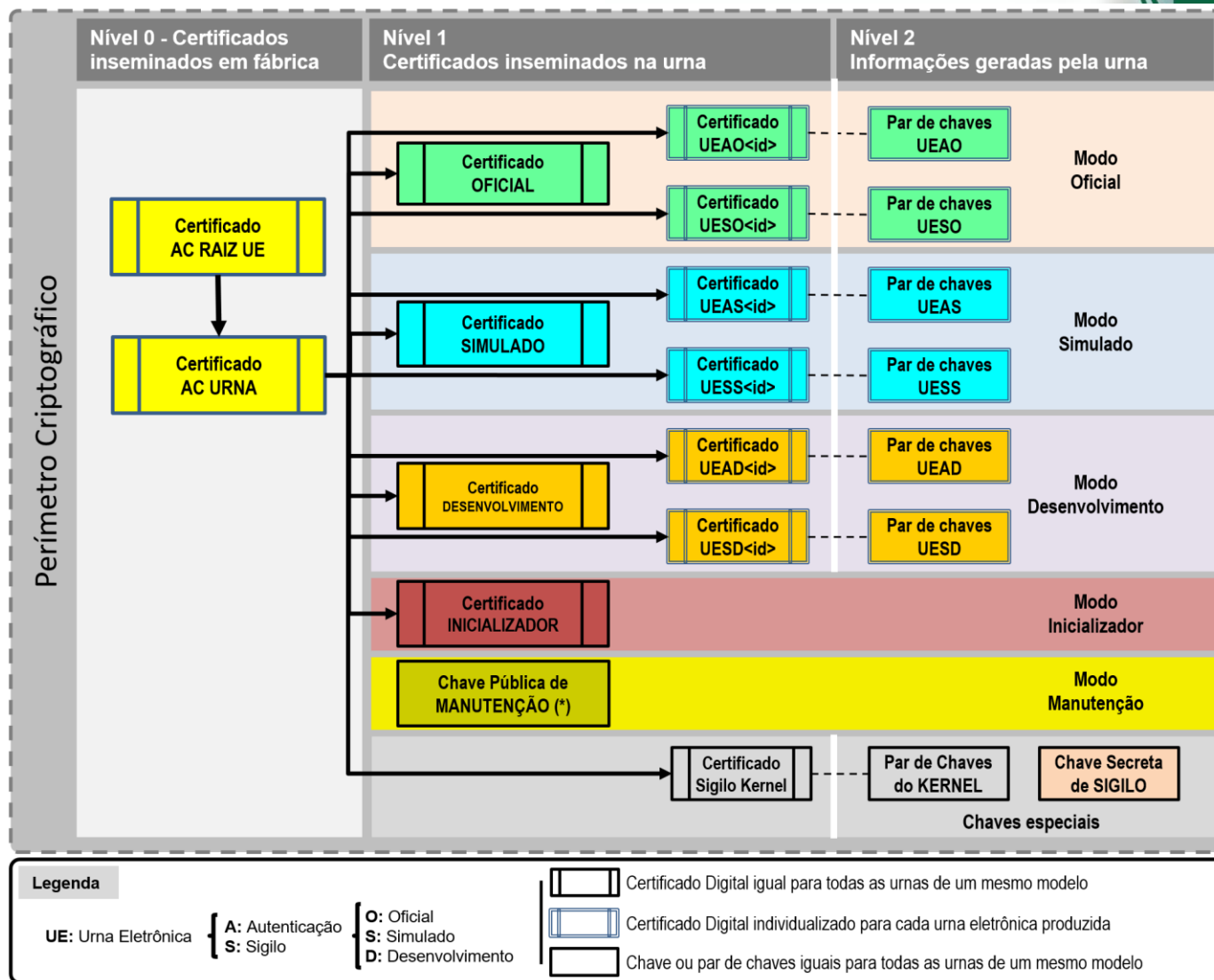
- geram chaves criptográficas não-exportáveis
 - usando o TRNG
- atualização segura dos firmwares
 - assinatura e verificação
 - garantia de que a atualização não deixa partes não verificadas da memória
- importam chaves secretas de maneira segura
 - utilizadas para
 - autenticar os periféricos, por meio de seus respectivos módulos de segurança
 - estabelecer canais cifrados de comunicação entre a CPU e o periférico com módulo de segurança em hardware
- fornecem serviços criptográficos
 - acessíveis ao desenvolvedor por meio de API
- abrigam, em memória não-regravável, identificador único para cada urna eletrônica (Número Interno)

Características das chaves dos dispositivos



- MSD
 - chaves principais (EC P-521)
 - geradas internamente
 - únicas para cada urna eletrônica
 - certificadas por AC própria e de uso exclusivo para urnas
- Periféricos (MSTE, MSTM e MSIR)
 - chaves principais
 - implantadas durante a fabricação, em sala segura
 - geradas internamente por dispositivo externo (SmartCard)
 - RSA 2048
 - únicas para todos os periféricos do mesmo tipo
 - cifração do canal usa chaves temporárias AES 256

Hierarquia de chaves das ACs de urnas



5 (Cinco) Perfis de Execução



- 2 perfis pré-operacionais (M-I)
 - Manutenção (M)
 - Utilizado em ambiente fabril, com muitas restrições operacionais
 - Inicializador (I)
 - Utilizado para manutenção, tais como atualização de firmwares e implantação de chaves
- 3 perfis operacionais de segurança (D-S-O)
 - Desenvolvimento (D)
 - Utilizado para executar *softwares* que se encontram em desenvolvimento
 - Simulado (S)
 - Utilizado para executar *softwares* em procedimentos de testes e simulados
 - Oficial (O)
 - Utilizado para executar *softwares* exclusivamente durante eleições oficiais
- Cada perfil dispõe de um conjunto de chaves específicas

Softwares Básicos



- As urnas eletrônicas têm como *softwares* básicos:
 - BIOS (Sistema Básico de Entrada/Saída)
 - Bootloader (carregador de SO)
 - Sistema Operacional UENUX
 - Firmwares do MSD, MSTE, MSTM, MSIR
 - Drivers dos dispositivos de E/S

Softwares Básicos – BIOS



- BIOS (Sistema Básico de Entrada/Saída):
 - Contém o código necessário para a comunicação com seus dispositivos
 - Gravado em memória não volátil
 - se a urna eletrônica não tiver qualquer fonte de energia, o BIOS permanecerá na memória em que está gravado
 - pode ser regravado pela própria urna
 - É assinado digitalmente pelo TSE
 - Sua assinatura é verificada pela chave pública previamente inseminada na urna (Inicializador)
 - Adquirido/desenvolvido pelo fabricante da urna (Diebold-Nixdorf/AMI)

Softwares Básicos - Bootloader



- Bootloader (carregador de SO):
 - Pequeno código cuja função principal é carregar o Sistema Operacional (UENUX) de uma memória CompactFlash (FE ou FI) para a memória RAM da urna eletrônica
 - Reside em posição previamente estabelecida da CompactFlash (FE ou FI)
 - no início, de acordo com a geometria de disco
 - o BIOS busca um Bootloader na FE
 - caso não encontrar, busca um Bootloader na FI
 - É assinado digitalmente pelo TSE
 - Sua assinatura é verificada pela chave pública previamente inseminada na urna (Desenvolvimento, Simulado ou Oficial)
 - Desenvolvido e mantido pela SEVIN – TSE

Softwares Básicos – UENUX



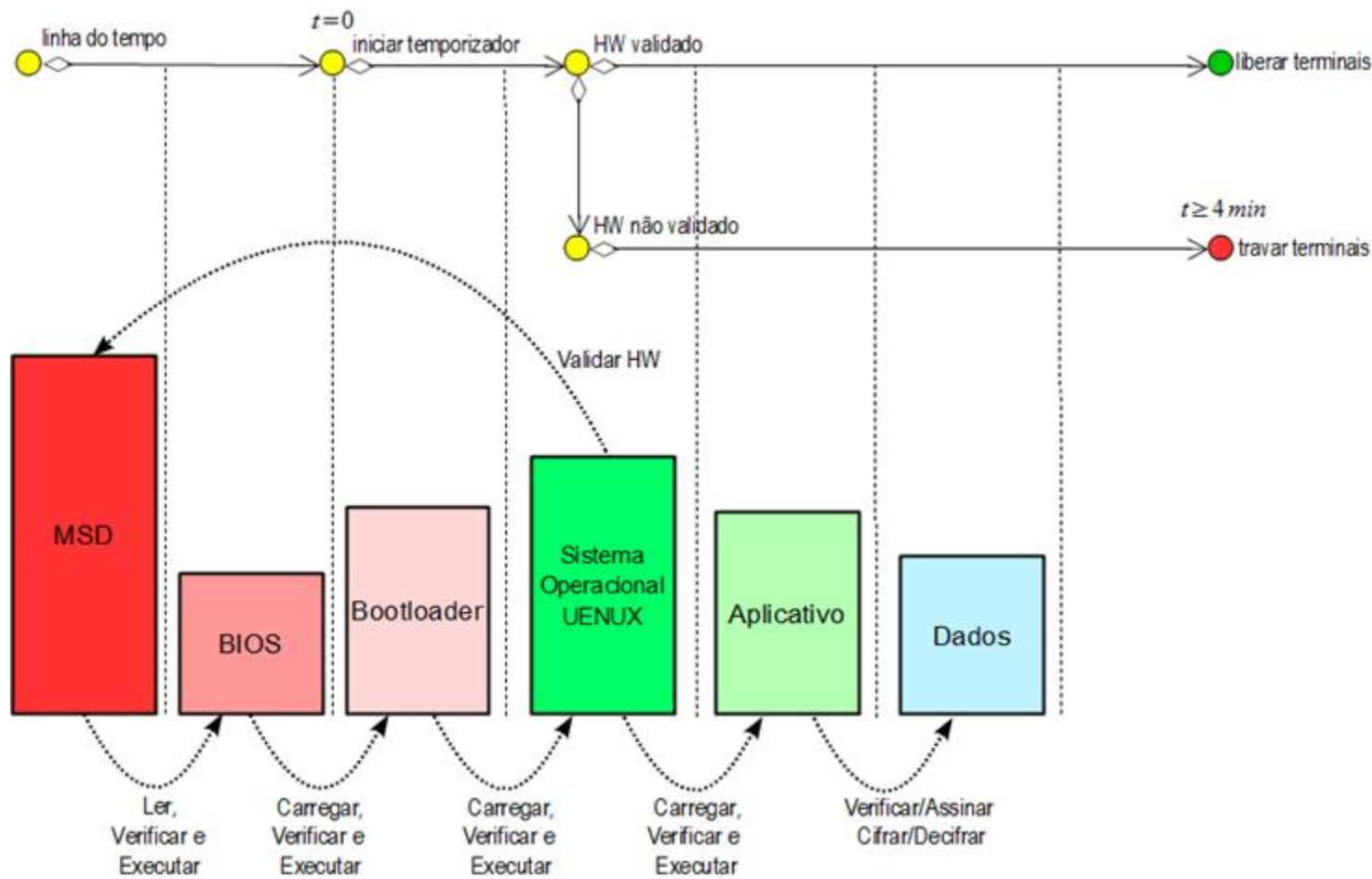
- UENUX – Sistema Operacional (SO) das urnas eletrônicas:
 - Distribuição Linux para uso exclusivo nas urnas eletrônicas
 - Fica gravado na FE ou FI
 - Pode ser regravado pela própria urna
 - É assinado digitalmente pelo TSE
 - Sua assinatura é verificada pela chave pública previamente inseminada na urna (Desenvolvimento, Simulado ou Oficial)
 - Customizado e mantido pela SEVIN – TSE

Softwares Básicos – MSD

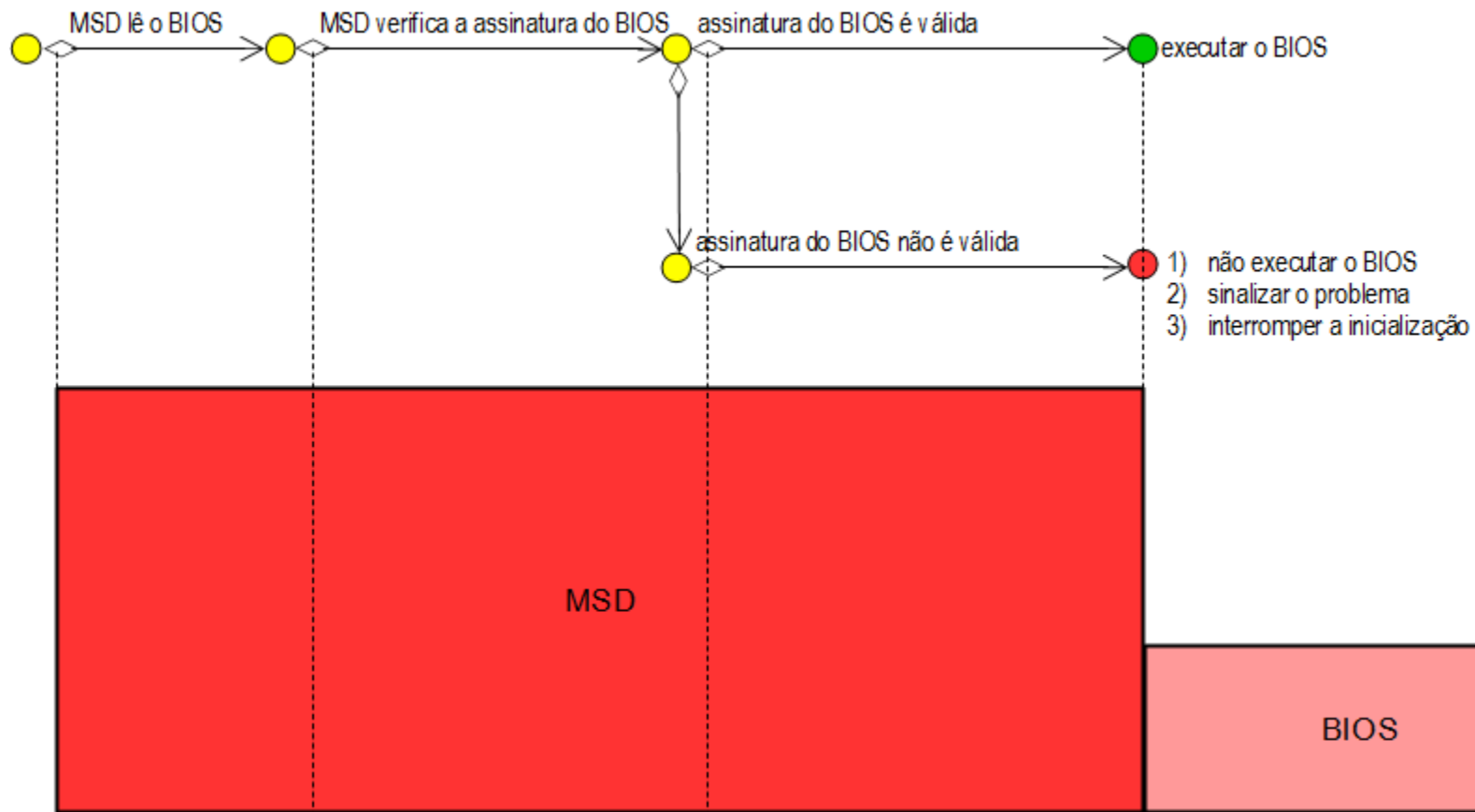


- MSD – Dispositivo Microcontrolado de Segurança
 - É um outro sistema computacional (processador e memória próprios)
 - Reside na mesma placa-mãe da urna – em um “Perímetro Criptográfico” – segregado e resinado
 - Contém como processador um ARM7 e um circuito TRNG (gerador de número realmente aleatório)
 - **É garantidamente o primeiro circuito da placa-mãe a ser energizado quando a urna é ligada**
 - *Firmware* mantido, adquirido e desenvolvido pela Diebold-Nixdorf

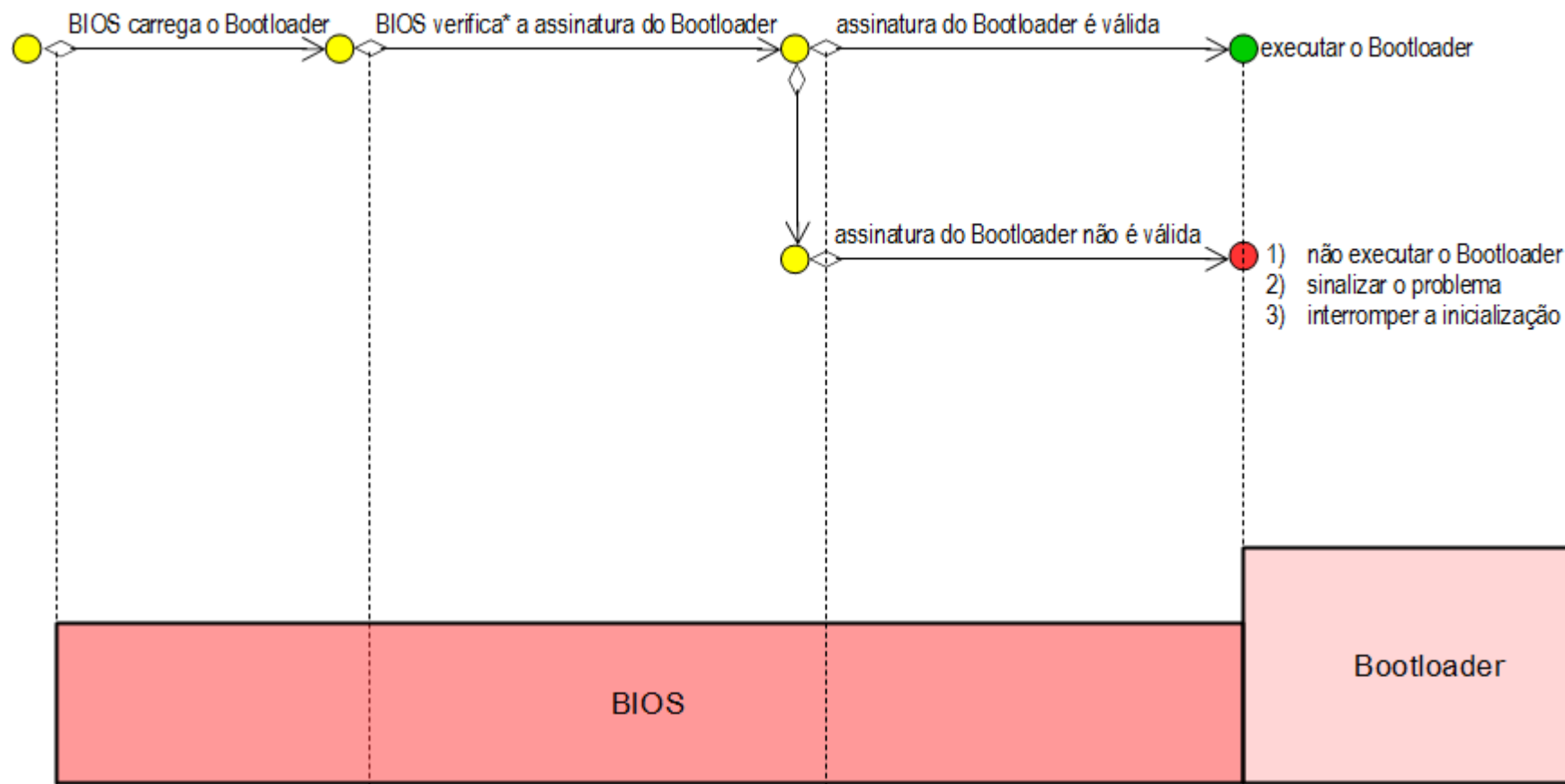
Encadeamento de segurança baseado em *hardware* – visão geral



MSD verifica e executa o BIOS

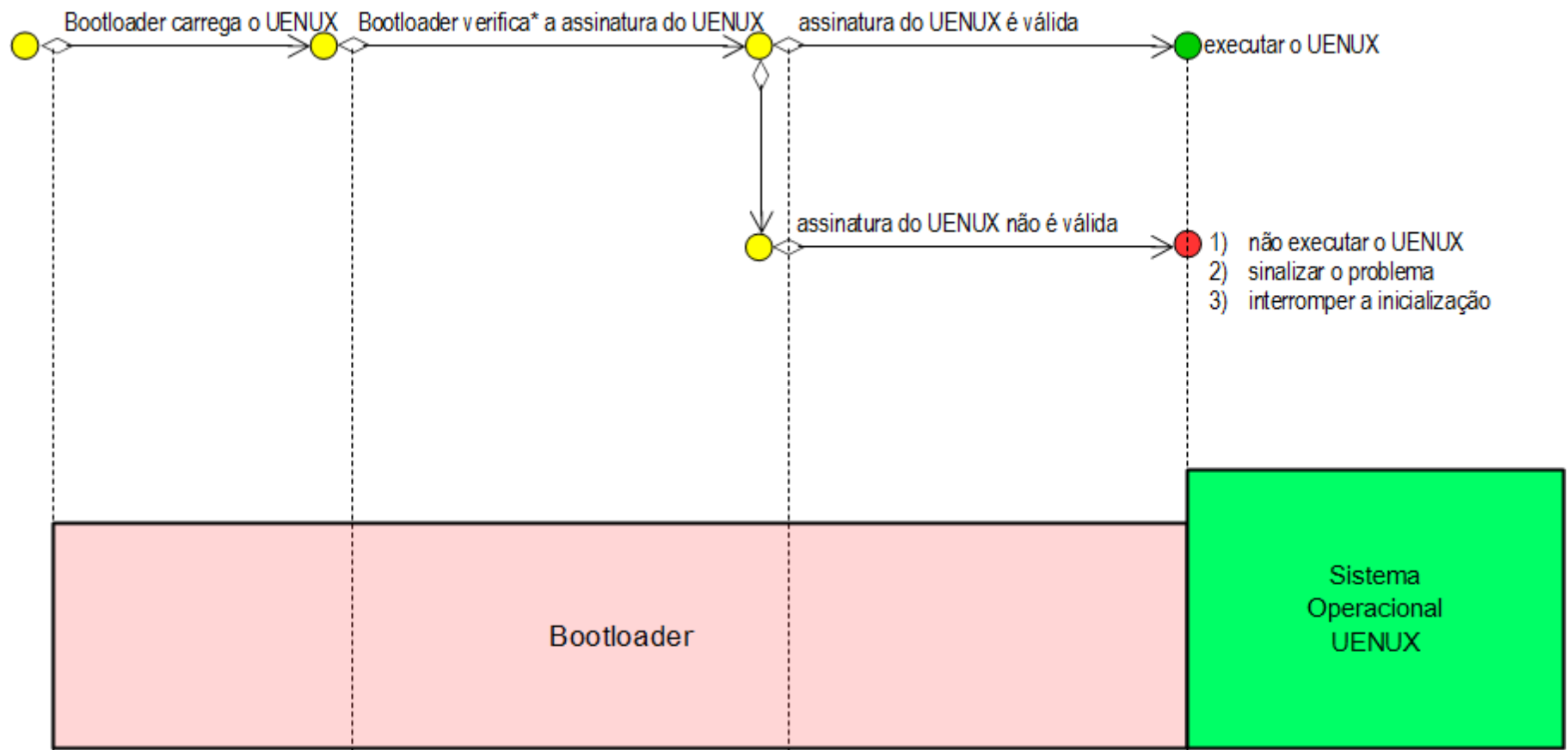


BIOS carrega, verifica e executa o Bootloader



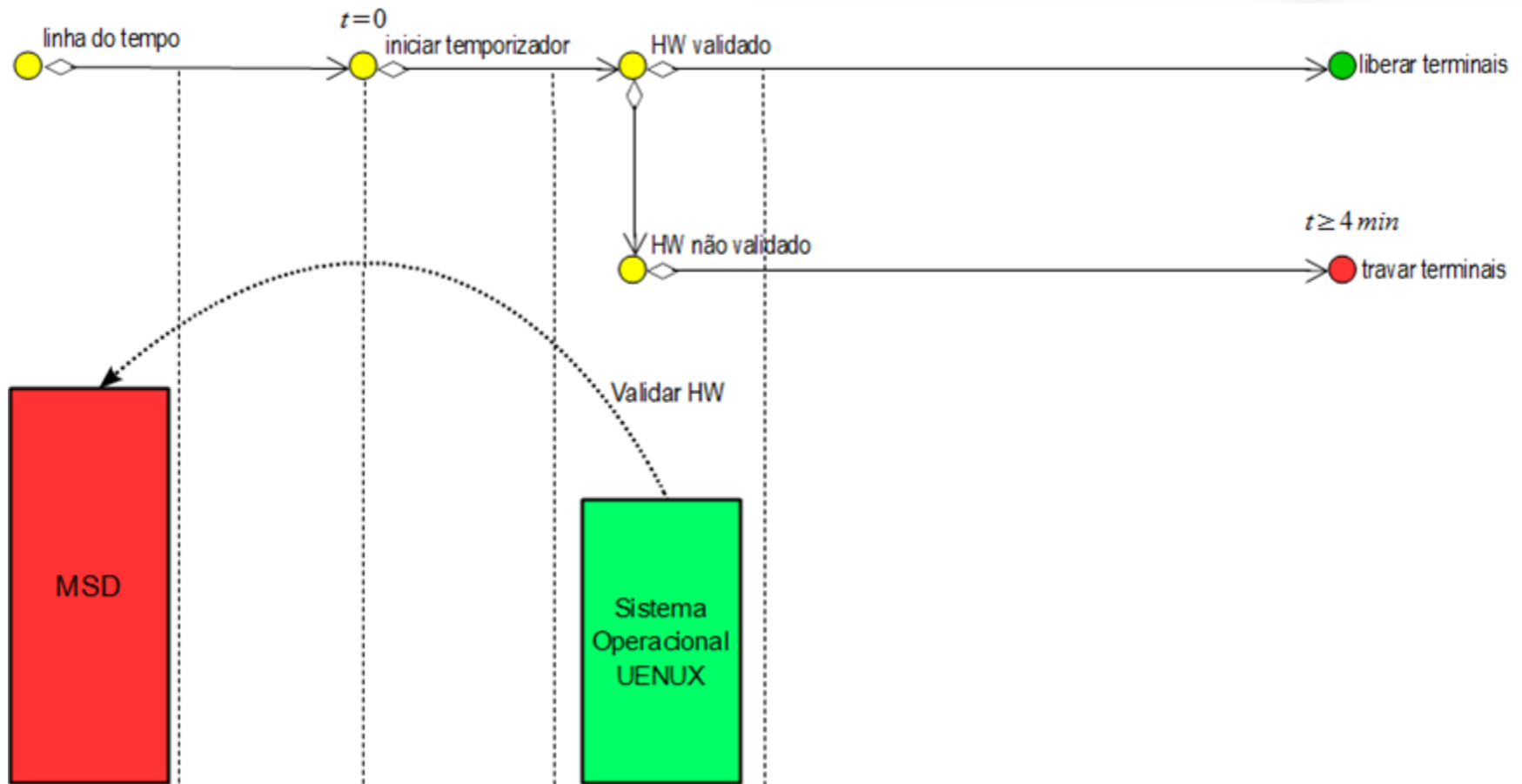
* a verificação da assinatura é executada usando o MSD

Bootloader carrega, verifica e executa o UENUX



* a verificação da assinatura é executada usando o MSD

UENUX valida o *hardware*



UENUX valida o *hardware*



- Do que consiste tal validação?
 - Um *driver* do UENUX
 - verifica qual é o modo de segurança (D-S-O)
 - executa um DESAFIO
- DESAFIO
 - O UENUX envia uma informação cifrada para o MSD decifrar
 - **SE** o MSD conseguir decifrar
 - **ENTÃO** o MSD sinaliza o UENUX de que o desafio foi resolvido
 - **SENÃO**
 - Depois de decorrido um tempo máximo (*timeout*)
 - Sinaliza que o desafio não foi resolvido e que o *hardware* não é válido



Obrigado!

Luís Augusto Consularo

segele@tse.jus.br

SEGELE/COTEL/STI



Informações adicionais sobre o hardware da UE2015

A Urna Eletrônica UE2015

Gabinete do TE

Envelope do TE

UE 2015

JUSTIÇA
ELEITORAL

Display LCD do TE

Teclado do TE

Display
alfanumérico
do TM

Leitor
Biométrico

Leds
Indicadores
do TM

Display TFT
do TM

Teclado
do TM

Teclado do TE

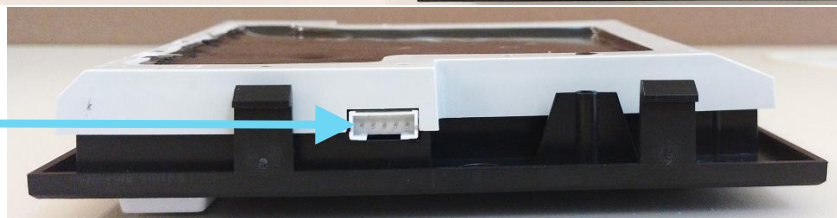


Circuitaria resinada



Disposição das teclas numéricas como no telefone (e não como na calculadora)

Conector para a placa-mãe

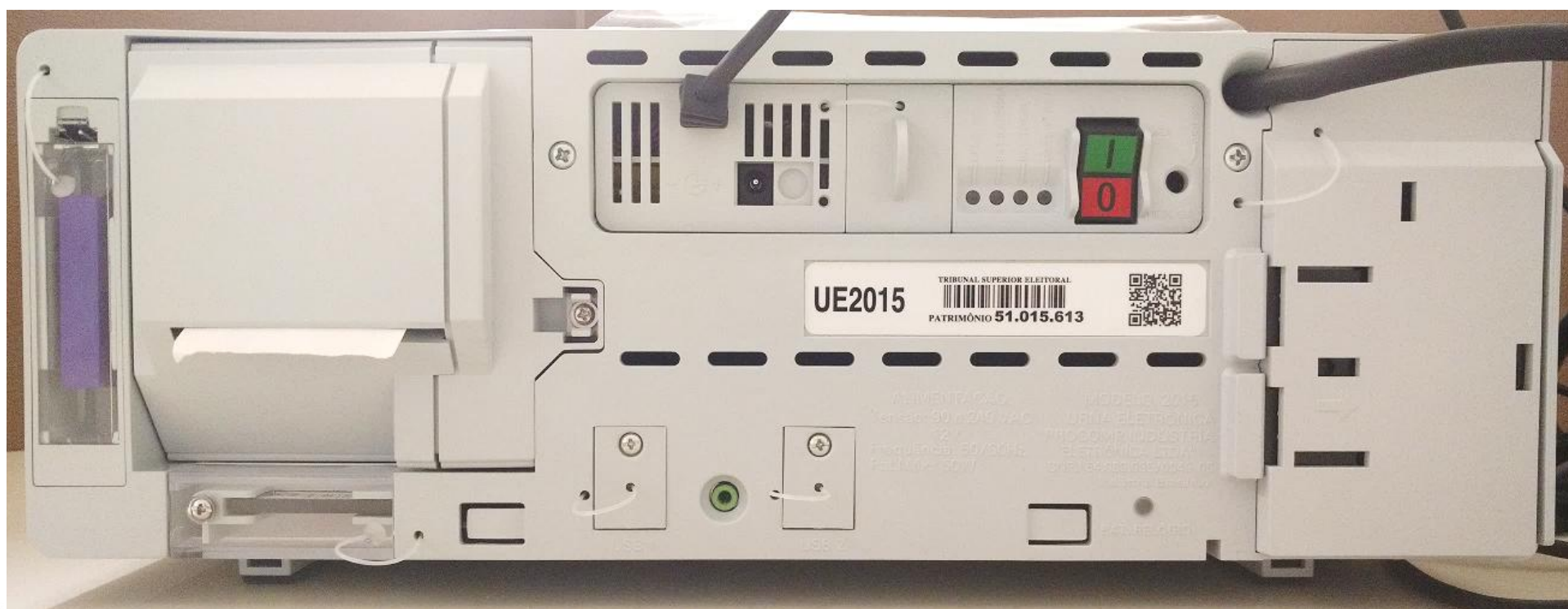


Fixação



Teclas com curso e limiar de força para acionamento especialmente especificados

Face traseira do TE

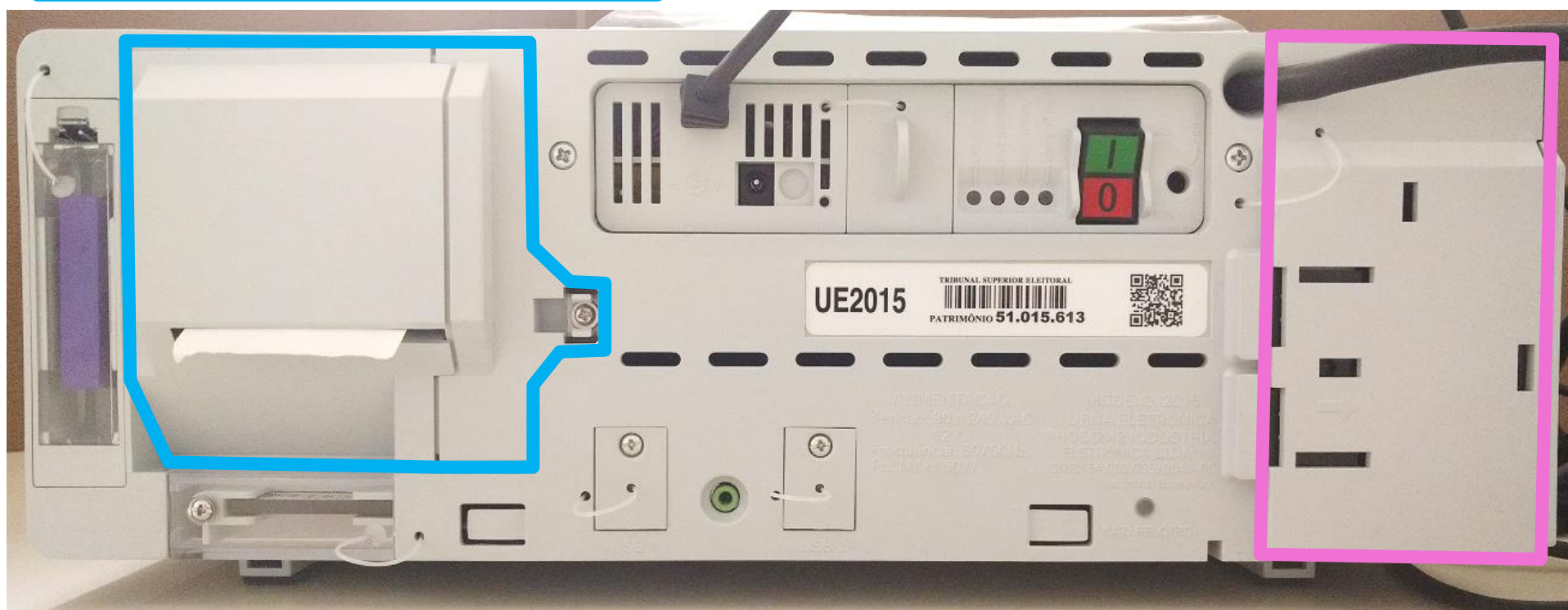


MI e Bateria Interna



Módulo Impressor - MI

Compartimento da Bateria Interna



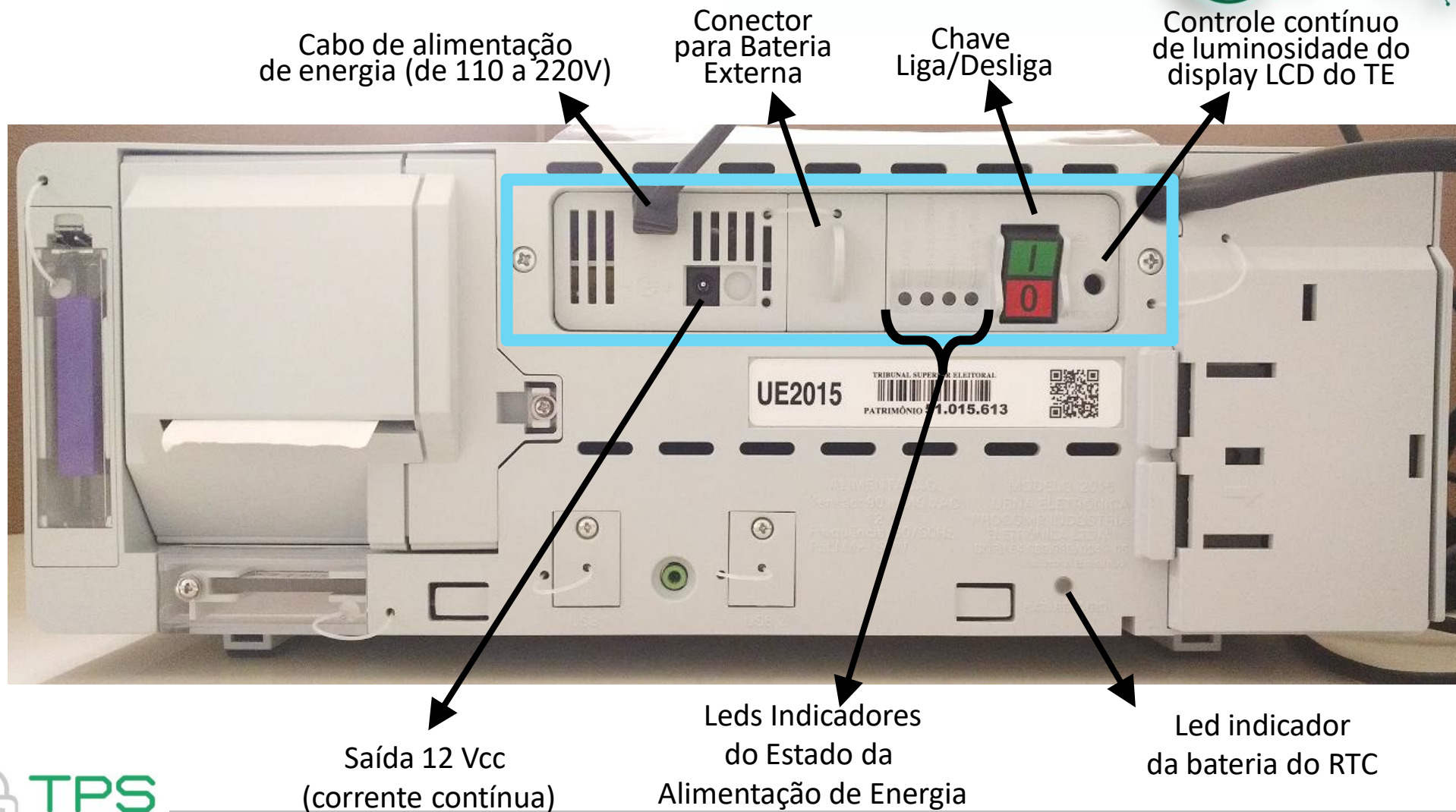
Módulo Impressor



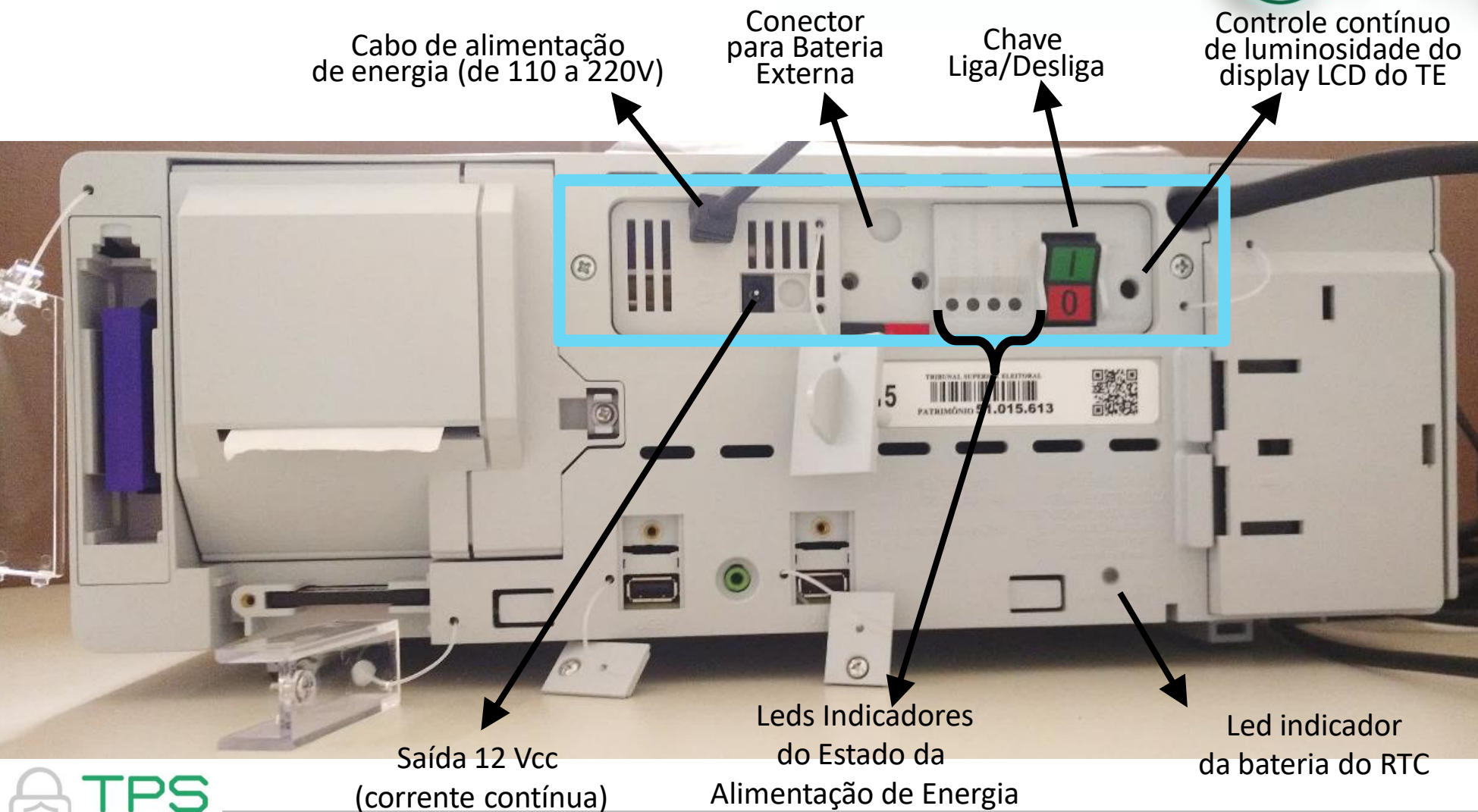
Bateria Interna



Fonte de Alimentação de Energia



Fonte de Alimentação de Energia



Fonte de Alimentação de Energia



Leds indicadores do TE

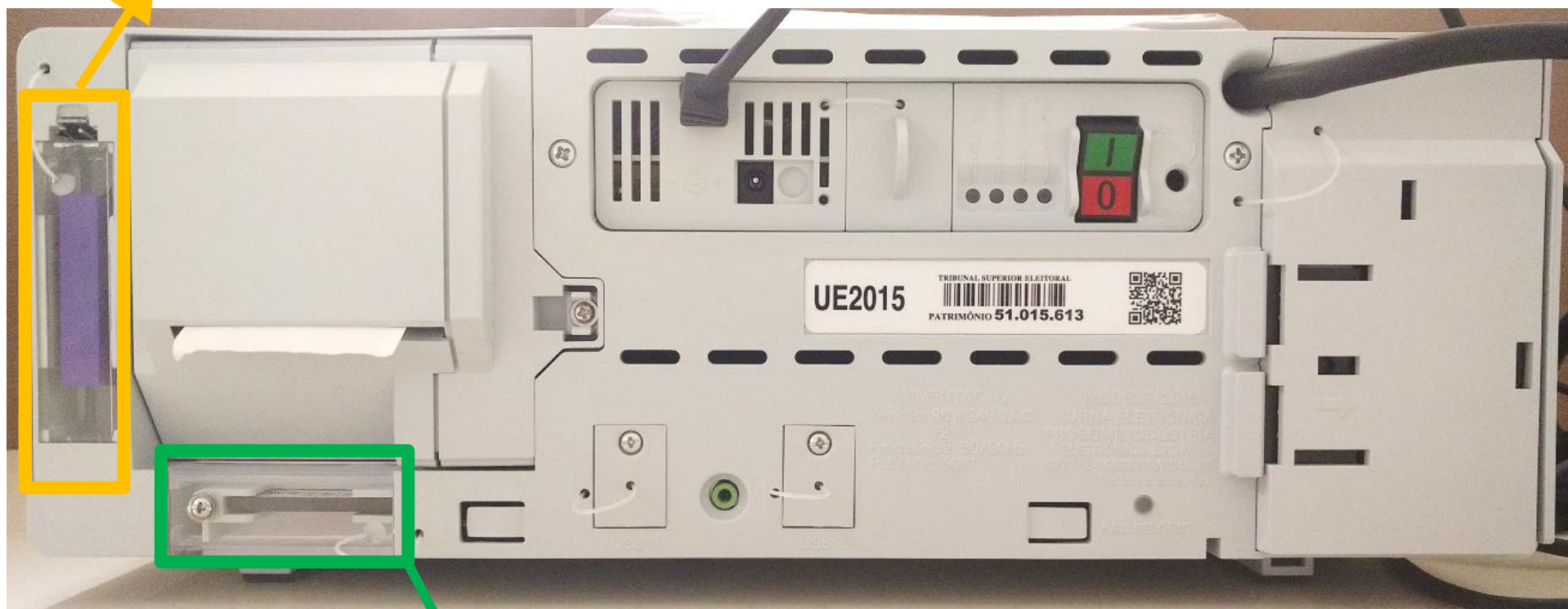


	Quando aceso
REDE AC	A urna está alimentada pela rede elétrica
BAT. EXTERNA	A urna está alimentada pela bateria externa
BAT. TOTAL	A bateria interna está plenamente carregada
BAT. CRÍTICO	A bateria interna está com carga em nível crítico

Armazenamento de dados



Memória de Resultado - MR

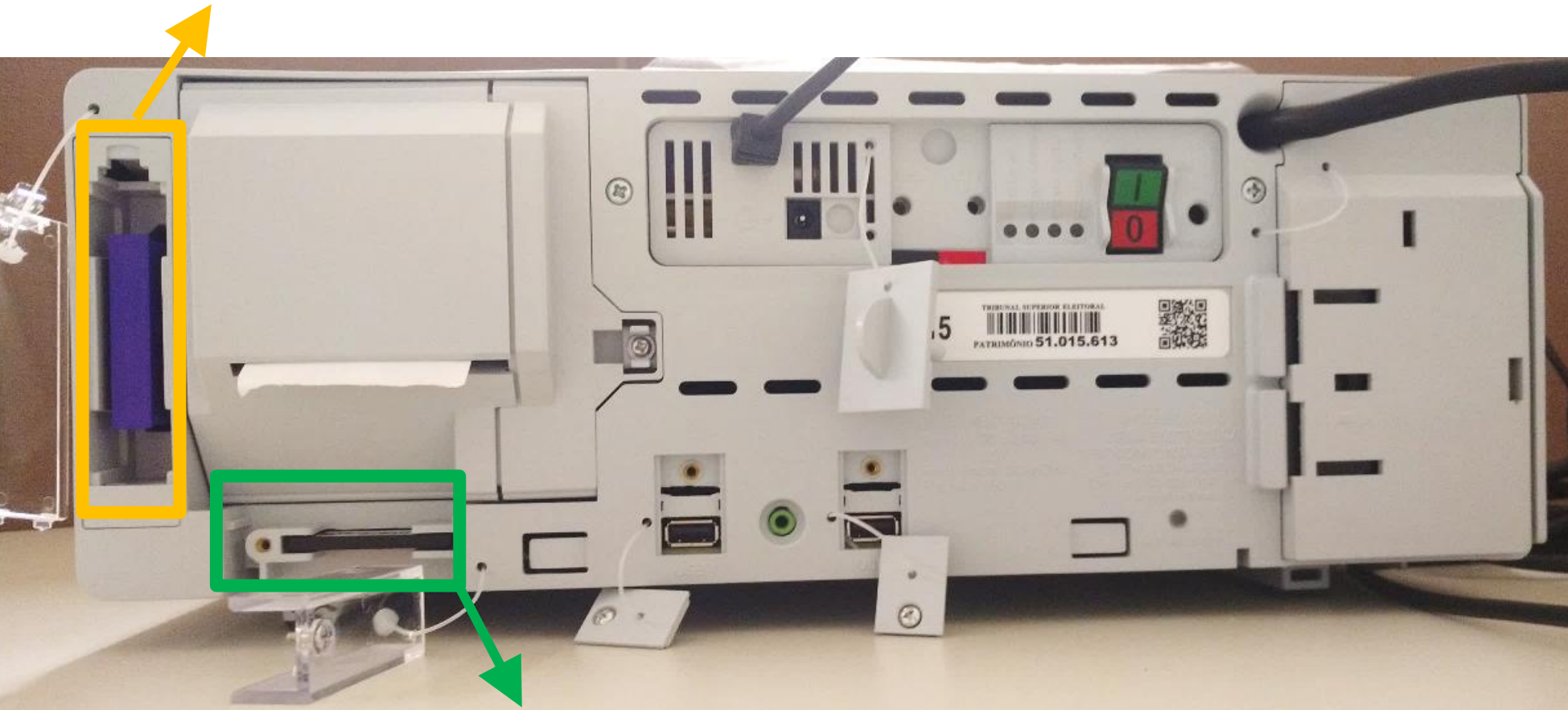


Flash Externa - FE

Armazenamento de dados

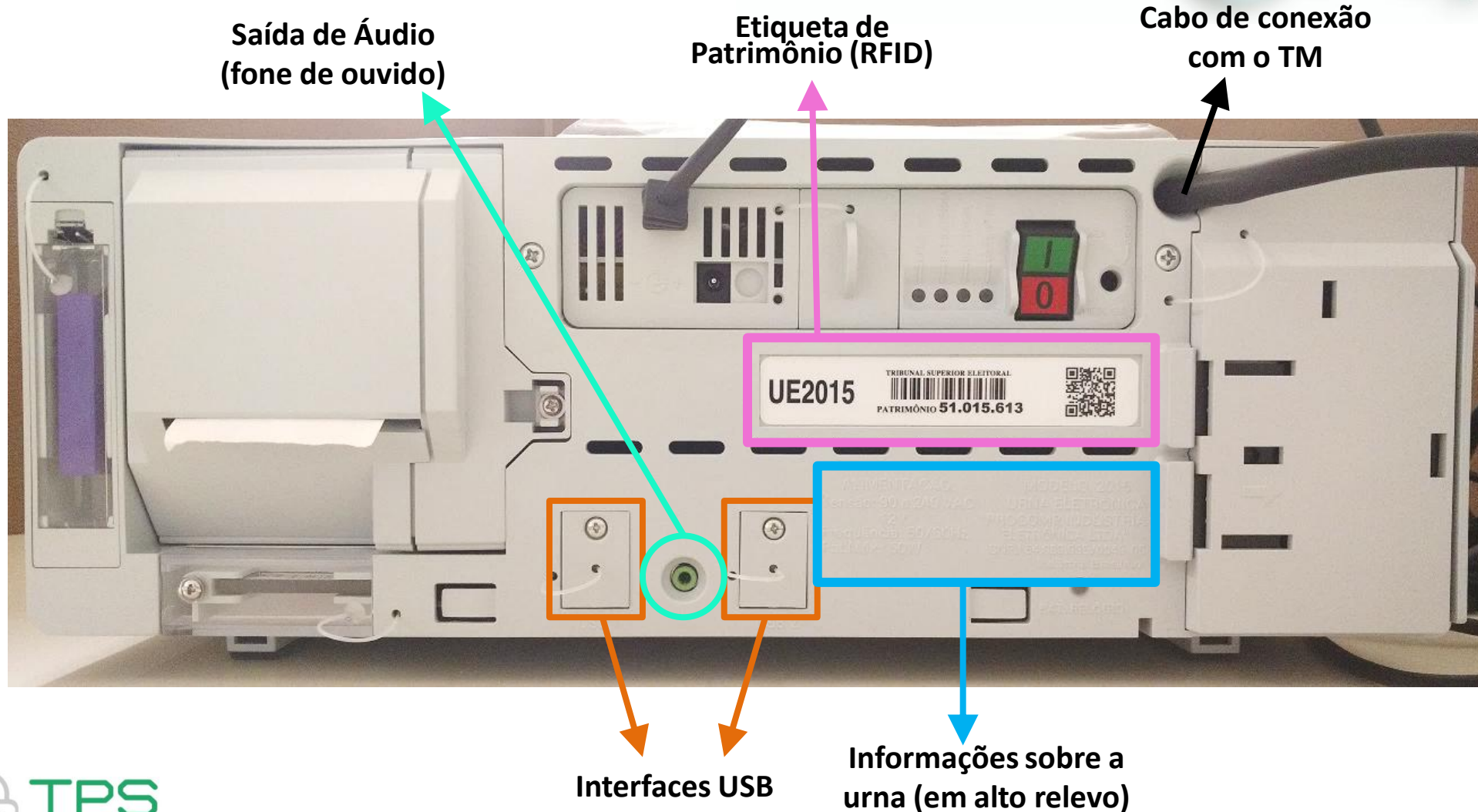


Memória de Resultado - MR



Flash Externa - FE

Interfaces e outros artefatos



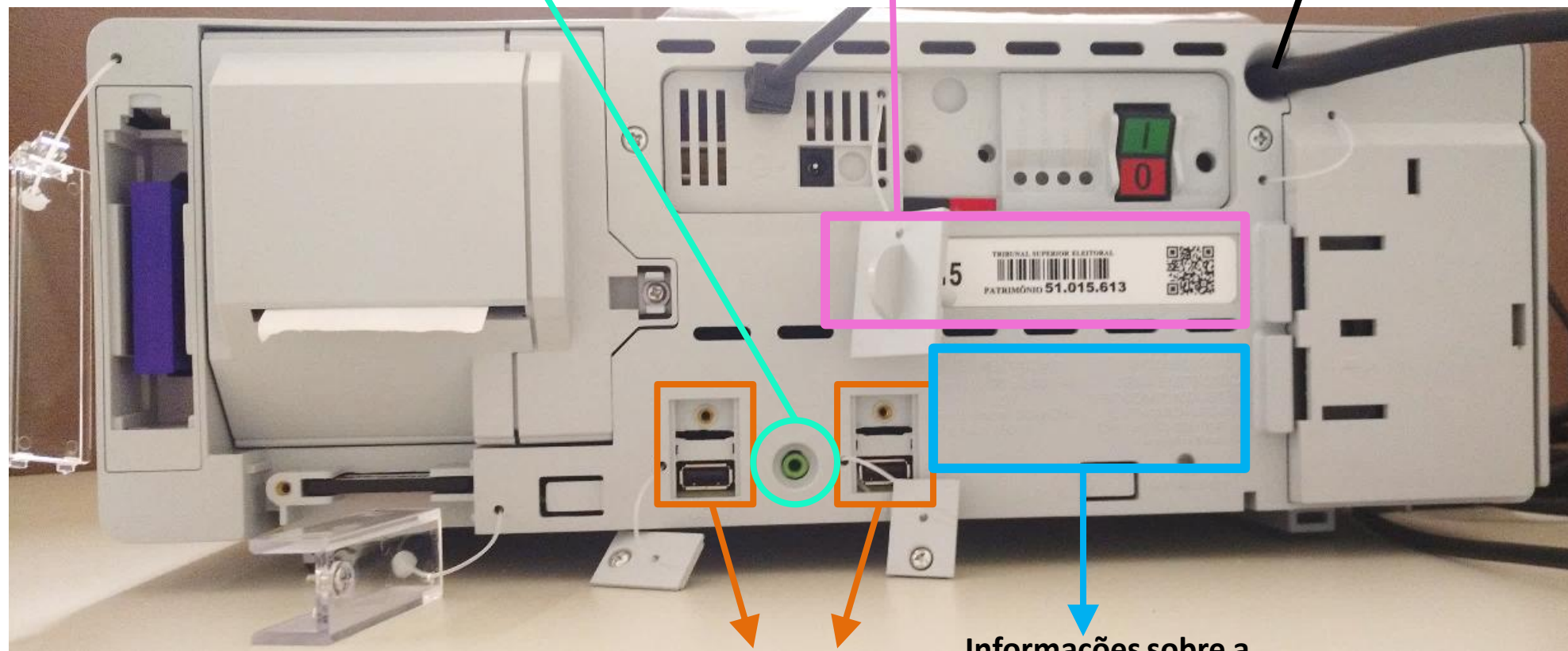
Interfaces e outros artefatos



Saída de Áudio
(fone de ouvido)

Etiqueta de
Patrimônio (RFID)

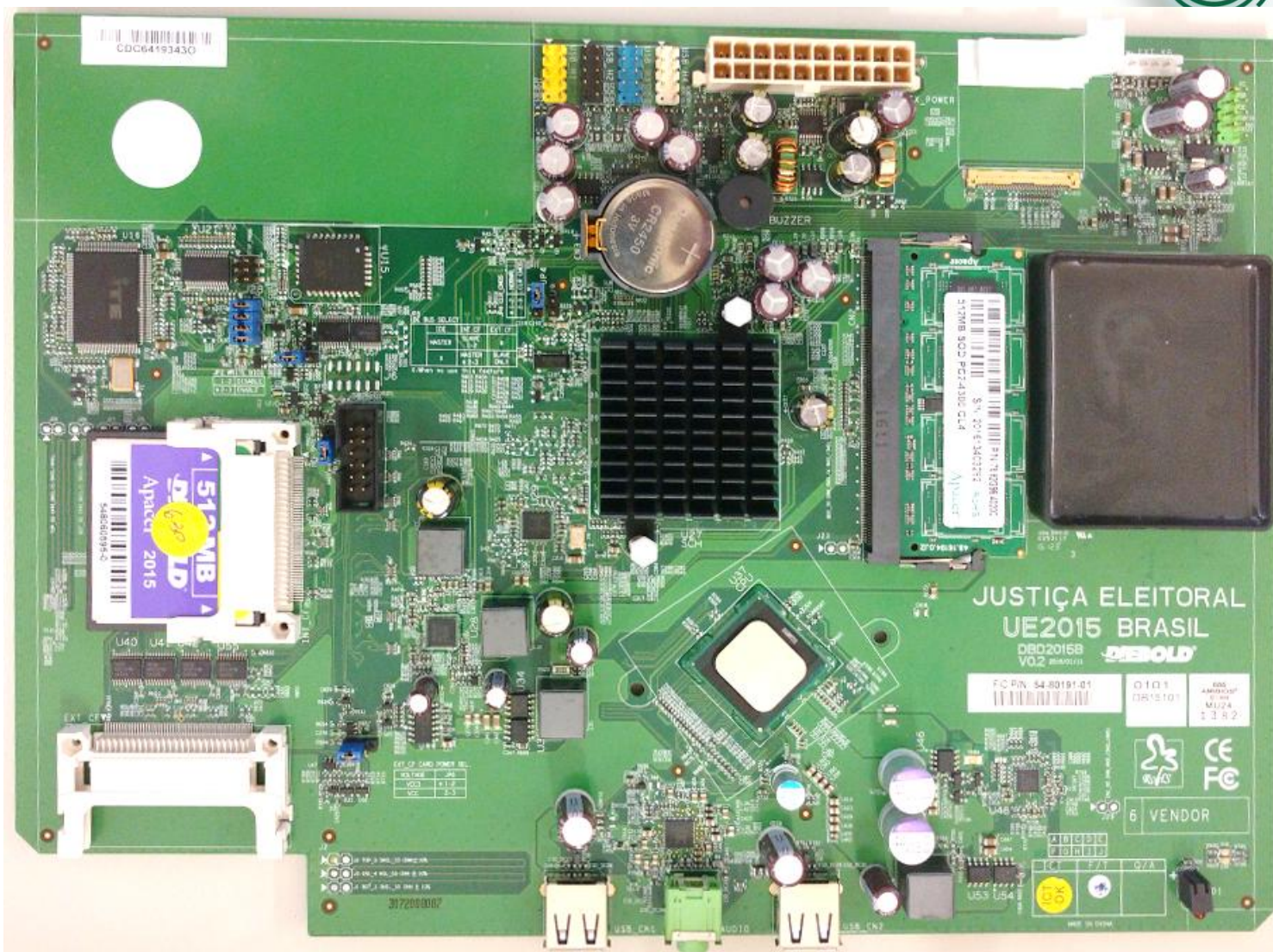
Cabo de conexão
com o TM



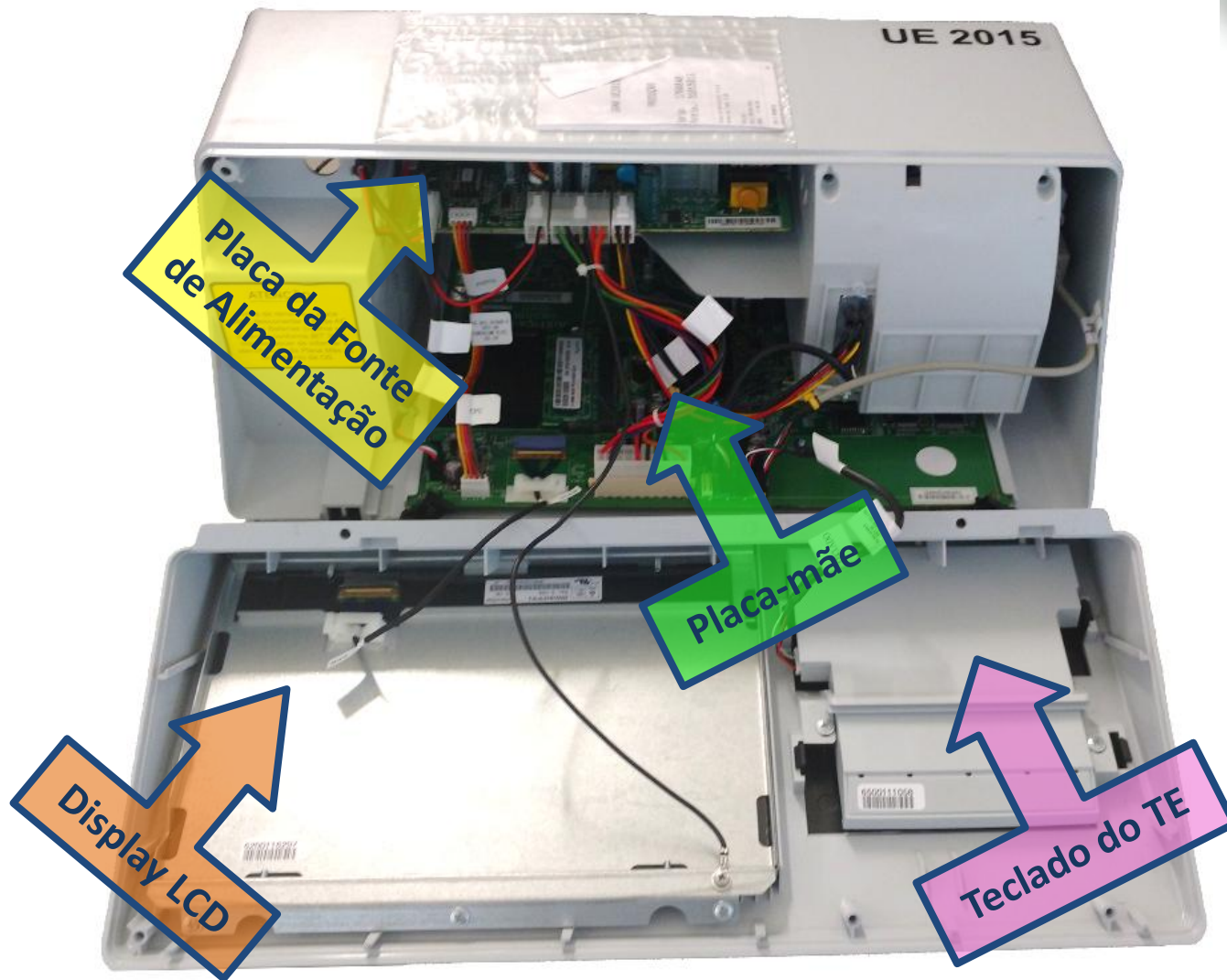
Interfaces USB

Informações sobre a
urna (em alto relevo)

Placa-mãe da UE2015



Acesso à placa-mãe



CDC64193430

512MB
Apacer 2015

512MB 90D PC7-430C CL4
Apacer

JUSTIÇA ELEITORAL
UE2015 BRASIL

DBD2015B
V0.2

DEBOLD

F0 PIN 54-80191-01

0101
08/15/10

EOS
AM9000P
M1/24
1382



6 VENDOR

LOC	F/I	C/A
101		

MADE IN CHINA

CDC64193430

MR
Teclado do TE
MI

Fonte de Energia

Fonte Dados

HUB do TM

Interface LVDS
Display do TE

Apaga
parâmetros do
BIOS - CMOS

Bateria
CMOS
RTC

Buzzer

Super
I/O

BIOS
(Flash)

Proteção contra
escrita do BIOS

Chipset

RAM

Dispositivo
Microcontrolado de
Segurança - ARM7
(Perímetro
Criptográfico)

Flash Interna - FI
CompactFlash
512 MB

CPU Intel
Atom
Z510P
1.10GHz

Flash Externa - FE
CompactFlash
512 MB

JUSTIÇA ELEITORAL
UE2015 BRASIL

DBD2015B
V0.2

0101
08/10/11

EOS
AM00000P
M1/24
1382

FIC PIN: 54-80191-01

CE
FC

6 VENDOR

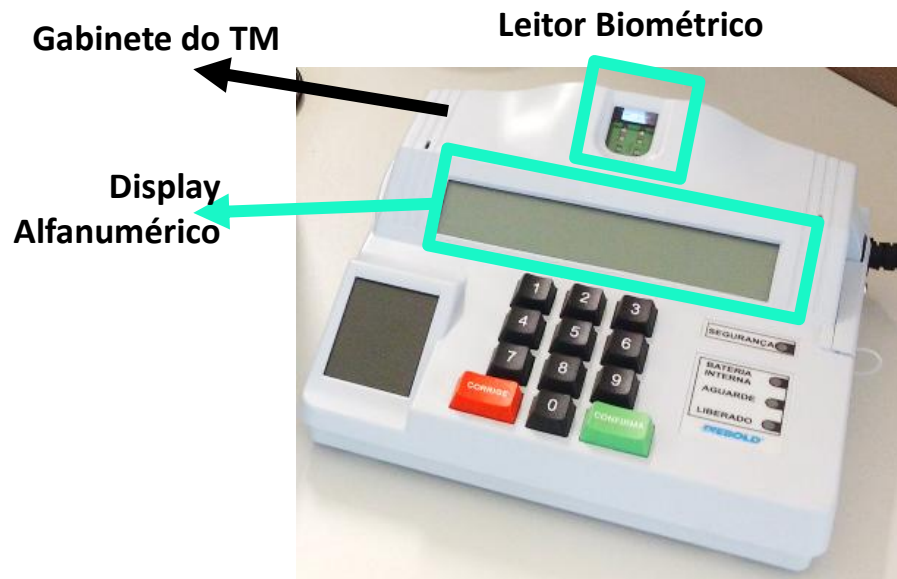
USB1

Áudio

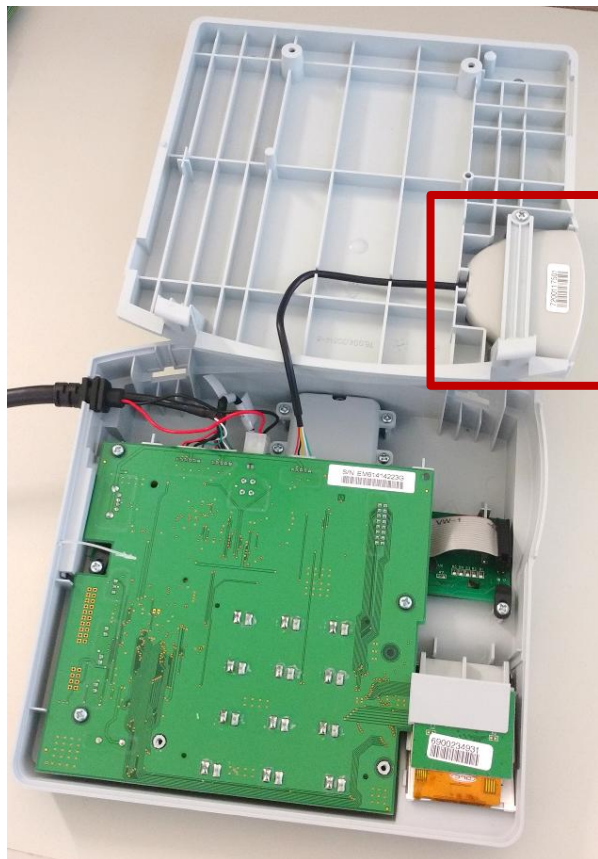
USB2



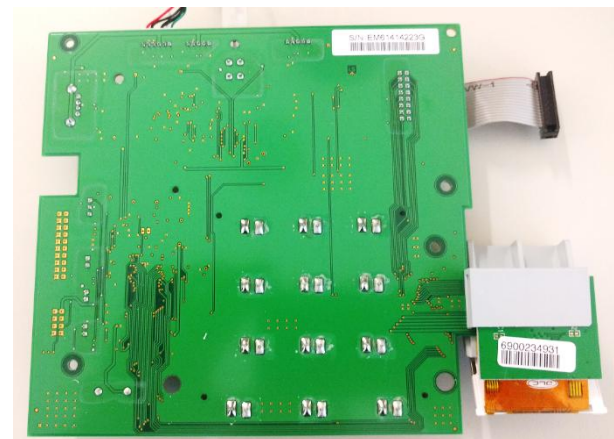
Terminal do Mesário – TM

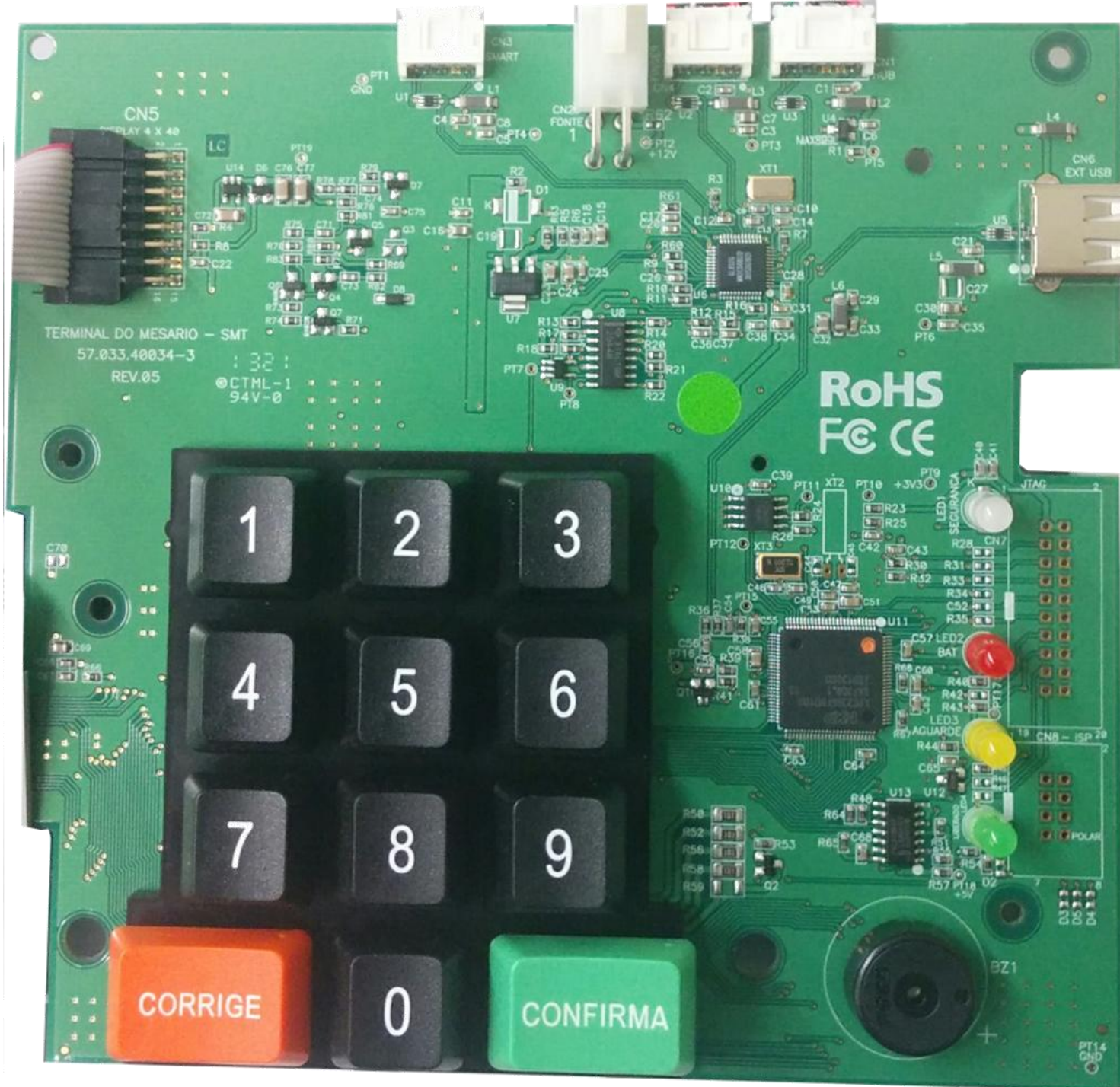


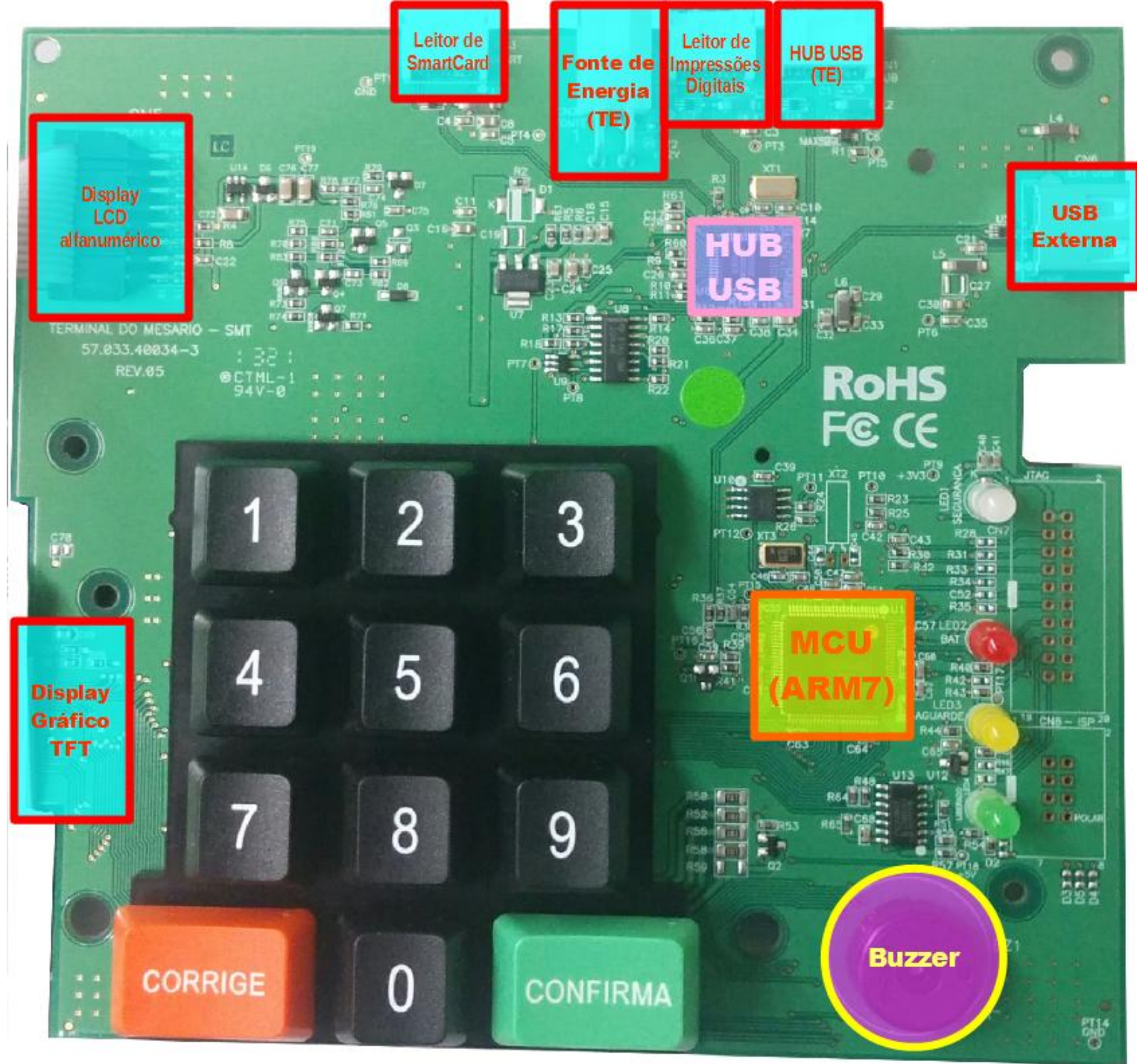
Terminal do Mesário – TM



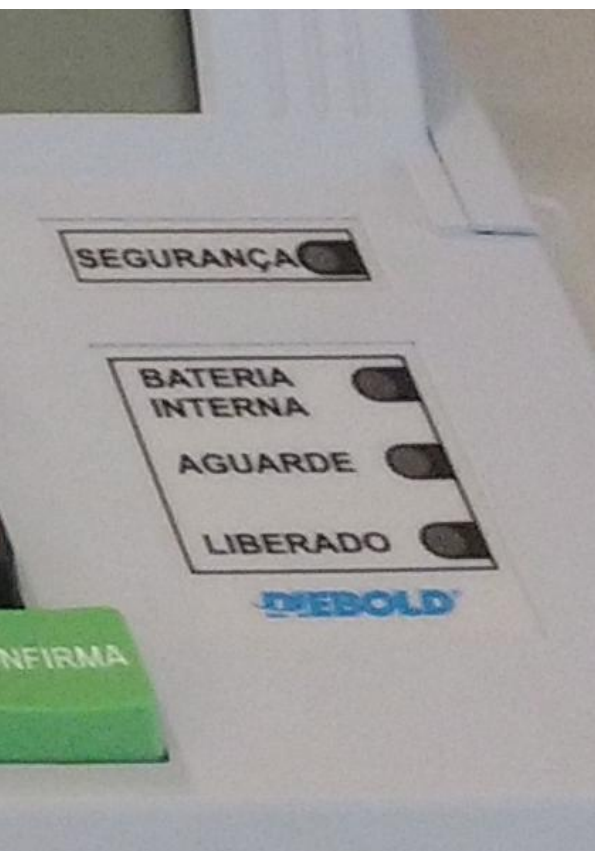
Leitor de
SmartCard







Leds Indicadores do TM



	Quando aceso	
SEGURANÇA	<i>Amarelo piscando</i>	autenticação em processamento
	<i>Vermelho</i>	o processo de autenticação foi finalizado com sucesso e com chave diferente da chave oficial do TSE
	<i>Vermelho piscando</i>	existiu uma falha no processo de autenticação
	<i>Verde</i>	o processo de autenticação foi finalizado com sucesso e com a chave oficial do TSE
BATERIA INTERNA	A urna está alimentada pela bateria interna ou externa (indica falta de energia elétrica)	
AGUARDE	A votação está em curso	
LIBERADO	A votação terminou e a urna está liberada para uma nova votação	