TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

TESTES PÚBLICOS DE SEGURANÇA

DO SISTEMA ELETRÔNICO DE VOTAÇÃO

Aspectos Técnicos da Segurança do Sistema Eletrônico de Votação

20, 21 e 22
MARÇO 2012

Rafael Azevedo
Coordenador de Logística - STI/TSE

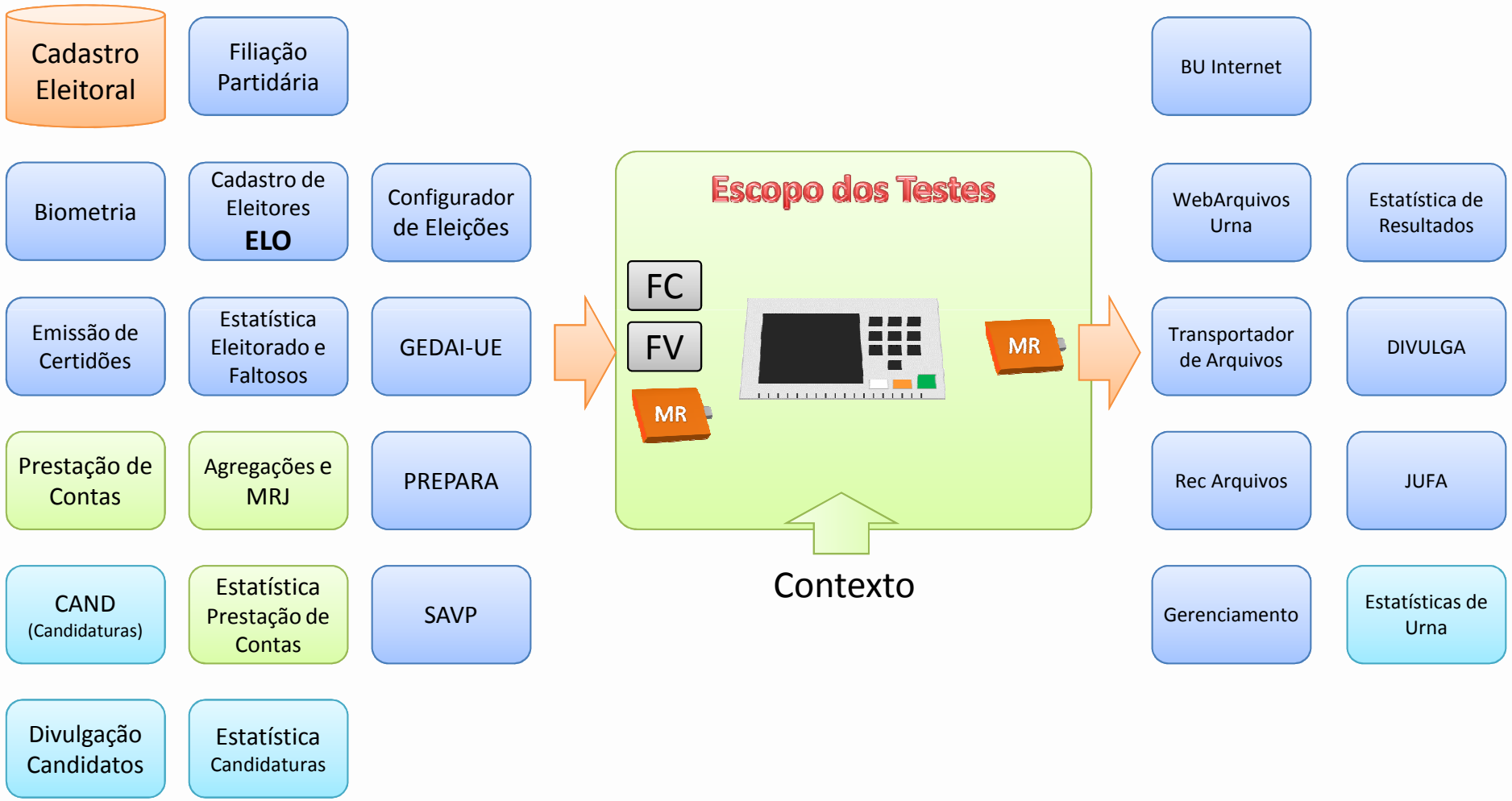
Objetivos

- Oferecer o entendimento básico do Processo Eletrônico de Votação;
- Prover melhor acesso às informações para:
  - Auxiliar na preparação e planejamento do Plano de Testes;
  - Escolha de ferramentas;

Agenda

- Visão Geral dos Sistemas
- O Hardware da Urna Eletrônica
- Mídias, Preparação e Votação
- Software, Sistema Operacional e Arquitetura
- Cadeia de Confiança em Hardware
- Perguntas.

Visão Geral do Processo Eletrônico de Votação



TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

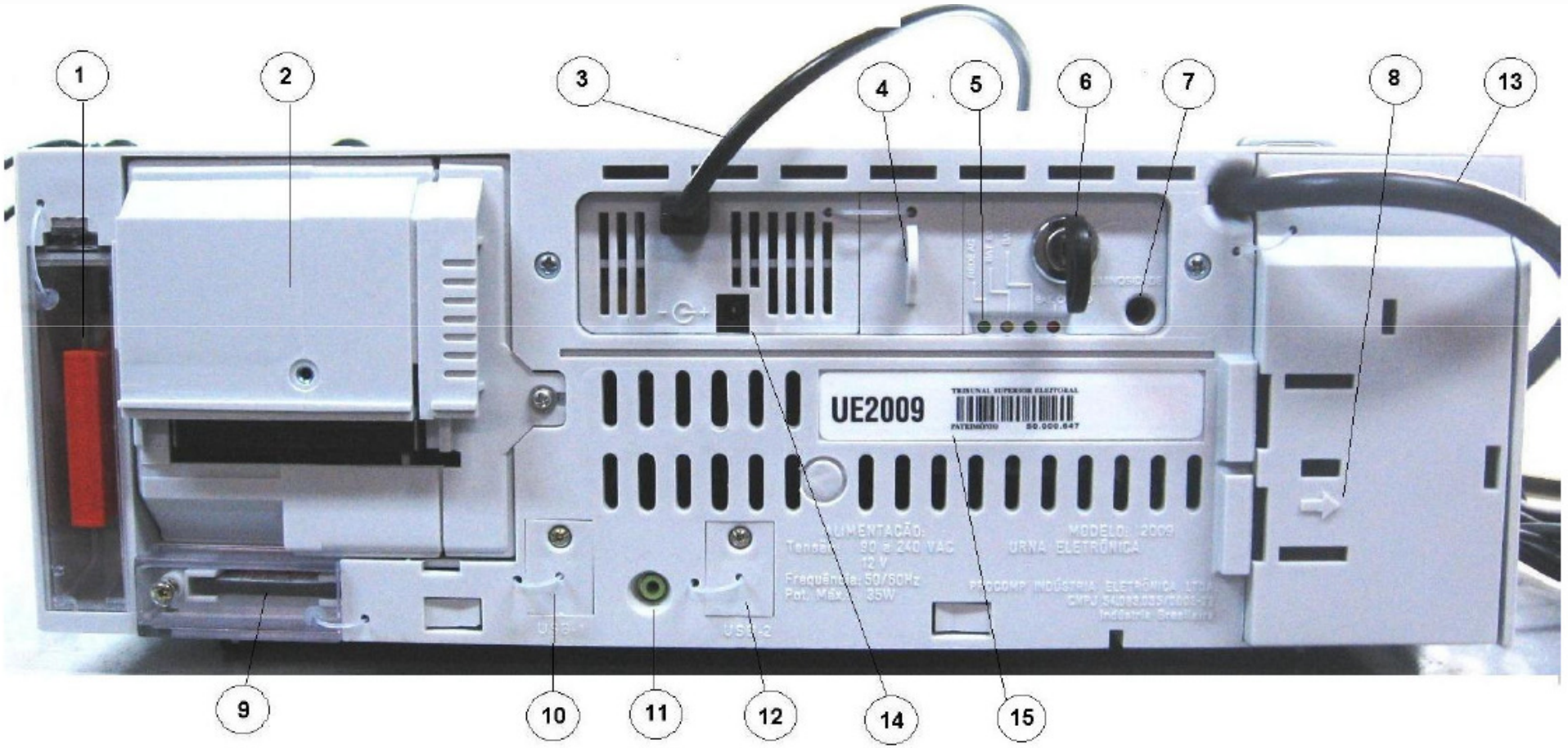
HARDWARE

A Urna Eletrônica

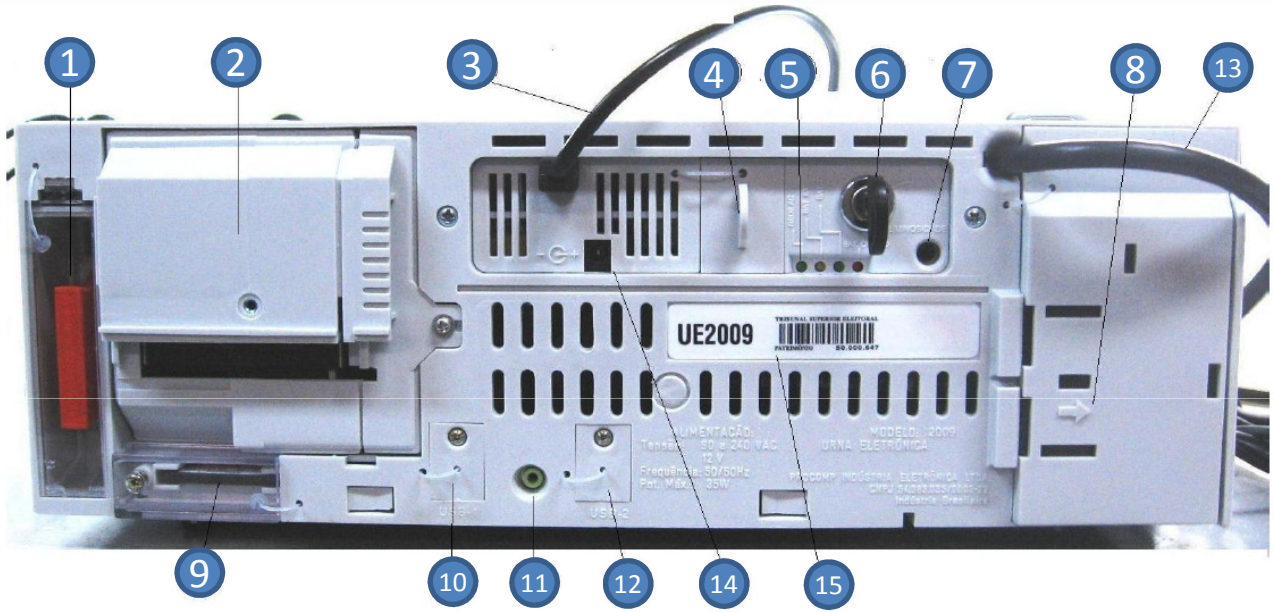
TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

UE2009



UE2009

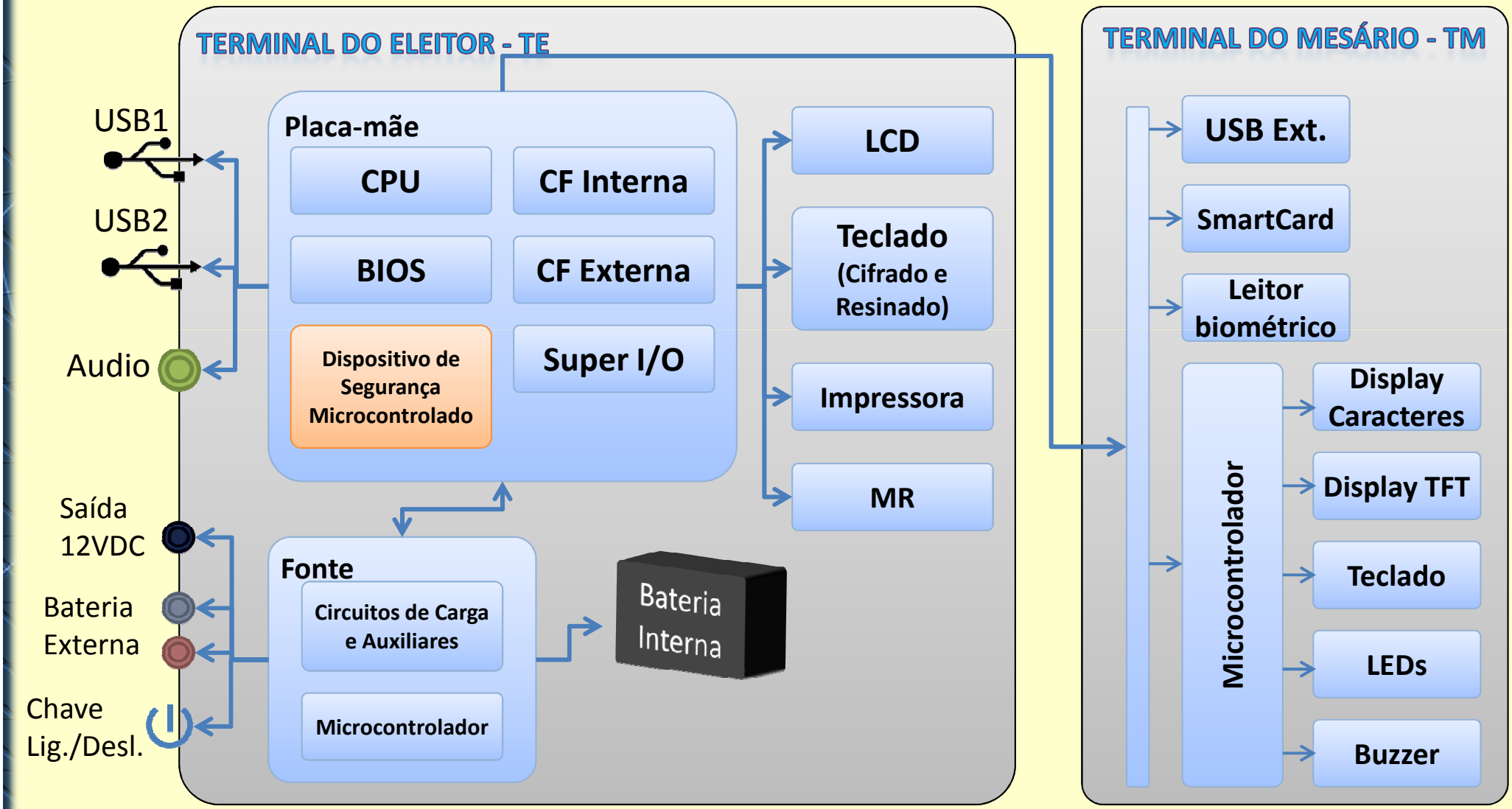


1. Memória de Resultado
2. Impressora
3. Cabo AC
4. Bateria Externa (IN)
5. Leds AC, etc.
6. Chave Liga/Desliga
7. Controle Luminosidade
8. Bateria Interna
9. CompactFlash Externa
10. USB1
11. Audio
12. USB2
13. Cabo AC
14. Saída DC
15. Patrimônio RFID

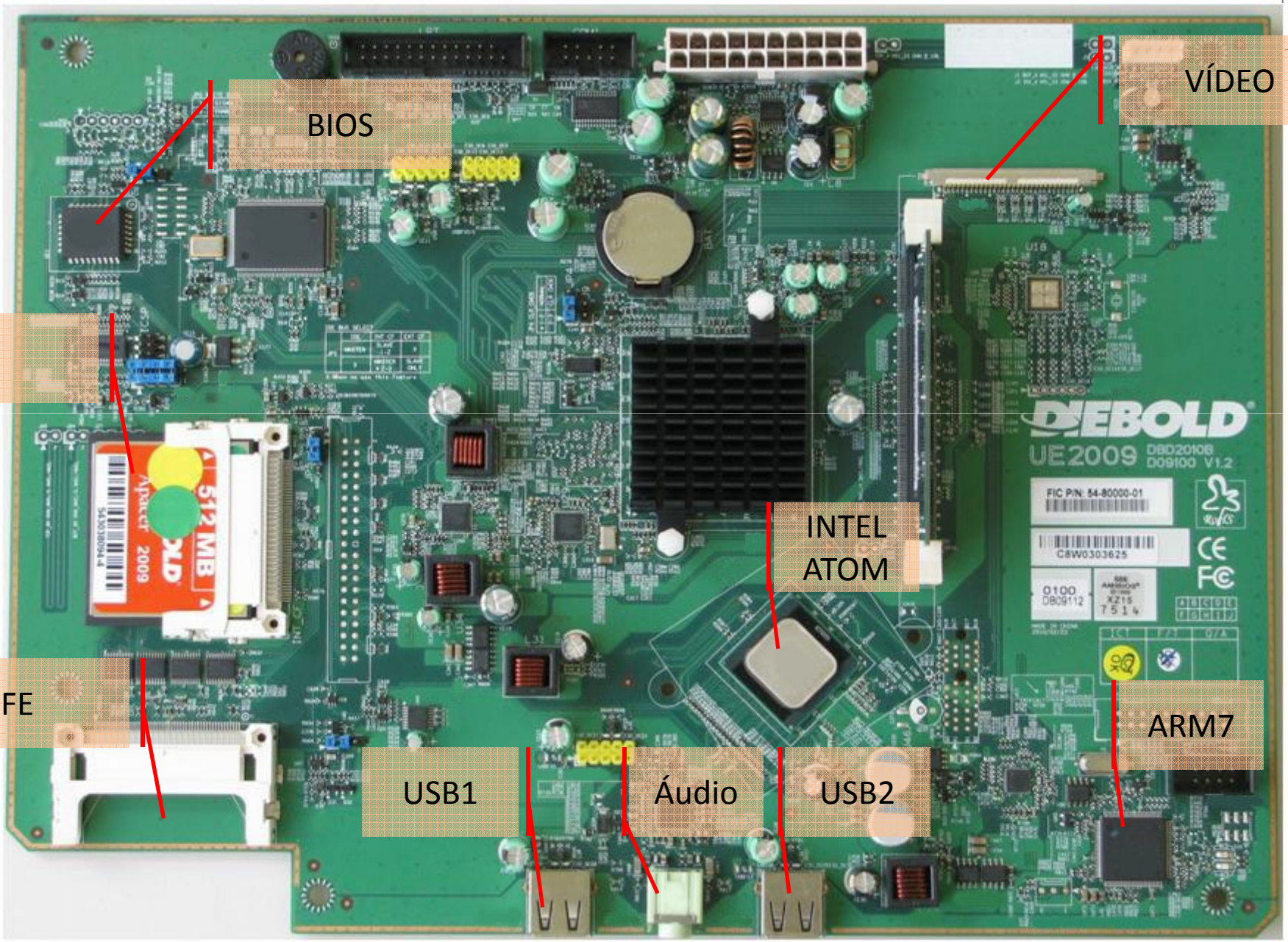
UE2009 - Especificações

• Placa mãe	Proprietária;
• CPU	Intel® Atom™ Z510P 1.10Ghz
• Fonte	Inteligente (proprietária)
• LCD	Policromático 10.1” Wide;
• Bateria	7,0Ah;
• CompactFlashs	Apacer 512Mb;
• Impressora	Térmica (proprietária).

Arquitetura de Hardware



Placa-mãe


BIOS
VÍDEO
FI
INTEL
ATOM
FE
ARM7
USB1
Áudio
USB2
DIEBOLD
UE2009

TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

MÍDIAS, PREPARAÇÃO E VOTAÇÃO

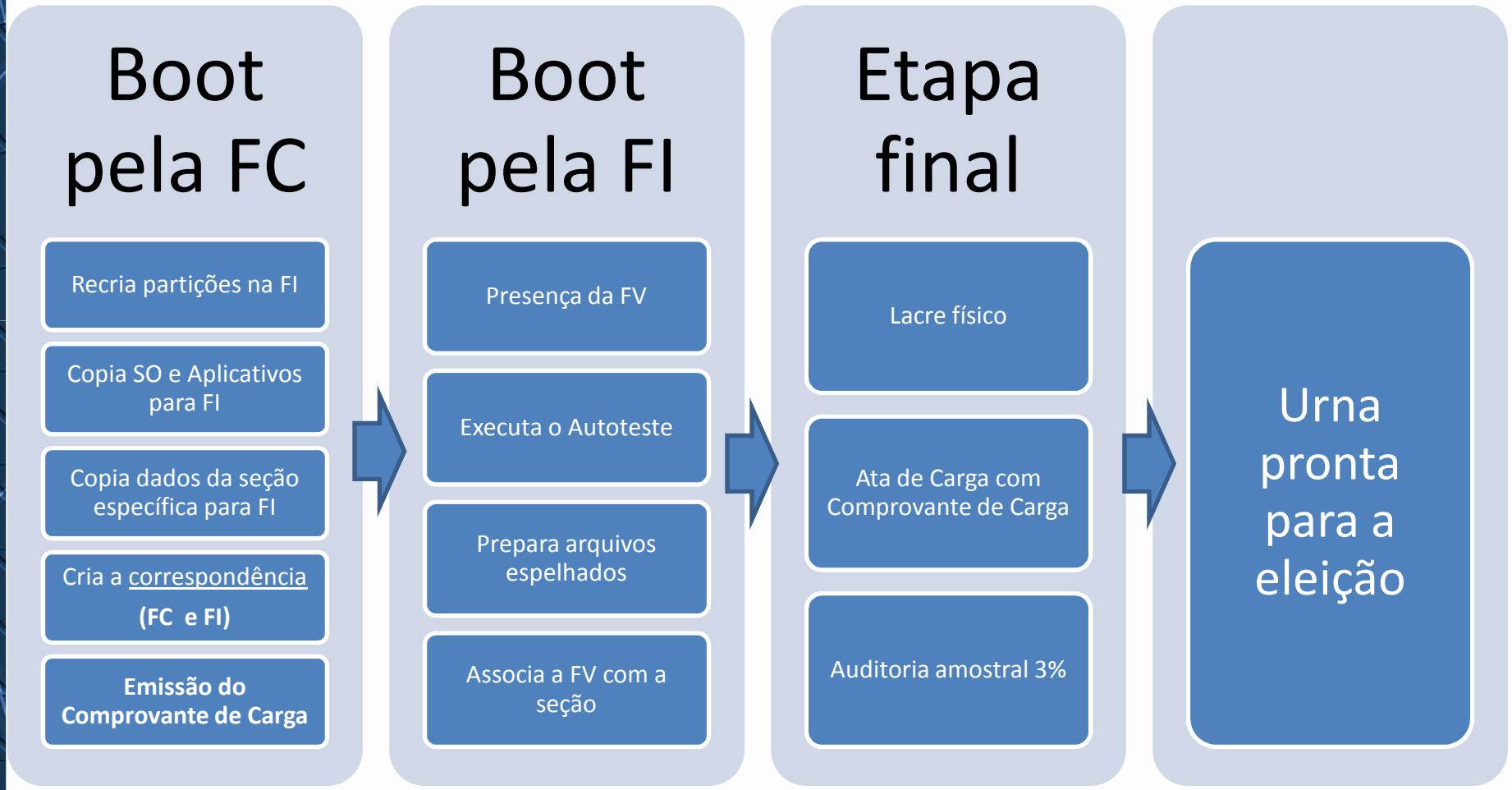
Flash Cards (Compactflashs)

- FI – Flash Interna (Equivalente a ***C:***);
  - Setor de Boot*;
  - Sistema Operacional;
  - Aplicativos;
  - Dados.

Prioridade de Boot é pela FC e depois pela FI

- FE – Flash Externa (Equivalente a ***D:***);
  - FV – Flash de Votação;
    - Dados Espelhados;
    - Fotos*.
  - FC – Flash de Carga
    - Setor de Boot*;
    - Sistema Operacional;
    - Software de Carga;
    - “Pacotes” de Instalação;
    - Dados de várias seções.

Como uma urna é preparada?



No dia da votação

Início da Votação

- Zerésima a partir das 7h
- Aguarda 8h
- Urna abre para o primeiro eleitor

Votação

- Votação do 1º eleitor
- Votação do 2º eleitor
- ...

Encerramento

- Aguarda 17h*
- Insere código de encerramento
- Emissão das 5 vias Obrigatórias
- Gravação da MR
- Emissão das Adicionais (até 15 vias)

TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

SOFTWARE

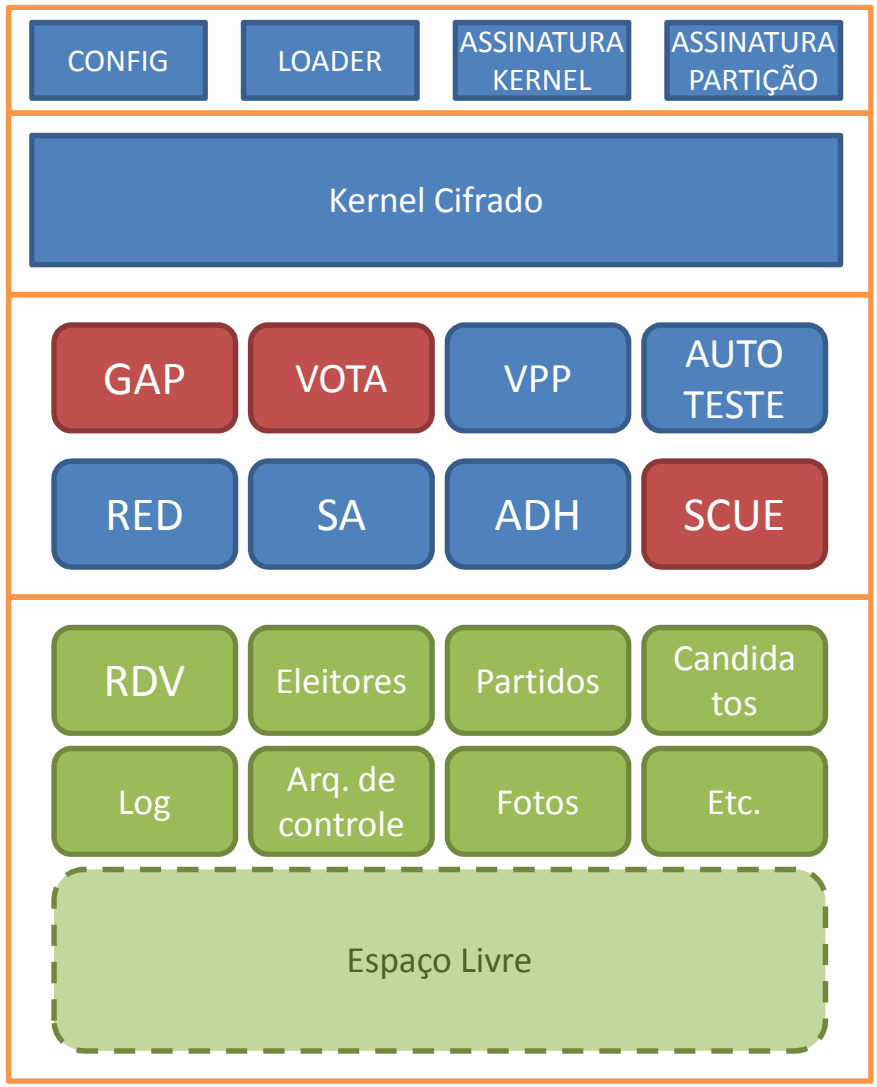
Sistema Operacional

- UENUX – “Distribuição” montada pelo TSE exclusivamente para as urnas
  - Kernel Linux 2.6.16.62
    - Suporte a UEMINIX para partição cifrada;
    - ELFLoader específico;
  - Bibliotecas GNU
    - GNU libc 2.9 – Biblioteca C
    - GNU libm 2.9 - Biblioteca de funções matematicas.
    - GNU libstdc++ 6.0.8 – Biblioteca C++
    - GNU libpthreads 2.9
  - LibSDL 1.2.11 – Biblioteca gráfica
    - SDL_image - 1.2.5
    - SDL_ttf - 2.0.8
    - SDL sobre framebuffer com acesso direto
  - Zlib – 1.2.3 - Compactação
  - LibJPEG - 6b – Formato JPEG
  - Salsa - 0.0.6 – Áudio
  - Freetype - 2.3.4 – Texto

Partições

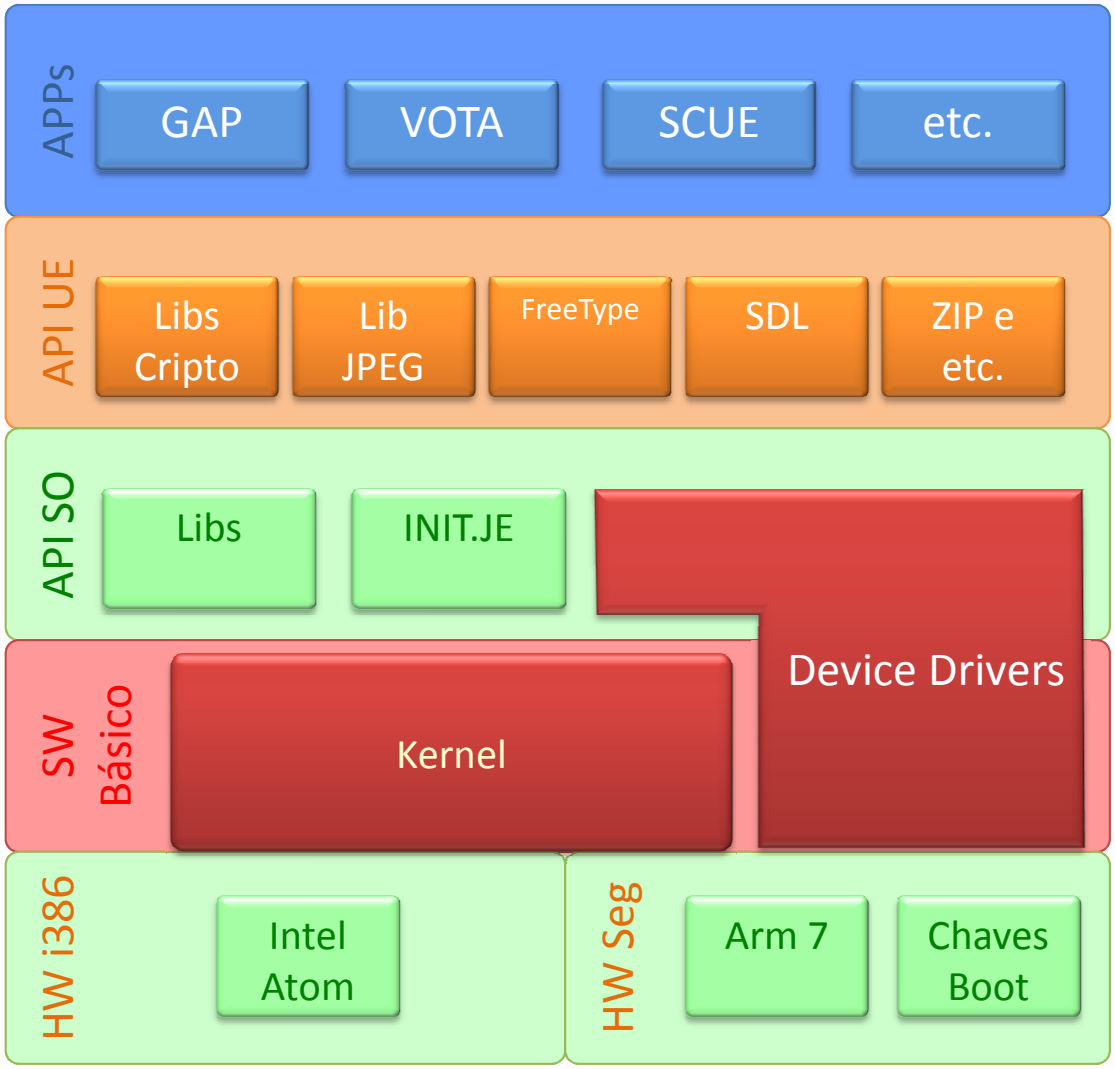
- As Flashs Interna e de Carga são divididas em 4 partições
- A Flash de Votação tem somente a partição UEMINIX cifrada.

Partições FI e FC



MODO	TIPO	Tamanho
Read Only	FAT	1 cluster
Read Only	MINIX	1Mb
Read Only	UEMINIX cifrada	18Mb
Read/Write	UEMINIX cifrada	Restante

Arquitetura de Software

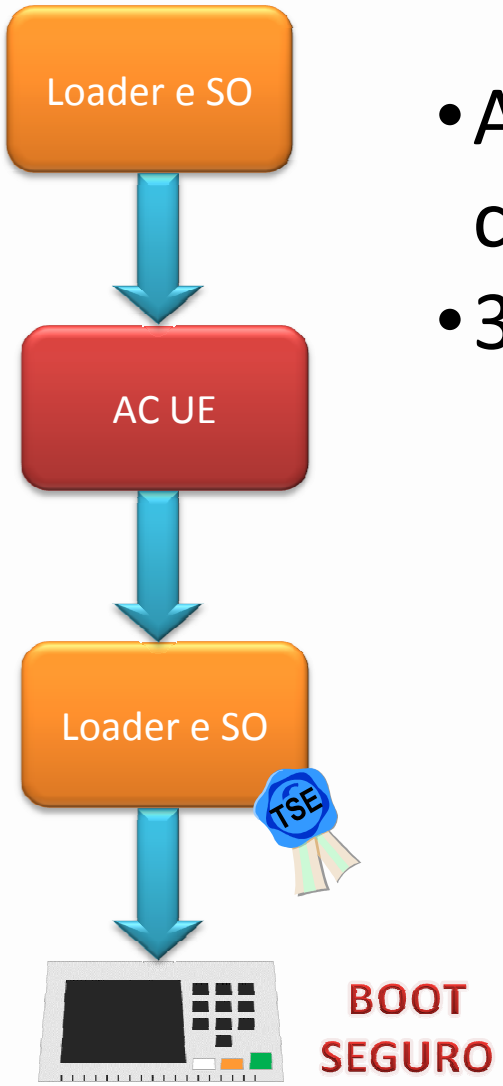


TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

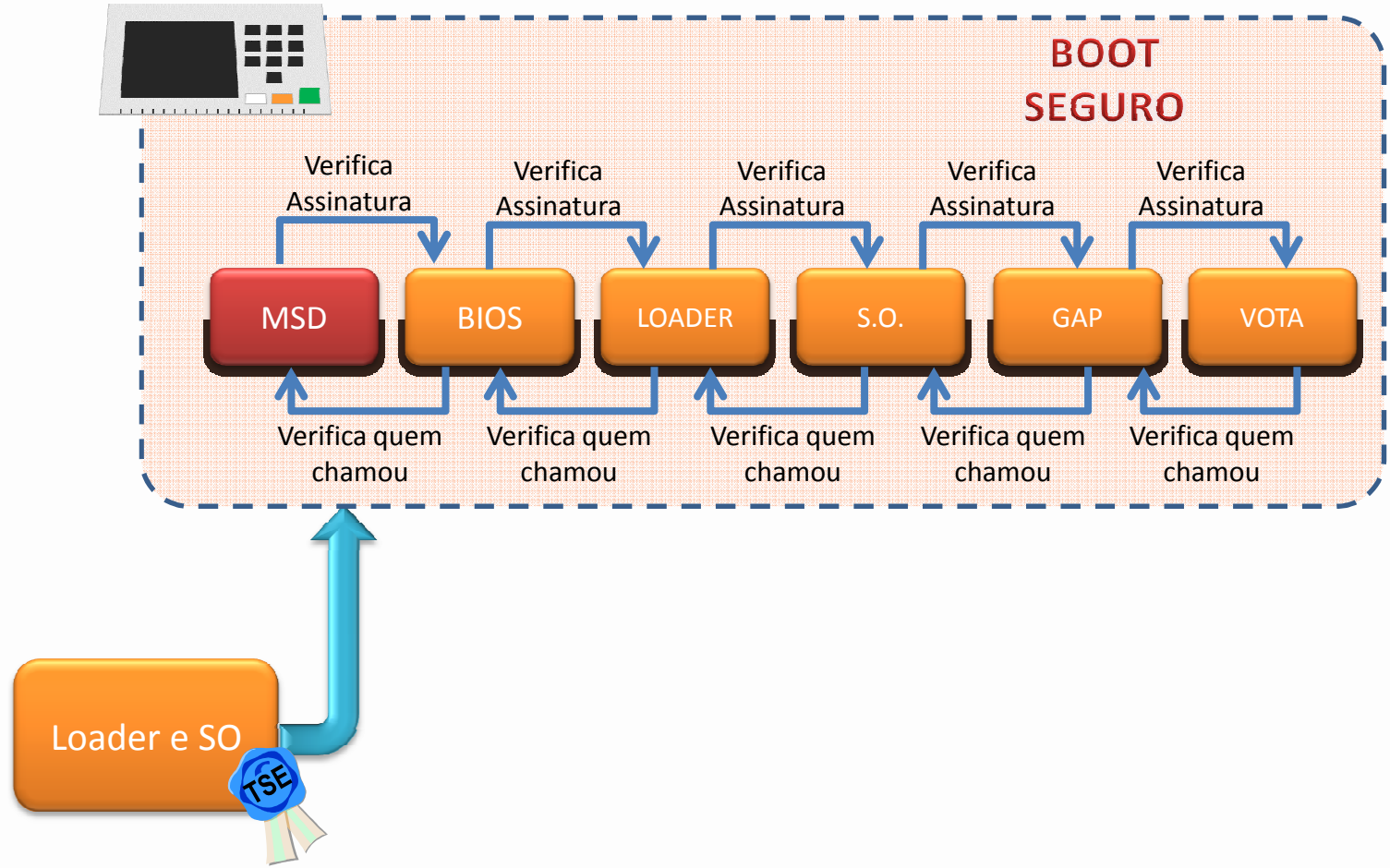
CADEIA DE CONFIANÇA EM HARDWARE

Boot Seguro



- Autenticação do SO e Loader com criptografia embarcada;
- 3 perfis de assinatura:
  - Oficial;
  - Simulado;
  - Desenvolvimento.

Cadeia de Confiança

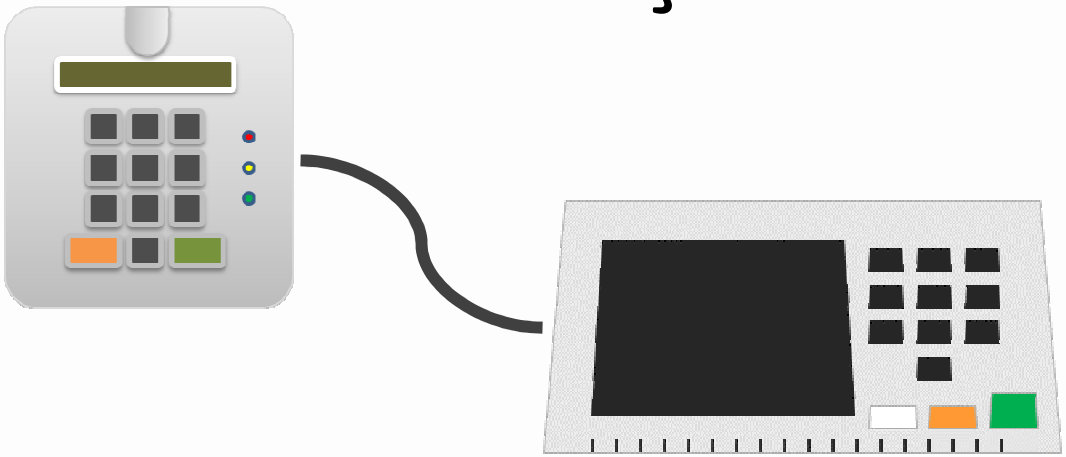


TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL

HABILITAÇÃO DO ELEITOR E RDV

Habilitação do Eleitor e RDV

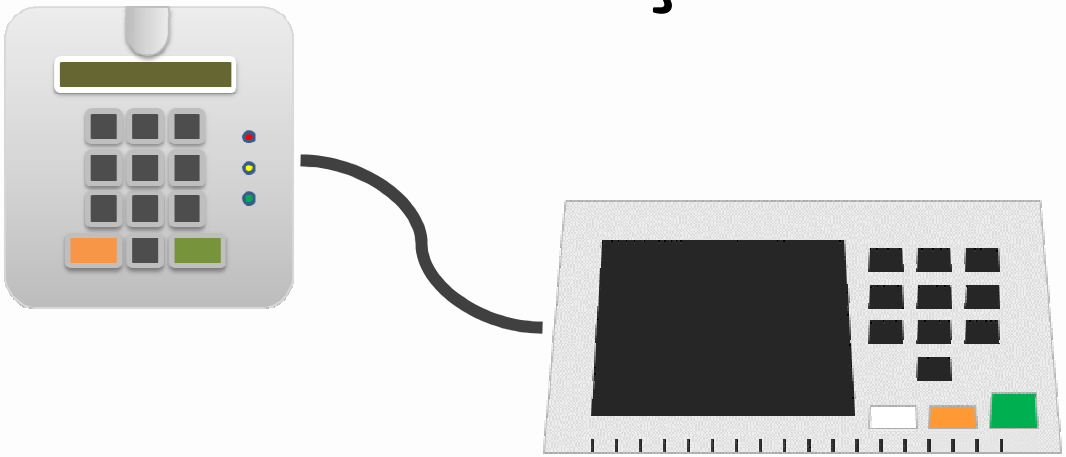


Exemplo:
5 eleitores aptos
3 compareceram

Eleitor	Votou?
Eleitor 1	
Eleitor 2	
Eleitor 3	
Eleitor 4	
Eleitor 5	

Vereador	Tipo	Prefeito	Tipo

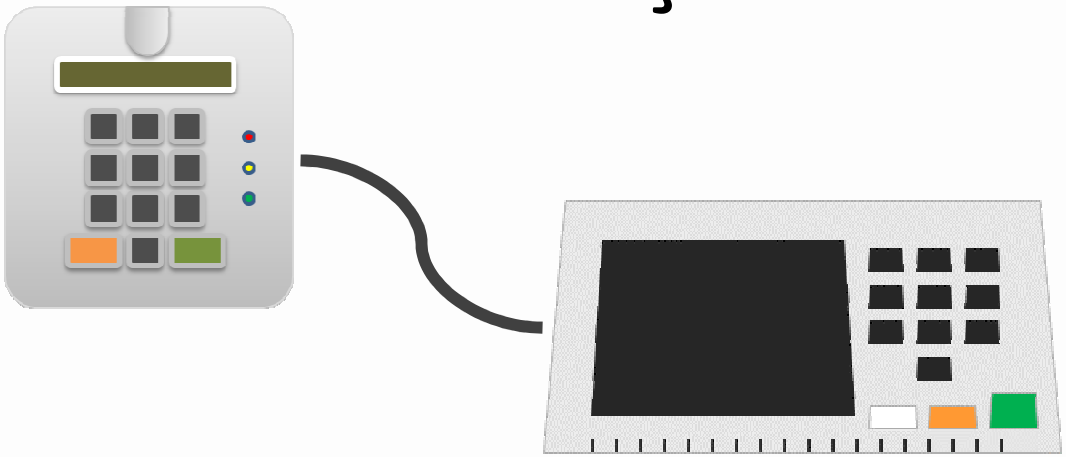
Habilitação do Eleitor e RDV



Eleitor	Votou?
Eleitor 1	✓
Eleitor 2	
Eleitor 3	
Eleitor 4	✓
Eleitor 5	✓

Vereador	Tipo	Prefeito	Tipo
<Branco>	Branco	92	Nominal
90123	Nominal	91	Nominal
92	Legenda		
		99	Nulo

Habilitação do Eleitor e RDV



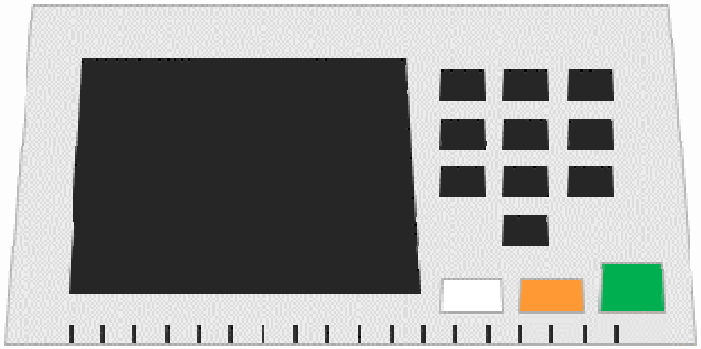
NÃO EXISTE INFORMAÇÃO ALGUMA SOBRE O ELEITOR E SEU RESPECTIVO VOTO

Eleitor	Votou?
Eleitor 1	✓
Eleitor 2	
Eleitor 3	
Eleitor 4	✓
Eleitor 5	✓

?

Vereador	Tipo	Prefeito	Tipo
<Branco>	Branco	92	Nominal
90123	Nominal	91	Nominal
92	Legenda		
		99	Nulo

Arquivos de Saída

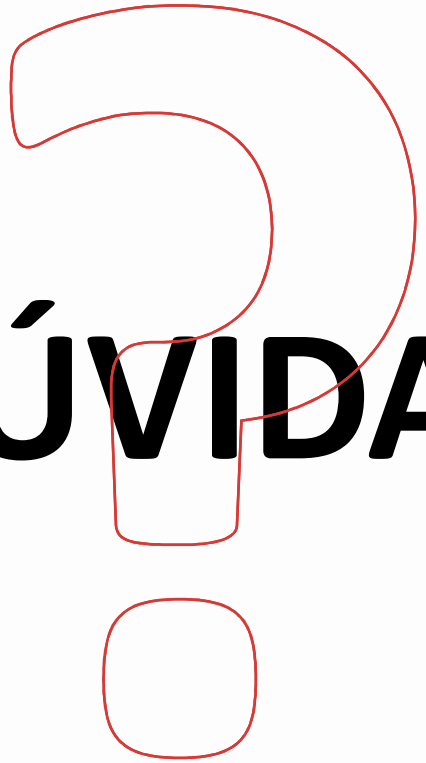


MR

- Boletim de Urna
- Registro Digital do Voto - RDV
- Faltosos
- Justificativa
- Log
- Imagem do BU

TESTES PÚBLICOS DE SEGURANÇA DO SISTEMA ELETRÔNICO DE VOTAÇÃO ELEIÇÕES 2012

TRIBUNAL SUPERIOR ELEITORAL



DÚVIDAS?