TRIBUNAL SUPERIOR ELEITORAL - TSE
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - STI
COORDENADORIA DE LOGÍSTICA

PB – PROJETO BÁSICO

AQUISIÇÃO DE URNAS ELETRÔNICAS – UE2009

Anexo VI - Software Básico, Segurança e Criptografia

ÍNDICE

1 INTRODUÇÃO

Para garantir a total integração entre o software e o hardware, o TSE fornecerá um aplicativo para ser executado na urna eletrônica que deverá ser utilizado para verificar o correto funcionamento de todos os recursos de todos os dispositivos. Com isso, a contratada deverá fazer as adequações para que as UE2009 estejam funcionais e compatíveis com esse aplicativo.

Juntamente com o aplicativo, o TSE deverá informar a versão do kernel do sistema operacional Linux que deverá ser utilizado durante o desenvolvimento, e poderá ser também disponibilizado o binário do kernel correspondente que for configurado para os outros modelos de urna eletrônica e que estiver sendo utilizado.

A Contratada deverá efetuar as adequações necessárias somente nos *drivers* de dispositivos da UE2009, e quando não for possível, deverá ser justificado e negociado com os técnicos do TSE alterações também na API dos sistemas da urna eletrônica.

2 REQUISITOS GERAIS

A contratada deverá cumprir as seguintes exigências:

a) Garantir que a UE2009 seja compatível com o aplicativo fornecido pelo TSE;

b) Disponibilizar todos os códigos fontes dos *drivers* e, quando for o caso, das modificações necessárias na API, com os respectivos roteiros de compilação (descrevendo ambiente, configurações, parâmetros, procedimentos e etc.);

c) Disponibilizar os meios para o TSE recompilar os *drivers* fornecidos pela **Contratada**;

d) A Justiça Eleitoral terá os direitos de propriedade sobre todas as implementações ou customizações necessárias no software básico (*drivers* e API). A Justiça Eleitoral não será obrigada a divulgar ou ceder qualquer parte da implementação realizada mesmo que sejam adaptações ou atualizações de códigos já existentes;

e) Não utilizar tecnologia tida como obsoleta tanto pelo mercado como pelo meio acadêmico;

f) A BIOS deverá permitir a inicialização da UE através da memória "Flash" interna (FI) ou "Flash Card" de carga (FC),

g) Não gravar o *loader* do Sistema Operacional na BIOS da UE2009. A tarefa da BIOS deverá ser a de carregar e dar partida no *loader*, obedecendo às definições repassadas pelo TSE;

2.1 Controle e Monitoração de Dispositivos

O controle e a monitoração de dispositivos têm como função:

a) Controlar o funcionamento dos dispositivos de entrada e saída de dados, unidades de armazenamento de dados, fonte de alimentação (bateria interna e externa);

b) Enviar dados por meio de um *driver* para comandar a impressão de caracteres compatíveis, no mínimo, com o especificado no código de páginas, do DOS™, 437 (inglês), 860 (português) e 850 (latino), incluindo os caracteres gráficos. Pode-se utilizar o formato UTF-8, especificado no padrão ISO/IEC 10646, para a codificação dos caracteres;

c) Enviar dados por meio de um *driver* para comandar o envio de informações para a impressão de imagem gráfica (ex. bit mapped);

d) Enviar dados por meio de um *driver* para comandar a impressão de código de barras, no mínimo, nos padrões Code 39, Code 93, Code 128, EAN 8, EAN 13, 2 de 5, Interleaved 2 de 5, UPC-A, UPC-E e Codabar;

e) Monitorar o comportamento e os alarmes (sensores) dos dispositivos que compõem a UE;

f) Respeitar os requisitos referentes à memória não volátil definidos no **Anexo A-III – Especificação da UE**;

g) Respeitar os requisitos do **Anexo A-IV-d – Software pata teste de Biometria**.

2.2 Gerenciador Ajuste de Data/Hora

O processo 'Ajuste de Data/Hora' deve considerar que:

a) O ajuste de data e hora de hardware será realizado em fábrica. A reconfiguração desses dados, quando da manutenção de urna, deverá ser possível somente via software através de código (A BIOS não deverá permitir o ajuste de data e hora pelo *setup*).

2.3 Dispositivo de segurança e autenticação

a) O sistema de boot das UEs é um derivado do sistema de boot padrão do PC, sendo que foram adicionados meios para prover segurança e impossibilitar sistemas operacionais não autorizados. No entanto, o loader do sistema operacional deverá estar fora da BIOS.

b) A Contratada deverá ser implementar solução baseada em dispositivo microcontrolado, dedicado à função de autenticação, criptografia utilizando algoritmos simétricos e assimétricos, armazenamento de chaves criptográficas de forma segura e bloqueio de funcionalidades de hardware;

c) A Contratada deverá prover solução com autenticação e comunicação segura entre a placa-mãe, microterminal e teclado do terminal do eleitor;

d) A comunicação entre os teclados do TE/UE e MT/UE com a placa mãe deverá ser criptografada;

e) Deverá ser instalado na placa-mãe e executará a autenticação do BIOS. Além disso, deve fornecer interface tanto para que o BIOS valide o BOOTLOADER e este valide o sistema operacional. O dispositivo deverá ainda permitir o bloqueio de funcionamento do hardware. A interface entre dispositivo, BIOS, BOOTLOADER e SO deverá ser aprovada pelo TSE.

f) Caso a autenticação do BIOS, BOOTLOADER, ou dispositivos de hardware não tenha sido completada com sucesso, o sistema de segurança da placa-mãe se encarregará de bloquear o funcionamento da urna eletrônica.

g) O bloqueio deverá ocorrer após a carga do sistema operacional. Caso o sistema não seja autêntico, a urna eletrônica terá o seu funcionamento impedido em no máximo 4 minutos e deverá apresentar a mensagem de erro: "URNA ELETRÔNICA BLOQUEADA" no display do micro terminal.

h) O estado inicial dos módulos TE e MT deve ser bloqueado e o desbloqueio só será realizado pelo sistema operacional.

i) Deverá ser previsto o armazenamento de pelo menos 5 chaves criptográficas de tamanho 2048 bits, sendo uma delas de autenticação para o processo fabril e manutenção das urnas. As demais chaves serão para a autenticação do TSE e serão fornecidas pelo TSE. Cada chave deverá possuir um campo de atributos adicional de 16 bytes.

j) Quando a autenticação pela chave de manutenção for utilizada, a mensagem de "MANUTENÇÃO" deverá ser exibida na tela do microterminal. Somente as chaves de autenticação do TSE poderão permitir que a urna eletrônica possa operar sem restrições.

k) Deverá ser permitida a troca das chaves criptográficas por um processo a ser definido entre o TSE e a licitante vencedora.

l) Deve possuir identificador único e não regravável (ROM), pré-programado durante a fabricação do chip, de no mínimo 64 bits de tamanho. A Contratada deverá fornecer os identificadores presentes em cada UE.

m) Todos os protocolos e algoritmos criptográficos a serem utilizados deverão ser aprovados pelo TSE.

n) Deverá fornecer os seguintes serviços:

a. Criptografia e Decriptografia simétrica (AES);
b. Criptografia e Decriptografia assimétrica (RSA);
c. Assinatura digital e verificação (RSA);
d. Algoritmo de resumo digital (SHA-1);
e. Gerador de número aleatório de 4bytes (inteiro).

2.4 API

A API corresponde a um conjunto de módulos que descrevem os recursos disponíveis no sistema e se comunicam com o sistema operacional.

Esta interface deverá possuir as seguintes características:

a) Disponibilizar aos aplicativos o acesso estruturado a todos os recursos da UE, como mostrar uma informação textual e gráfica, armazenar, recuperar, imprimir e transmitir as informações tratadas e geradas na UE;

b) Permitir que o desenvolvimento de aplicativos baseie-se somente nas interfaces especificadas na API;

c) Quando da inexistência de definições específicas seguir padrões de mercado:

c.1) ISO 15435/1999.

c.2) ISO 9945-1/2002 [IEE 1003.1-2001].

c.3) WOSA;

c.4) X;

c.5) Motif.

d) A API da UEs devem prover, no mínimo, os seguintes grupos de funções:

d.1) Áudio:

d.1.1) Interface para tratamento de áudio;

d.1.2) Possibilitar a inicialização de áudio independente do término da execução anterior. Sendo que o *driver* de Áudio deverá interromper a execução do áudio se um outro for iniciado.

d.2) Gráfica:

d.2.1) Inicialização e encerramento de interface gráfica;

d.2.2) Funções para manipulação de Fontes Escalonáveis (ex.: TrueType) com suporte a UNICODE;

d.2.3) Manipulador de tela (interface de usuário textual e gráfica);

d.2.4) Interface para objetos gráficos 2D (ponto, linha, retângulo, círculo, polígonos e preenchimento);

d.2.5) Interface apresentação de imagens JPEG;

d.2.6) Interface para apresentação de imagens BMP.

d.3) Impressão

d.3.1) Impressão de arquivos;

d.3.2) Impressão de "*buffers*";

d.3.3) Controle de status da impressora;

d.3.4) Interromper impressão;

d.3.5) Corte de papel;

d.3.6) Impressão de códigos de barras;

d.3.7) Impressão de caracteres expandido e negrito;

d.3.8) Impressão de imagem (bit mapped);

d.3.9) Impressão de código de barras (vide descrição do módulo impressor no Anexo A-II – Especificação dos requisitos do ME/UE2006;

d.4) Reconhecimento biométrico:

d.4.1) Interface para os dispositivos de reconhecimento biométrico;

d.4.2) Teste de comunicação com o dispositivo de reconhecimento biométrico;

d.4.3) grupos de funções definidos no Anexo A-V-1.b – Integração com a Identificação Biométrica.

d.5) Compactação e Criptografia:

d.5.1) Interface para compactação e descompactação de arquivos (zip);

d.5.2) Interface para assinatura digital;

d.5.3) Interface para criptografia simétrica e assimétrica para arquivos;

d.6) Exclusivas das UEs:

d.6.1) Interface para todos os dispositivos das UEs 2006 (USB, seriais, fonte, impressoras, teclado do eleitor e outros);

d.6.2) Interface para depuração dos programas via Serial, USB ou outro meio disponível na urna.

d.7) Intercambio com o SO.

d.7.1) Criação, encerramento, ativação, suspensão de *threads* e tarefas;

d.7.2) Definição, cancelamento, entrada, saída de seção crítica;

d.7.3) Tratamento de mensagens;

d.7.4) Alocação, liberação de partição de memória para *threads* e tarefas;

d.7.5) Definição, cancelamento, ativação, desativação de contexto;

d.7.6) Definição, chamada de interrupção;

d.7.7) Leitura, ajuste de relógio de tempo real;

d.7.8) Leitura de status dos componentes da UE;

d.7.9) Funções de tarefas do temporizador;

d.7.10) Funções de entrada e saída de dispositivos;

d.7.11) Funções especiais (a definir).

3 PRODUTOS A SEREM ENTREGUES AO TSE

A Contratada deverá entregar os produtos descritos abaixo, de acordo com o Cronograma da Tabela 7-1 do Anexo A.

a) Drivers dos dispositivos da UE2009 compatíveis com o aplicativo fornecido pelo TSE;

b) Documentação de alterações necessárias na API, caso os drivers dos dispositivos não tenham sido suficientes para compatibilização do aplicativo fornecido pelo TSE com a UE2009.

4 ACEITAÇÃO DOS PRODUTOS

O aceite dos produtos descritos neste anexo será efetuado pela equipe técnica do Tribunal Superior Eleitoral após a realização de todos os testes e validação da documentação.

A Contratada deverá fornecer todos os meios e recursos necessários para a realização dos procedimentos de aceitação dos produtos, que ocorrerá no Tribunal Superior Eleitoral, com o acompanhamento de técnicos da contratada responsáveis pelo desenvolvimento e teste do produto desenvolvido.

5 GARANTIA

A contratada deverá corrigir, imediatamente, quaisquer falhas ou erros encontrados nos produtos, assim como, omissões em documentação, inclusive após a aceitação dos produtos.

6 SEGURANÇA

A segurança lógica da urna eletrônica objetiva assegurar a transparência do processo, garantindo integridade, autenticidade, autoria e confidencialidade da informação gerada, tratada e manipulada pelos sistemas e produtos a serem desenvolvidos e fornecidos para a eleição 2008.

Os produtos e serviços definidos visam a complementação dos procedimentos a serem estabelecidos para o controle das informações. A Contratada deverá fornecer todas as facilidades, em todos os ambientes computacionais envolvidos (SO da UE, WinNT, HP-UX e Linux), para desenvolver e implementar os requisitos necessários para:

a) **Integridade da informação** – procedimentos e produtos para a geração e verificação da assinatura da informação (message digest) para assegurar a consistência da mesma e a identificação de alteração indevida, ou inadvertida, ou por falhas que venham a ocorrer;

b) **Autenticidade da informação** – procedimentos e produtos para a geração e verificação da autenticidade da informação (não repúdio);

c) **Autoria da informação** – procedimentos e produtos para a geração e verificação da identificação da autoria da informação;

d) **Confidencialidade da informação** – procedimentos e produtos para cifrar e decifrar as informações críticas no processo e os arquivos contendo os resultados da eleição para o seu transporte.

7 CRIPTOGRAFIA E ASSINATURA DIGITAL

A criptografia será utilizada nos sistemas da eleição 2010 para as seguintes finalidades:

a) Proteção dos arquivos e informações a serem transportados de um ambiente a outro, garantindo o sigilo na operação (criptografia simétrica);

b) Proteção das informações de assinatura digital e demais informações de controle, garantindo a autenticidade e autoria da informação (criptografia assimétrica).

O TSE fornecerá a biblioteca de criptografia, assinatura digital e hash.

Cabe à contratada efetivar as alterações necessárias no software básico para o funcionamento da biblioteca de criptografia do TSE.

8 IDENTIFICAÇÃO INTERNA DA URNA

A identificação interna da urna é um código único para cada urna que deverá ser gravado conforme instruções que serão entregues pelo TSE à Contratada. Este código identificará todas as urnas eletrônicas de forma única e será utilizado pelas rotinas de segurança.