

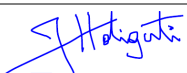
**LET-ABECS-RE 2395-6460-01-N – 01.00 (Pt)**  
**03-Dez-2019**

# **RELATÓRIO DE ENSAIO**

## **Certificação de Segurança em Terminal POS**

Modelo: T6900

Responsável pela  
Emissão do Relatório

  
**Jaqueline Yuri Holiguti**

Responsável Técnico  
do Laboratório

  
**Marcos Pimentel Rezende**

*Este relatório não poderá ser reproduzido parcialmente sem autorização formal do Instituto de Pesquisas Eldorado. Caso seja necessária a impressão do mesmo, esta deve ser feita utilizando-se o padrão A4 (210mm x 297mm).*

*As informações aqui contidas são de propriedade do solicitante, não podendo ser divulgadas sem sua autorização.*

*Os resultados desse relatório são válidos apenas para o item testado.*

*As opiniões e interpretações expressas neste relatório não fazem parte do escopo de acreditação do laboratório.*

*Esta versão substitui e cancela todas as versões anteriores.*

### **Sugestões / Reclamações / Comentários**

Por favor, enviar e-mail para: [qualidade@eldorado.org.br](mailto:qualidade@eldorado.org.br)

## Sumário

1. ESCOPO .....	3
2. LOCAL DOS ENSAIOS .....	3
3. TERMO DE RESPONSABILIDADE .....	3
4. DADOS DO SOLICITANTE .....	3
5. INFORMAÇÕES GERAIS DO EQUIPAMENTO SOB ENSAIO (ESE).....	4
6. IDENTIFICAÇÃO DO EQUIPAMENTO SOB ENSAIO (ESE).....	4
7. LISTA DE ENSAIOS .....	5
8. ITENS UTILIZADOS.....	5
9. RESULTADOS DOS ENSAIOS .....	6
9.1. Requisito ABECS 1 .....	6
9.2. Requisito ABECS 2 .....	11
9.3. Requisito ABECS 3 .....	12
9.4. Requisito ABECS 4 .....	14
9.5. Requisito ABECS 5 .....	16
9.6. Requisito ABECS 6 .....	18
9.7. Requisito ABECS 7 .....	19
9.8. Check List.....	20
10.CONCLUSÃO .....	22
11.FOTOS GERAIS .....	23
12.CONSIDERAÇÕES.....	24
13.LISTA DE GERAL DE INSTRUMENTOS .....	25
14.HISTÓRICO DE REVISÕES .....	26

## 1. ESCOPO

Testes de certificação de segurança no Terminal de POS de acordo com os seguintes documentos normativos:

Documento Normativo	Data de Emissão
Manual ABECS – Versão 7.0 Dispositivos de captura de certificação de segurança por senha	2016

## 2. LOCAL DOS ENSAIOS

Instituto de Pesquisas Eldorado – Laboratório de Ensaios e Testes  
Av. Alan Turing, 275 – Cidade Universitária – Barão Geraldo – Campinas/SP - Brasil  
CEP: 13083-898 – Telefone: +55 (19) 3757-3144 e +55 (19) 99161-8100  
[www.eldorado.org.br/laboratorios](http://www.eldorado.org.br/laboratorios)

## 3. TERMO DE RESPONSABILIDADE

Este relatório de ensaios é válido exclusivamente para o objeto ensaiado, não sendo extensivo a quaisquer lotes, mesmo que similares.

A partir do momento em que o item é retirado do laboratório esgota-se a possibilidade de contestação dos resultados ou mesmo de repetição deles, já que o laboratório deixa de ser responsável pela manutenção e integridade desses itens.

A análise dos resultados obtidos durante os ensaios, declarando conformidade ou não aos requisitos aplicáveis, é de responsabilidade dos organismos de certificação, homologação ou aprovação de equipamentos.

## 4. DADOS DO SOLICITANTE

Solicitante	
Razão Social	TEC TOY S.A.
Endereço	Av. Buriti, 3149, CEP: 69.075-000, Distrito Industrial Manaus - AM, Brasil
CNPJ	22.770.366/0001-82
Inscrição Estadual	06.200.249-0
Contato	Heriberto - <a href="mailto:heriberto@tectoy.com.br">heriberto@tectoy.com.br</a> ; José Carlos - <a href="mailto:jose.carmo@paxbr.com.br">jose.carmo@paxbr.com.br</a>

## 5. INFORMAÇÕES GERAIS DO EQUIPAMENTO SOB ENSAIO (ESE)

Dados Gerais	
Classificação	Point of Sale (POS) Terminal
Modelo	T6900

## 6. IDENTIFICAÇÃO DO EQUIPAMENTO SOB ENSAIO (ESE)

Recebimento	ESE	Descrição	Modelo Declarado	Número de série (ou similar)
18/11/2019	01	PED	T6900	PB0419AL60864
18/11/2019	02			PB0419AL60876
18/11/2019	03			PB0419AL60837
18/11/2019	04			PB0419AL60846
18/11/2019	05			PB0419AL60736

Tabela 1 – Identificação do equipamento sob ensaio (ESE)

ESE Informação Adicional	
Identificação do ESE	T6900
Período dos Testes	26-Nov-2019 a 03-Dez-2019
PCI-PED Numero de Aprovação	4-90067
Versão PCI	5.x
Tipo de Equipamento	PED
Tipo Online e Offline	Online & Offline
Tipo de Criptografia	TDES: MK/SK,DUKPT AES: MK/SK,DUKPT
Versão de Hardware	P2_00_xx
Versão de Firmware	V1.0.x

Tabela 2 – Informação adicional do ESE

Link PCI: [https://www.pcisecuritystandards.org/popups/pts\\_device.php?appnum=4-90067](https://www.pcisecuritystandards.org/popups/pts_device.php?appnum=4-90067)

## 7. LISTA DE ENSAIOS

Item Norma	Ensaio	Item Rel.
<b>ABECS Manual Versão 7.0</b>		
ABECS 01	Proteção física (leitor de smart card / leitor de cartão de tarja magnética)	9.1
ABECS 02	Mecanismo de proteção de PinPad (cabo de comunicação)	9.2
ABECS 03	Número de série (unicidade)	9.3
ABECS 04	Proteção contra tentativa de violação	9.4
ABECS 05	Integridade de software (assinatura digital)	9.5
ABECS 06	Funcionalidades de segurança do dispositivo	9.6
ABECS 07	Proteção contra acesso ao leitor de cartão magnético	9.7

Tabela 3 – Lista de ensaios realizados

## 8. ITENS UTILIZADOS

Item Norma	Ensaio	Itens
<b>ABECS Manual Versão 7.0</b>		
ABECS 01	Proteção física (leitor de smart card / leitor de cartão de tarja magnética)	01 e 02
ABECS 02	Mecanismo de proteção de PinPad (cabo de comunicação)	N/A
ABECS 03	Número de série (unidade)	01 ao 05
ABECS 04	Proteção contra tentativa de violação	01 e 02
ABECS 05	Integridade de software (assinatura digital)	04
ABECS 06	Funcionalidades de segurança do dispositivo	03
ABECS 07	Proteção contra acesso ao leitor de cartão magnético	N/A

Tabela 4 – Lista de ensaios realizados

## 9. RESULTADOS DOS ENSAIOS

### 9.1. Requisito ABECS 1

#### 9.1.1. Requisito Normativo

Deverá existir uma proteção física que impeça a neutralização da segurança do terminal, através do acesso aos sensores de segurança por orifícios existentes ou criados na carcaça. Esta implementação deverá ser feita de tal sorte que não seja possível neutralizar a segurança do terminal independente da quantidade de sensores que foram protegidos, isto é, mesmo neutralizando alguns sensores, a segurança do terminal não poderá ser neutralizada. (Manual ABECS Versão 7.0 - Item 6.1.1)

#### 9.1.2. Critério de Avaliação

Neste item, os laboratórios de teste devem considerar apto o equipamento quando:

- a.) Não for possível quebrar esta barreira em até cinco dias úteis, usando equipamentos convencionais (chave de fenda, alicate, clips, multímetro, osciloscópio, etc) e sem o conhecimento prévio dos circuitos ou uso de equipamentos mais sofisticados como por exemplo Raios-X.
- b.) Usando no máximo 5 equipamentos
- c.) Avalie o sistema de segurança e proteção adicional para o circuito de segurança de pressão.
- d.) Avalie a quantidade de camadas de malha aplicadas no circuito de segurança quando a malha foi usada

### 9.1.3. Leitora de Tarja

#### 9.1.3.1. Descrição

Tentativa de acesso à leitora de tarja.

#### 9.1.3.2. Detalhamento / Resultado

A leitora de tarja é conectada à placa principal por meio de um flat cable. Foi evidenciado que não é possível acessar a leitora sem alterações visíveis na carcaça ou sem que o alarme seja acionado. E não existe espaço interno suficiente para alocar qualquer tipo de dispositivo de captura no terminal.

#### 9.1.3.3. Imagens de teste / Evidências



Figura 1 - Leitora de Tarja

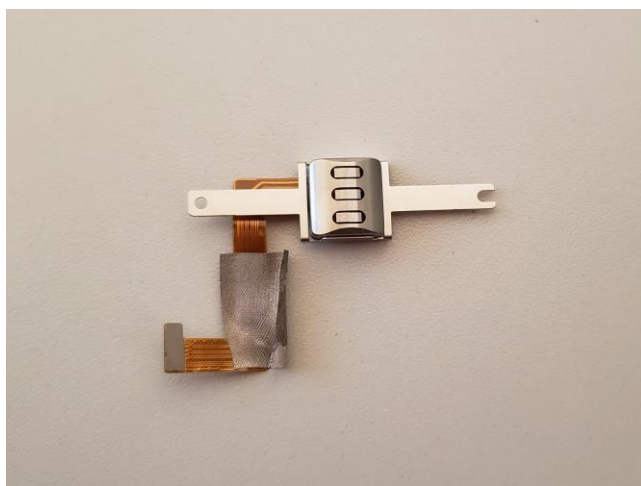


Figura 2 - Leitora de Tarja

#### 9.1.4. Leitora de Smart

##### 9.1.4.1. Descrição

Tentativa de acesso à leitora de smart.

##### 9.1.4.2. Detalhamento / Resultado

A leitora de smart é soldada à placa principal. Possui 3 sensores de proteção ligados à carcaça frontal. Qualquer tentativa de acesso acionará o alarme, ocasionando o Tamper.

##### 9.1.4.3. Imagens de teste / Evidências



Figura 3 - Leitora de Smart

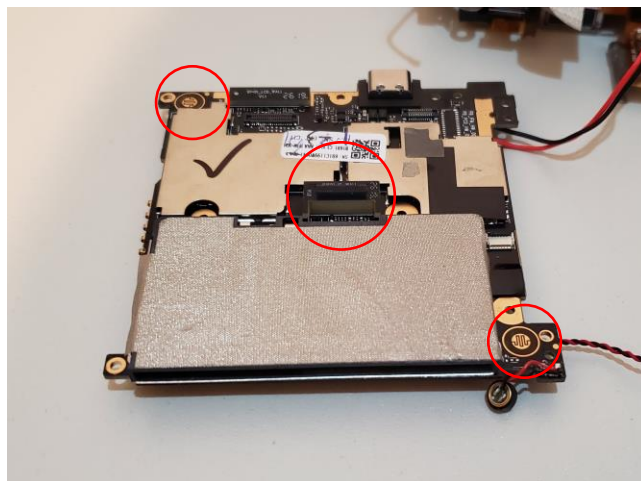


Figura 4 - Leitora de Smart



### 9.1.5. Carcaça Traseira

#### 9.1.5.1. Descrição

Tentativa de neutralizar os sensores e verificar espaços internos.

#### 9.1.5.2. Detalhamento / Resultado

Possui 3 sensores de proteção que se conecta à placa principal. Foi realizada uma verificação na carcaça traseira com o intuito de abrir o terminal sem que os sensores fossem acionados, porém ao tentar retirar a tampa traseira, os sensores detectaram a invasão ocasionando o Tamper no terminal, impossibilitando sua utilização. Não há espaço suficiente para alocar qualquer dispositivo de captura.

#### 9.1.5.3. Imagens de teste / Evidências



Figura 5 - Carcaça Traseira



Figura 6 - Carcaça Traseira

### 9.1.6. Carcaça Frontal

#### 9.1.6.1. Descrição

Tentativa de neutralizar os sensores e invadir o terminal pela parte frontal.

#### 9.1.6.2. Detalhamento / Resultado

A carcaça frontal possui 2 sensores de proteção que se conectam à placa principal. Qualquer tentativa de acesso acionará o alarme, ocasionando o Tamper.

#### 9.1.6.3. Imagens de teste / Evidências



Figura 7 - Carcaça Frontal

## 9.2. Requisito ABECS 2

### 9.2.1. Requisito Normativo

O PinPad deve prover um mecanismo de proteção na conexão com seu cabo de comunicação, de forma que fique visível ao lojista qualquer tentativa de substituição e que dificulte a substituição deste dispositivo de forma rápida (o que ocorre atualmente com os equipamentos com conectores rj11/rj45). Para os casos em que não há comprovadamente formas de inserir dispositivos de captura de dados no pinpad, pela segurança ou por espaço exíguo, é suficiente o uso de selo de lacre (exceto selos adesivos) , o qual deve necessariamente ser rompido para a troca do cabo.

### 9.2.2. Critério de Avaliação

Neste item, os laboratórios considerarão apto o equipamento se para sua substituição for necessário o uso de ferramentas especiais (exemplo chave de fenda) ou rompimento de lacre (cuja ação exija esforço e tempo para execução).

### 9.2.3. Cabo de Comunicação

#### 9.2.3.1. Descrição

Análise para verificação da segurança do cabo de comunicação.

#### 9.2.3.2. Detalhamento / Resultado

Não aplicável: O terminal não possui cabo de comunicação.

#### 9.2.3.3. Imagens de Teste / Evidências

Não aplicável

### 9.3. Requisito ABECS 3

#### 9.3.1. Requisito Normativo

O fabricante deve manter a unicidade dos números de série dos dispositivos por ele fabricados de modo a garantir uma identidade única para cada dispositivo de captura.

Não há impeditivos para que um fabricante insira um número já existente em uma nova placa devido a necessidade de substituição de uma placa defeituosa.

#### 9.3.2. Critério de Avaliação

Os laboratórios devem solicitar do fabricante a lógica de geração do número de série e acrescentar esta informação ao seu laudo.

#### 9.3.3. Unicidade do Número de Série

##### 9.3.3.1. Descrição

Cada terminal possui um número de série único que é utilizado para rastreamento dos dispositivos durante todo o seu ciclo de vida.

##### 9.3.3.2. Detalhamento / Resultado

O Número de série do terminal é composto por 13 caracteres. Os dois primeiros representam o nome do modelo do terminal. O terceiro e quarto representam a versão do terminal. E os próximos quatro caracteres representam a data de fabricação. Os últimos cinco caracteres representam o número de produção.

Sendo:

"PB" = Modelo

"04" = Representa a configuração do terminal. Por exemplo, "04" significa versão em inglês (câmera de 500 W, cartão Dual SIM para 4G, adaptador padrão dos EUA).

"19AL" = Data

Os dois primeiros caracteres referente ao ano.

O terceiro caractere referente ao mês e o último caractere referente ao dia, segundo as tabelas abaixo:

Mês	Número/Letra	Mês	Número/Letra	Mês	Número/Letra
Janeiro	1	Fevereiro	2	Março	3
Abril	4	Maio	5	Junho	6
Julho	7	Agosto	8	Setembro	9
Outubro	A	Novembro	B	Dezembro	C

Dia	Número/Letra	Dia	Número/Letra	Dia	Número/Letra	Dia	Número/Letra
1	1	2	2	3	3	4	4
5	5	6	6	7	7	8	8
9	9	10	A	11	B	12	C
13	D	14	E	15	F	16	G
17	H	18	J	19	K	20	L
21	M	22	N	23	P	24	Q
25	R	26	S	27	T	28	U
29	V	30	W	31	X		

Nota: A Lógica de geração do número de série foi fornecida pelo interessado.

### 9.3.3.3. Imagens de Teste / Evidências

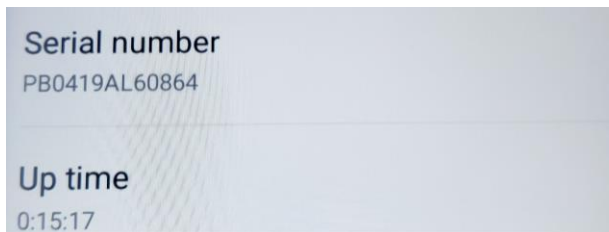


Figura 8 - Número de Série Armazenado na memória do Terminal (#01)

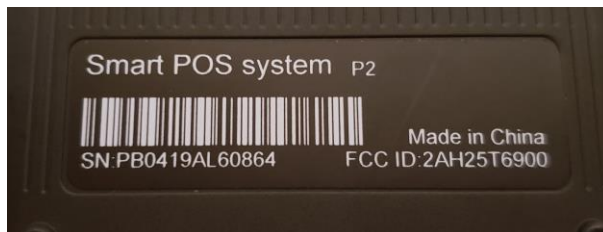


Figura 9 - Número de Série Armazenado na etiqueta do Terminal (#01)

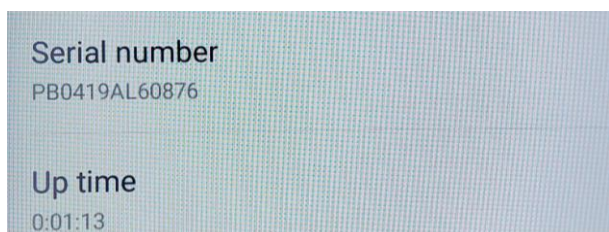


Figura 10 - Número de Série Armazenado na memória do Terminal (#02)



Figura 11 - Número de Série Armazenado na etiqueta do Terminal (#02)

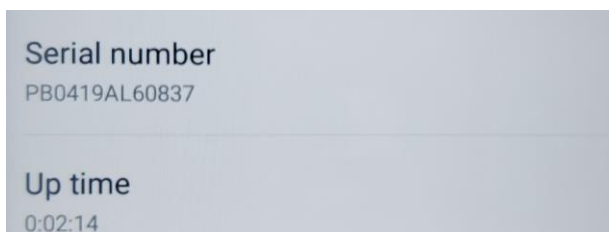


Figura 12 - Número de Série Armazenado na memória do Terminal (#03)



Figura 13 - Número de Série Armazenado na etiqueta do Terminal (#03)

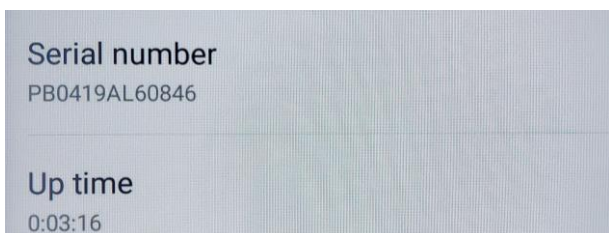


Figura 14 - Número de Série Armazenado na memória do Terminal (#04)



Figura 15 - Número de Série Armazenado na etiqueta do Terminal (#04)

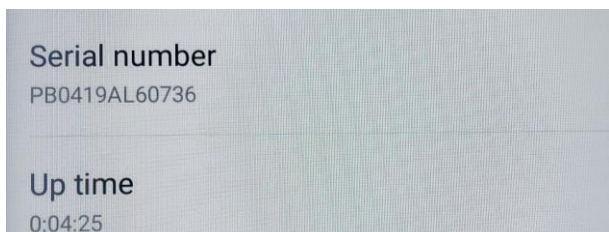


Figura 16 - Número de Série Armazenado na memória do Terminal (#05)



Figura 17 - Número de Série Armazenado na etiqueta do Terminal (#05)

## 9.4. Requisito ABECS 4

### 9.4.1. Requisito Normativo

Em uma tentativa de violação, o dispositivo ativará um mecanismo de resposta que inclui:

- Remoção das chaves de criptografia
- Remoção de dados de configuração
- Remoção de todo o software instalado, com exceção do sistema operacional
- O terminal deve permanecer “morto”, portanto, não sendo possível que o dispositivo funcione sem a intervenção de um laboratório autorizado.

(Manual ABECS Versão 7.0 - Item 6.1.4)

### 9.4.2. Critério de Avaliação

Os laboratórios devem verificar se o terminal perdeu as chaves de criptografia e também os aplicativos sendo que os mesmos não devem funcionar somente com uma carga do aplicativo.

**Recomendação ABECS:** Que quando em TAMPER o terminal deverá mostrar o número de série do equipamento registrado no firmware além da mensagem de TAMPER.

### 9.4.3. Inoperabilidade do Terminal

#### 9.4.3.1. Descrição

Verificação da inoperabilidade do terminal após uma violação.

#### 9.4.3.2. Detalhamento / Resultado

Foi evidenciado que:

- Não foi possível visualizar as chaves de criptografia antes de o terminal entrar em TAMPER;
- Ao identificar uma ameaça, o dispositivo alterou o status para TAMPER;
- O terminal não exibiu o número de série junto da mensagem de TAMPER;

#### 9.4.3.3. Imagens de Teste / Evidências

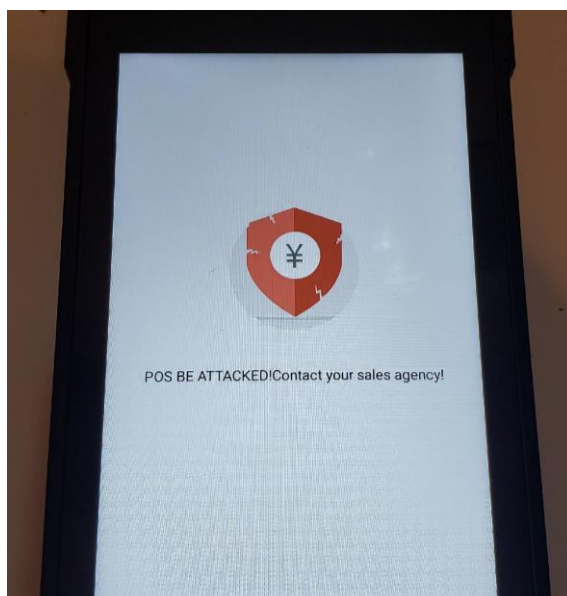


Figura 18 - Mensagem de Tamper

#### 9.4.4. Remoção de todo Software instalado

##### 9.4.4.1. Descrição

Verificação da remoção de todos os softwares instalados.

##### 9.4.4.2. Detalhamento / Resultado

Depois de identificar uma ameaça, o dispositivo alterou o status para TAMPER.

Não foi possível verificar se todo o software instalado foi removido pois quando o terminal foi reinicializado, a mensagem TAMPER permaneceu visível, impossibilitando o uso do terminal, e não há nenhum software disponível no laboratório para verificar se o software instalado está presente no terminal após a ocorrência de TAMPER.

##### 9.4.4.3. Imagens de Teste / Evidências

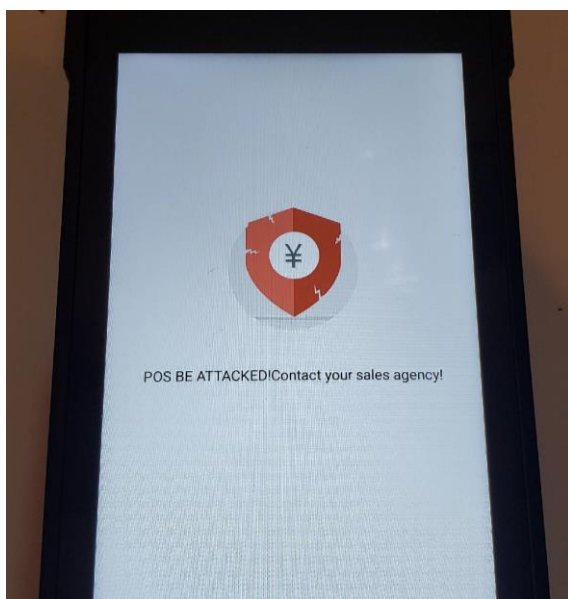


Figura 19 – Sistema Operacional (Após o TAMPER)



## 9.5. Requisito ABECS 5

### 9.5.1. Requisito Normativo

Todo o software carregado no dispositivo deve ser assinado digitalmente pelo fabricante do terminal, com a possibilidade de ser assinado digitalmente pelo desenvolvedor do software e pelo adquirente.

### 9.5.2. Critério de Avaliação

Os laboratórios devem estar disponíveis:

- a.) Se existe como carregar uma aplicação não assinada em um terminal com assinatura digital.
- b.) Se houver como carregar um aplicativo assinado com um certificado diferente de injetado pelo fabricante.

O fabricante deve fornecer os meios para esses testes.

### 9.5.3. Carregar aplicação não assinada no terminal.

#### 9.5.3.1. Descrição

Verificar a possibilidade de carregar uma aplicação não assinada em um terminal com assinatura digital.

#### 9.5.3.2. Detalhamento / Resultado

Utilizando a ferramenta disponibilizada pelo fabricante, o laboratório tentou carregar um aplicativo não assinado no terminal com assinatura digital e o aplicativo não assinado foi rejeitado.

#### 9.5.3.3. Imagens de Teste / Evidências

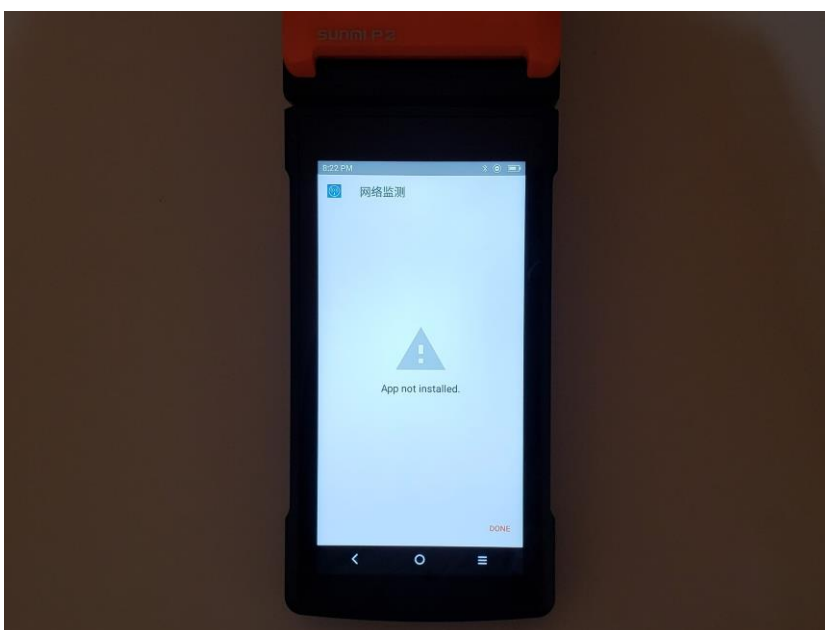


Figura 20 - Aplicação não assinada



#### 9.5.4. Carregar um aplicativo assinado com certificado diferente

##### 9.5.4.1. Descrição

Verifique a possibilidade de carregar um aplicativo assinado com certificado diferente do injetado pelo fabricante.

##### 9.5.4.2. Detalhamento / Resultado

Utilizando a ferramenta disponibilizada pelo fabricante, o laboratório tentou carregar um aplicativo assinado com certificado diferente do injetado pelo fabricante e o aplicativo foi rejeitado pelo terminal.

##### 9.5.4.3. Imagens de Teste / Evidências

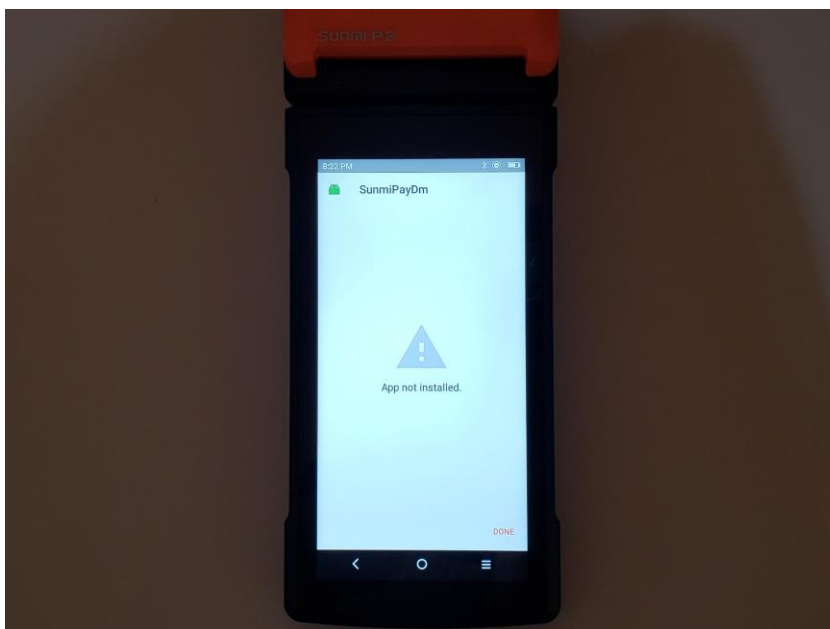


Figura 21 - Aplicação assinada com certificado diferente

## 9.6. Requisito ABECS 6

### 9.6.1. Requisito Normativo

Nos dispositivos de captura em produção não deverá ser possível:

- A desativação de funcionalidades de segurança;
- A impressão ou visualização no display da trilha completa de cartões;
- A visualização da chave de criptografia;
- A inserção manual de chaves de criptografia;

### 9.6.2. Critério de Avaliação

Os laboratórios devem verificar se existem condições de execução das ações acima. Devem contar com a colaboração do fabricante.

### 9.6.3. Desativação de funcionalidades de segurança

#### 9.6.3.1. Descrição

Verificação da possibilidade de desativar as funcionalidades de segurança.

#### 9.6.3.2. Detalhamento / Resultado

Não foi possível desativar as funcionalidades de segurança.

### 9.6.4. Visualização completa das trilhas do cartão no display

#### 9.6.4.1. Descrição

Verificação das trilhas do cartão no display do terminal.

#### 9.6.4.2. Detalhamento / Resultado

Não foi possível visualizar nenhuma trilha passando o cartão, tanto pela leitora de tarja quanto pela leitora de smart do terminal. O terminal também não possui nenhuma opção para verificação das leitoras.

### 9.6.5. Visualização e inserção de chaves de criptografia

#### 9.6.5.1. Descrição

Verificação de chaves de criptografia em claro no terminal.

#### 9.6.5.2. Detalhamento / Resultado

Não foi possível visualizar ou inserir chaves manualmente.

## 9.7. Requisito ABECS 7

### 9.7.1. Requisito Normativo

Não deverá ser possível o acesso à leitora de cartão magnético do terminal, através de orifícios existentes ou criados na carcaça sem que fique evidenciado ou por alterações visíveis no gabinete do terminal ou pelo acionamento do mecanismo de segurança.

Devem estar protegidos:

- a.) Os conectores de cabeça magnética, tanto a cabeça como os conectores da cabeça magnética na placa do equipamento;
  - b.) conectores do leitor CHIP;
  - c.) Potenciais vias eletrônicas, como: resistores, transistores, ponto de teste da placa onde pode trafegar os dados do portador de cartão antes que os dados atinjam o processador criptográfico.
- (Manual ABECS versão 7.0 - item 6.1.6)

### 9.7.2. Critério de Avaliação

Caso o laboratório consiga acessar a área onde está instalada a leitora de cartão magnético, sem alterações visíveis no gabinete ou bloqueio do terminal, é necessário evidenciar a captura de dados a partir deste ponto.

A evidência deve ser colhida da seguinte forma:

- a.) Instalação de dispositivo paralelo à leitora de cartão magnético ou em conector.
- b.) Deverá demonstrar o log da informação capturada pelo dispositivo paralelo.
- c.) Demonstrar se a informação está legível ou criptografada.

### 9.7.3. Captura de Dados

#### 9.7.3.1. Descrição

Tentativa de captura de dados de cartão.

#### 9.7.3.2. Detalhamento / Resultado

Em vista da não possibilidade de violação do equipamento, este requisito torna-se não aplicável aos testes.

## 9.8. Check List

Requisito	Critério de Avaliação	Ref.	Status	Observação
ABECS 01	1. Não for possível a quebra da barreira de segurança no prazo estabelecido.	9.1.2	OK	
	2. Utilizar 5 equipamentos por modelo.	9.1.2	OK	
	3. Avaliação dos sistemas de segurança e meios de proteção adicionais.	9.1.2	OK	
	4. Avaliar a quantidade de layers das mesh, quando utilizada.	9.1.2	N/A	O terminal não possui manta de proteção
ABECS 02	1. Proteção do Cabo de comunicação.	9.2.2	N/A	O terminal não possui cabo de comunicação.
ABECS 03	1. Lógica de geração do número de série.	9.3.2	OK	
	2. O número de série interno deve ser idêntico ao número de série da etiqueta externa.	9.3.2	OK	
	3. Apresentação do número de série.	9.3.2	OK	
ABECS 04	1. Remoção das chaves de criptografia e aplicativos após o TAMPER.	9.4.2	OK	
	Recomendação ABECS: Visualização do número de série além da mensagem de TAMPER.	9.4.2	N/A	O Terminal não mostra número de série quando em TAMPER
ABECS 05	1. Impede a instalação de aplicação não assinada em terminal com assinatura digital.	9.5.2	OK	
	2. Impede a instalação de aplicação assinada com um certificado diferente.	9.5.2	OK	
ABECS 06	1. Proteção contra visualização da trilha dos cartões e das chaves de criptografia.	9.6.2	OK	
ABECS 07	1. Acesso à leitora de cartão magnético do terminal sem que fique evidenciado.	9.7.2	N/A	Não foi possível acessar o leitor de cartão magnético.
*Para o sub-item 4 do Requerimento ABECS 1 só será aplicável quando houver Mesh/Manta de proteção. Caso o equipamento não possua tal proteção obrigatoriamente o campo observação deverá ser preenchido.				

Tabela 5 – Check List

Itens a proteger	Sub-itens	Nota	Observação
Cabeça Magnética	Cabeça-magnética em si.	4	
	Dados em claro na cabeça magnética	4	Não foi possível capturar nenhuma informação
	Pontos expostos no conector da cabeça magnética na placa	4	Não conseguimos acessar a cabeça magnética
	Cabo de comunicação entre a cabeça-magnética e a placa	4	
Leitora de Chip	Conector	4	
Pontos expostos na placa	Resistores	4	
	Capacitores	4	
	Pontos de testes	4	
	Outros pontos eletrônicos no terminal.	4	
Nota	Critério		
1	Sem segurança – fácil obtenção de dados		
2	Segurança básica – não foi encontrada dificuldades para exploração da vulnerabilidade.		
3	Segurança intermediária – há um sistema de segurança que evidencia o TAMPER no terminal caso seja violado, mas que foi burlado.		
4	Segurança avançada – há um sistema de segurança com TAMPER que não foi possível burlar.		
5	Não há pontos Expostos - Essa nota só poderá ser utilizada para os itens: Resistores, Capacitores, Pontos de testes e outros pontos eletrônicos no terminal.		

Tabela 6 – Check List

## 10. CONCLUSÃO

Após os testes, concluí-se que:

- O smart reader está bem protegido;
- Não é possível inserir dispositivos de captura de dados pelo leitor, porque não há espaço interno suficiente.
- Não foi possível visualizar a versão completa ou inserir chaves criptografadas no dispositivo;
- Não foi possível neutralizar os sensores de segurança da caixa;
- Não há espaço interno suficiente para instalar dispositivos extras.

Conclui-se que o terminal atende corretamente aos requisitos especificados pela ABECS.

## 11. FOTOS GERAIS

O equipamento sob ensaio (ESE) pode ser visualizado nas seguintes imagens:



Figura 22 - Vista Frontal do Dispositivo



Figura 23 - Vista Traseira do Dispositivo



Figura 24 - Vista Lateral



Figura 25 - Vista Lateral



Figura 26 - Vista Interna



Figura 27 - Vista Interna

## 12. CONSIDERAÇÕES

A definição de conformidade (ou não conformidade) de um ESE é estabelecida de acordo com os parâmetros e critérios definidos no padrão de referência.



### 13. LISTA DE GERAL DE INSTRUMENTOS

A lista geral de instrumentos segue apresentada abaixo. Os registros relativos aos equipamentos utilizados para cada ensaio citado neste documento está disponível para consulta mediante solicitação ao laboratório.

Ferramentas / Acessórios
Chave de Fenda
Chave Torx
Mini Retífica
Estilete
Ferro de Solda
Alicates
Multímetro
Fonte de Alimentação

*Tabela 6 – Lista generica de Ferramentas*



*Figura 30 – Ferramentas Utilizadas*

## 14. HISTÓRICO DE REVISÕES

Data	Versão	Histórico
03-Dez-2019	01.00	Emissão Inicial