

# ***FIRST TECH***®

Construindo relações duradouras

## **PAYSHIELD MANAGER**

[www.first-tech.com](http://www.first-tech.com)

**MATRIZ – SP**

AV. ANGÉLICA, 2248 – 4º ANDAR SÃO PAULO

**(11)3024-3200**

**FILIAL – RJ**

RUA DA QUITANDA, 60 – 12º ANDAR RIO DE JANEIRO

**(21) 3543-1650**

# Introdução

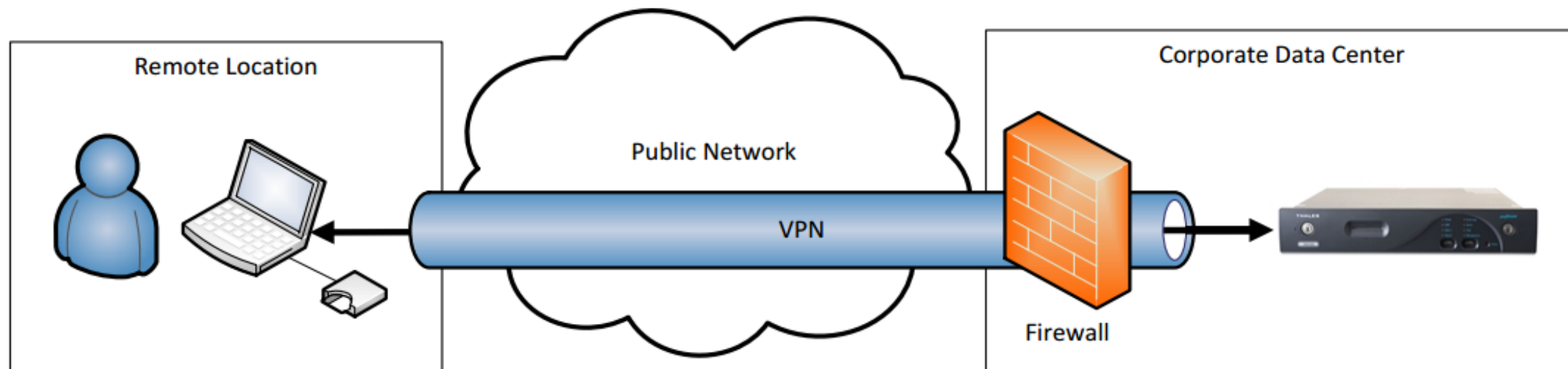
O payShield Manager é uma aplicação que utiliza abordagem web para oferecer a usuários privilegiados a habilidade de gerenciar seus HSMs payShield 9000 e 10k.

O payShield Manager permite as seguintes características:

- **Configuração do HSM** – configuração das portas, configuração de segurança etc.
- **Instalação do HSM** – geração e instalação de LMKs através de Smartcards.
- **Gestão de chaves do HSM** – geração de chaves, importação e exportação de chaves etc.
- **Manutenção do HSM** – visualização, impressão e eliminação de logs de auditoria e erros, informação de versão etc.
- **Mudança de estados do HSM** – transições entres os modos Online, Offline, Secure e Autorizado.
- Carregamento de firmware e licenças.

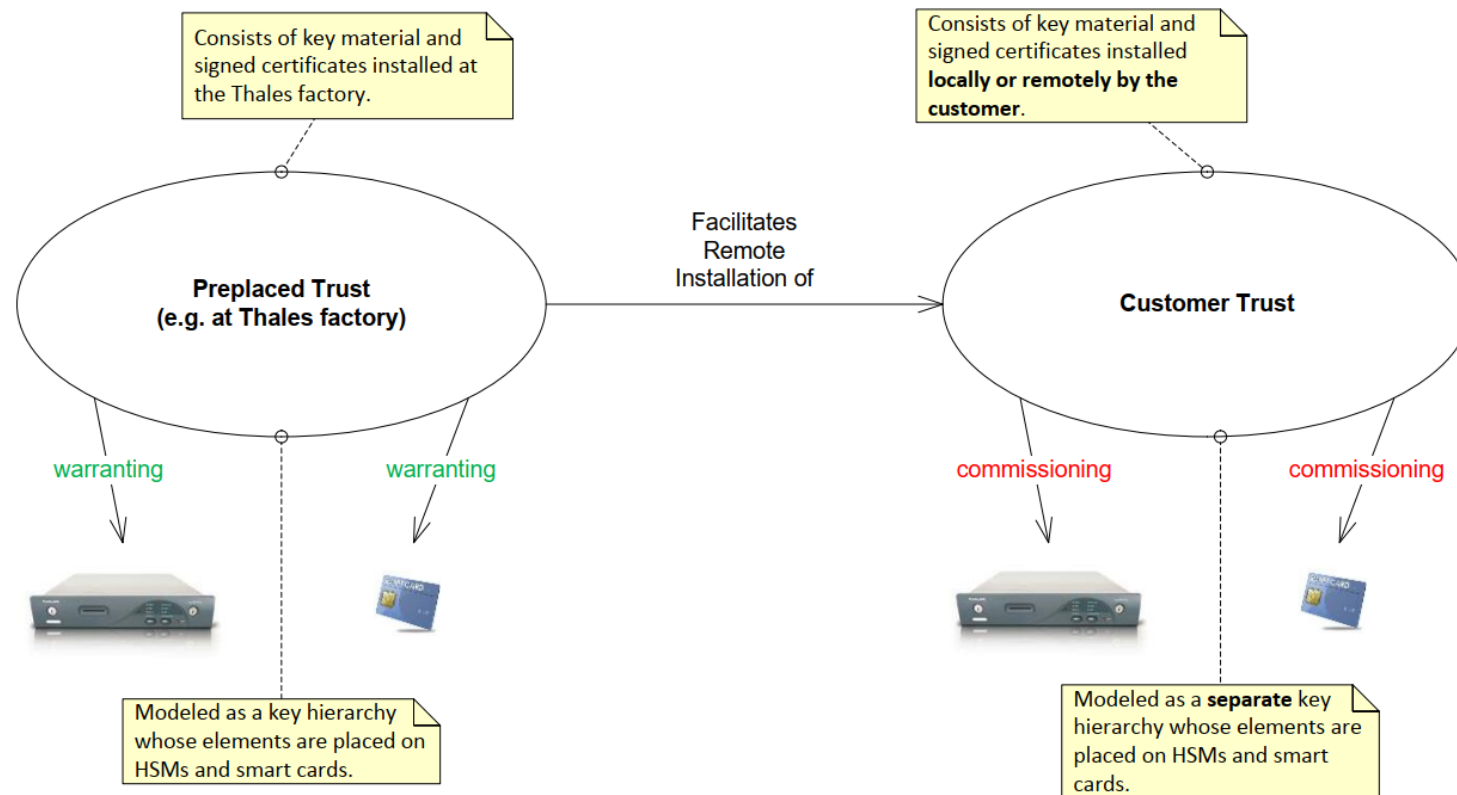
# Gestão Remota

O elemento chave do payShield Manager é que ele não necessita que suas atividades sejam executadas diretamente no HSM. Ao invés disso, a gerência pode ser efetuada usando uma conexão via web-browser comum ao HSM sob uma rede TCP/IP onde o HSM se localiza protegido pelo data center da organização, sob múltiplas camadas de segurança e controle de acesso.



# Modelo de confiança do payShield Manager

O payShield Manager opera num modelo de confiança que permite usuários configurar e operar o HSM. Este modelo de confiança se apoia em 2 hierarquias paralelas de chaves, *Domain Authority* e *Customer Trust Anchor*.





# | Domínio de Segurança

Um domínio de segurança é composto por:

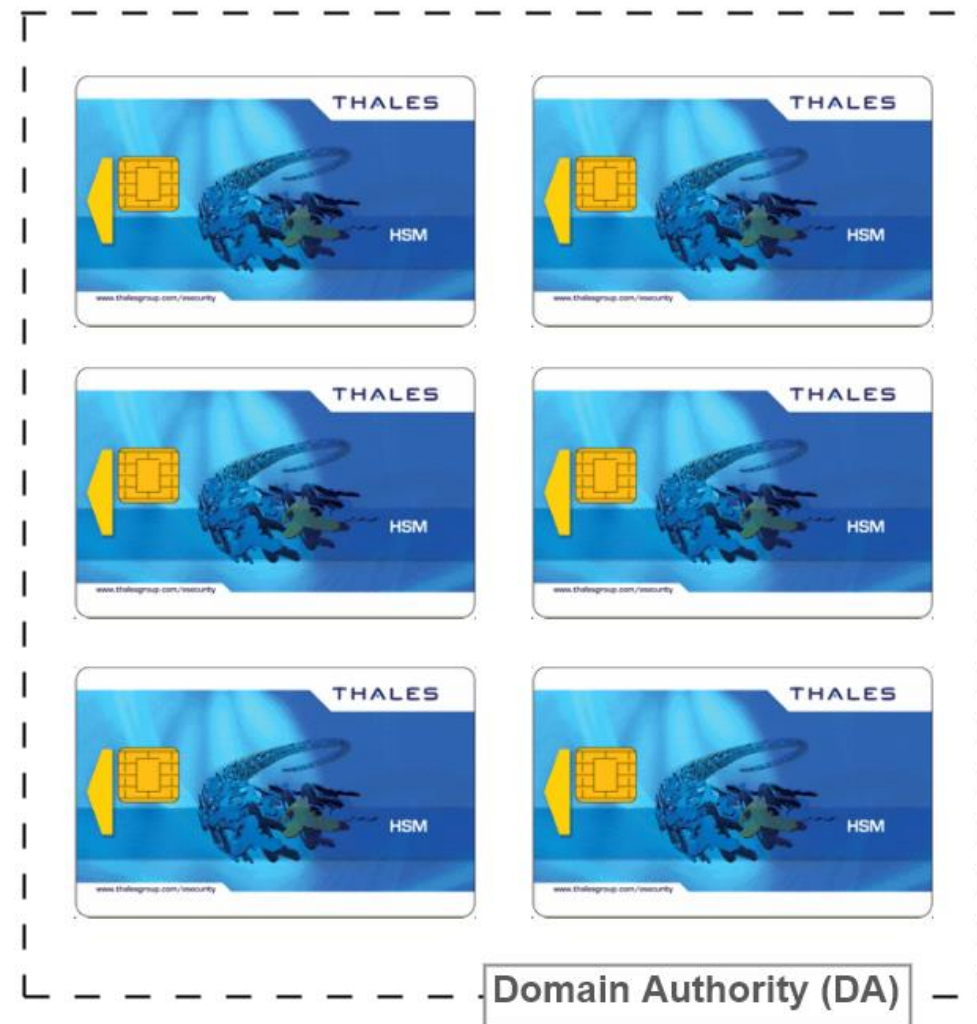
- Qualquer quantidade de payShield 9000 (com firmware v3.0b ou posterior)
- Conjunto de RACCs

As unidades de HSM e smartcards que formam o domínio de segurança identificam-se entre si por certificados (uma parte do CTA), mantidos em cada HSM e em cada smartcard.

# Domain Authority (DA)

Estes cartões funcionam como certificados e permitem a inclusão de mais equipamentos no domínio criptográfico operacional, ou seja, o domínio do payShield Manager.

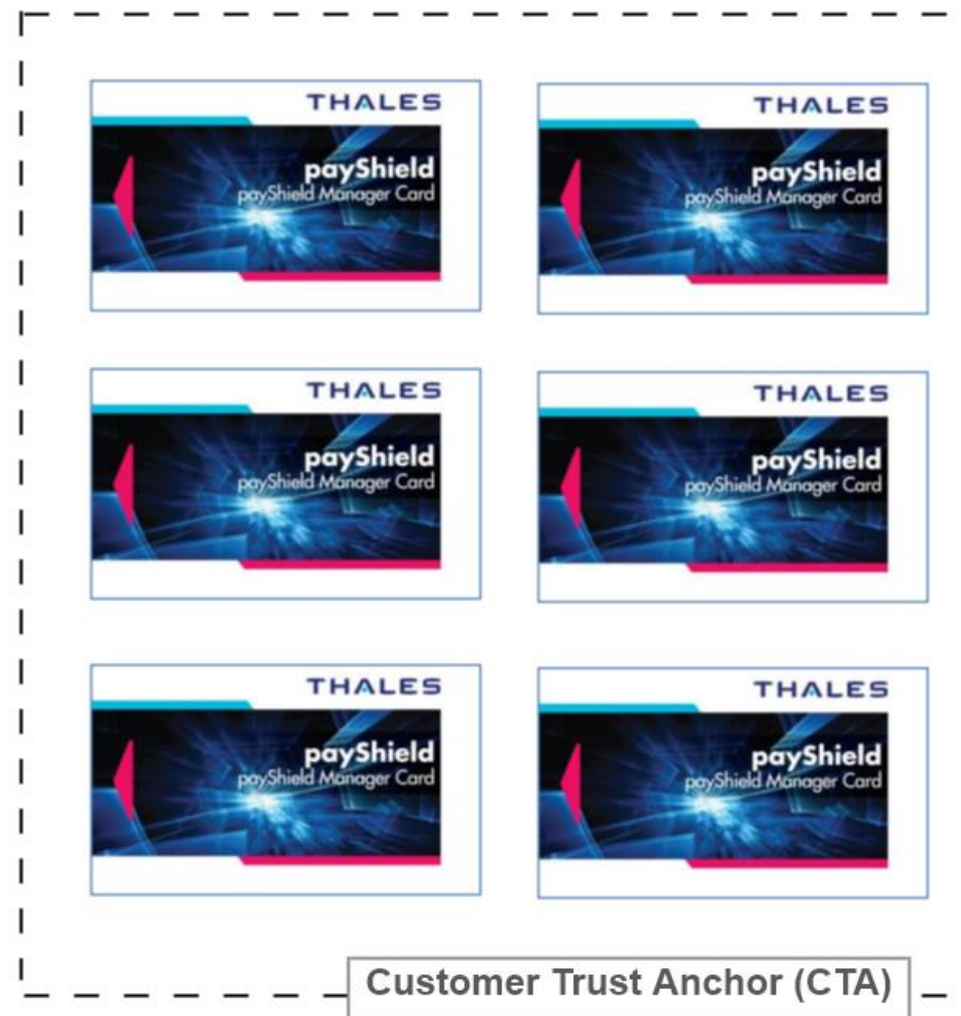
A política de controle destes cartões é “*m-de-n*”. São criados “*n*” cartões dos quais apenas “*m*” são necessários para recuperar o conteúdo armazenado compartilhado.



# Customer Trust Anchor (CTA)

Estes cartões também funcionam como certificados e permitem a inclusão de mais equipamentos e RACCs no domínio criptográfico operacional (domínio do payShield Manager) em conjunto com os cartões **DA**.

A política de controle destes cartões segue o mesmo processo do item anterior.



# Smartcards

Quando gerenciando o HSM usando o payShield Manager (local ou remotamente), as chaves físicas serão substituídas pelo Smartcards e seus respectivos PINs. Os Smartcards do payShield Manager são referidos como RACCs, *Remote Access Control Cards*.









# | Cartões de Acesso (RACCs)

Os cartões de acesso são criados durante o processo de inicialização do domínio criptográfico operacional e, após comissionados, permitem o acesso remoto nos equipamentos determinados. Existem 3 tipos de cartões de acesso:

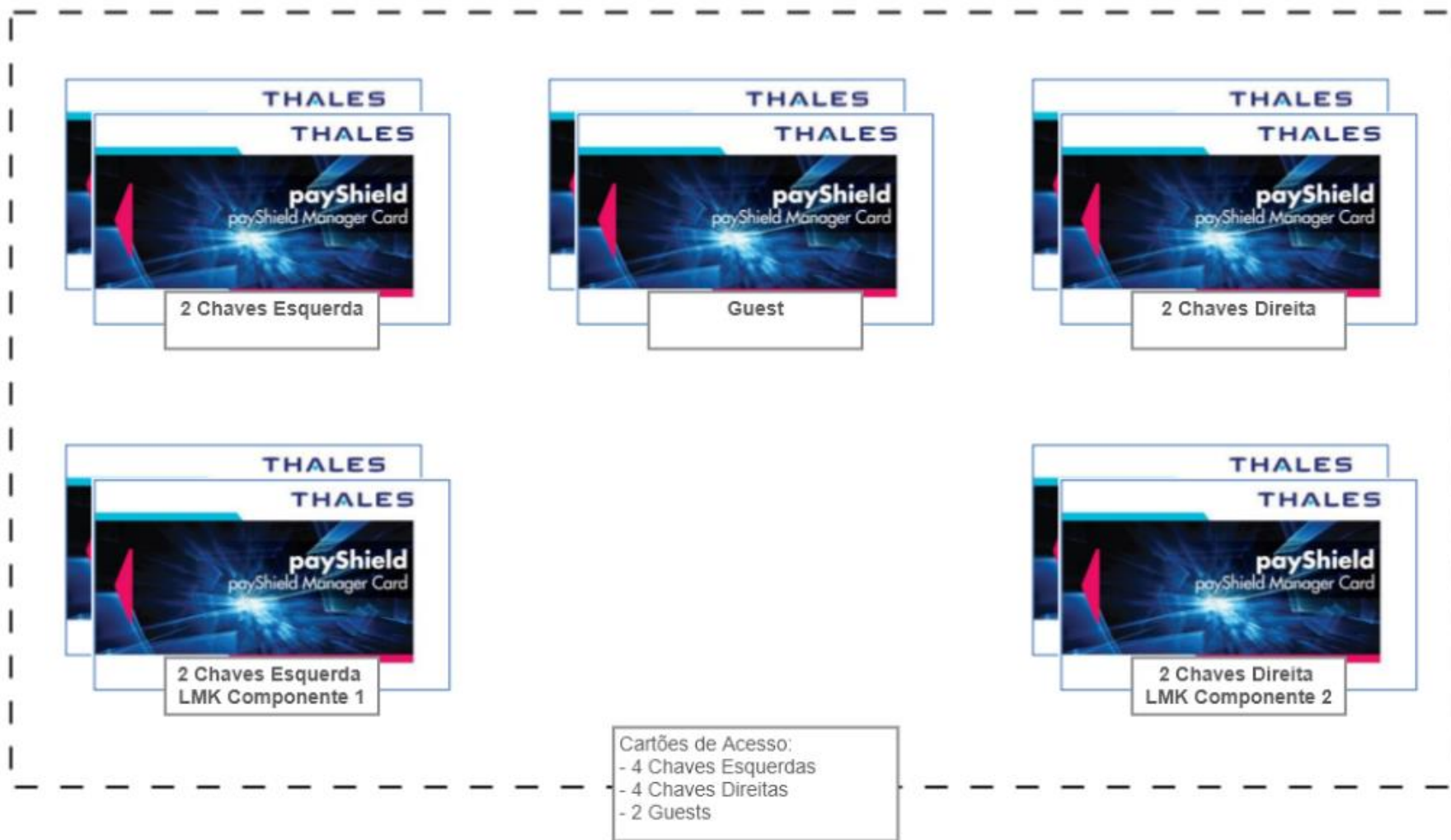
- Chave Esquerda (LK)
- Chave Direita (RK)
- Guest (G)

Além das funções inerentes estes cartões podem ser portadores de componente de LMK.

# Cartões de Acesso (RACCs)

| <br>Smartcard RACC Esquerdo         | <br>Smartcard RACC Direito      | <br>Smartcard (RLMK)  | <br>Smartcard (RACC Restrito)   |
|--|---|--|--|
| Um RACC Esquerdo substitui a chave física esquerda usada no HSM. Ela compreende as mesmas funções da chave esquerda. | Um RACC Direito substitui a chave física direita usada no HSM. Ela compreende as mesmas funções da chave direita. | Uma RLMK é usada substituindo os componentes da LMK usados no payShield 9000. Os cartões RLMK, como os dois RACCs, têm mecanismos de autenticação que os permitem ser usados com segurança em operações remotas. | O RACC restrito (Guest) permite que um usuário se conecte e visualize qualquer informação que pudesse ser visível pela console com o HSM no modo 'Online'. |

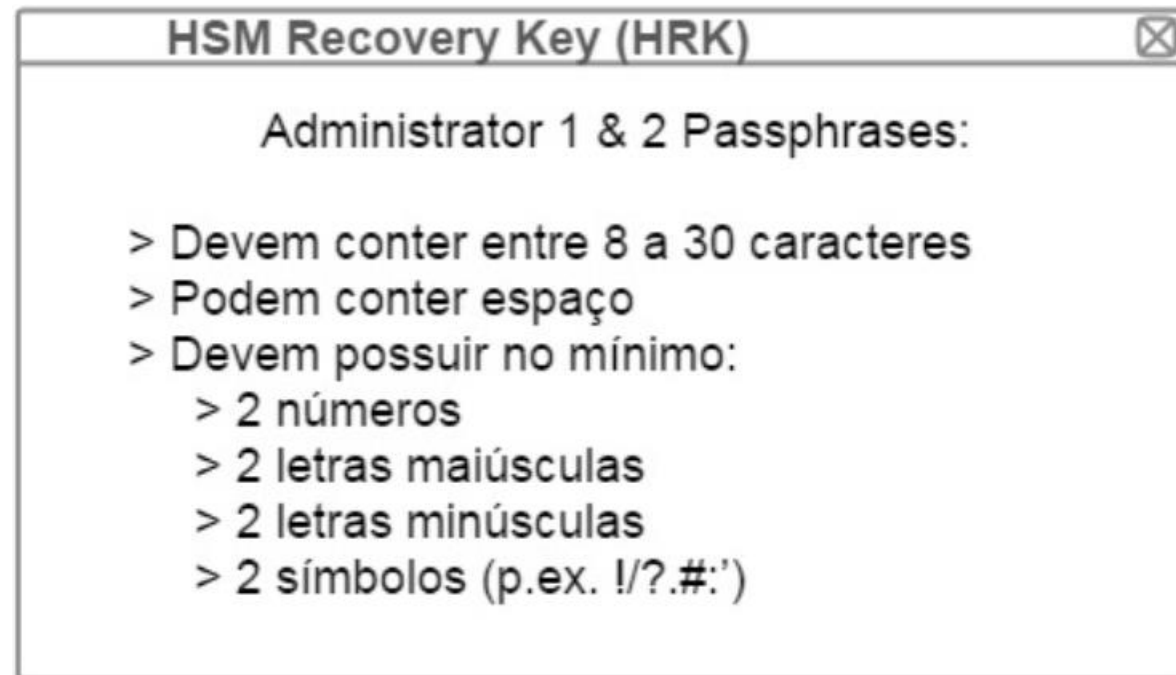
# Cartões de Acesso (RACCs)



# A Chave de Recuperação do HSM (HRK)

A HRK é usada para encriptar as chaves privadas do HSM usadas por ele no estabelecimento de sessões TLS/SSL com os hosts e interfaces de gerência.

A HRK é gerada pelo HSM usando 2 *passphrases* digitadas pelos *security officers*. Estas *passphrases* devem ser fornecidas para reconstituírem a HRK quando se está recuperando a chave privada após um evento de violação.





# Operação Local vs Remota

Quando acessando o HSM via payShield Manager a console local será desabilitada. Quando a sessão do payShield Manager finalizar a console local estará acessível.

Uma sessão de payShield Manager será terminada instantaneamente e a conexão local via console reestabelecida quando uma das chaves físicas for usada e alterar o estado de Online para qualquer outro estado, Offline ou Secure, no HSM.

# Acesso ao payShield Manager

O payShield 9000 é configurado por padrão para usar DHCP na porta de gerência. O nome de rede padrão da interface é “<serial number>-mgmt”. Por exemplo, se o serial number da unidade for A4665000014P, então o nome padrão seria A4665000014P-mgmt.

Pode-se usar o comando de console CM para configurar a porta de gerência e alterar o método de obtenção de endereço de IP e definir um endereço de IP que seja compatível com as definições internas de rede de sua organização (IP Fixo). Neste caso, o acesso se daria por https://<IP de gerência>

# Acesso ao payShield Manager

Dependendo da arquitetura de rede de seu ambiente, as portas de gerência podem estar protegidas por um firewall. Para usar o payShield Manager, deve-se permitir a comunicação pela porta HTTP segura (443 e opcionalmente a porta 80, caso não deseje digitar HTTPS em seu browser)

```
Secure> CM <Return>
```

```
Management Ethernet Port:
```

```
IP Configuration Method? [D]HCP or [S]tatic (DHCP): <Return>
```

```
Network Name (B46652712260-mgmt): HSM-Mngmnt <Return>
```

```
Enter speed setting for this port:
```

```
SPEED OPTIONS:
```

- 0 Autoselect
- 1 10BaseT half-duplex
- 2 10BaseT full-duplex
- 3 100BaseTX half-duplex
- 4 100BaseTX full-duplex
- 5 1000BaseT half-duplex
- 6 1000BaseT full-duplex

```
Speed setting (0): <Return>
```

```
Enable payShield Manager connection: <Return>
```

```
Enable or Disabled? (E): <Return>
```

```
Would you like to apply the changes now? [Y/N]: Y <Return>
```

# Acessando o payShield Manager

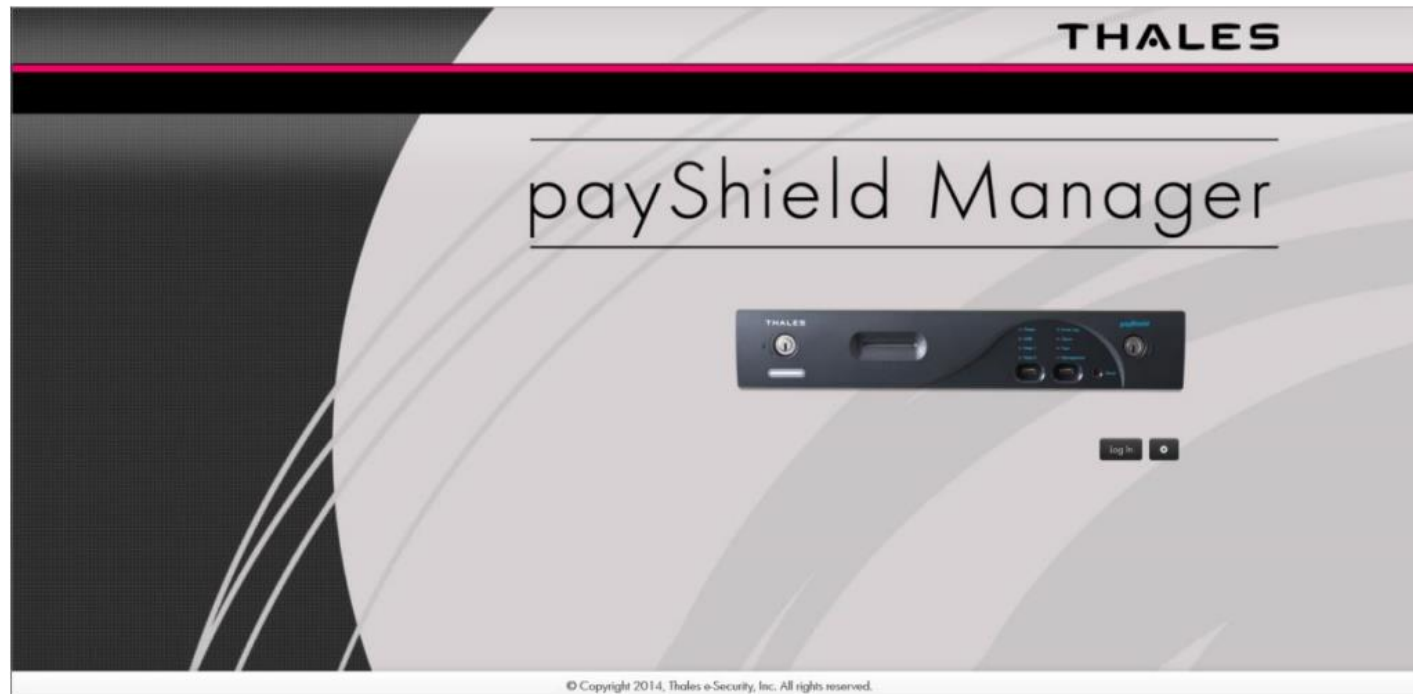
Conecte uma leitora de smartcards em uma das portas USB do computador e certifique-se de esteja funcionando corretamente, ou se uma leitora de smartcards embutida está sendo usada. Garanta também que o sistema operacional a reconheça.

Ao acessar o payShield Manager pelo browser e PC vigente pela primeira vez, será necessário fazer o download e instalação do plug-in para smartcards do browser. Este plug-in pode ser baixado diretamente do payShield.



# Acessando o payShield Manager

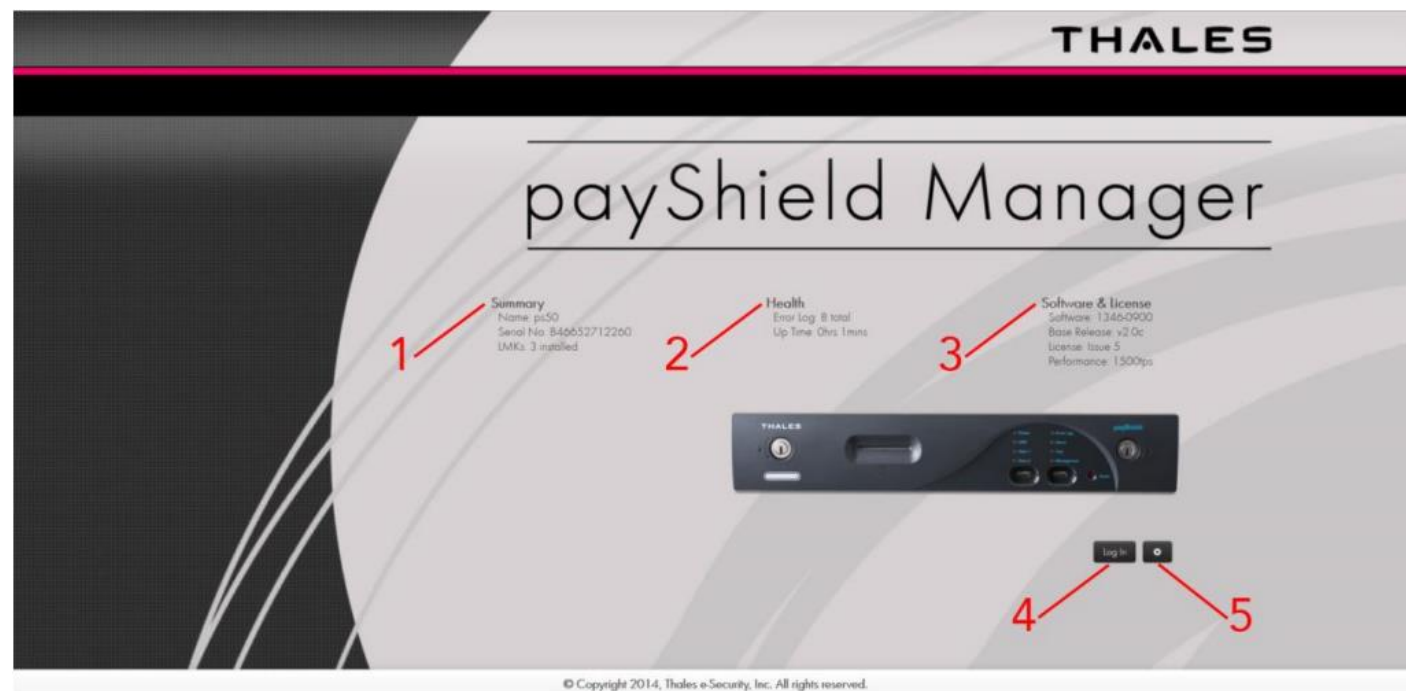
Para obter o plug-in, navegue até a página do payShield Manager e siga a ajuda exibida na tela após clicar no botão de login. Assim que o plug-in for instalado, é mandatório que se reinicie o browser.



# Acessando o payShield Manager

Se seu payShield está configurado para exibir informações gerais na Página Inicial, então as seguintes informações estarão disponíveis na Página Inicial:

1. *Summary Info*: Fornece algumas informações do equipamento em contato.
2. *Health*: Fornece a contagem dos logs de erro e o tempo de funcionamento do sistema.
3. *Software & License*: Informações da versão e realease do software



# Acessando o payShield Manager

Os botões e ferramentas mostrados a seguir são sempre exibidos na Página Inicial:

4. *Login*: Abre uma caixa de diálogo para a inserção do PIN e acessar o equipamento conectado.
5. *Tool Icon*: Permite a configuração da leitora de smartcards, o download do certificado TLS e a inspeção do smartcard.

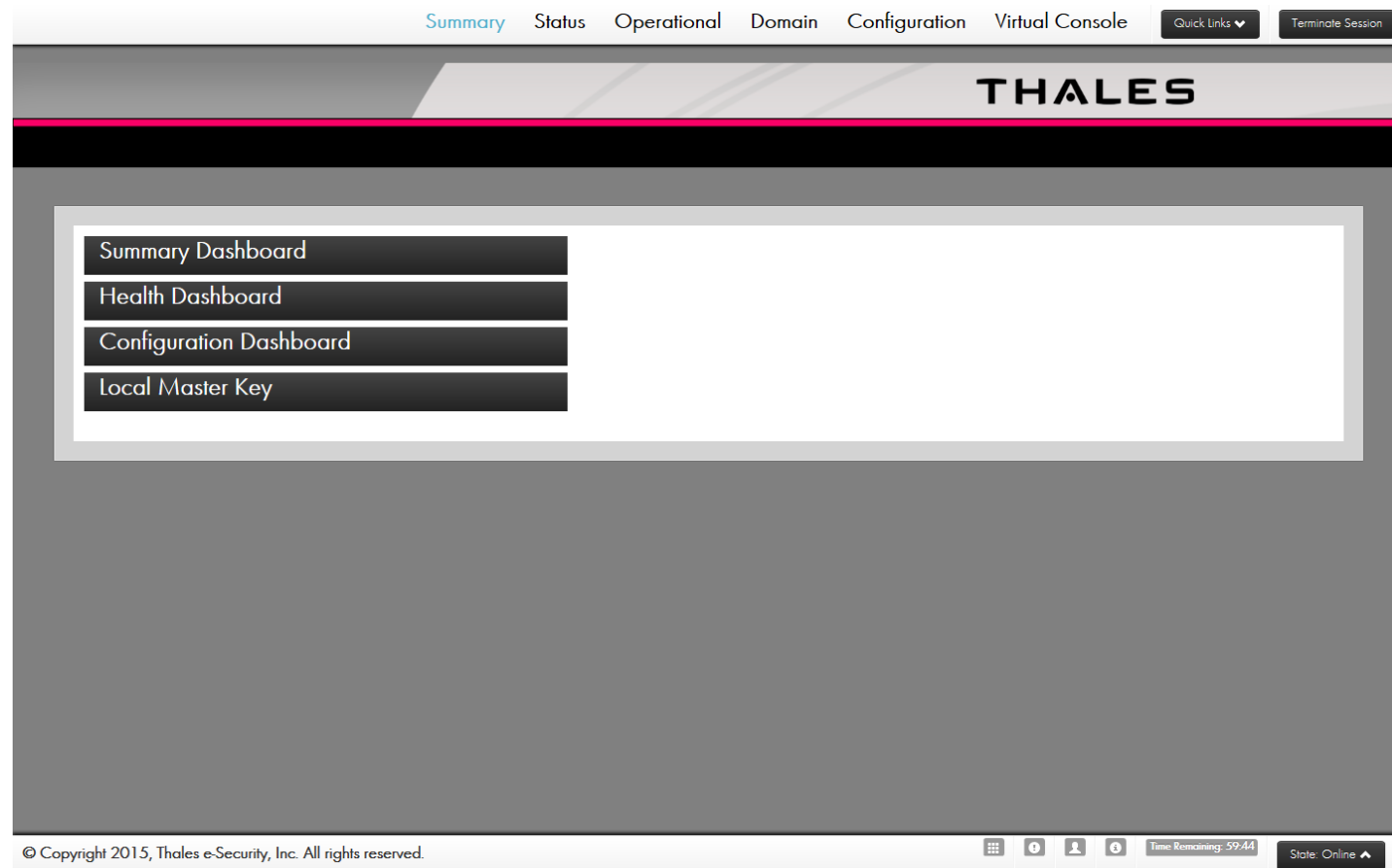


# Acessando o payShield Manager

Se o payShield já está comissionado, apenas insira o RACC esquerdo ou direito na leitora de smartcards e click no botão “Log in” e digite o PIN.

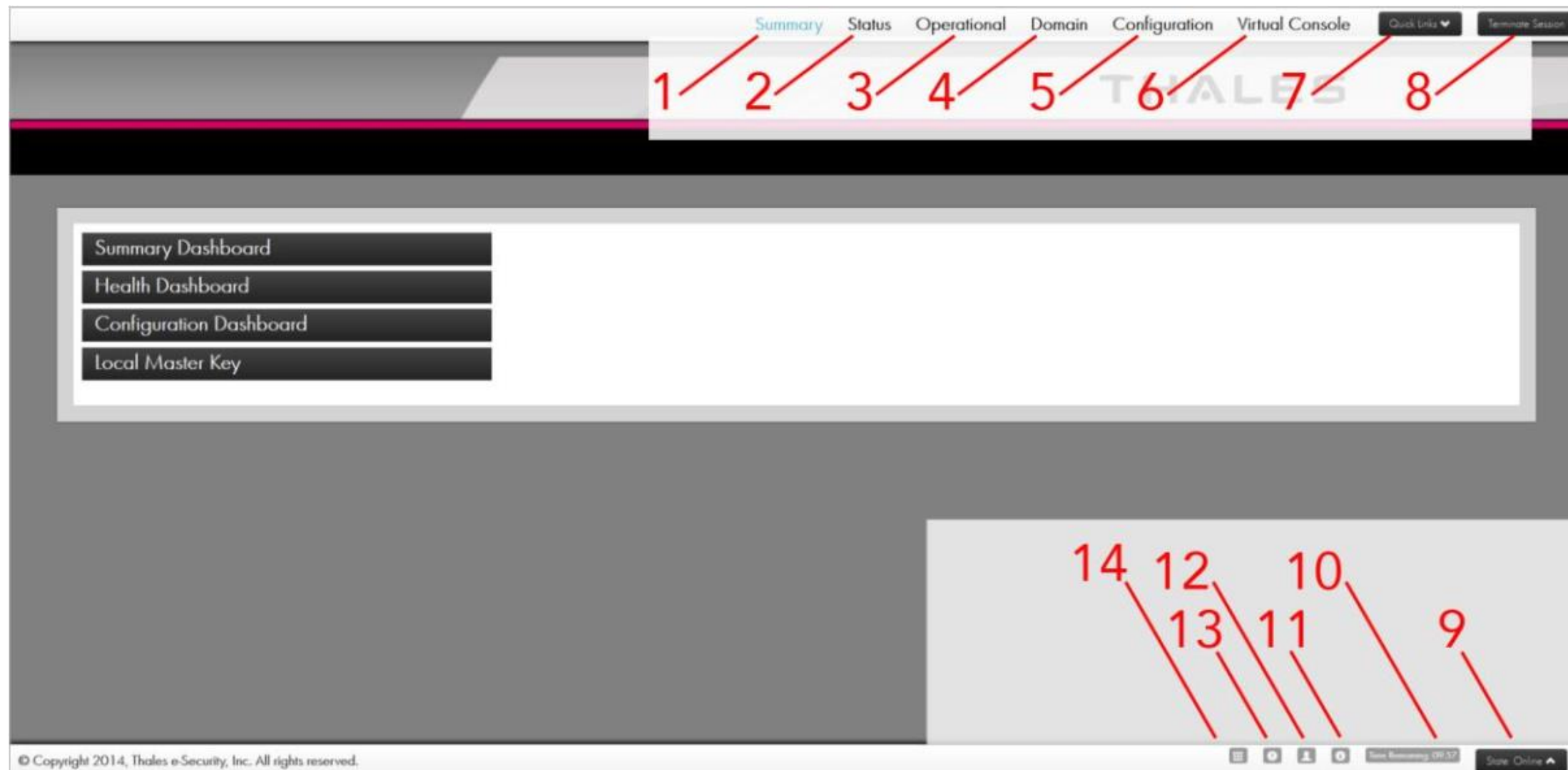
Se o PIN for correto o processo de autenticação se iniciará, o qual levará alguns segundos até ser completado.

Se a autenticação for feita com sucesso, a página principal do payShield Manager será exibida como se segue:





# Principais Funções



# | Principais Funções

## 1. Summary

Pressionando esta aba a página do payShield Manager disponibiliza as informações gerais do HSM resumidas.

## 2. Status

Ao pressionar, pode-se:

- Verificar informações detalhadas sobre a unidade
- Reinicializar o HSM
- Visualizar/Baixar/Resetar as estatísticas de utilização e configurar sua coleta
- Visualizar/Baixar/Resetar as estatísticas de saúde e configurar sua coleta
- Rodar diagnósticos e configurar a verificação automatizada
- Visualizar/Baixar os logs de erro e apagá-los
- Visualizar/Baixar os logs de auditoria e apagá-los
- Verificar os detalhes da versão do software
- Realizar o upgrade de firmware
- Verificar informações detalhas do licenciamento
- Verificar os detalhes dos algoritmos validados pela FIPS

# Principais Funções

## 3. Operational

Acessar esta aba permite que se realize as seguintes funções:

- Para cada LMK individualmente:
  - Substituir uma LMK
  - Deletar uma LMK
  - Definir a LMK como default
  - Definir a LMK como default de gerência
  - Habilitar as atividades autorizadas
- Para cada LMK no slot de transição
  - Substituir uma LMK
  - Deletar uma LMK
- Verificar os componentes de LMK nos smartcards
- Criar cartões autorizadores
- Duplicar componentes de LMK
- Gerar LMKs
- Instalar LMKs
- Instalar LMKs nos slots de transição

# | Principais Funções

## 4. Domain

Esta aba permite-se que:

- Visualize e gerencie os grupos de smartcard do payShield manager na whitelist
- Visualize e gerencie o domínio criptográfico operacional
  - Ver a cadeia de certificados e seus parâmetros
  - Comissionar um smartcard para o domínio
  - Descomissionar um smartcard
  - Copiar um smartcard do domínio
  - Criar um novo conjunto de CTA
- Alterar as passphrases da HRK



# Principais Funções

## 5. Configuration

Nesta aba pode-se:

- Visualizar e gerenciar as configurações das portas de host do HSM, incluindo:
  - Definir o tamanho do cabeçalho das mensagens de host
  - Definir e configurar os tipos de interface
  - Definir IP, ACL, TCP/UDP e TLS para as portas ethernet
- Visualizar e gerenciar as configurações da interface de console
- Visualizar e gerenciar as configurações de segurança
- Visualizar e gerenciar as configurações da porta de gerência:
  - IP
  - Timeouts
  - Ver o certificado TLS
- Ver e selecionar os formatos de PIN Block que o HSM pode processar
- Ver e gerenciar as configurações de alarme
- Ver e definir a data e hora do HSM
- Ver e definir nome e descrição para o HSM
- Definir as operações de auditoria e seus contadores
- Selecionar os comandos de console, host e gerência a serem auditados
- Ver e definir as configurações de SNMP
- Resetar o HSM para as configurações de fábrica

# | Principais Funções

## 6. Virtual Console

Esta aba simula a interface de console, os comandos de console funcionam da mesma forma, exceto os que exigem o uso da leitora de cartões integrada à unidade.

## 7. Quick Links

Fornece um atalho para as configurações das interfaces de host, configuração de segurança, configuração de salvamento e carregamento e operação com a LMK.

## 8. Terminate Session

Ao pressionar este botão a sessão com o payShield Manager será finalizada.

# | Principais Funções

## 9. State

Controla os estados do HSM: Offline/Online/Secure. A alteração dos estados é permitida mediante usuários logados, onde cada usuário é representado por um respectivo RACC. Se apenas um RACC, esquerdo ou direito, estiver conectado no HSM, então os únicos estados possíveis são Online ou Offline. Se, ao menos, um RACC esquerdo e um RACC direito estiverem conectados, então os 3 estados disponíveis podem ser habilitados.

## 10. Time remaining

Exibe a quantidade de tempo restante antes da finalização automática da sessão.

## 11. Information

Ao pressionar este botão, o payShield Manager exibe informações gerais da unidade

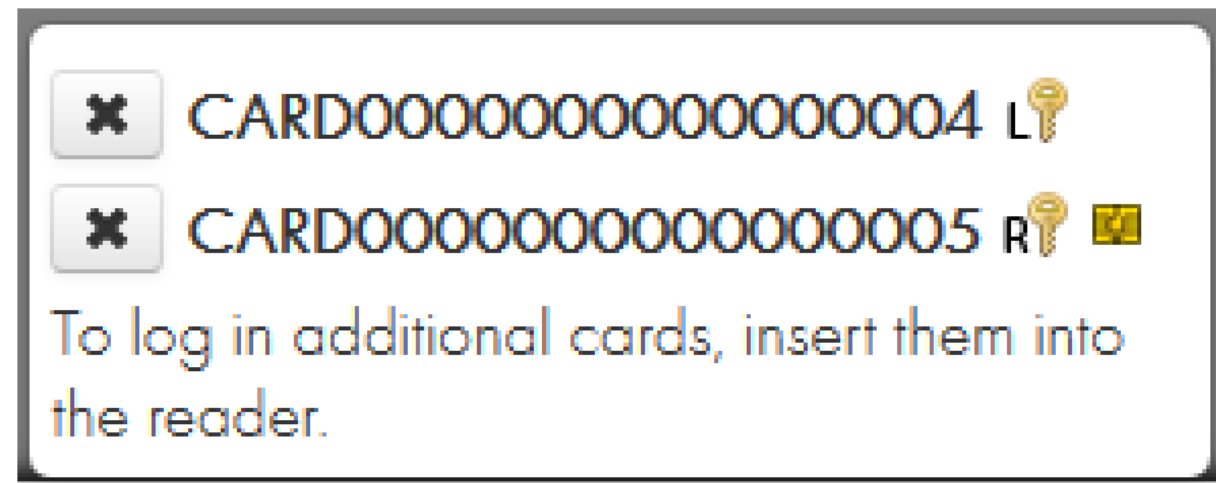
- Serial Number do payShield
- Versão de software
- Status da unidade de alimentação (PSU)

# Principais Funções

## 12. User

Este botão, pressionado, exibe informações dos usuários (smartcards) logados na unidade, ao pressionar o botão “X” próximo ao serial number do smartcard exibido, a sessão deste usuário é finalizada.

As letras “L” e “R” à frente do serial number indicam se o cartão é uma chave esquerda ou se é uma chave direita. Já o símbolo de chip indica que este é o atual cartão inserido na leitora de smartcards.



# | Principais Funções

## 13. Status

Ao pressionar este botão o payShield Manager exibe o número de logs de erro e auditoria, o uptime do sistema e o número de LMKs instalada.

## 14. Smartcard Operations

Ao pressionar este botão o payShield Manager permite a uso de utilitários para smartcards como mudança de PIN e inspeção do smartcard.



# ***FIRST TECH***®

Construindo relações duradouras

[www.first-tech.com](http://www.first-tech.com)

**MATRIZ – SP**

AV. ANGÉLICA, 2248 – 4º ANDAR SÃO PAULO

**(11)3024-3200**

**FILIAL – RJ**

RUA DA QUITANDA, 60 – 12º ANDAR RIO DE JANEIRO

**(21) 3543-1650**