

**payShield Manager**

Arquitetura de Smartcards

Getnet

|  |  |  |  |
| --- | --- | --- | --- |
| Processo: |  | Versão: | 1.1 |
| Autor: | Eduardo Mendes Campos | Data: | 29/10/2019 |
| Revisor: | Geovanne de Oliveira Souza | Data: | 30/10/2019 |
| Revisor: | Caio Abreu Ferreira | Data: | 01/11/2019 |
| Aprovador: |  | Data: |  |

Índice

[1. Introdução 4](#_Toc23500609)

[2. Sobre o gerenciamento remoto 4](#_Toc23500610)

[3. Modelo de confiança do payShield Manager 6](#_Toc23500611)

[4. Estados do HSM payShield 9000 7](#_Toc23500612)

[5. Domínio de Segurança 7](#_Toc23500613)

[6. A Chave de Recuperação do HSM (HRK) 7](#_Toc23500614)

[7. Contenção entre operações Locais e Remotas 8](#_Toc23500615)

[8. Acesso via payShield Manager 8](#_Toc23500616)

[9. Preparando-se para usar a Aplicação 8](#_Toc23500617)

[10. Conexão com o HSM 9](#_Toc23500618)

[11. Arquitetura de Cartões - Getnet 11](#_Toc23500619)

[11.1. Quantidade de cartões 11](#_Toc23500620)

[11.2. Domain Authority (DA) 11](#_Toc23500621)

[11.3. Customer Trust Anchor (CTA) 12](#_Toc23500622)

[11.4. Cartões de Acesso 13](#_Toc23500623)

[11.4.1. Whitelist 14](#_Toc23500624)

[11.5. Processo de implantação - Getnet 14](#_Toc23500625)

[12. Carregamento Remoto da LMK 15](#_Toc23500626)

[12.1. LMK 16](#_Toc23500627)

# Introdução

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

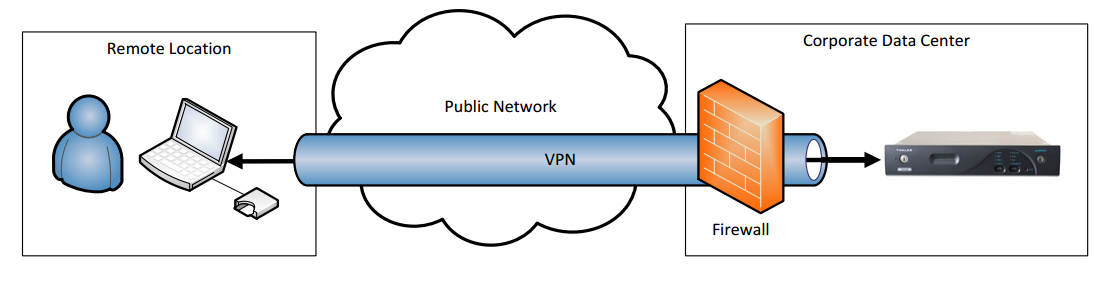
Usando um PC comum com web-browsers padrões de mercado, um usuário pode se conectar ao HSM via HTTP(S) através de um endereço IP ou FQDN. O payShield Manager proporciona uma conexão autenticada e segura permitindo uma completa console remota.

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.

# Sobre o gerenciamento remoto

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.



Quando gerenciando o HSM usando o payShield Manager (local ou remotamente), as chaves físicas serão substituídas pelo Smartcards e seus respectivos PINs. Estes Smartcards serão inseridos em leitoras remotas para ações tais como ganhar acesso ao HSM, mudar o estado do HSM e gerenciar LMKs. Os Smartcards do payShield Manager são referidos como RACCs, Remote Access Control Cards.

No payShield Manager apenas um tipo de smartcard é usado, como mostrado a seguir:



Frente do Smartcard payShield Manager Parte de trás do Smartcard payShield Manager

Os Smartcards do payShield Manager são utilizados da seguinte forma:

|  |  |  |  |
| --- | --- | --- | --- |
| Smartcard RACC Esquerdo | Smartcard RACC Direito | Smartcard (RLMK) | 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 permite que um usuário se conecte e visualize qualquer informação que pudesse ser visível pela console com o HSM no modo ‘Online’. |

Esta disposição permite que todas as atividades do HSM sejam realizadas remotamente enquanto o HSM está armazenado em um local seguro.

**Notas**:

* O payShield Manager pode ser conectado apenas se o HSM estiver estabelecido no estado de Online.
* Apenas uma conexão de payShield Manager por vez é possível. Gerenciamento por múltiplas sessões não está disponível.

# 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. A primeira hierarquia de chaves consiste em materiais de chaves e certificados assinados instalados na fábrica da Thales. A segunda hierarquia consiste em certificados assinados e instalados local ou remotamente pelo cliente.

A coleção de certificados assinados da segunda hierarquia é chamada de CTA, *Customer Trust Anchor* (Âncora de Confiança do Cliente)

Facilita a instalação remota de

Consiste em certificados assinados e instalados local ou remotamente pelo cliente

Modelado como uma hirerarquia de chaves separada onde os elementos são dispostos em HSMs e smartcards.

Comissionamento

Comissionamento

Garantia

Garantia

Modelado como uma hirerarquia de chaves onde os elementos são dispostos em HSMs e smartcards.

Consiste em materiais de chaves e certificados assinados instalados na fábrica da Thales

A “Confiança Pré Depositada” é usada apenas para facilitar a segurança e autenticação durante o carregamento da “Confiança do Cliente” em um ambiente remoto. Assim que a Confiança do Cliente é instalada em um HSM, este é considerado comissionado e as operações de gerência podem ser utilizadas.

# Estados do HSM payShield 9000

O HSM pode estar nos seguintes estados no que diz respeito ao material de chaves gerenciais:

* Garantido: O payShield 9000 tem apenas a confiança pré depositada instalada. Este é o estado padrão de fábrica. A unidade irá retornar a este estado quando detectar uma violação.
* Comissionado: O payShield 9000 possui a confiança do cliente. O cliente depositou elementos de confiança no HSM.

Violação

Descomissionando HSM

Comissionando HSM

Comissionado

Garantido

# Domínio de Segurança

Um domínio de segurança é composto por:

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

A 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.

# 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 chave privada encriptada pela HRK é mantida fora da memória protegida de violações para o caso de o HSM detectar um evento de violação, ela não seja perdida: a chave privada não encriptada é usada em produção e é armazenada na memória na protegida por violações e será perdida no caso de o HSM detectar um evento de violação.

Portanto, a chave privada pode ser recuperada após um evento de violação, assim que a HRK é instalada, ao decriptar a versão encriptada da chave privada.

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. A chave privada é mantida em uma memória protegida de violações para que seja automaticamente apagada caso o HSM detecte uma tentativa de violação.

# Contenção entre operações Locais e Remotas

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 via 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.

Se está configurando os browsers a direcionarem o tráfego através de um proxy, garanta que o item “Usar este servidor proxy para todos os protocolos” seja selecionado. No Internet Explorer e Firefox, esta caixa de seleção deve ser selecionada. Se esta ação não for feita, então a página da web será exibida, mas o login não poderá ser efetuado.

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).

# Preparando-se para usar a Aplicação

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.

Se a leitora de smartcards possuir um PIN-pad integrado, talvez seja necessário instalar os drivers do software em seu PC para que este reconheça a leitora como um equipamento que suporte “Secure PIN Entry”, inserção segura de PIN.

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.

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.

O plug-in também está disponível no CD de software do payShield.



# Conexão com o HSM

Para acessar o payShield, abra o browser e digite “https://” seguido pelo nome DNS ou endereço de IP configurado, por exemplo, “https://A4665000014P-mgmt”. As imagens mostradas abaixo exibem as possibilidades de página dependendo das configurações de seu payShield. Estas páginas são chamadas de “Landing Page”, Página Inicial.

**Nota**:

* Recarregar a página inicial pode reparar a maioria dos problemas de conectividade da página inicial. Entretanto, ao passo que o usuário estiver logado, recarregar qualquer página além do login irá terminar a sessão e o usuário será requisitado a logar novamente.

Por exemplo: suponhamos que as comunicações da porta de host do payShield estejam nos estados off-line ou secure e o usuário tenha tentado se conectar ao payShield usando o payShield Manager e o browser é deixado aberto na Página Inicial. O usuário então gira as chaves físicas para o estado de online. Antes de tentar se logar, o usuário deve primeiro recarregar a Página Inicial e então realizar a operação de login.



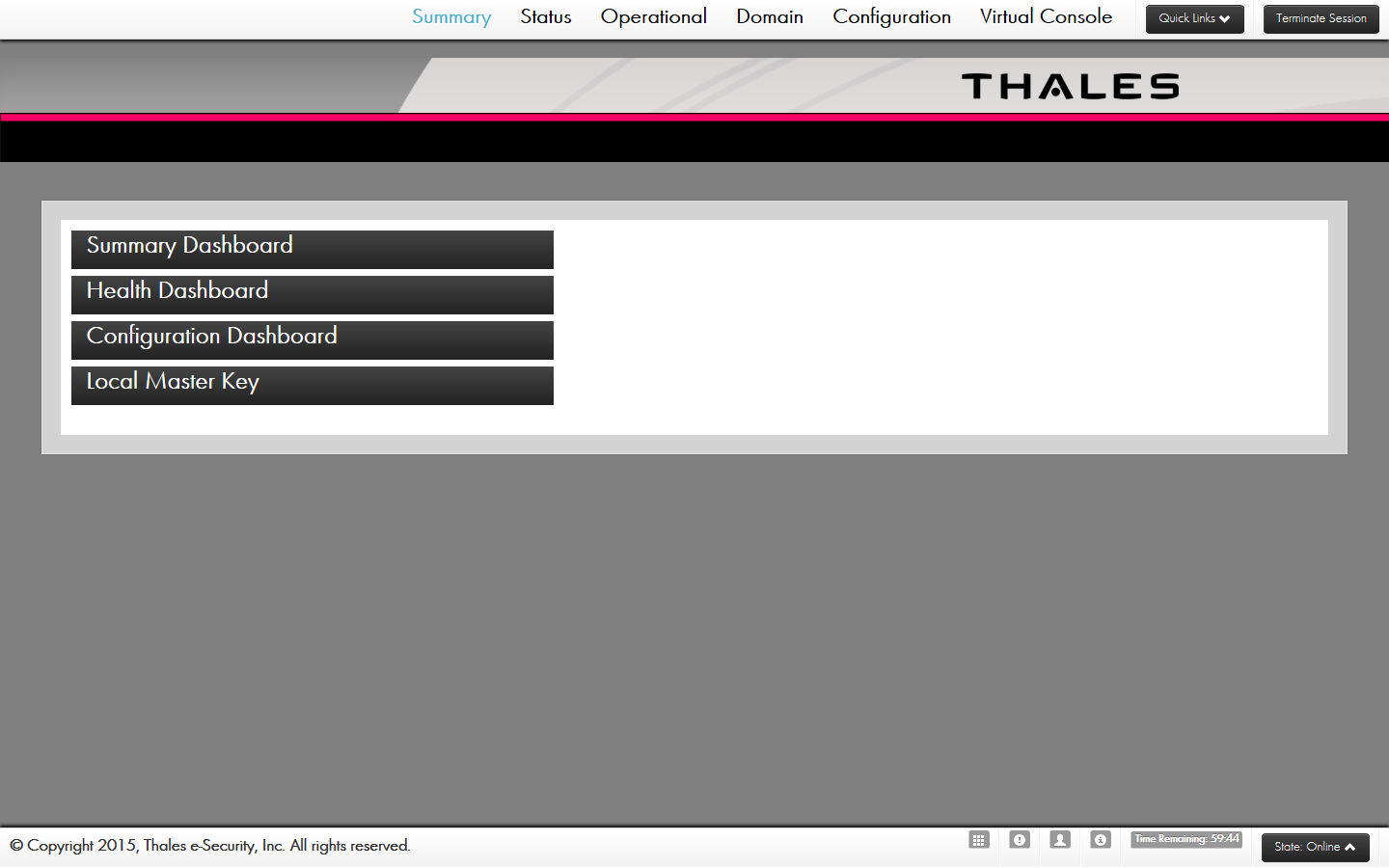
Se seu payShield está configurado para exibir informações gerais na Página Inicial, então as seguintes informações estarão disponíveis na Página Inicial:

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

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

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

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:



# Arquitetura de Cartões - Getnet

A arquitetura de cartões aqui apresentada visa a segmentação de funções bem como a hierarquização das permissões de uso do equipamento.

## Quantidade de cartões

Cada unidade de payShield 9000 traz consigo um conjunto de 12 smartcards sendo 6 cartões para uso específico na leitora integrada no payShield e 6 cartões para payShield Manager para uso na leitora de cartões acoplada ao PC.

A Getnet possui 6 unidades que geram um total de 36 cartões de payShield Manager e 36 cartões de payShield HSM. Tal quantia permite a formação da seguinte distribuição:

* 6 cartões Domain Authority baseados em cartões payShield HSM
* 6 cartões CTA baseados em cartões payShield Manager
* 10 cartões de acesso baseados em cartões payShield Manager

## Domain Authority (DA)

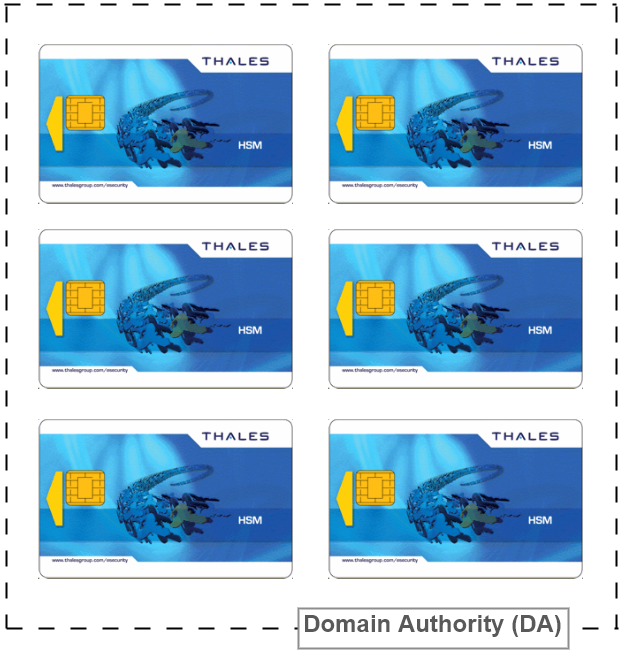
Serão utilizados seis cartões que compõe o grupo que representa a Confiança pré Depositada do fabricante. Estes cartões funcionam como certificados e permitem a inclusão de mais equipamentos no domínio criptográfico operacional, ou seja, o domínio do payShield Manager.

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.

O “*m-de-n”* a ser adotado na Getnet será:

* n = 6
* m = 3

Dos 6 cartões criados na inicialização quaisquer 3 podem ser usados durante o processo de comissionamento. A implementação *“m-de-n”* é uma alternativa à criação de cartões back-up.



## Customer Trust Anchor (CTA)

Serão utilizados seis cartões que compõe o grupo que representa a Confiança do Cliente. Estes cartões também funcionam como certificados e permitem a inclusão de mais equipamentos 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 11.2.

O “*m-de-n”* a ser adotado na Getnet será:

* n = 6
* m = 3

Dos 6 cartões criados na inicialização quaisquer 3 podem ser usados durante o processo de comissionamento. Os cartões **CTA** são também responsáveis pela inclusão dos cartões de acesso no domínio criptográfico operacional.



## Cartões de Acesso

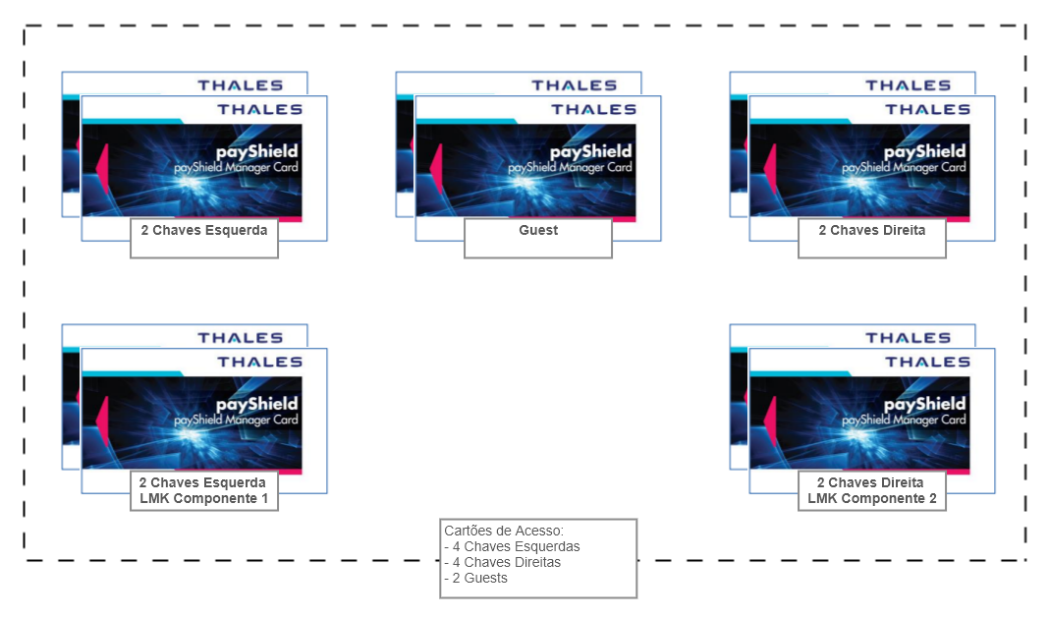
Os cartões de acesso são criados durante o processo de inicialização do domínio criptográfico operacional e, após comissionados, permitem o acesso remoto nos equipamentos determinados. Existem 3 tipos de cartões de acesso:

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

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

Para a Getnet os 10 cartões serão distribuídos da seguinte maneira:

* 4 cartões Chave Esquerda dos quais 2 possuem o componente 1 da LMK
* 4 cartões Chave Direita dos quais 2 possuem o componente 2 da LMK
* 2 cartões Guest

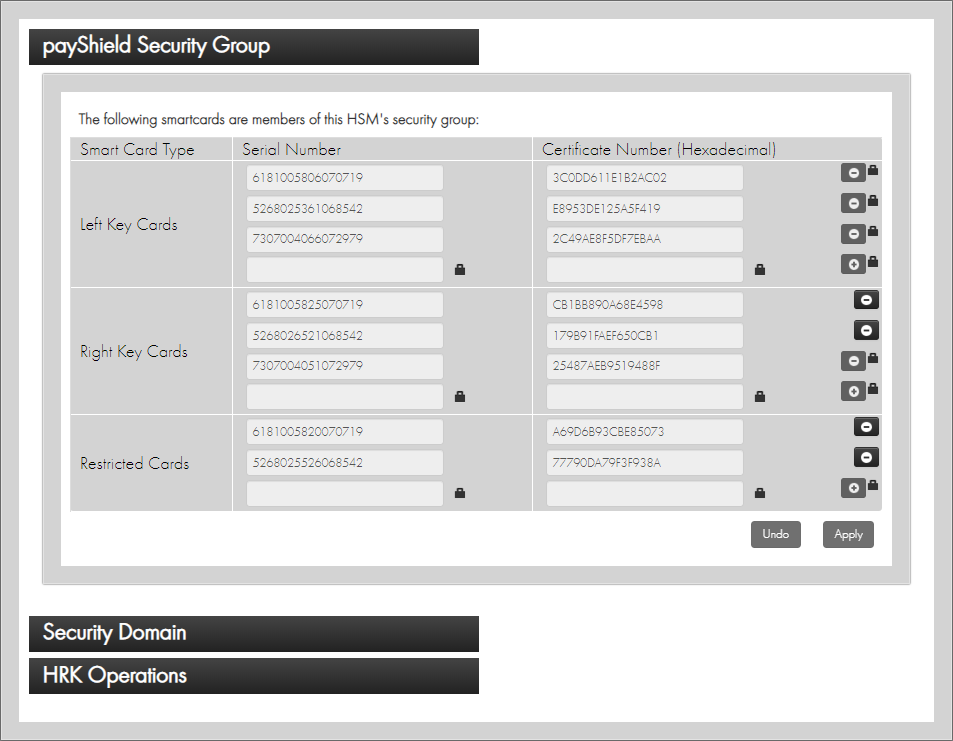


**Nota:**

* A LMK distribuída nestes cartões só pode ser carregada em HSMs que foram previamente comissionados por ambos os conjuntos DA e CTA. Além disso, o cartão de acesso usado deve ter sido previamente adicionado à *whitelist* do equipamento.

### Whitelist

A *whitelist* dos cartões de acesso é a lista que enumera e indica quais os cartões estão permitidos a acessar determinado equipamento.



Cada cartão tem seu próprio serial number e após comissionado recebe a numeração de certificado. O comissionamento dos cartões de acesso é feito pelo conjunto de cartões CTA.

Os cartões na *whitelist* podem ser removidos ou inseridos mediante a presença dos custódios dos cartões chave esquerda e chave direita colocando o HSM no modo Secure. Cada HSM tem sua própria *whitelist*, ou seja, cada uma deve ser configurada individualmente em cada equipamento.

## Processo de implantação - Getnet

Os HSMs da Getnet estão distribuídos em locais diferentes e distantes, isto torna a instalação mais sensível do que o usual. 5 HSMs estão localizados nos EUA tornando este local o primeiro a ser configurado. A configuração do payShield Manager e posterior instalação das LMKs seguirão os seguintes passos:

1. Definição prévia de ambas as *passphrases* da HRK
2. Definição prévia dos PINs dos Smartcards (DA, CTA e Cartões de Acesso)
3. Configuração da HRK
4. Criação dos cartões DA
5. Instalação dos cartões DA
6. Criação dos cartões CTA
7. Instalação dos cartões CTA
8. Criação dos cartões de Acesso
9. Adicionar os cartões de Acesso à *whitelist*
10. Testar Acesso

Os passos acima são executados apenas no primeiro HSM, as unidades subsequentes passam apenas pelos passos 3, 5, 7, 9 e 10.

**Nota:**

* Os passos acima não contemplam nenhuma interação com a LMK e não dependem dela ou de sua criação.

Após a configuração de todos os equipamentos no site EUA, todos os cartões retornam ao Brasil e serão utilizados para configurar a unidade restante como se segue:

1. Configuração da HRK
2. Instalação dos cartões DA
3. Instalação dos cartões CTA
4. Adicionar os cartões de Acesso à *whitelist* (apenas os que receberão LMK)
5. Carregar LMK nos Cartões de Acesso (2 LK e 2 RK) previamente definidos.

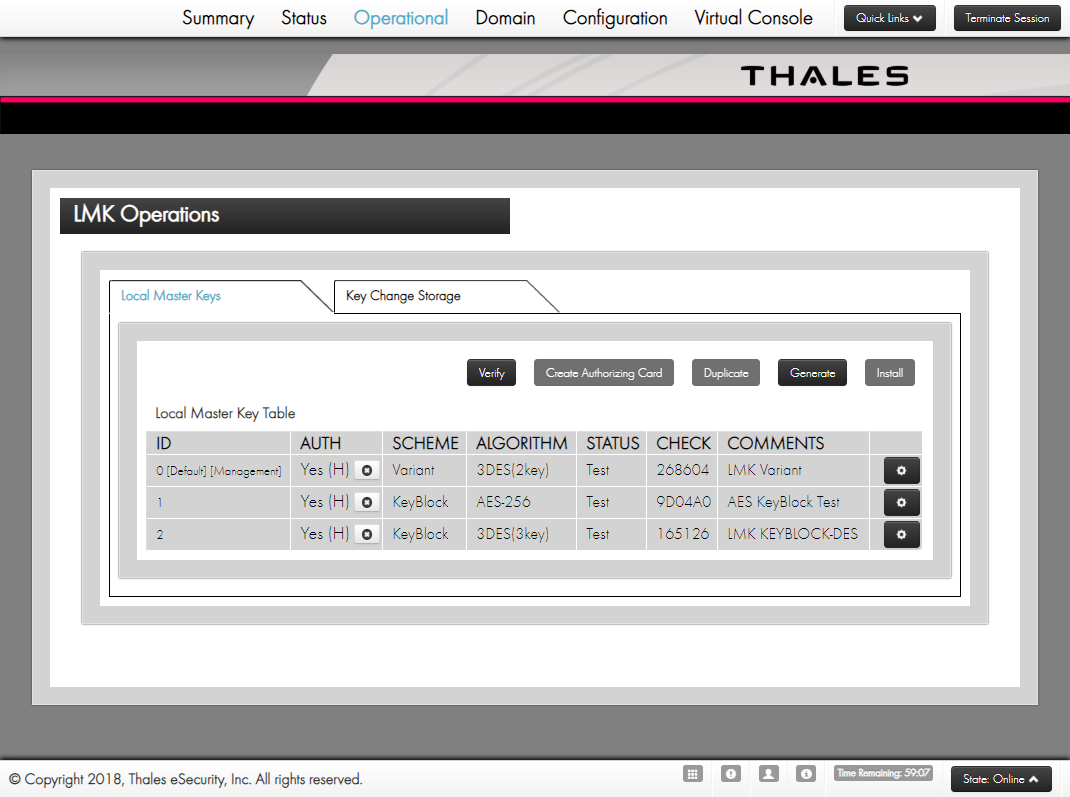
Desta maneira, todo o conjunto de cartões do domínio criptográfico operacional (domínio do payShield Manager) está criado e implementado.

**Nota:**

* O payShield da acima será utilizado para cerimonial de chaves em sala segura, portanto não haverá conexão remota no mesmo. Por este motivo, apenas o conjunto de Cartões de Acesso que recebe a LMK foi adicionado à sua *whitelist*.

# Carregamento Remoto da LMK

Para instalação remota da LMK deve-se reunir os custodiantes dos componentes da LMK remota (RLMK) com seus respectivos cartões (RK e LK) e proceder com o processo de instalação em cada HSM.



Ao final da instalação, a tabela acima exibirá a LMK instalada.

## LMK

Os componentes da LMK devem obedecer a políticas e processos para garantir a confiabilidade e segurança do domínio criptográfico transacional. Tais políticas e processos são herdados pelos componentes da RLMK, mesmo que estes tenham um nível de segurança intrínseco muito maior.

A execução dos procedimentos descritos neste documento permite que os custódios da LMK não tenham a necessidade de se deslocar aos sites onde os HSMs serão instalados. Sendo apenas convocados para a criação da LMK e posterior instalação nos Cartões de Acesso RLMK.

A função de custódio da LMK e RLMK pode ser atribuída a um mesmo indivíduo desde que se respeite a segmentação dos componentes e que este indivíduo não tenha acesso ao conjunto completo de componentes que formam a LMK.