

**payShield Manager**

Arquitetura de Smartcards

SUPERDIGITAL

Índice

[1. Arquitetura de Cartões - SUPERDIGITAL 2](#_Toc45264275)

[1.1. Quantidade de cartões 2](#_Toc45264276)

[1.2. Domain Authority (DA) 3](#_Toc45264277)

[1.3. Customer Trust Anchor (CTA) 3](#_Toc45264278)

[1.4. Cartões de Acesso 4](#_Toc45264279)

[1.4.1. Whitelist 5](#_Toc45264280)

[1.5. Processo de implantação - SUPERDIGITAL 6](#_Toc45264281)

[2. Carregamento Remoto da LMK 7](#_Toc45264282)

[3. Envio smartcards para os EUA. 7](#_Toc45264283)

[4. Procedimento para execução do Técnico da EQUINIX. 8](#_Toc45264284)

[4.1 . Pré requisitos – parte 1 8](#_Toc45264285)

[4.1.1. Roteiro 8](#_Toc45264286)

[4.2. Pré requisitos – parte 2 11](#_Toc45264287)

[4.2.1. Roteiro 11](#_Toc45264288)

[5. Release Note 13](#_Toc45264289)

# Arquitetura de Cartões - SUPERDIGITAL

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

## Quantidade de cartões

A SUPERDIGITAL possui conjunto de 12 smartcards sendo 6 cartões para uso específico na leitora integrada no payShield e 6 cartões de payShield Manager para uso na leitora de cartões acoplada ao PC.

Existem mais 7 cartões de payShield Manager da FIRST TECH que serão cedidos por empréstimo para SUPERDIGITAL para compor arquitetura planejada totalizando 19 cartões de payShield Manager e 6 cartões payShield HSM.

Tal quantia permite a formação da seguinte distribuição:

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

## Domain Authority (DA)

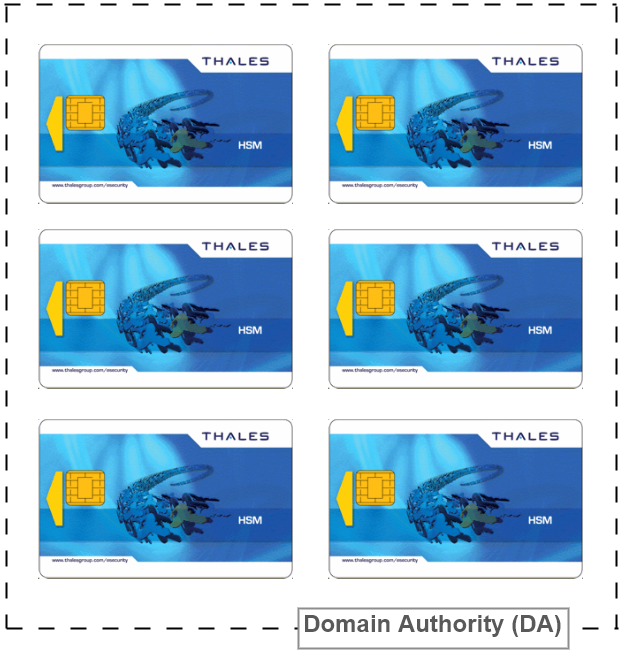
Serão utilizados seis cartões que compõe o grupo que representa a Confiança pré Depositada do fabricante. Estes cartões funcionam como certificados e permitem a inclusão de mais equipamentos no domínio criptográfico operacional, ou seja, o domínio do payShield Manager.

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 SUPERDIGITAL será:

* n = 6
* m = 3

Dos 6 cartões criados na inicialização quaisquer 3 podem ser EUAdos 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 1.2.

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

* n = 9
* m = 3

Dos 9 cartões criados na inicialização quaisquer 3 podem ser EUAdos durante o processo de comissionamento. Os cartões **CTA** são também responsáveis pela inclusão dos cartões de acesso no domínio criptográfico operacional.



## Cartões de Acesso

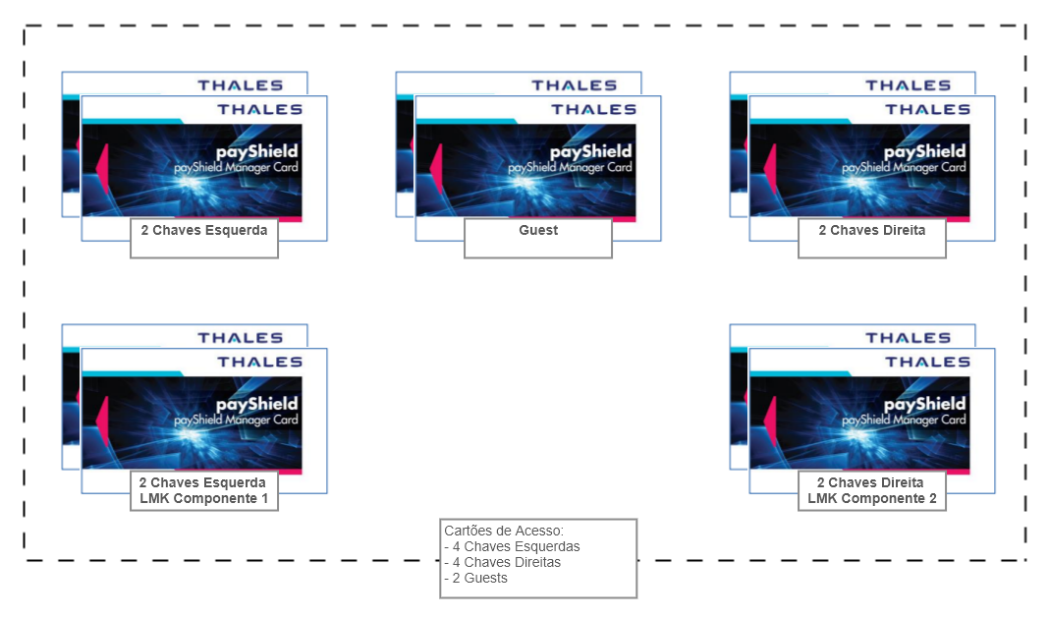
Os cartões de acesso são criados durante o processo de inicialização do domínio criptográfico operacional e, após comissionados, permitem o acesso remoto nos equipamentos determinados. Existem 3 tipos de cartões de acesso:

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

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

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

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

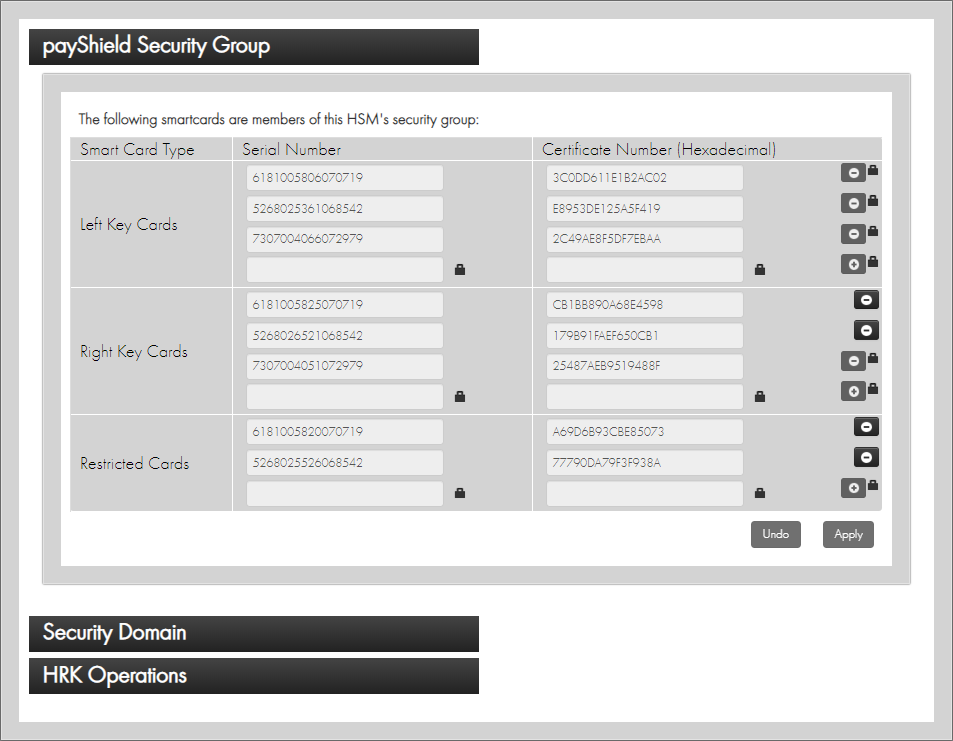


**Nota:**

* A LMK distribuída nestes cartões só pode ser carregada em HSMs 9K que foram previamente comissionados por ambos os conjuntos DA e CTA. Para os HSMs 10k não é necessário o uso dos cartões de DA. 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 - SUPERDIGITAL

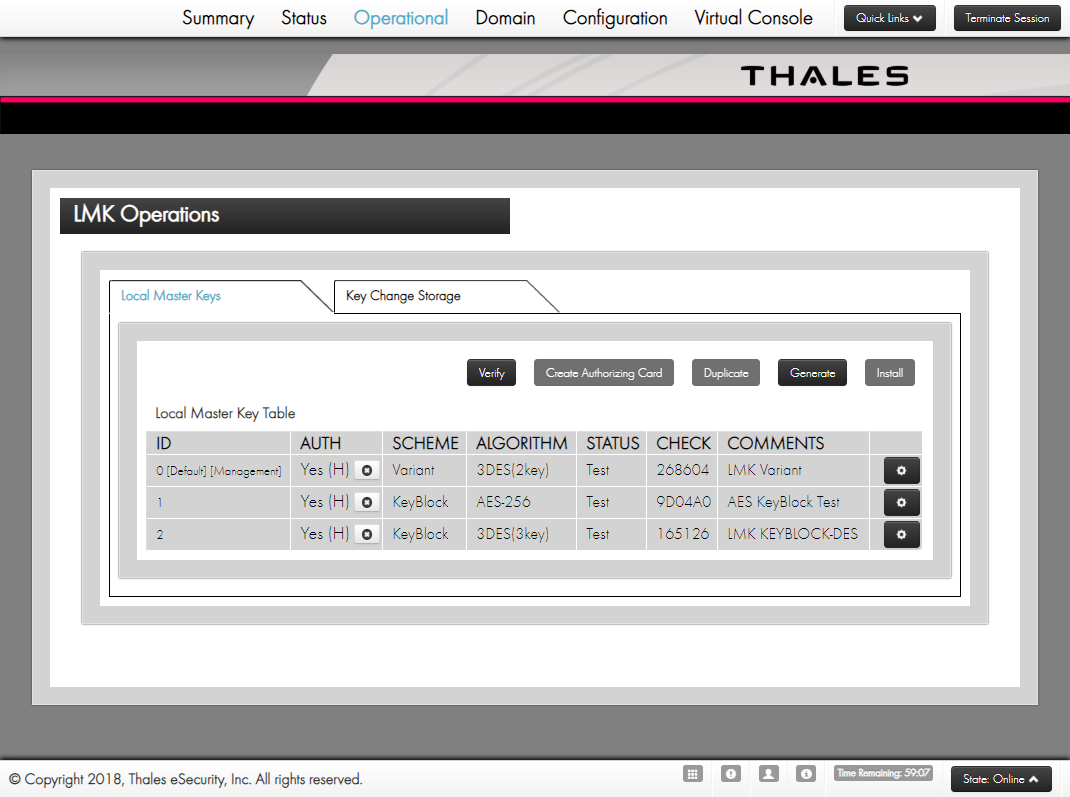
Os HSMs da SUPERDIGITAL estão distribuídos em locais diferentes e distantes, isto torna a instalação mais sensível do que a usual. 4 HSMs estão localizados nos EUA tornando este local o segundo local a ser configurado. A configuração do payShield Manager e posterior instalação das LMKs seguirão os seguintes passos:

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

Os passos 3, 7 e 9 do processo de implantação serão repetidos nos EUA.

# 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.

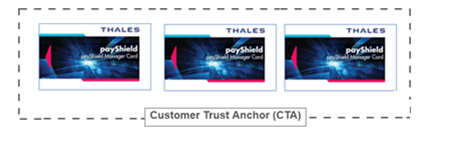


Ao final da instalação, a tabela acima exibirá a LMK instalada.

# Envio smartcards para os EUA.

## 

Pelo menos 5 Smartcard serão enviados para os EUA.





# Procedimento para execução do Técnico da EQUINIX.

Requisitos, roteiro e responsabilidades das partes.

# . Pré requisitos – parte 1

- Alinhar solução que atenda necessidade de acesso remoto com compartilhamento de tela, como por exemplo o microsoft teams . Necessário testar previamente com validação da FIRST TECH, SUPERDIGITAL e EQUINIX EUA.

- Laptop com interfaces de rede (requisito mínimo).

- Placa Wi-Fi 802.11 ac (1x1) para conectar-se à Internet e ser uma ponte para acesso remoto via WI-FI.

- Placa de rede e internet Fast Ethernet [10/100] para conectar a porta de gerenciamento do HSM.

- Sistema operacional Windows.

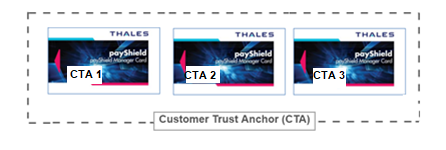
### Roteiro

- Identificar os periféricos, o cabo console USB do HSM e Leitora de cartões.

- Identificar os Smartcards.

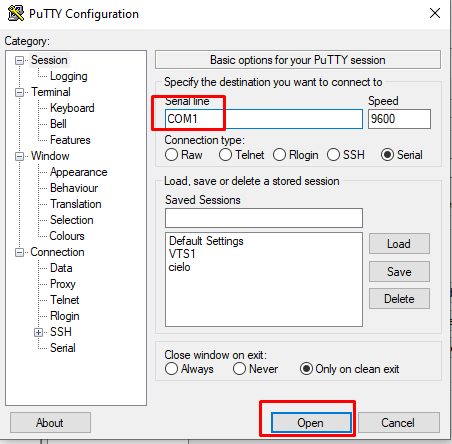




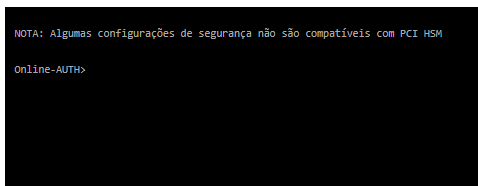


- Conecte o cabo USB ao HSM e ao notebook.

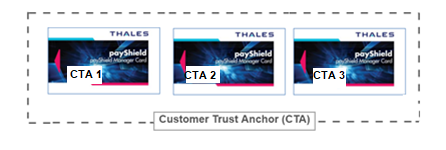
- Abra o putty identificando o COM da porta USB conectada para acessar o HSM.



- Após abrir o terminal deverá aparecer ONLINE> na tela.



Será necessário colocar os cartões CTA’s conforme orientação do consultor FT.



Será necessário colocar os cartões Right e Left na leitora acoplada no HSM conforme orientação do consultor FT.



Será necessário colocar IP na porta de gerência do HSM será definido pela SUPERGITAL e EQUINIX e inserido pela FIRST TECH.

## Pré requisitos – parte 2

• O payShield 10K estar instalado no rack.

• Seu laptop estar conectado à porta de gerenciamento payShield 10K via Ethernet

(Conferido pelo técnico da EQUINIX no local sob orientação da FIRST TECH)

NOTA: A licença do Remote payShield Manager (PS10-LIC-RMGT) oferece a opção de conectar-se ao payShield10K remotamente.

(Conferido previamente pela FIRST TECH e SUPERDIGITAL)

• A fechadura de chave payShield 10K estão na posição destravada, colocando o HSM no estado ONLINE

(Conferido pelo técnico EQUINIX no local sob orientação da FIRST TECH)

• Pelo menos 5 cartões inteligentes estão disponíveis

(Conferido pelo técnico EQUINIX no local sob orientação da FIRST TECH)

### Roteiro

- Conecte o cabo UTP RJ45 à porta de gerenciamento do HSM e a outra extremidade à interface de rede do notebook.

- Configurar a placa ethernet do notebook para o mesmo range de IP e máscara que está configurado no HSM na porta de gerência do HSM. (não é necessário colocar IP de gateway, nem DNS);

- Abra o navegador para conectar ao HSM via HTTP(S) coloque o IP da porta de gerência do HSM.

- Conecte o leitor a uma porta USB do notebook e permita o acesso remoto ao consultor da FIRST TECH para realize o primeiro acesso e configuração do leitor.

Driver do leitor de Smartcard pode ser necessário fazer o download do driver do seu leitor de Smartcard.

  Para o secodificador cyberJack® (USB):

1. Siga este link: www.reiner-sct.com/lang/en/support/support-anfrage /? Product = 77304824 & productGroup = 77304735 # choice3

2. Clique em Downloads de drivers para o HID® Leitor de smartcard OMNIKEY®: 1. Siga este link: www.hidglobal.com/drivers 2. Selecione a marca: OMNIKEY

3. Selecione o produto: OMNIKEY 3821 USB CARD READER

4. Clique com base no sistema operacional apropriado

Será necessário colocar os cartões Right ou Left no leitor conectado ao notebook, conforme instruções do consultor da FT.



Do Brasil, vamos inserir os demais cartões da SUPERDIGITAL na whitelist através do acesso remoto concedido pelo técnico da EQUINIX.

Após concluir os testes será validado o acesso do HSM remotamente pelo Brasil, se a VPN da EQUINIX estiver funcional com conectividade de ping IP da porta de gerência entre os sites SUPERDIGITAL Brasil e a EQUINIX nos EUA.

Podem ser necessários outras janelas para os testes.

Após checagens mencionadas o técnico da EQUINIX estará liberado.

Demais configurações serão feitas do Brasil através do payShield Manager

# Release Note

|  |  |  |  |
| --- | --- | --- | --- |
| Processo: |  | Versão: | 1.1 |
| Autor: | Eduardo Mendes Campos | Data: | 29/10/2019 |
| Revisor: | Geovanne de Oliveira Souza | Data: | 30/10/2019 |
| Editado: | Bruno Rodrigues de Araujo | Data: | 02/06/2020 |
| Aprovador: |  | Data: |  |