

CryptoPanel

edycja #22

Już za moment
zaczynamy...



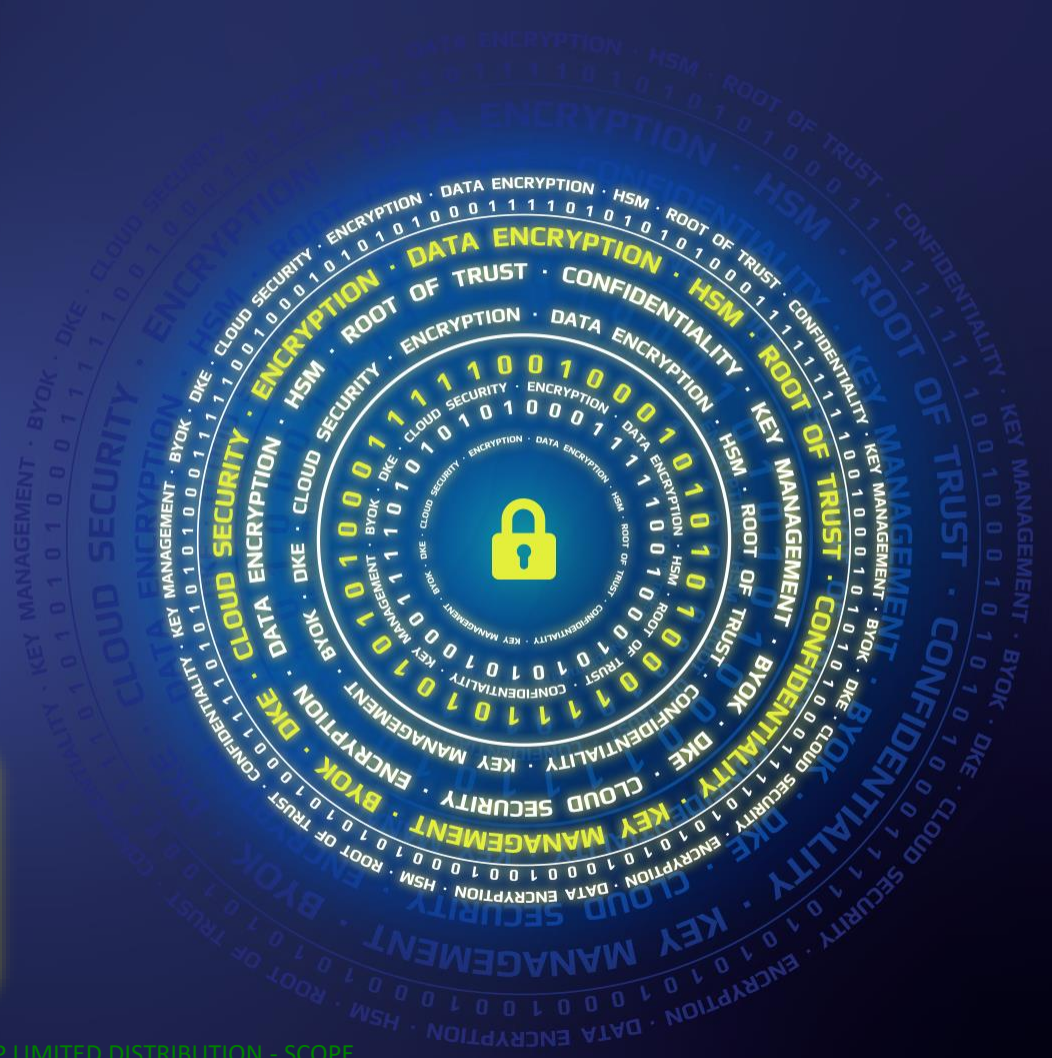
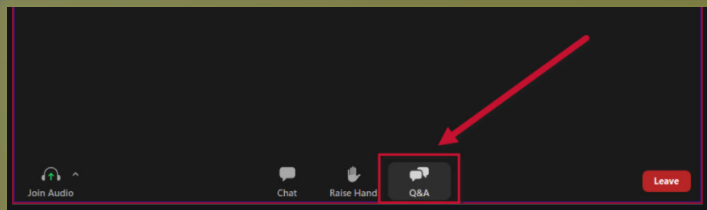
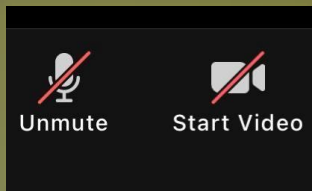
CryptoPanel



THALES



CryptoPanel



CryptoPanel

edycja #22

Rozszerzone zarządzanie domenami – sposób na migrację kluczy szyfrujących z Luny PED do Luna PWD i nie tylko... !



CryptoPanel

dziś dyskutują



Piotr Majek

Security Specialist

piotr.majek@clico.pl

mob. +48 663 994 996



Jarosław Ulczok

Pre-sales Consultant

Jaroslaw.Ulczok@thalesgroup.com

mob. +48 603 056 667



CryptoPanel

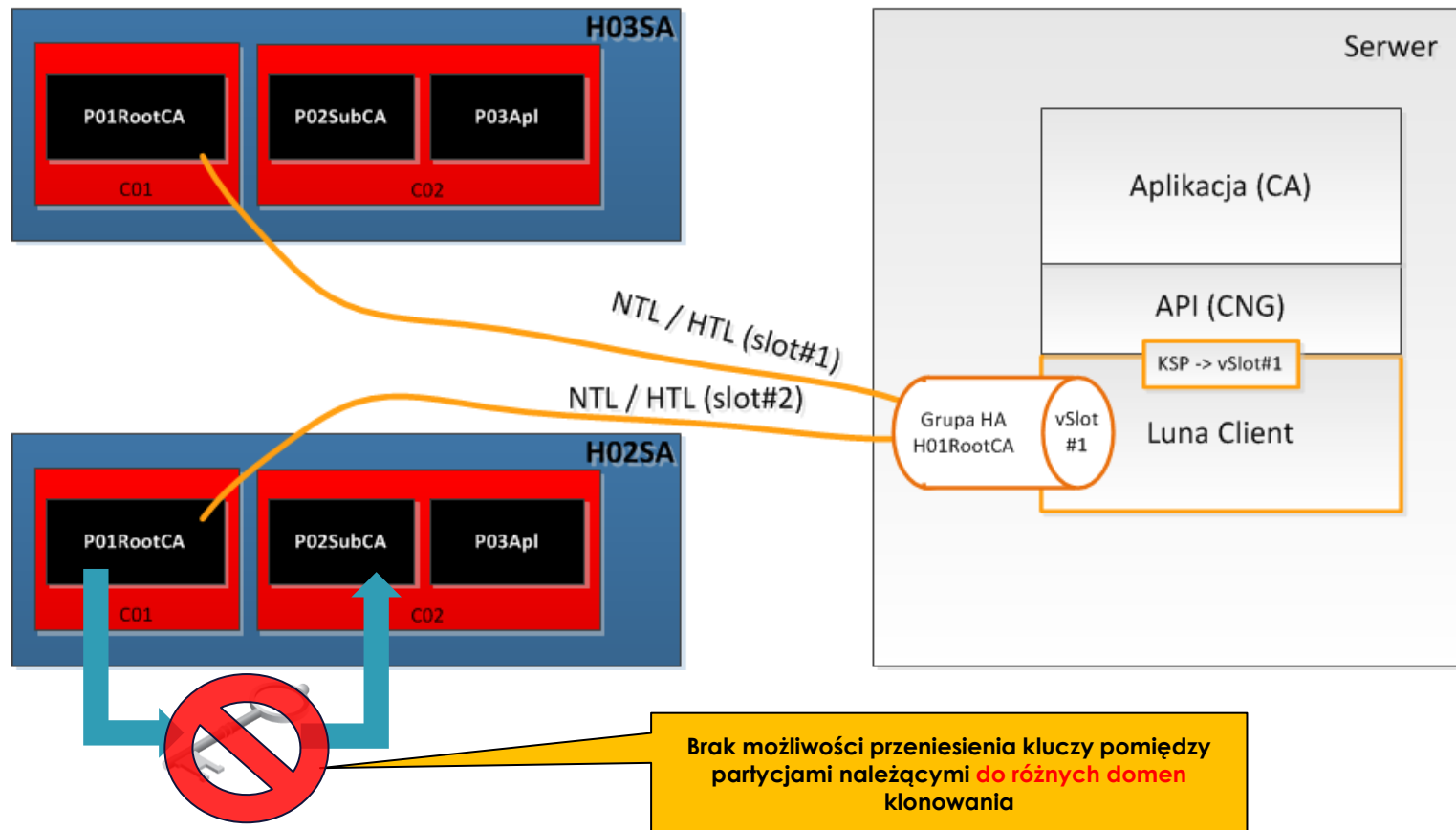


problem



- 

Koncepcja domeny klonowania i partycji (Luna 5/6 i 7)



Dla przypomnienia skąd całe zamieszanie

Przeszłość (Luna 5/6)



PED albo PWD – **ustalane w fabryce**
KE – **ustalane w fabryce per urządzenie**

Partycje (i klucze) przypisane do **jednej** domeny klonowania



1:1



Enter the domain name: *****

Teraźniejszość (Luna 7)



PED albo PWD – **ustalane w fabryce**
KE – **ustalane per partycja!**

Partycje (i klucze) mogą być przypisane **do wielu (3)** domen klonowania (od FW 7.8)



1:N



Enter the domain name: *****

Enter the domain name: *****

CryptoPanel



rozwiązanie



Rozwiązanie:

Universal Cloning

(klonowanie uniwersalne)



Uniwersalne klonowanie (Universal Key Cloning) w Luna 7

Uniwersalne klonowanie to połączenie dwóch funkcji dostępnych dzięki zastosowaniu **firmware 7.8.0+** i klienta **Luna 10.5.0+**:

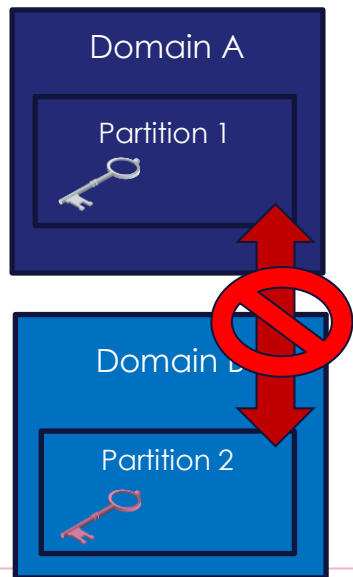
- **Protokół klonowania** w wersji 4 (**CPv4**), który udostępnia nowe zestawy szyfrów dla procesu klonowania i dodaje elastyczność w obsłudze procesu klonowania.
- **Rozszerzone zarządzanie domenami.**
 - Polityka **partycji** 44 (44: Allow Extended Domain Management : 1) - **not destructive**
 - Mechanizm rozszerzonego zarządzania domenami dostępny jest dla urządzenia Luna 7 sieciowego i karty PCIe*
 - Mechanizm nieodstępny dla Luna USB (G7) i HSMaaS/DPoD * (brak w firmware)

* - stan na maj, 2024 roku.

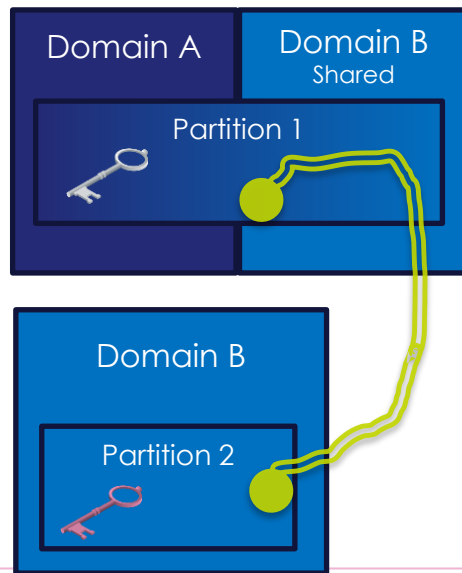
Jak działa UC?

Partycje należące do tych samych domen pozwalają na przenoszenie kluczy między nimi za pomocą mechanizmu **klonowania**

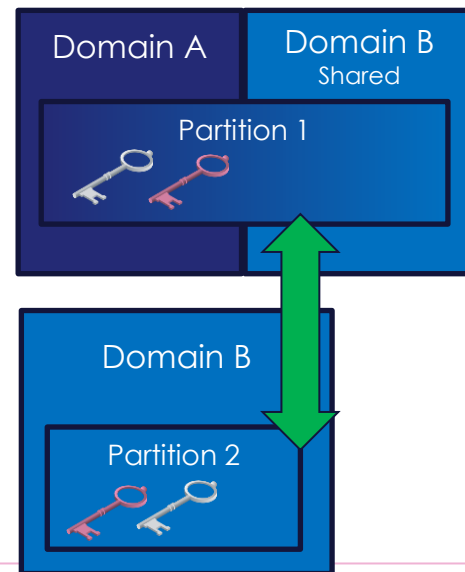
Konfiguracja początkowa



Krok 1: Dodajemy domenę wspólną



Krok 2: Wymieniamy kucze



Rozszerzone zarządzanie domenami w szczególe

Nowa polityka partycji “Allow Extended Domain Management” umożliwia rozszerzone zarządzanie domenami.

- Do **3 domen klonowania** na partycję.
- Umożliwia zastosowanie etykiety dla domeny (wymagane dla wielu domen)
- Pozwala na mieszanie domen *pwd-auth* i *ped-auth*.
- Kontrolowana polityką nr 44 (**44: Allow Extended Domain Management : 1**) – domyślnie jest OFF
- Dla zarządzania domenami wymagana jest **rola PO**
- Domena podstawowa (*primary*) będzie używana podczas klonowania z oprogramowaniem sprzętowym starszym niż 7.8.x.
- Nowe komendy zarządzania domenami:

```
lunacm> par domainAdd (with parameter -p to set a primary domain)
lunacm> par domainDelete
lunacm> par domainChangeLabel
lunacm> par domainList
```

https://www.thalesdocs.com/gphsm/luna/7/docs/network/Content/lunacm/commands/partition/partition_domainadd.htm

CryptoPanel



CryptoPanel

Problem



SW/FW 6.3.0/6.27
(brak rozszerzonego
zarządzania
domenami)



FW 7.8.0+
(Extended Domain
Management)

Gra wstępna



Uzyskujemy dostęp do obu partycji

Administrator: C:\Windows\system32\cmd.exe - lunacm

Available HSMS:

Slot Id -> 0
Label -> P01RootCA
Serial Number -> 508001014
Model -> LunaSA 6.3.0
Firmware Version -> 6.27.0
Configuration -> Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 1
Label -> P01zPED
Serial Number -> 149802742827
Model -> LunaSA 7.8.1
Firmware Version -> 7.8.1
Bootloader Version -> 1.1.5
Configuration -> Luna User Partition With SO (PW) Key Support With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Slot Id -> 5
Label -> P01zPED
Serial Number -> 1334054176432
Model -> Cryptovisor7
Firmware Version -> 7.3.0
CV Firmware Version -> 2.0.0
Plugin Version -> Cloud 2.2.0-740
Configuration -> Luna User Partition With SO (PW) Signing With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Not Supported

Current Slot Id: 0

lunacm:> slot set slot 1

10.10.11.202 - PuTTY

[L6-202] lunash:>partition showcontents -par P01RootCA

Please enter the password for the partition:
> *****

Partition Name: P01RootCA
Partition SN: 508001014
Partition Label: P01RootCA
Storage (Bytes): Total=1039256, Used=3688, Free=1035568
Number objects: 2

Object Label: WIN-QJ0M04H7MPL-CA
Object Type: Private Key
Object Handle: 52

Object Label: WIN-QJ0M04H7MPL-CA
Object Type: Public Key
Object Handle: 49

Command Result : 0 (Success)

[L6-202] lunash:>

Partycja w slotie 1 jest niezainicjowana

Włączamy Extended Domain Management

```
Administrator: C:\Windows\system32\cmd.exe - lunacm

Configuration -> Luna User Partition, No SO (PED) Signing With Cloning Mode
Slot Description -> Net Token Slot

Slot Id -> 1
Label -> P02RootCA
Serial Number -> 1498027423827
Model -> LunaSA 7.8.1
Firmware Version -> 7.8.1
Bootloader Version -> 1.1.5
Configuration -> Luna User Partition With SO (PW) Key Export With Cloning Mode
Slot Description -> Net Token Slot
FM HW Status -> FM Ready

Slot Id ->
Label ->
Serial Number ->
Model ->
Firmware Version ->
CV Firmware Version ->
Plugin Version ->
Configuration ->
Slot Description ->
FM HW Status ->

Current Slot Id: 1

Command Result : No Error

lunacm:> par changePo -p 44 -v 1

Command Result : No Error

lunacm:>

lunacm:> role login -n po

enter password: *****
```

Na partycji docelowej (P02RootCA) w Luna 7 włączamy politykę 44.

Operacja wymaga poświden PO.

Dodajemy domenę z Luny 6 (z klucza PED) do Luny 7

```
Administrator: C:\Windows\system32\cmd.exe - lunacm
Syntax: partition <sub command>
Command Result : No Error

lunacm:> par d1

Number of supported domains 3
Defined Domain
Domain #1 without label. Defined as primary domain.

Command Result : No Error

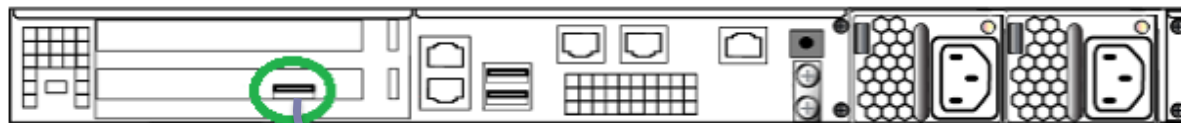
lunacm:> par da -dped -d1 zLuna6PED -p

Please attend to the PED.

Command Result : No Error
```

Dodajemy **dodatkowa** domenę klonowania do partycji P02RootCA, dla której sekret zostaje pobrany z klucza PED.

Uwaga PED i klucz PED należy podłączyć **lokalnie** do portu USB w module HSM w Luna 7



Po wylistowaniu otrzymujemy 2 domeny

```
Administrator: C:\Windows\system32\cmd.exe - lunacm

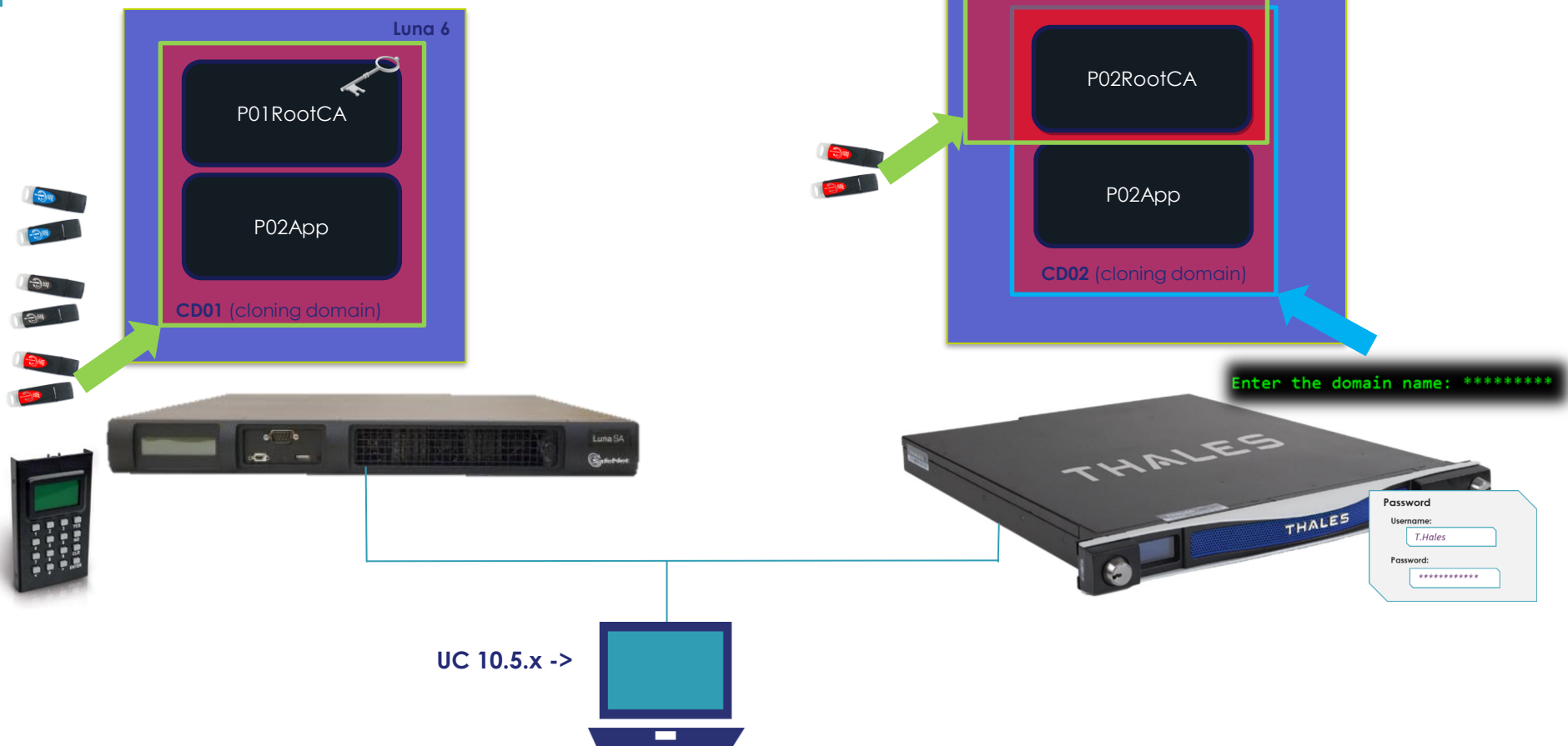
lunacm:> par d1

    Number of supported domains 3
    Defined Domains
        Domain #1 without label.
        Domain #2 with label "zLuna6PED". Defined as primary domain.

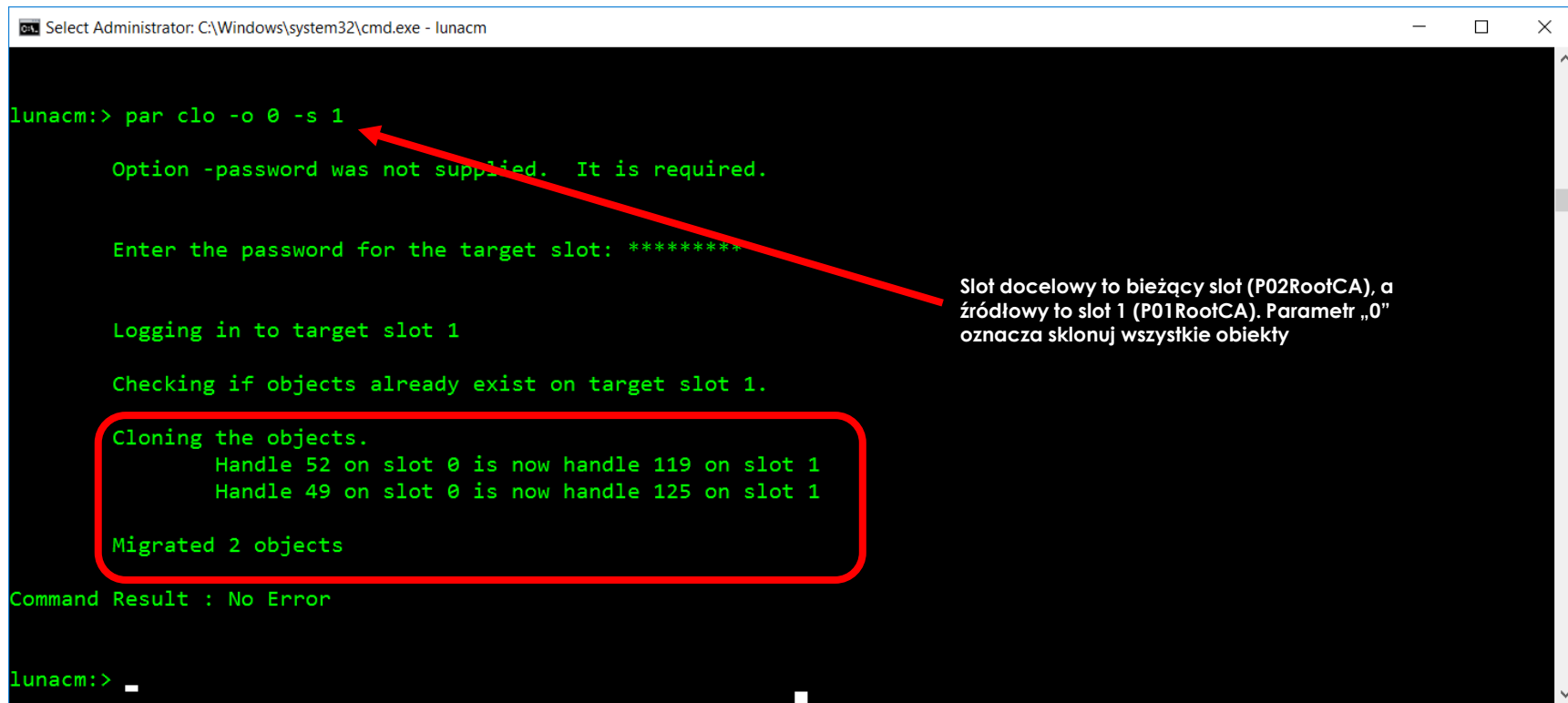
Command Result : No Error

lunacm:> _
```

Zilustrujmy co się stało



Przenosimy klucze



```
Select Administrator: C:\Windows\system32\cmd.exe - lunacm

lunacm:> par clo -o 0 -s 1

Option -password was not supplied. It is required.

Enter the password for the target slot: *****

Logging in to target slot 1

Checking if objects already exist on target slot 1.

Cloning the objects.
    Handle 52 on slot 0 is now handle 119 on slot 1
    Handle 49 on slot 0 is now handle 125 on slot 1

Migrated 2 objects

Command Result : No Error

lunacm:> _
```

Slot docelowy to bieżący slot (P02RootCA), a źródłowy to slot 1 (P01RootCA). Parametr „0” oznacza sklonuj wszystkie obiekty

Po przenosinach

```
Administrator: C:\Windows\system32\cmd.exe - lunacm

lunacm:> par con

The 'Crypto Officer' is currently logged in. Looking for objects
accessible to the 'Crypto Officer'.

Object list:

Label:      WIN-QJ0M04H7MPL-CA
Handle:     125
Object Type: Public Key
Usage Limit: none
Object UID: 050000007500000261c00700

Label:      WIN-QJ0M04H7MPL-CA
Handle:     119
Object Type: Private Key
Usage Limit: none
Object UID: 060000007500000261c00700

Number of objects: 2

Command Result : No Error

lunacm:>
```

```
10.10.11.202 - PuTTY

[L6-202] lunash:>partition showcontents -par F01RootCA

Please enter the password for the partition:
> *****

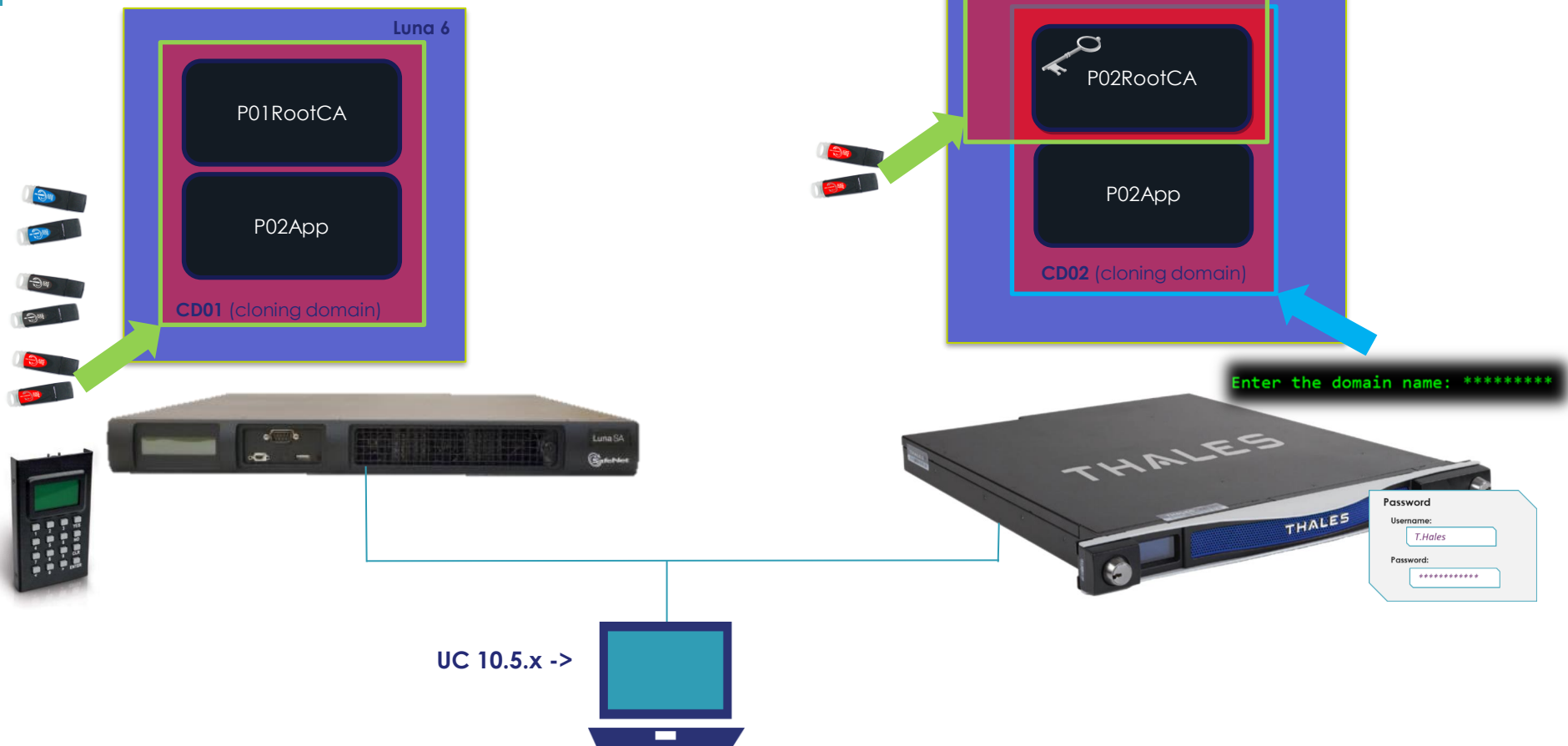
Partition Name:      F01RootCA
Partition SN:        508001014
Partition Label:     F01RootCA
Storage (Bytes): Total=1039256, Used=3688, Free=1035568
Number objects: 2

Object Label: WIN-QJ0M04H7MPL-CA
Object Type: Private Key
Object Handle: 52

Object Label: WIN-QJ0M04H7MPL-CA
Object Type: Public Key
Object Handle: 49

Command Result : 0 (Success)
[L6-202] lunash:>
```

Gotowe. Czy o czymś nie zapomnieliśmy?



Ponownie dodajemy CD02 jako *primary*

```
Select Administrator: C:\Windows\system32\cmd.exe - lunacm

lunacm:> par dl

      Number of supported domains 3
      Defined Domain
          Domain #1 with label "zLuna6PED". Defined as primary domain.

Command Result : No Error

lunacm:> par domainadd -domain [REDACTED] -primary

Command Result : No Error

lunacm:> par dl

      Number of supported domains 3
      Defined Domains
          Domain #1 without label. Defined as primary domain.
          Domain #2 with label "zLuna6PED".

Command Result : No Error

lunacm:>
```

Oryginalna
domena (CD02)
została ponownie
dodana jako
podstawowa...

Teraz możemy się pozbyć domeny dodanej z klucza PED

```
Administrator: C:\Windows\system32\cmd.exe - lunacm

lunacm:> par dd -dl zLuna6PED
You are about to delete the domain with label "zLuna6PED".
Are you sure you wish to continue?

Type 'proceed' to continue, or 'quit' to quit now -> proceed

Command Result : No Error

lunacm:> par dl

Number of supported domains 3
Defined Domain
Domain #1 without label. Defined as primary domain.

Command Result : No Error

lunacm:>
```

Teraz partycja
(P02RootCA)
należy tylko do
jednej domeny
(CD02)

Na koniec warto wyłączyć rozszerzone zarządzanie domenami

```
Administrator: Command Prompt - lunacm

41: Partition Version : 0
42: Allow CPv1 : 1
43: Allow non-FIPS algorithms : 1
44: Allow Extended Domain Management : 1

Command Result : No Error

lunacm:> par changepolicy -p 44 -v 0
Command Result : No Error

lunacm:> _
```

PO po
zalogowaniu
może wyłączyć
rozszerzone
zarządzanie
domenami na
partycji
docelowej
(P02RootCA)

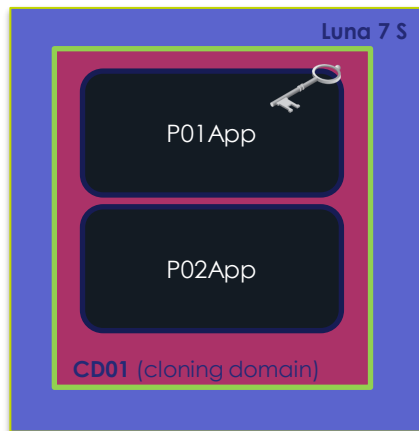
Po robocie...



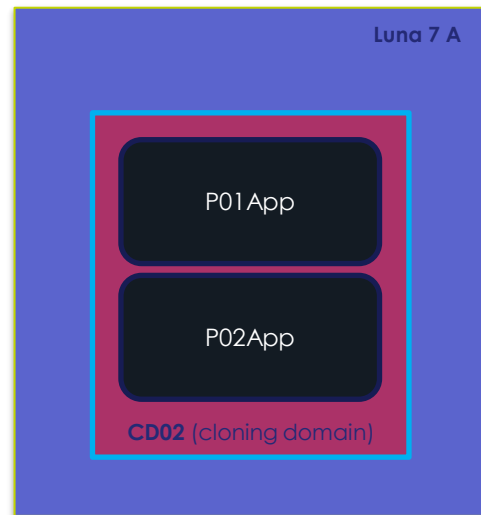
Czy istnieje możliwość migracji z Luny S na A



Problem



FW dowolny wspierany



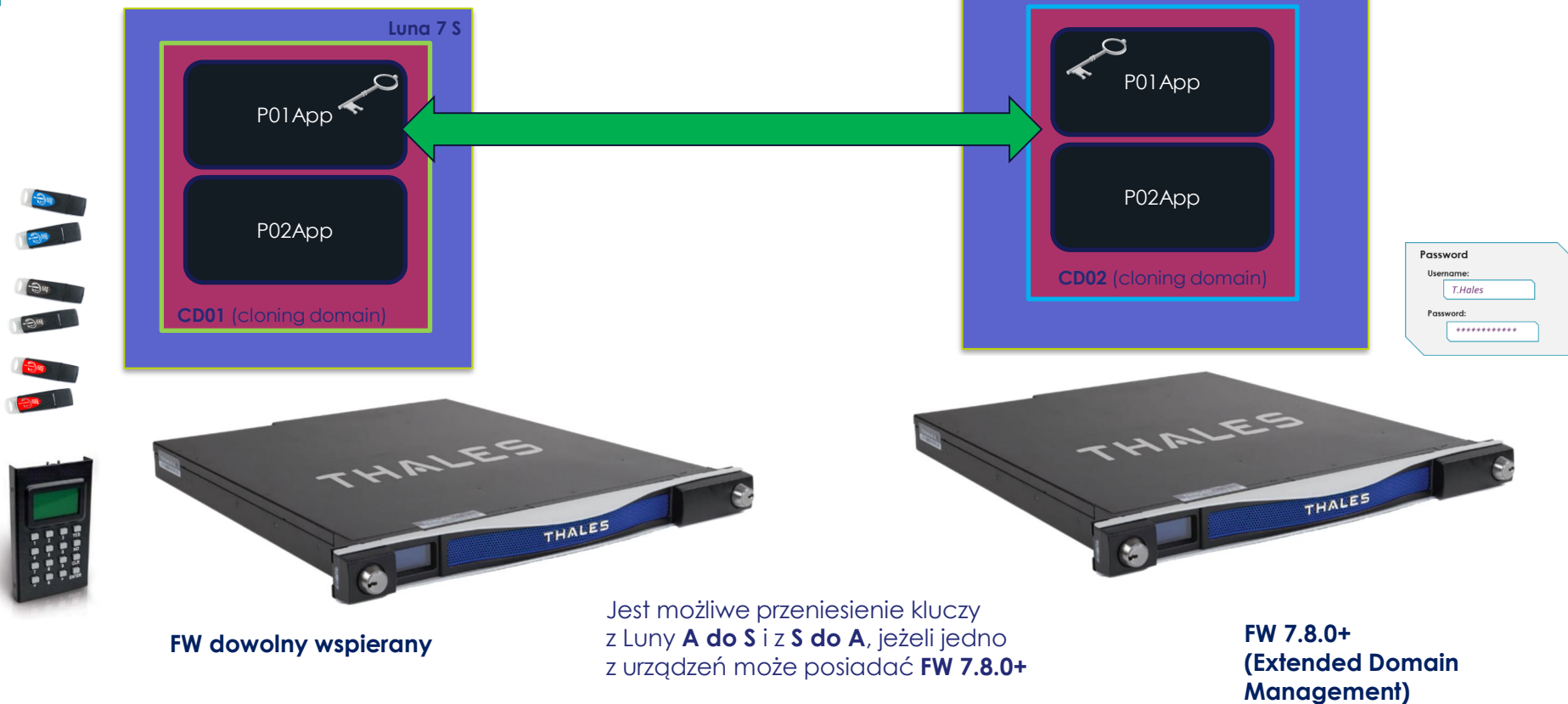
FW dowolny wspierany

Password

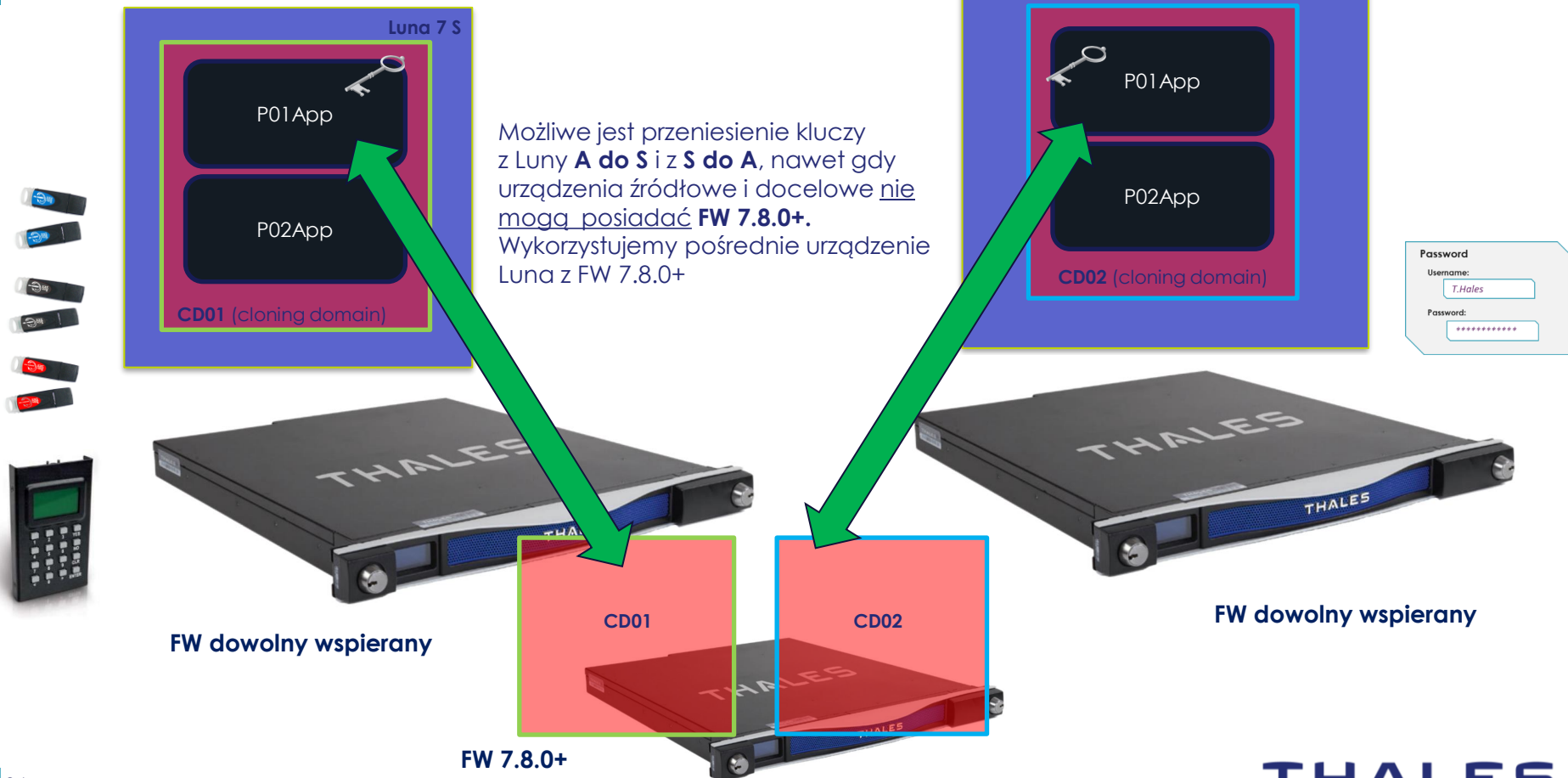
Username:

Password:

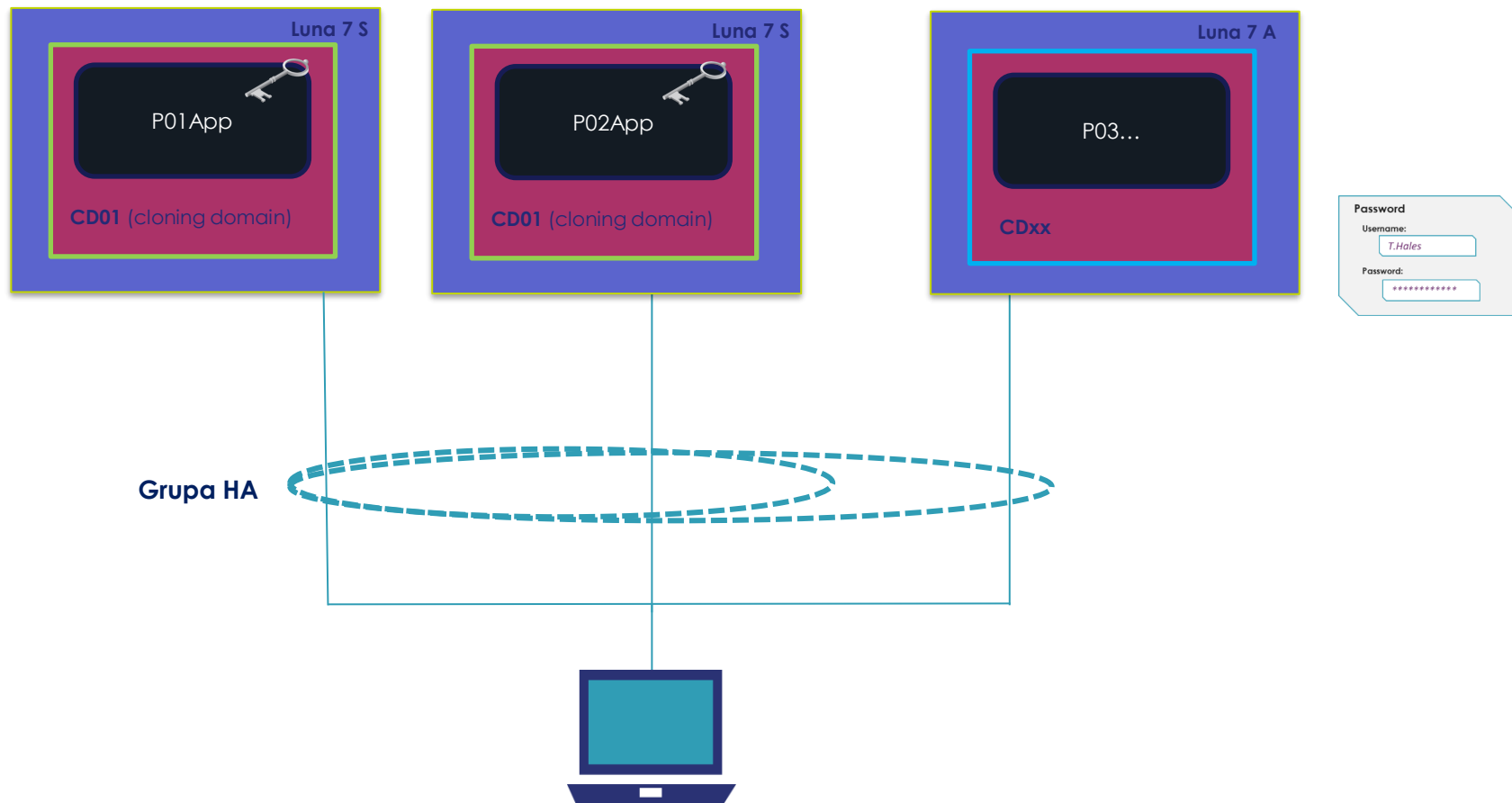
Rozwiązanie #1



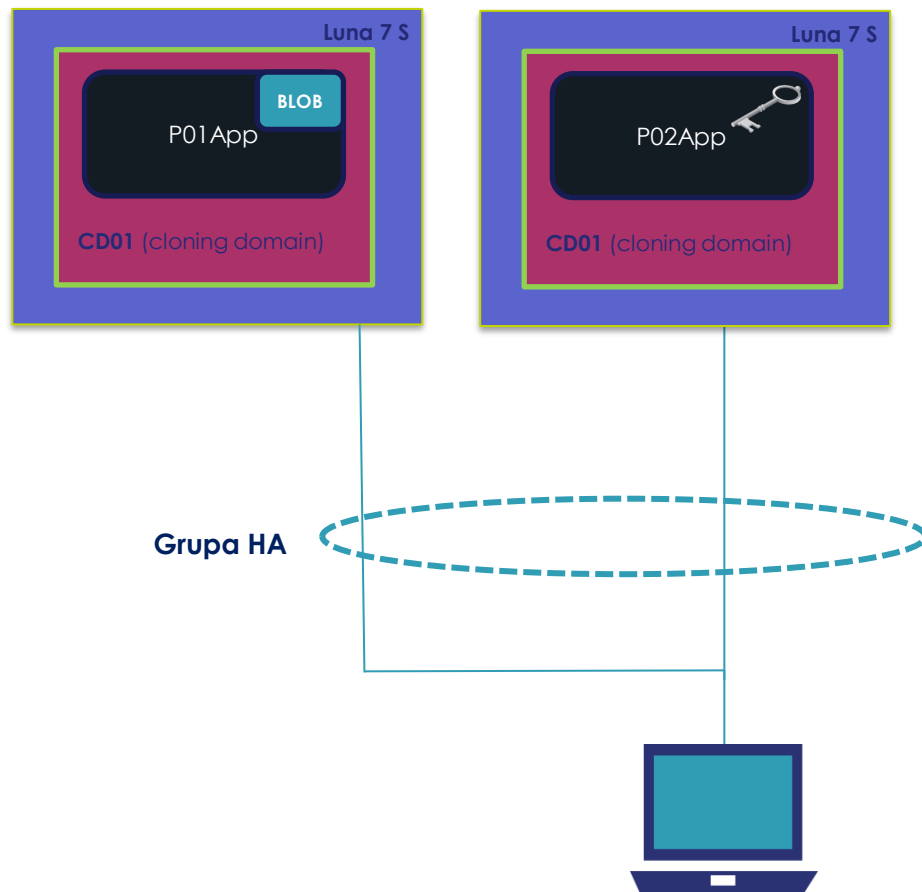
Rozwiązanie #2



Problem



Nim z ilustrujemy problem, drobne przypomnienie...

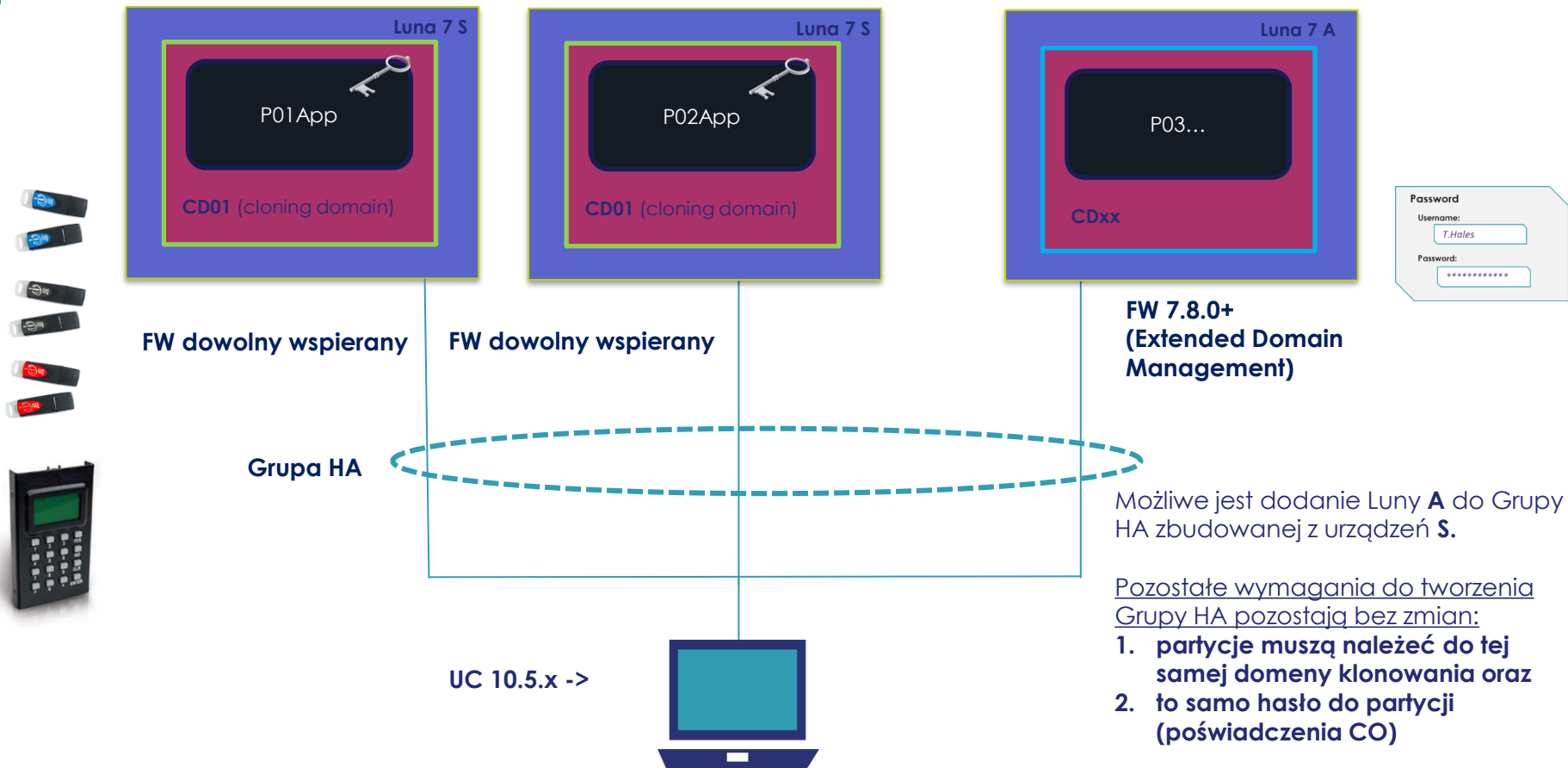


W przypadku budowy Grupy HA partycje muszą należeć do **tej samej domeny klonowania** (tu: **CD01**). W przypadku urządzeń Luna S, sekret domeny jest przechowywany na czerwonym kluczy PED.



Synchronizacja obiektów pomiędzy partycjami tworzącymi Grupę HA odbywa się za pomocą protokołu klonowania poprzez **przenoszenie zaszyfrowanych obiektów** binarnych w ramach **tej samej domeny klonowania**.

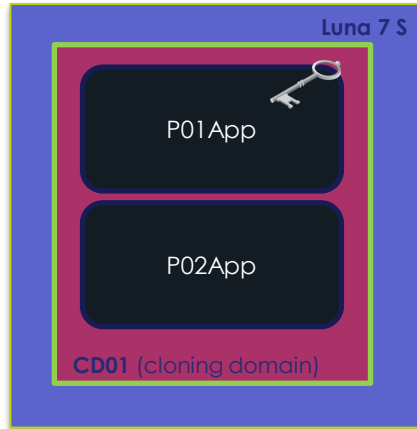
Rozwiązanie



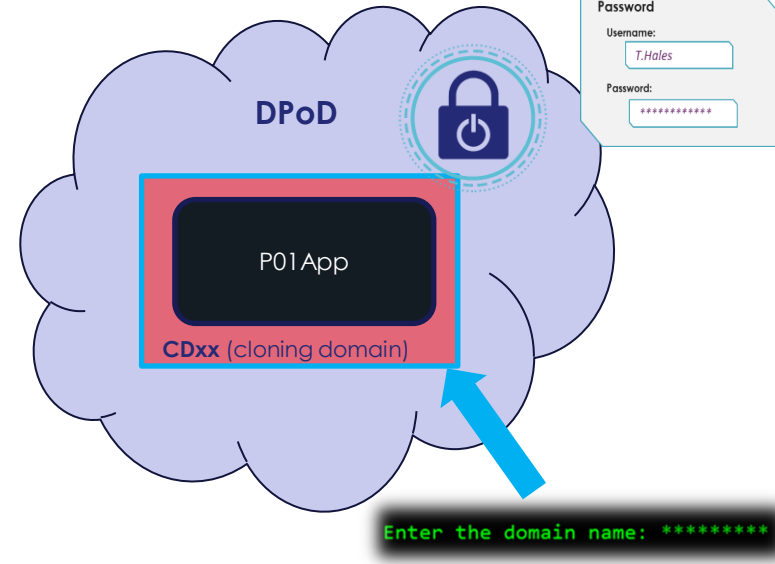
**Czy mogę zmigrować moje klucze
z lokalnego HSM chronionego PED-em do
HSM chmurowego (DPoD) chronionego
hasłem?**



Problem



FW dowolny wspierany



Form for authentication:

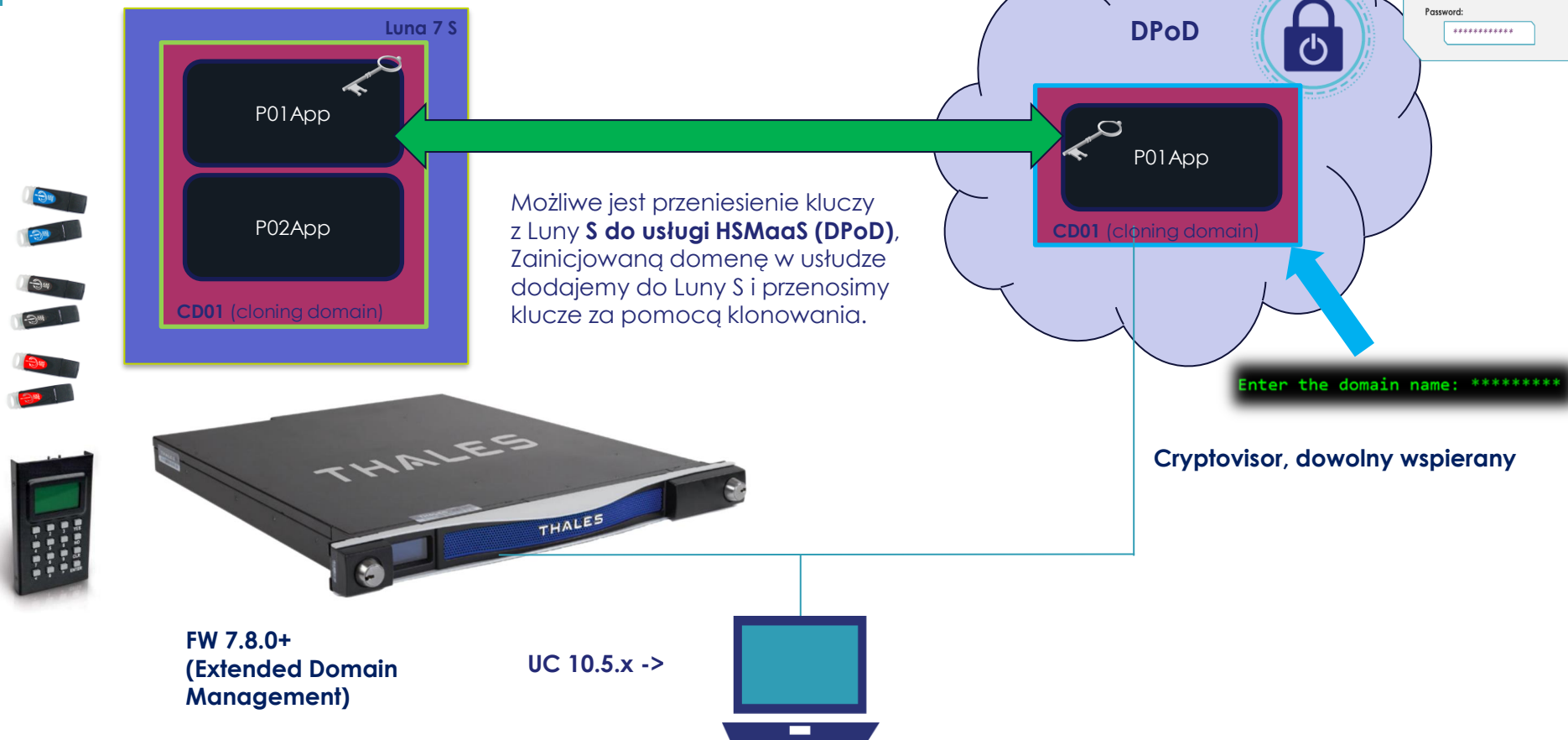
Password

Username:

Password:

Cryptovisor, dowolny wspierany

Rozwiązanie (jedno z możliwych)



**Czy mogę przenieść klucze mojego
RootCA z Luny G5 PED do Luny USB
(G7) PWD?**



Problem



Czy da się
przenieść?

Jakieś
pomysły?



46



Uff...! 😊



Nauczki...

Pamiętajmy: uniwersalne klonowanie i rozszerzone zarządzanie domenami nie jest i nie będzie lekarstwem na:

- **zapomniane hasło** (nazwę) domeny klonowania (DPoD, Luna 5/6)
- **zgubione czerwone klucze PED** domeny klonowania w Luna 5/6
- **zapomniane PINy do kluczy PED** domeny klonowania w Luna 5/6



Uniwersalne klonowanie zachowuje atrybuty klucza.

EDM i UC pozwoli odzyskać („zapomnianą”) domenę klonowania w Luna 7

- Wymagana aktualizacja do FW 7.8.0+

Nawet jeżeli urządzenie źródłowe i docelowe nie mogą być zaktualizowane dla wsparcia EDM i UC (FW 7.8.0+)... to można pokombinować 😊.

- Podziel się z nami Twoim przypadkiem!



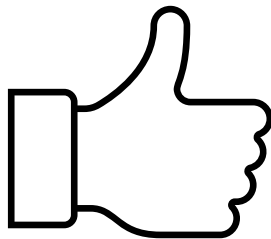
CryptoPanel



podsumowanie



- Urządzenie Luna 7 network lub PCIe
- FW 7.8.0+ i UC 10.5.0+



CryptoPanel



CryptoPanel



A teraz quiz



Punkty za inwencję

6. Jakie zagadnie chciałbyś aby zostały poruszone na przyszłych CryptoPanelach? *

☐

„Szyfrowanie backupów – podejścia, strategię, itd.”

☐

„Zabezpieczanie baz danych, które nie posiadają mechanizmu natywnego”

7. Może jakiś własny pomysł? Zachęcamy do inwencji twórczej *

Wprowadź odpowiedź

Prześlij

