

CryptoPanel

edycja #8

Porządkowanie rozproszonych kluczy szyfrujących wewnątrz organizacji i zarządzanie nimi z poziomu jednego repozytorium.



CryptoPanel

dziś dyskutują



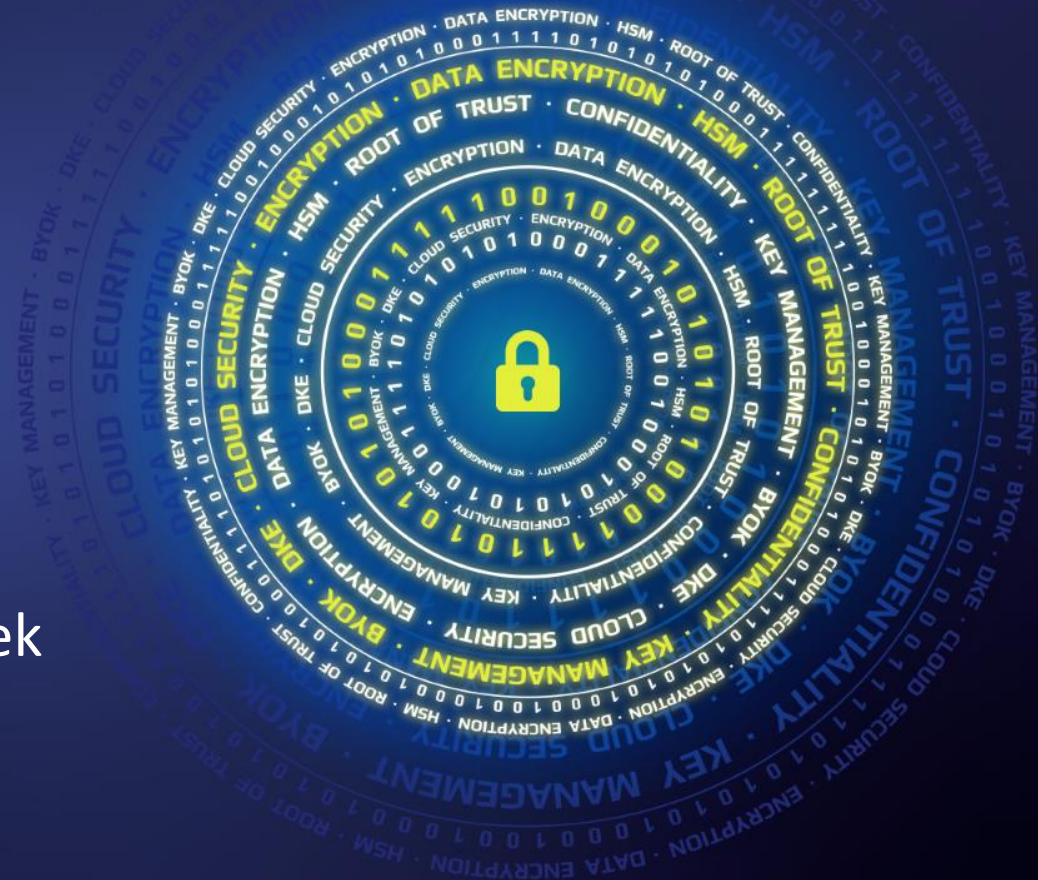
Piotr Majek

Security Specialist
piotr.majek@clico.pl
mob. +48 663 994 996



Artur Holeczek

Partner Account Manager /
Product Manager
artur.holeczek@clico.pl
mob. +48 667 699 444



CryptoPanel



Dzisiejszy problem

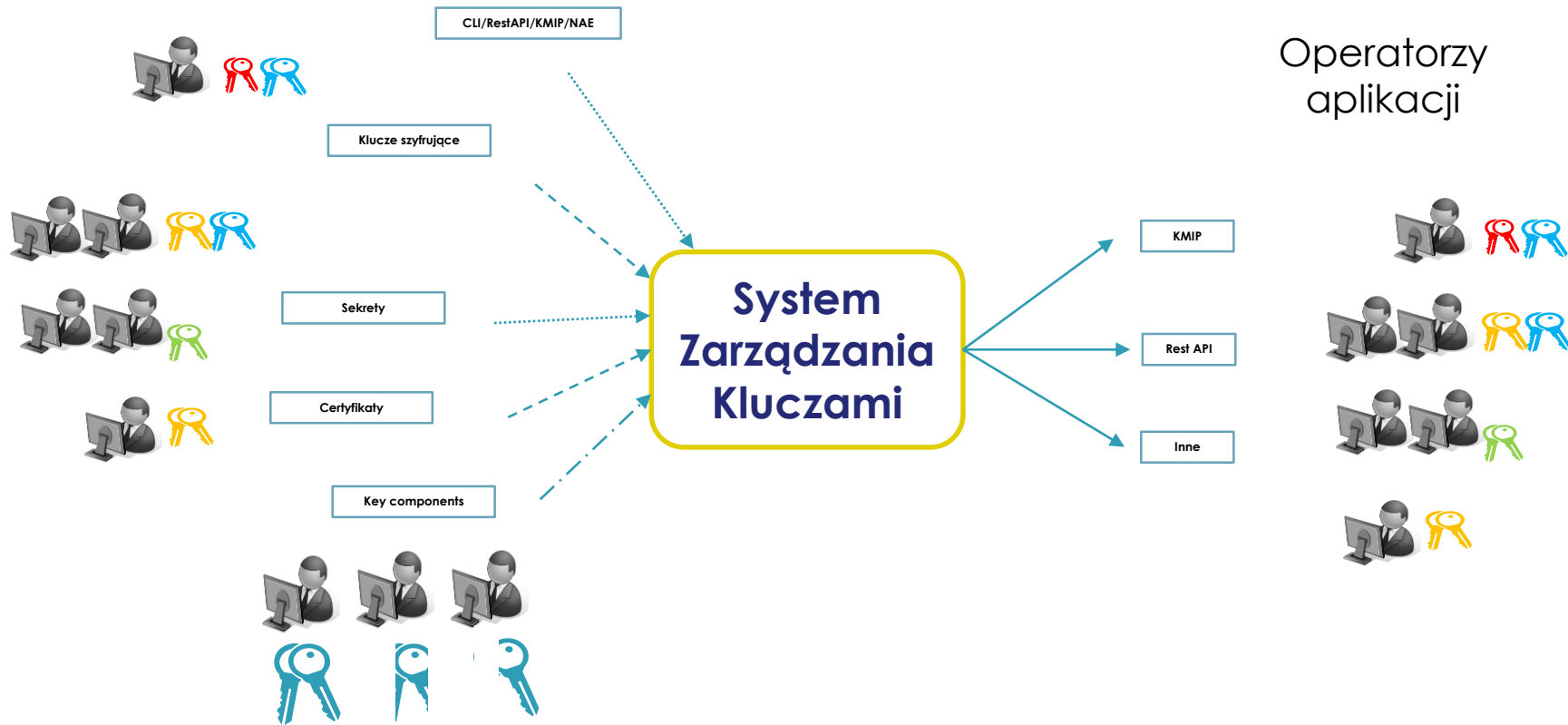


Co nas boli...

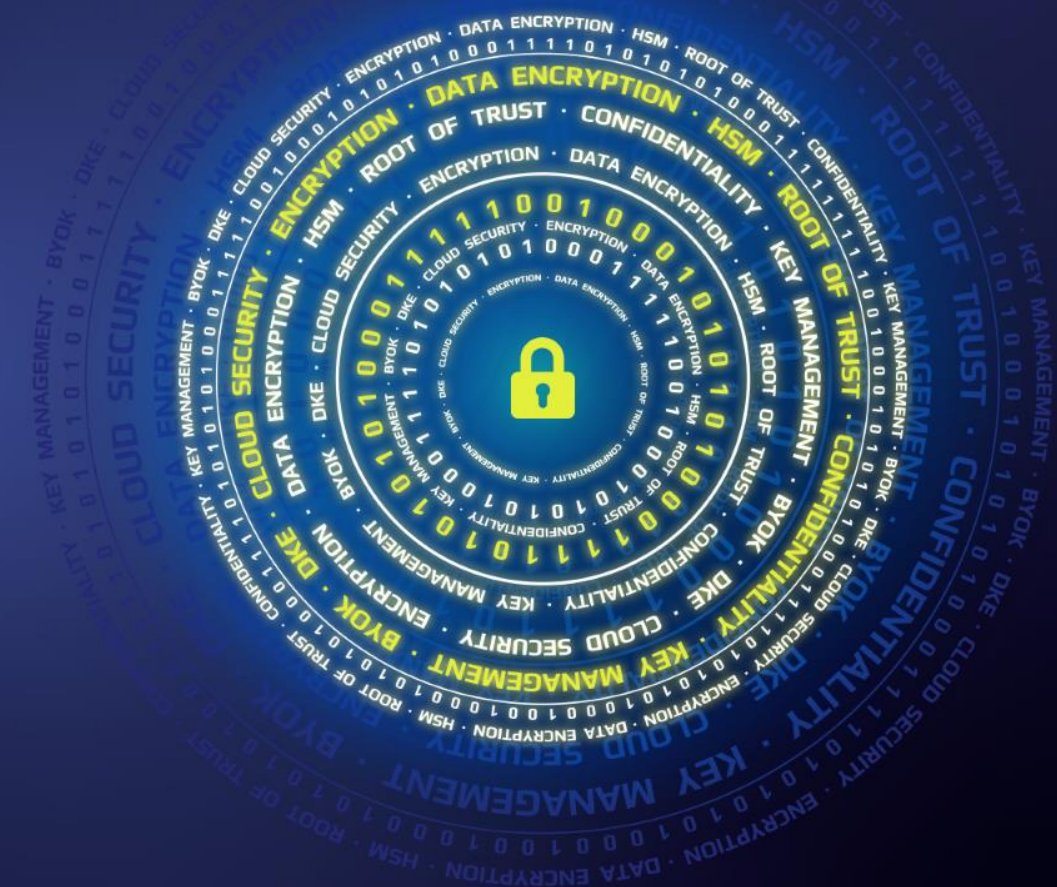
- Jesteśmy instytucją rynku finansowego;
- Z racji swojej działalności posługujemy się ogromną ilością kluczy szyfrujących w rozwiązaniach IT i paymentowych, generowanych często z wykorzystaniem darmowych narzędzi programowych;
- Klucze szyfrujące wykorzystywane są w wielu różnych systemach i aplikacjach oraz często brakuje im wspólnego interfejsu (np. KMIP czy RestAPI);
- Klucze zarządzane i wykorzystywane są przez określone zespoły ludzkie (musimy utrzymać ten podział!)
- ...poszukujemy rozwiązania do realizacji centralnego systemu zarządzania kluczami.
- ...chcemy zaprzestać przechowywania kluczy w plikach PEM, na papierze (key components). Generalnie: poza centralnym repozytorium.
- ...w pierwszym etapie chcemy stworzyć niezawodne repozytorium kluczy z podziałem uprawnień. Możliwość eksportu i importu materiału kryptograficznego.
- ...w kolejnych etapach chcemy wprowadzić pełne zarządzanie cyklem życia kluczy (utworzenie, udostępnienie, monitorowanie, wstrzymanie, odwołanie, archiwizacja, kasowanie)
- ...potrzebujemy automatycznej archiwizacji kluczy (najlepiej offsite).
- ...chcemy przechowywać także inne „sekrety”, takie jak certyfikaty.



Co posiadamy, a co chcemy posiadać?



CryptoPanel



Rozwiązanie

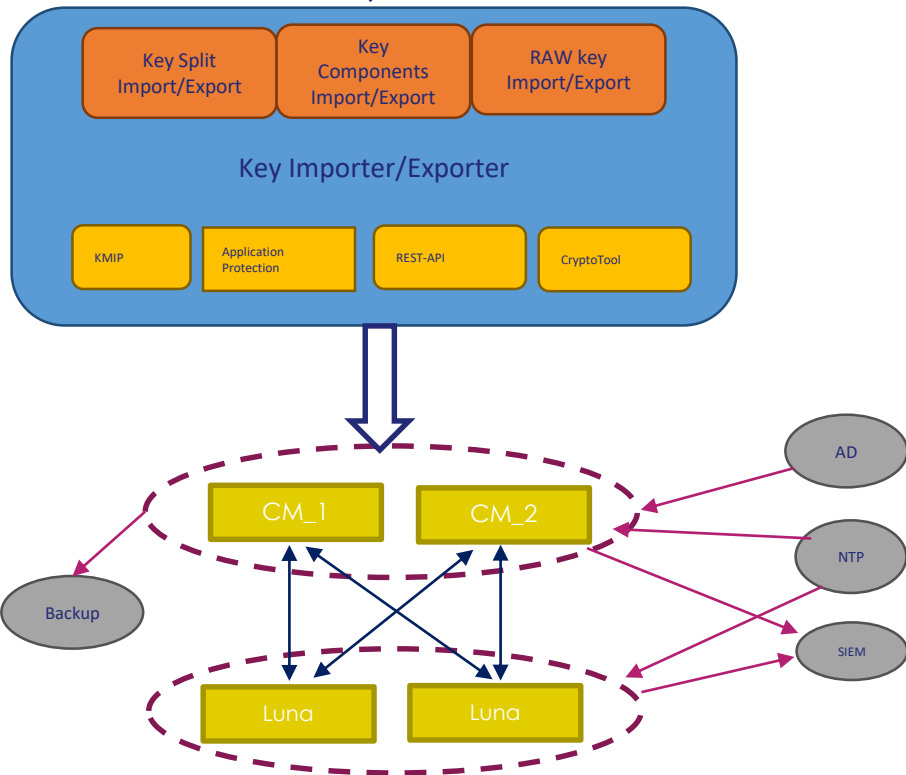
Rozwiązanie:

CipherTrust Manager. I wystarczy!

Dodatkowo – rozbudowa o CipherTrust Application Protection (CAP)



Koncepcja



Koncepcja systemu:

System zaprojektowano jako system 3 warstwowy. Sprzętowy HSM (Luna) zapewnia źródło zaufania do generowania/przechowywania kluczy. CipherTrust Manager zapewnia większość funkcji zarządzania kluczami (dostępne za pośrednictwem REST-API i CryptoTool). Jednak niektóre możliwości importu/eksportu kluczy muszą zostać zaprojektowane i zakodowane (np. podział kluczy, kluczowe komponenty itp.)

1. Key Import/Export (KIE) – komponent należy zaprojektować i zakodować. Wykorzystuje Application Protection do niektórych podstawowych funkcjonalności od razu po wyjęciu z pudełka (np. eksport/import klucza RAW), inne muszą zostać zaprojektowane i zakodowane.
2. CipherTrust Manager (klaster) – dostarczany jako urządzenie wirtualne zapewnia najwięcej możliwości zarządzania kluczami (generowanie, użycie, zniszczenie).
3. Luna (klaster) – sprzętowy HSM zapewniający źródło zaufania do generowania i ochrony kluczy

Co może CipherTrust Manager w kwestii importu/eksportu kluczy?



Możliwości CipherTrust Managera

- „Z pudełka” mamy dostęp do obsługi zapytań REST-API,
- Możliwość rozbudowy o konektor obsługujące inne biblioteki – CipherTrust Application Protection.



Application Data Protection

Application Encryption

CipherTrust Manager i domeny - czyli przydział kluczy do konkretnych grup użytkowników



Domeny – czym są i co nam dają?


- Domena – możliwość separacji kluczy, użytkowników i aplikacji w ramach jednego CipherTrust Managera,
- Zwiększona elastyczność zarządzania,
- Osobne domeny – brak „mieszania się” kluczy, niezależne kopie zapasowe.



Domeny – zmiana zasobnika kluczy „w locie”

Domains

Name	Id	Parent Domain	CA
CloudAdmins	74fdaf0c	root	98b0992.
WebAdmins	3eeacccb	root	173ea69.

☰ root/admin 

- ▼ Switch Domains
- CloudAdmins
- WebAdmins
- ⚙ User Settings
- 🚪 Logout




Domeny – podział kluczy

Keys 

Keys 

Name

Name 

Filters Basic Raw

Filters Basic Raw






Latest Version Only

Latest Version Only

Key Name	Version	Owner	Modified	Type
▶ uliAES256	0	WebAdmins admin	21 Feb 2022, 10:20	Symmetric
▶ DELETED	0	local admin	13 Feb 2022, 01:53	Symmetric
▶ DDestroyed	0	local admin	13 Feb 2022, 01:15	Symmetric
▶ pgp-public-key-test	0	No owner	10 Feb 2022, 10:25	Public
▶ SeedGeneratora1	0	No owner	10 Feb 2022, 10:12	Secret Data
▶ HasloReklamoweDoStrony	0	No owner	10 Feb 2022, 10:10	Secret Data
▶ 4WebAdmin-SSL-thales-lab	0	No owner	10 Feb 2022, 09:24	Certificate

WebAdmins/admin 

Key Name

No Keys

Jak załadować różne klucze do
CipherTrust Managera:
RestAPI
JCE CryptoTool



Piaskownica - przez RestAPI, załadujesz klucze i sekrety...

THALES CLI Guide API Guide

Domain WebAdmins 77 seconds Clear Credentials Re Authenticate

key

Keys

- /v1/vault/keys2/
List - [get](#)
Create - [post](#)
- /v1/vault/keys2/{id}
Get - [get](#)
Update - [patch](#)
Delete - [delete](#)
- /v1/vault/keys2/{id}/versions/
List versions - [get](#)
Create version - [post](#)
- /v1/vault/keys2/{id}/destroy
Destroy - [post](#)
- /v1/vault/keys2/{id}/archive
Archive - [post](#)
- /v1/vault/keys2/{id}/recover
Recover - [post](#)

includeMaterial *<query> optional* string

body *<body>*

```
{
  "name": "uliAES256",
  "usageMask": 12,
  "algorithm": "aes",
  "meta": {
    "ownerId": "WebAdmins|admin"
  },
  "usageMask": 12,
  "material": "9278fe7c7313a7ae602f4b2ad1b5bde854a766e6c51707a79bb03ab8abc52fd7"
}
```

schema

POST Curl

Mon, 21 Feb 2022 09:20:28 GMT

201



Piaskownica - przez RestAPI, załadujesz klucze i sekrety


The screenshot shows the THALES CipherTrust Manager interface. The top navigation bar includes the product name, an information icon, an API icon, and a user profile for 'WebAdmins/admin'. The left sidebar contains a menu with items: Products, Access Management, Keys (highlighted), CA, Alarms, Records, Quorums, and Admin Settings. The main content area features several filter dropdowns: 'Type / Algorithm', 'Size / Curve ID', 'State / Revocation', and 'Event Dates'. There is also a checkbox for 'Latest Version Only' and a '+ Create a New Key' button. A table lists the keys with columns: Key Name, Version, Owner, Modified, Type, Algorithm, Size, and Links. The table content is highlighted with a red rounded rectangle.

Key Name	Version	Owner	Modified	Type	Algorithm	Size	Links
uliAES256	0	WebAdmins admin	21 Feb 2022, 10:20	Symmetric	AES	256	...
DELETED	0	local admin	13 Feb 2022, 01:53	Symmetric	AES	256	...
DDestroyed	0	local admin	13 Feb 2022, 01:15	Symmetric	AES	256	...
pgp-public-key-test	0	No owner	10 Feb 2022, 10:25	Public	RSA	2048	...
SeedGeneratora1	0	No owner	10 Feb 2022, 10:12	Secret Data	SECRETSEED		...
HasloReklamoweDoStrony	0	No owner	10 Feb 2022, 10:10	Secret Data	SECRETPASSWORD		...



Piaskownica - przez RestAPI, załadujesz wszystko

Keys

Name 

Filters Basic Raw 

Type / Algorithm

Size / Curve ID

State / Revocation

Event Dates

Latest Version Only

[+ Create a New Key](#)

Key Name	Version	Owner	Modified	Type	Algorithm	Size	Links
▶ JARO-SSL-thales-lab	0	No owner	10 Feb 2022, 09:16	Certificate	RSA	2048	...
▶ ks-ea9566a53cbc47759914b73a0258da2c5748e32342e84fb8...	0	No owner	10 Feb 2022, 01:15	Opaque Object	OPAQUE		...
▶ CCKM-Azure-Key:northeurope:CCKM-demo-JU::7a79a515-9e...	0	a2365e0a-1dfe-42fa-9c6e-f5c7f992aa82 undefined	10 Feb 2022, 01:07	Opaque Object	OPAQUE		...



Użyj CryptoTool – gdy nie jest niestandardowo...

- CryptoTool może zostać użyty jako narzędzie do debugu, aby zweryfikować poprawną instalację bibliotek SafeNet JCE Provider.
- CryptoTool wykonuje również operacje kryptograficzne z poziomu linii poleceń lub jako skrypty.

Ważne: KMIP nie jest częścią CryptoTool.



CryptoTool – Opcje

```
C:\Program Files\Java\jre7\bin>java CryptoTool -help
USAGE:      java CryptoTool OPERATION options
SUPPORTED CRYPTO OPERATIONS:
            ENCRYPT, DECRYPT, MAC, MACU, SIGN, SIGNU
SUPPORTED KEY MANAGEMENT OPERATIONS:
            GENERATE, DELETE, EXPORT, IMPORT, LIST
SUPPORTED OPTIONS:
-in filename      specify a file instead of stdin
-out filename     specify a file instead of stdout
-key keyname      key name
-alg alname       algorithm
-iv value         initialization vector when required <must be hex ASCII encoded>
-sig value        provide signature value as an argument to use for verification <must be
hex ASCII encoded>
-sigfile filename alternative to -sig; provide signature value in a file
-mac value        provide mac value as an argument to use for verification <must be hex A
SCII encoded>
-macfile filename alternative to -mac; provide mac value in a file
-auth username:passwd username and password for authentication
-keysize size     key size to use for key generation
-exportable       create exportable key
-deletable        create deletable key
-ip ip           NAE server IP to use <can be a colon separated list of IP addresses>
-port port        NAE server port to use
-protocol prot    protocol to use <ssl or tcp>
-edgeseecure edgeseecure
to specify EdgeSecure name
```

Dostępne opcje w aplikacji
dostępne są po dodaniu opcji
-help.

```
java CryptoTool -help
```

CryptoTool – wykonywanie przykładowych komend

CryptoTool – Generowanie klucza RSA

```
C:\Program Files\Java\jre7\bin>java CryptoTool GENERATE -auth test1:asdf1234 -key rsakey12 -alg RSA -keysize 2048  
Key generated OK
```

```
C:\Program Files\Java\jre7\bin>java CryptoTool GENERATE -auth test1:asdf1234 -key mykey33 -alg AES -keysize 256  
Key generated OK
```

CryptoTool – wyświetlenie listy dostępnych kluczy

```
C:\Program Files\Java\jre7\bin>  
C:\Program Files\Java\jre7\bin>java CryptoTool LIST -auth test1:asdf1234  
CA_Cert : RSA  
hmackey : HmacSHA1  
hmackey222 : HmacSHA1  
key1 : AES  
mykey256 : AES  
mykey33 : AES  
protectDBkey3 : AES  
rsakey : RSA  
rsakey1 : RSA  
rsakey12 : RSA  
rsakey2 : RSA  
TMHMAC : HmacSHA256  
TMKEY : AES  
token_hash_key : HmacSHA256  
token_key : AES  
C:\Program Files\Java\jre7\bin>
```

„Nauczki“, czyli *lessons learned* i „w dokumentacji nie znajdziecie“

- Kiedy myślimy o scentralizowanym systemie przechowywania i udostępniania kluczy szyfrujących weźmy **pod uwagę ich dotychczasowy sposób wykorzystania** (np.: papier->KMS->papier – czy warto?)
- Import/Export komponentów: z powodu braku mechanizmu XOR_DATA w CM oraz zabronienia tego mechanizmu (jako niebezpiecznego) w HSM, składanie klucza komponentowego odbywa się w aplikacji w pamięci stacji/systemu. Dlatego należy zadbać aby była to wydzielona stacja administracyjna objęta dodatkowymi zabezpieczeniami.
- Czy wykorzystanie RestAPI wymaga licencji? Nie! 😊



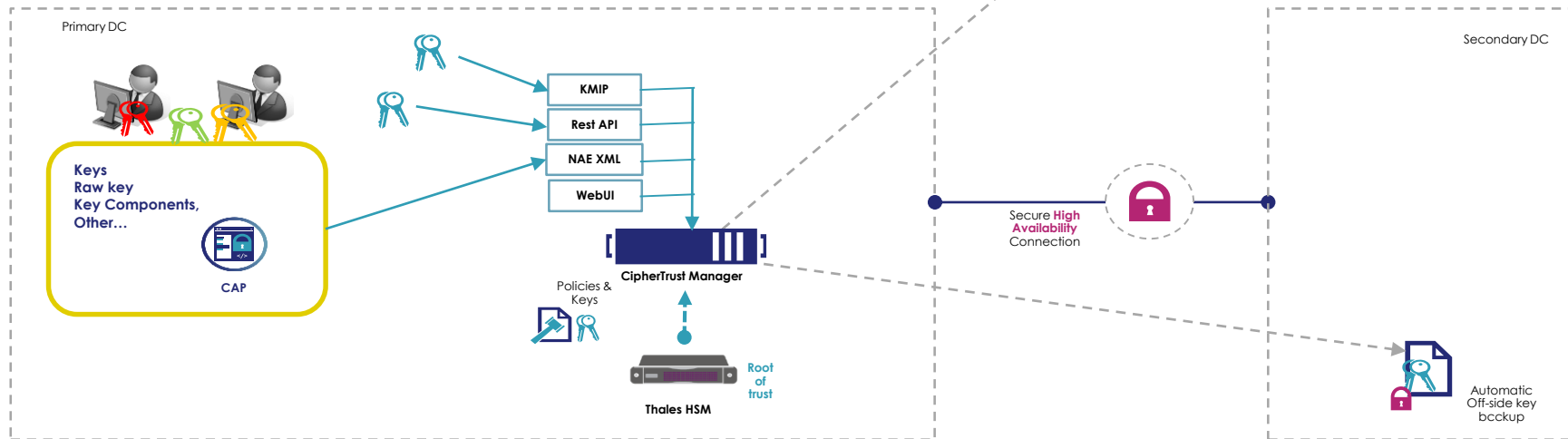
CryptoPanel



podsumowanie



Podsumowanie



Wystarczy licencja na CM

Dostępny model subskrypcyjny lub dożywotni

Licencja demo do testów dostarczana wraz z produktem

Nie trzeba ale warto: HSM

CipherTrust Manager – 14,4k Euro netto

CipherTrust Flex Connector - Advanced, Perpetual – 8,6 k Euro netto



Materiały

- Oprogramowanie do pobrania lub wersja ewaluacyjna...
 - Bardzo prosimy o kontakt z nami!
- Dokumentacja...
 - CipherTrust Manger: <https://www.thalesdocs.com/ctp/cm/latest/>
- Zapraszamy także na... Kolejny CryptoPanel
- QUIZ Z NAGRODAMI
<https://forms.office.com/r/sKORYRzHi1>

