CryptoPanel

edycja #17

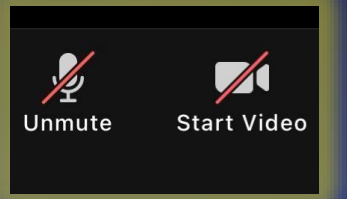
za chwilę zaczynamy...

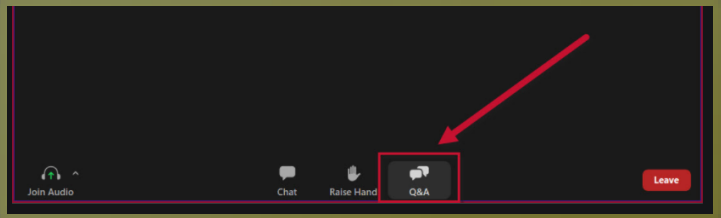
CryptoPanel

THALES

CLICO

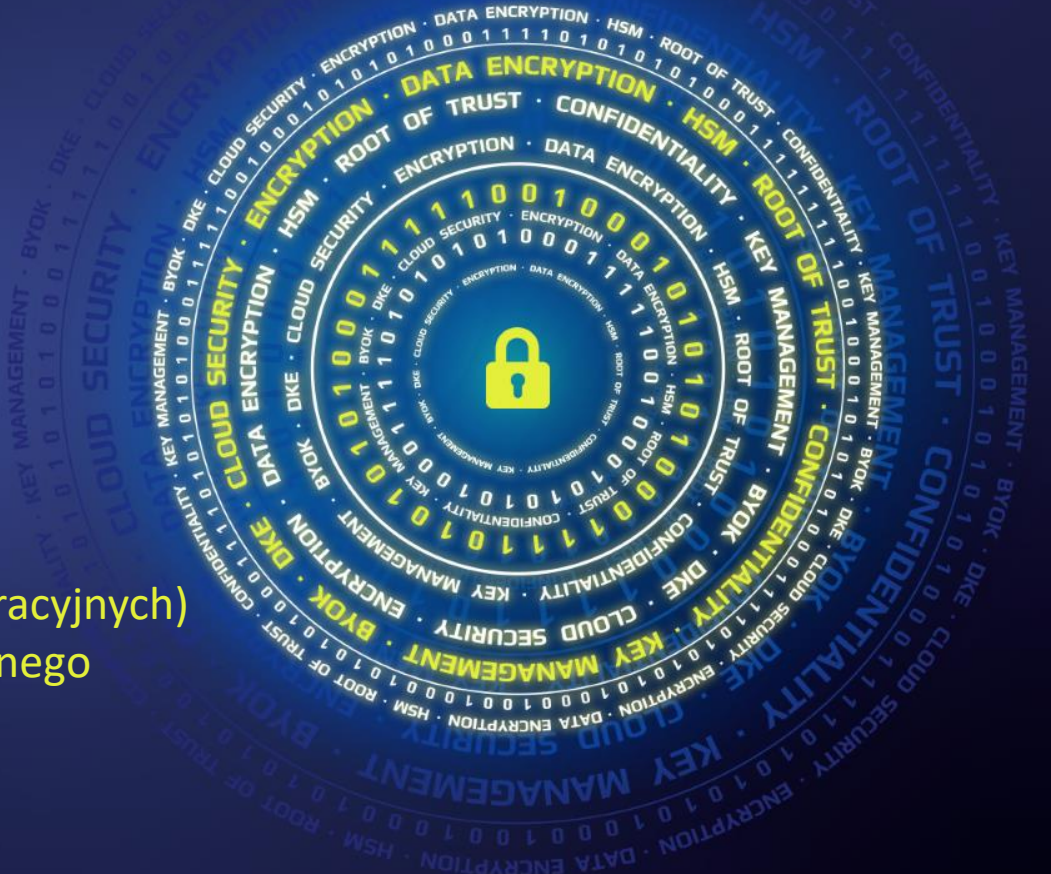
CryptoPanel





CryptoPanel

edycja #17



Ochrona wrażliwych plików (np. konfiguracyjnych) za pomocą szyfrowania ze wsparciem silnego uwierzytelniania.

CryptoPanel

dziś dyskutują

Patryk Jonczyk

Security Specialist
Patryk.jonczyk@clico.pl
mob. +48 667 440 442

Jarosław Ulczok

Pre-sales Consultant
Jaroslaw.Ulczok@thalesgroup.com
mob. +48 603 056 667

CryptoPanel

TEST WIEDZY #17

Ochrona wrażliwych plików (np. konfiguracyjnych) za pomocą szyfrowania ze wsparciem silnego uwierzytelniania

CryptoPanel

problem

co nas boli...

- **Jesteśmy firmą, która opiekuje się zasobami IT innych firm.**
- **Część zasobów naszych klientów utrzymujemy w naszych DC, a cześć usług świadczymy w DC klientów**
- **Poszukujemy rozwiązania ochrony szczególnie wrażliwych plików z punktu widzenia konfiguracji i utrzymania systemów:**
  - Pliki konfiguracyjne
  - Pliki PEM (certyfikaty, klucze prywatne, itp.)
  - Pliki INI (np. CyberArk dbparm.ini)
  - I inne
- **Rozwiązanie powinno pozwalać na uwierzytelnianie (2 składnikowe) naszych administratorów przy dostępie do plików.**
- **Rozliczalność…**

- **… rozwiązanie powinno być przeźroczyste dla aplikacji korzystających z plików konfiguracyjnych (silniki baz, serwerów WWW, PAM-ów, itp.)**
- **… aplikacje/usługi (korzystające z plików konfiguracyjnych) muszą być wyłączone z 2FA!**
- **… czy rozwiązanie jest dostępne dla platform Windows i Linux (kilka dystrybucji) a może i MacOS?**
- **… czy rozwiązanie będzie działać w chmurze - np. DC klienta?**

CryptoPanel

rozwiązanie

Skoro wymieniłeś CyberArk… ☺

…to pokażmy co może znajdować się w pliku konfiguracyjnym…

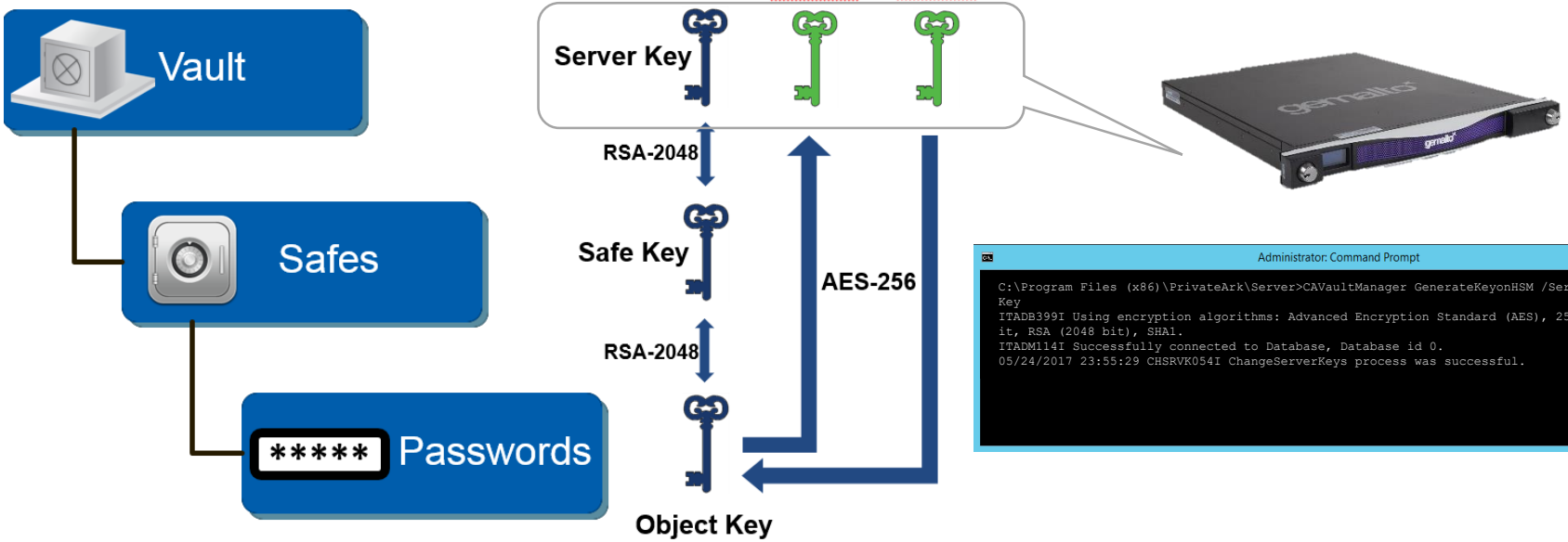
CyberArk & HSM – znana integracja

Security Issues

The security of the Vault relies heavily on the strength, protection, and controlled accessibility of the keys.

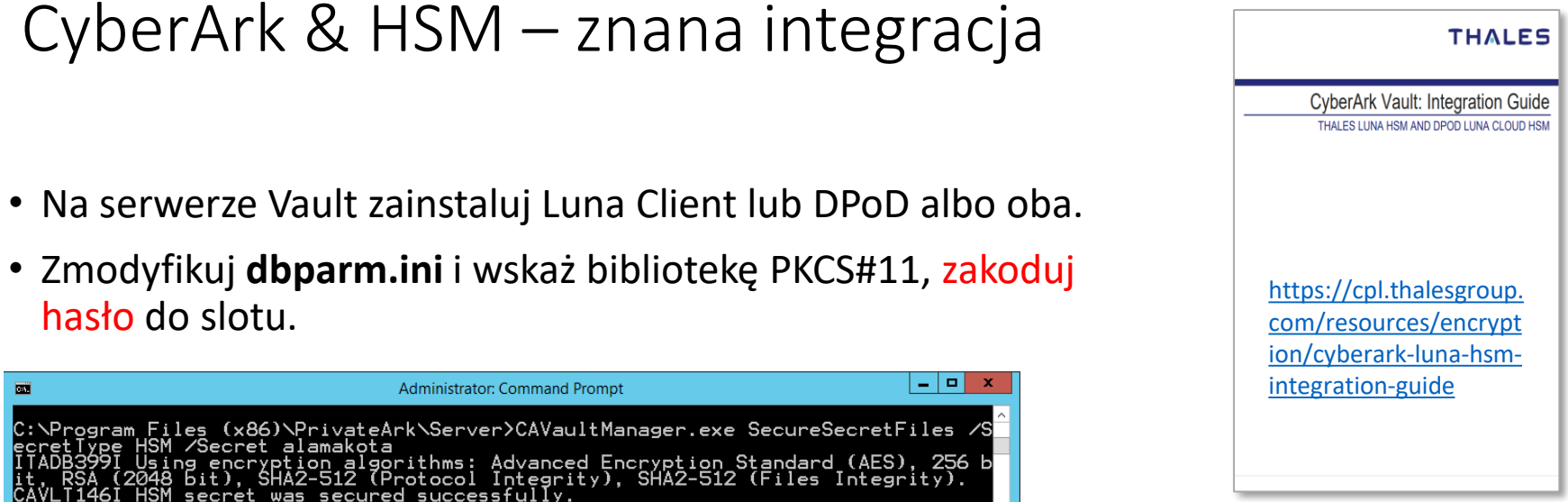
Key strength and protection

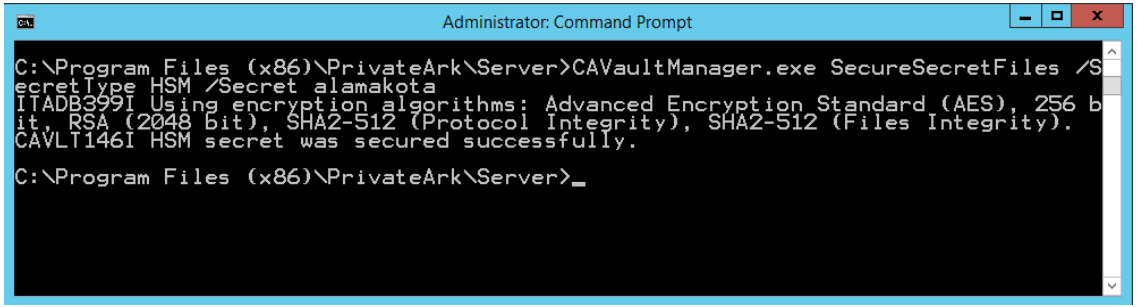
If an unauthorized party guesses or compromises either the Server Key or the Recovery Private Key, they may be able to decrypt all the information that is stored on the Vault server, or backed up elsewhere. Therefore, it is essential to generate strong, hard-to-guess keys and protect them with controlled access.

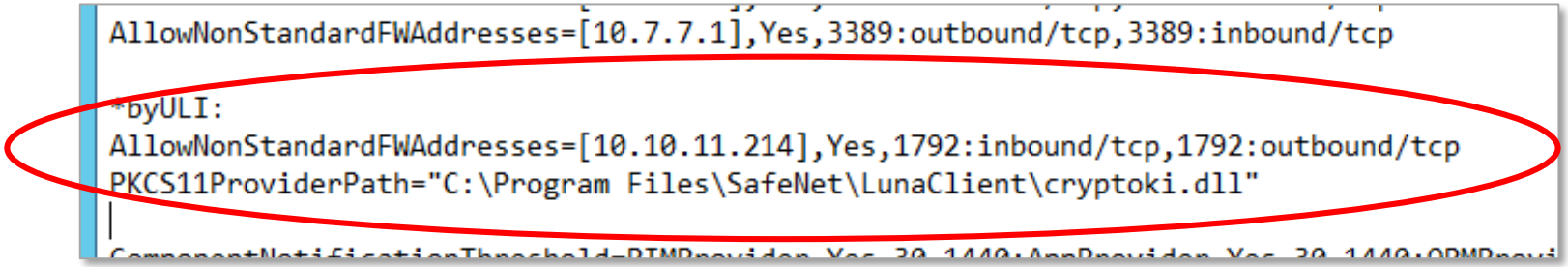


CyberArk & HSM – znana integracja

- Na serwerze Vault zainstaluj Luna Client lub DPoD albo oba.
- Zmodyfikuj **dbparm.ini** i wskaż bibliotekę PKCS#11, zakoduj hasło do slotu.

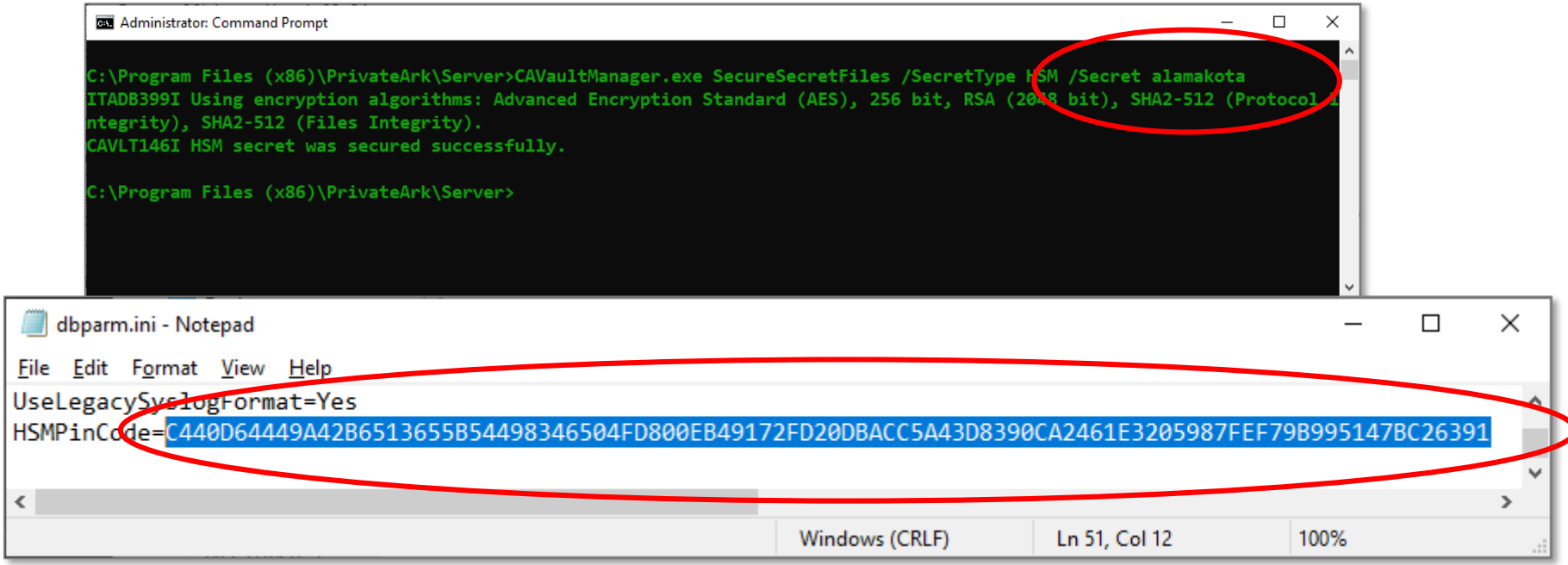




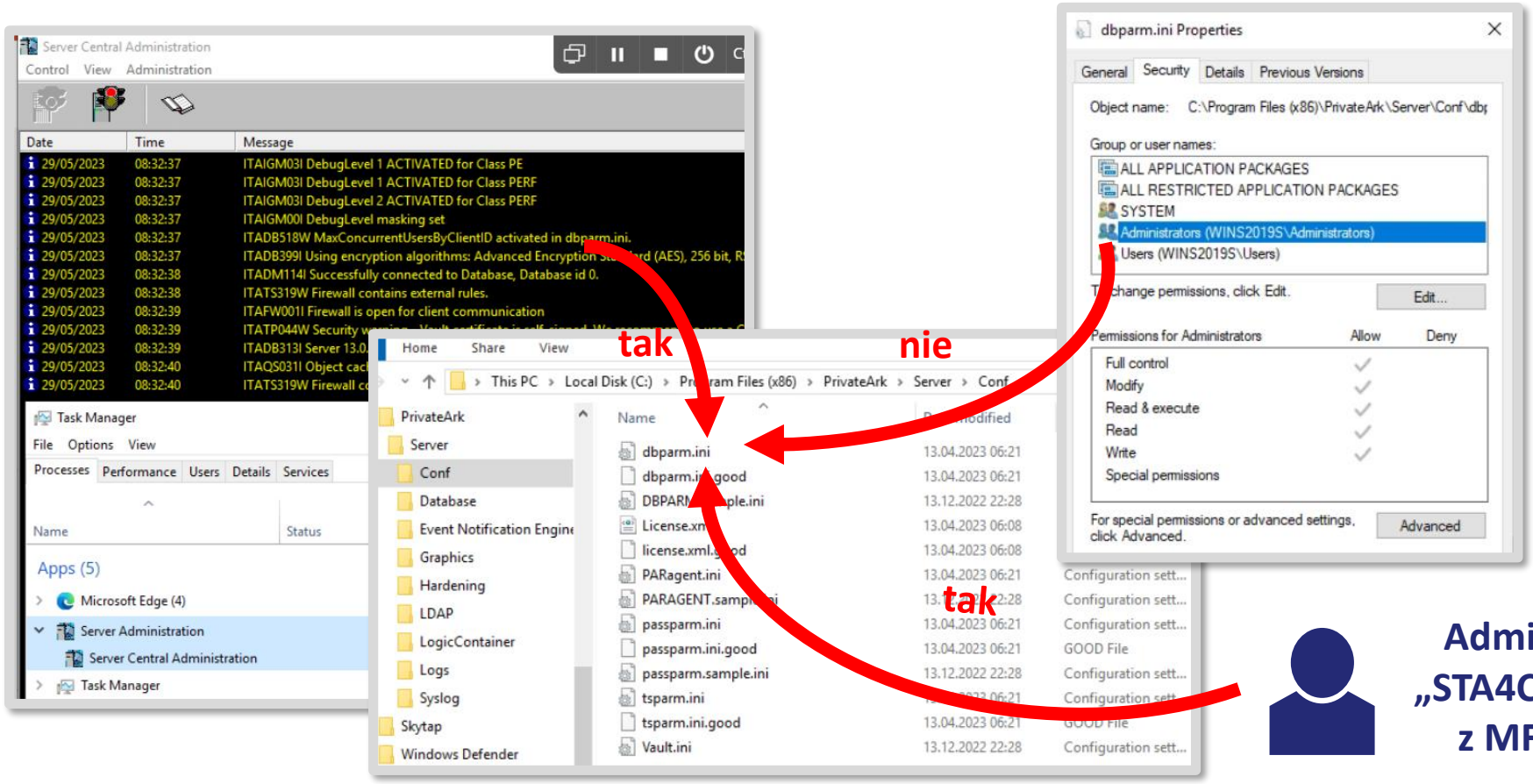


CyberArk & HSM – znana integracja

- Utwórz hasło (do slotu/partycji)
- Będzie przechowywane w **dbparm.ini**



CyberArk - tak, Admin - nie, CTE4STA - tak

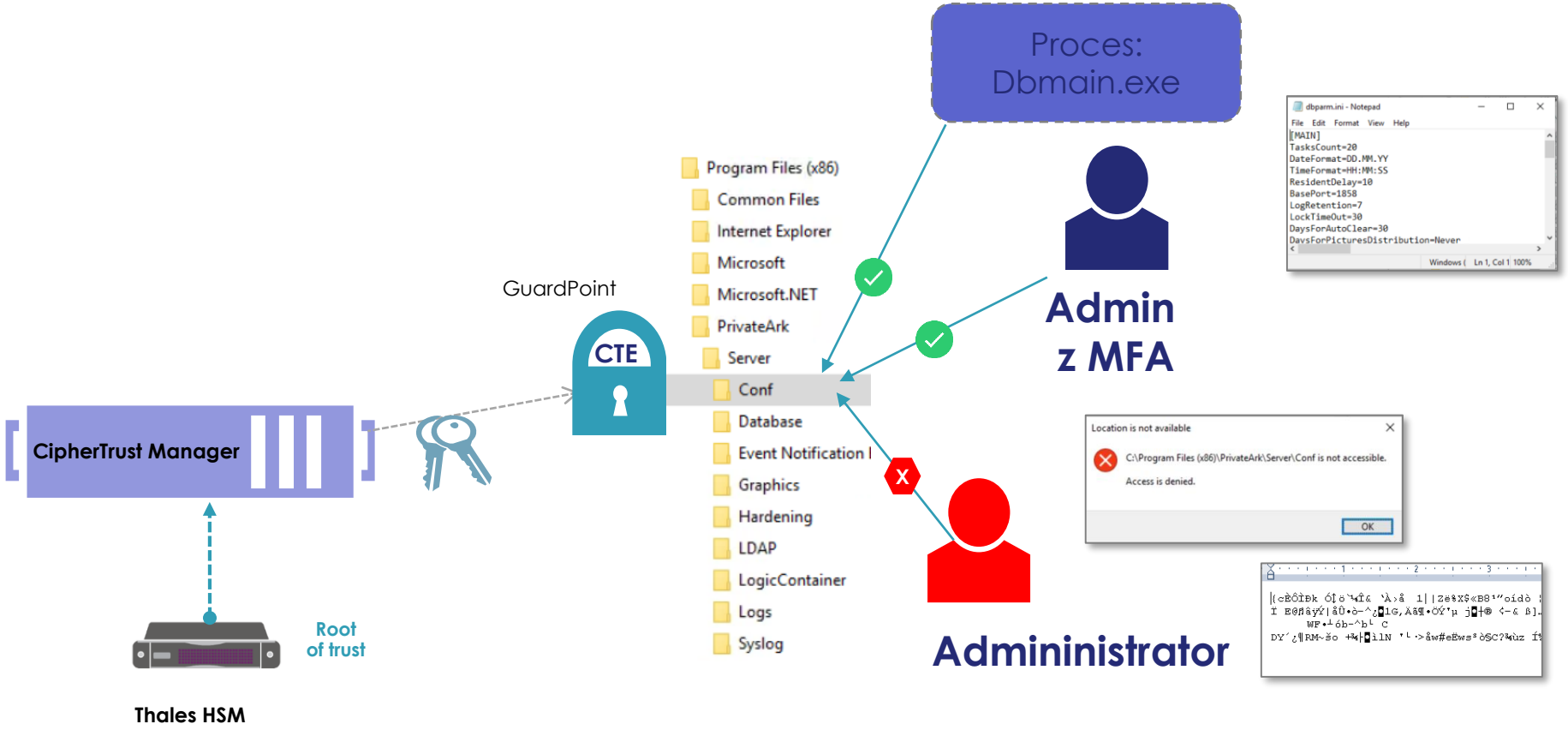


Rozwiązanie to:

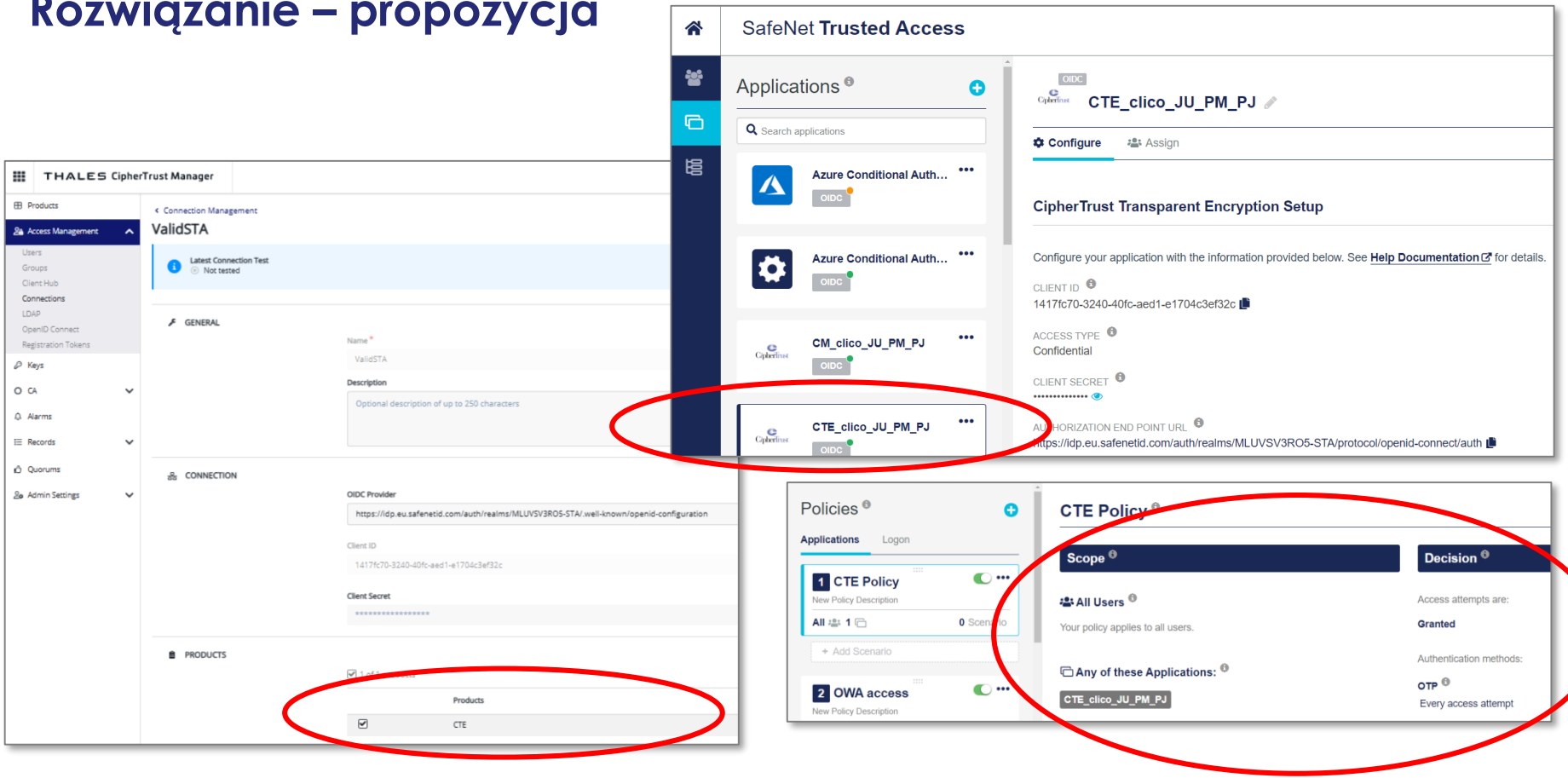
1. Zastosowanie CipherTrust Transparent Encryption (CTE) do ochrony (zaszyfrowania plików) oraz

2. Dodanie MFA (wspieranego przez CTE) przy dostępie do tych plików

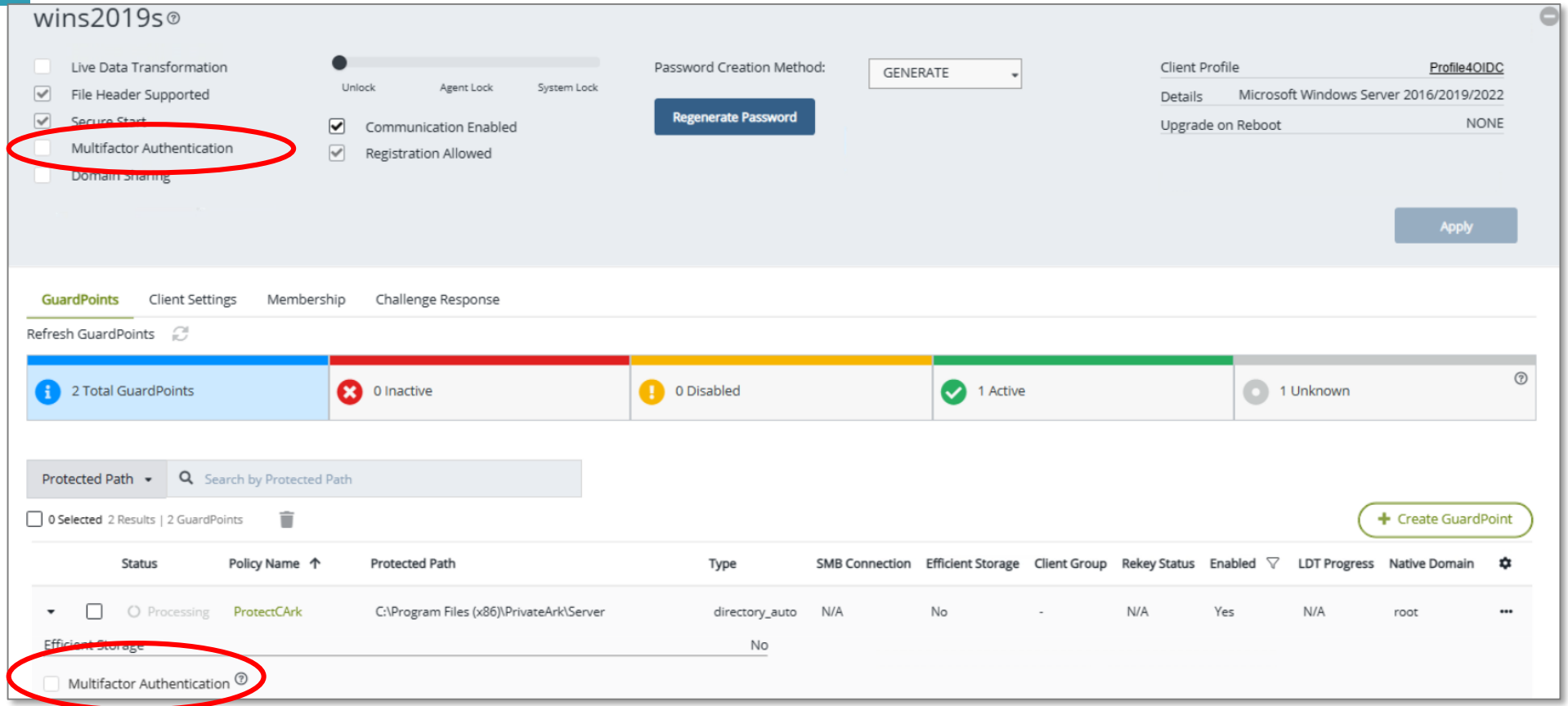
Rozwiązanie – propozycja



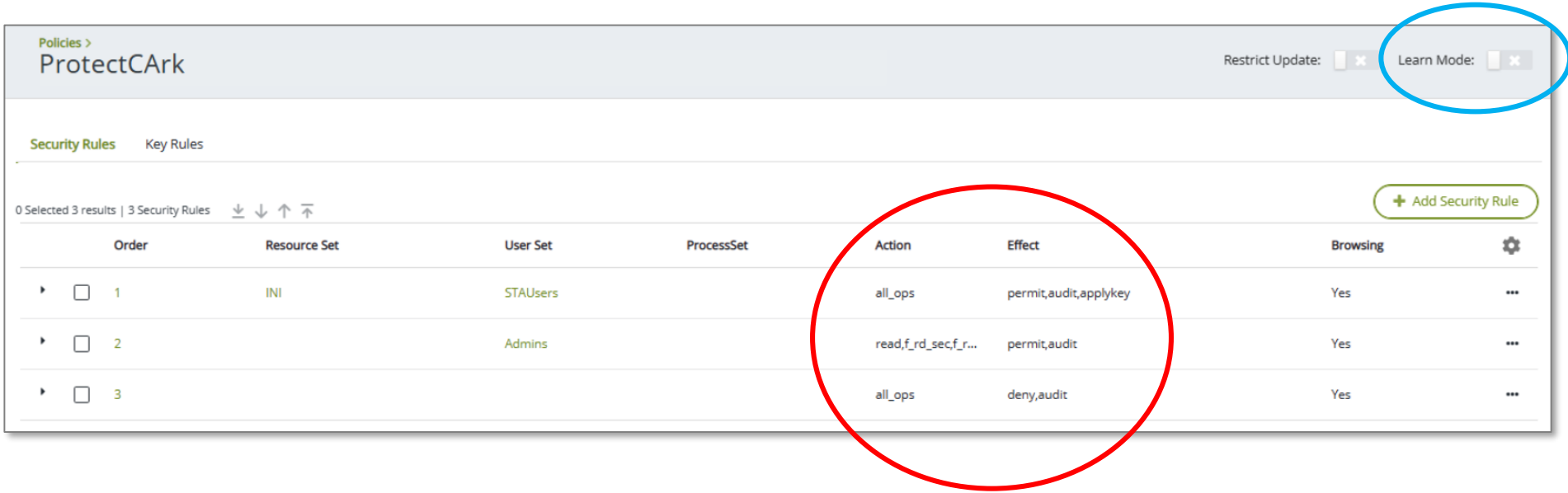
Rozwiązanie – propozycja



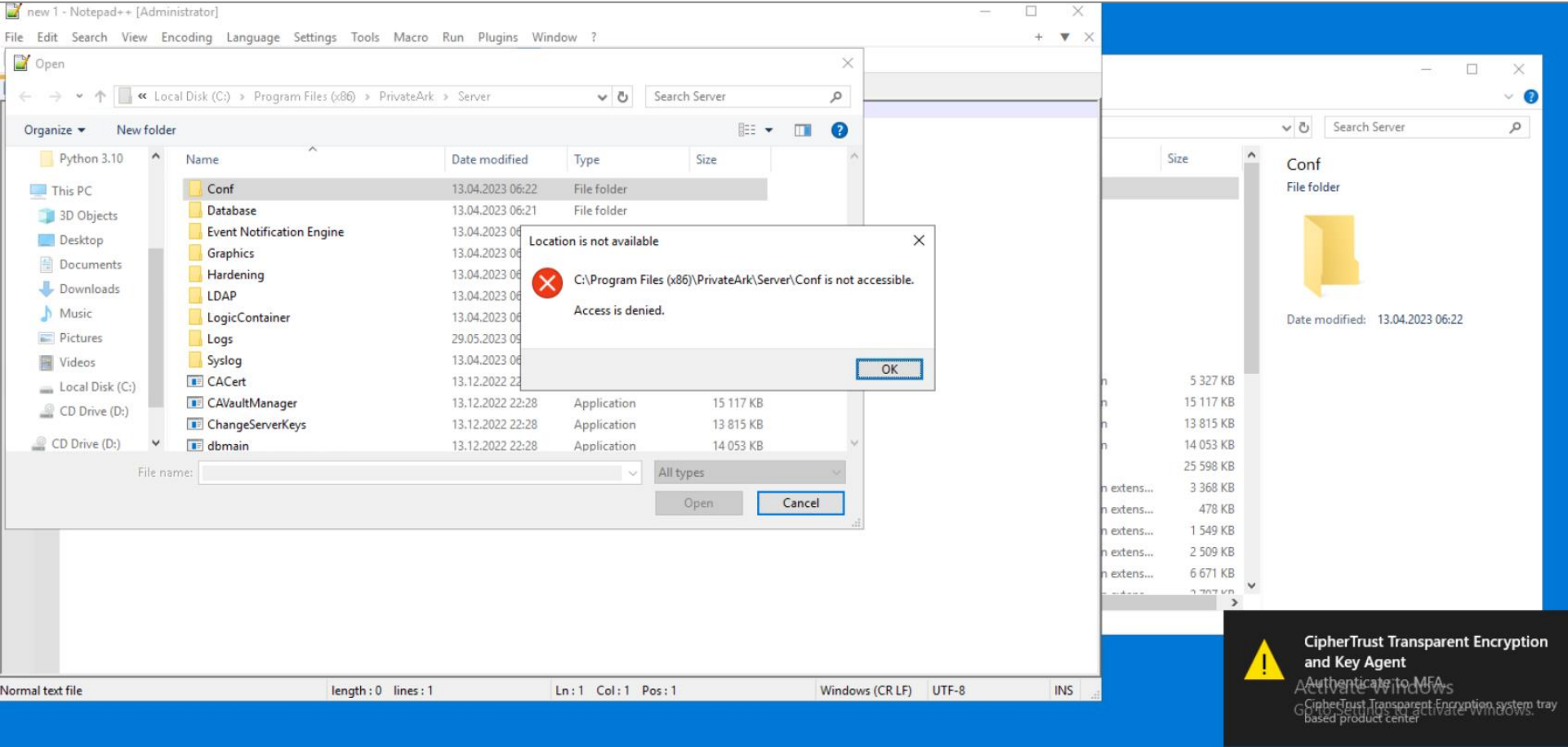
Rozwiązanie – propozycja

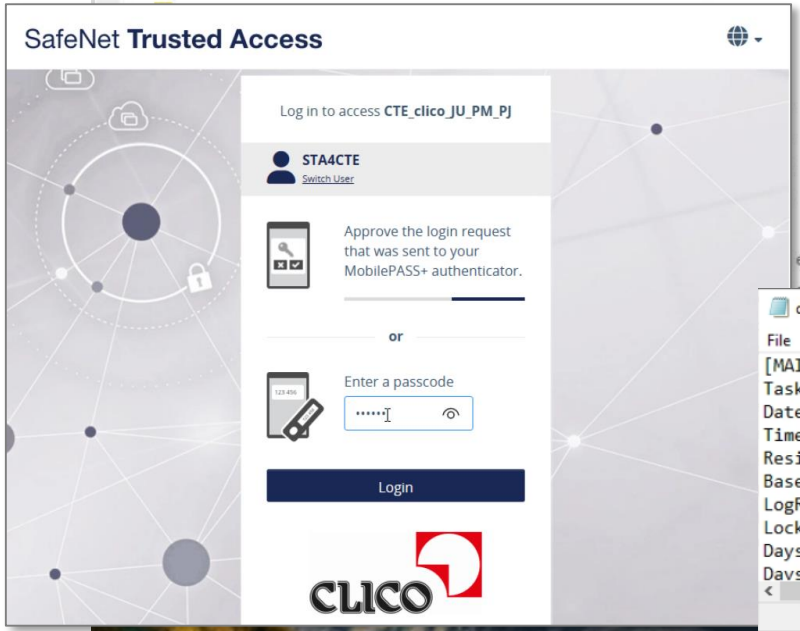


Rozwiązanie – propozycja

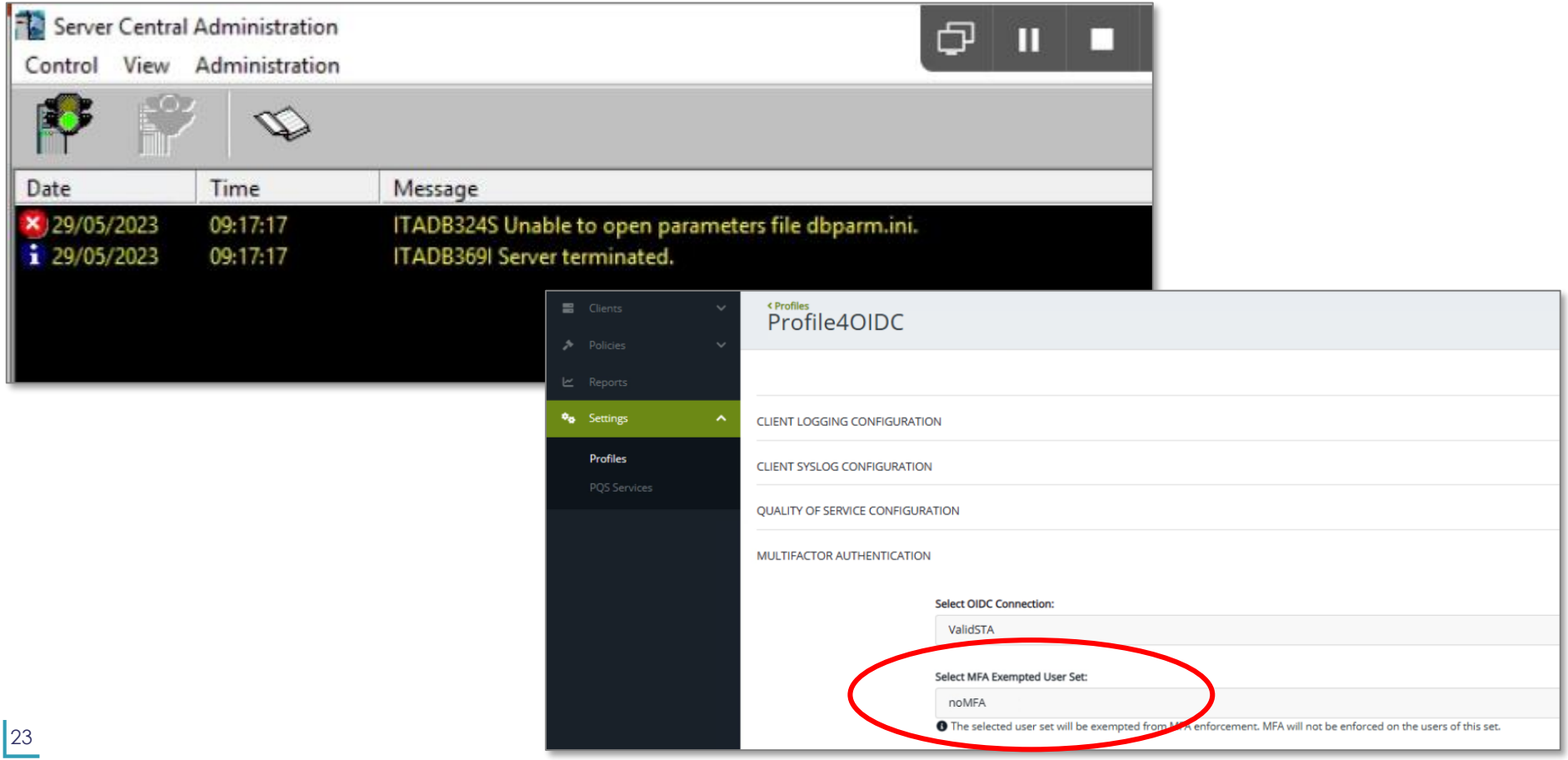


Rozwiązanie – propozycja

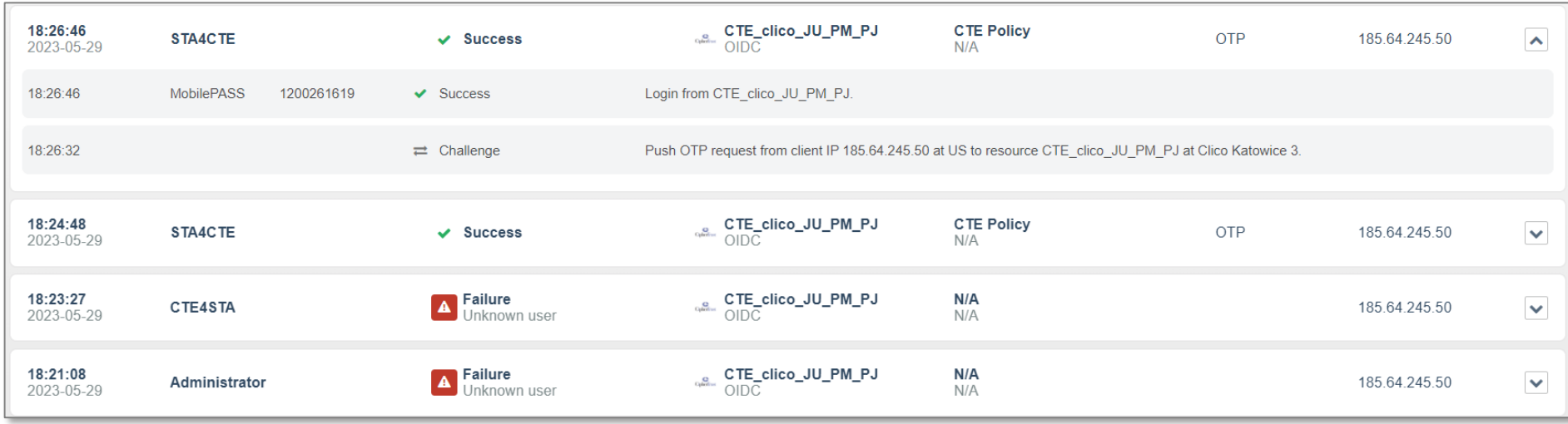



SafeNet Trusted Access
Log in to access CTE_clico_JU_PM_PJ
STA4CTE
Switch User
Approve the login request that was sent to your MobilePASS+ authenticator.
or
Enter a passcode
Login
CLICO

Pozostał jeszcze mały szczegół: dbmain.exe



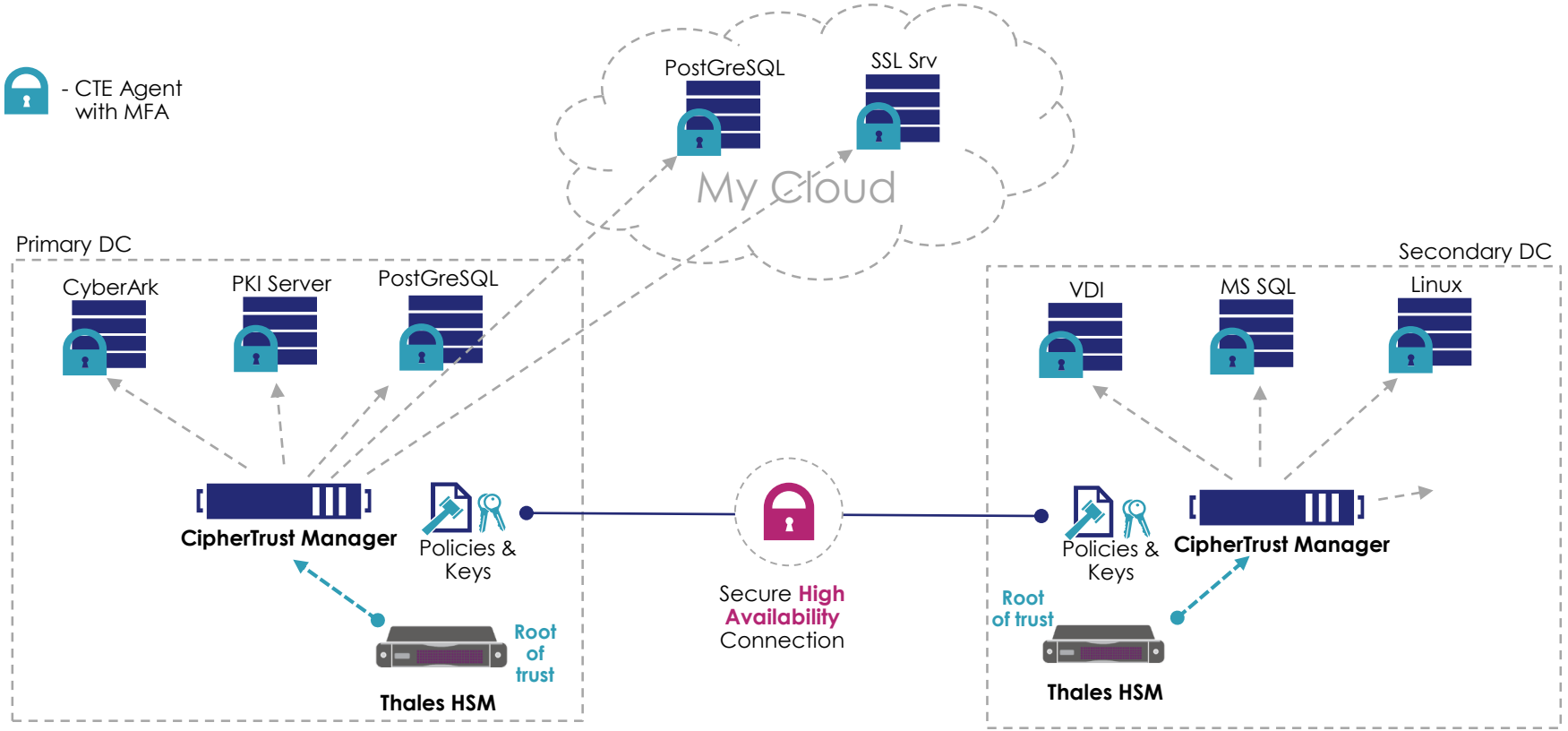
A jak to wygląda w logach?



18:26:46 2023-05-29	**STA4CTE**		✔ **Success**	**CTE_clico_JU_PM_PJ** OIDC	**CTE Policy** N/A	OTP	185.64.245.50
18:26:46	MobilePASS	1200261619	✔ Success	Login from CTE_clico_JU_PM_PJ.			
18:26:32			⇄ Challenge	Push OTP request from client IP 185.64.245.50 at US to resource CTE_clico_JU_PM_PJ at Clico Katowice 3.			
18:24:48 2023-05-29	**STA4CTE**		✔ **Success**	**CTE_clico_JU_PM_PJ** OIDC	**CTE Policy** N/A	OTP	185.64.245.50
18:23:27 2023-05-29	**CTE4STA**		⚠ **Failure** Unknown user	**CTE_clico_JU_PM_PJ** OIDC	**N/A** N/A		185.64.245.50
18:21:08 2023-05-29	**Administrator**		⚠ **Failure** Unknown user	**CTE_clico_JU_PM_PJ** OIDC	**N/A** N/A		185.64.245.50

THALES

Proponowana architektura



„Nauczki“, czyli *lessons learned #1/1*

Nie wszystkie systemy MFA OIDC są sprawdzone pod kątem kompatybilności

- Lista: https://thalesdocs.com/ctp/cte-con/cte/latest/user-manuals/win-adv/win-adv-getting/win-adv-2fa/win-adv-2fa-providers/index.html

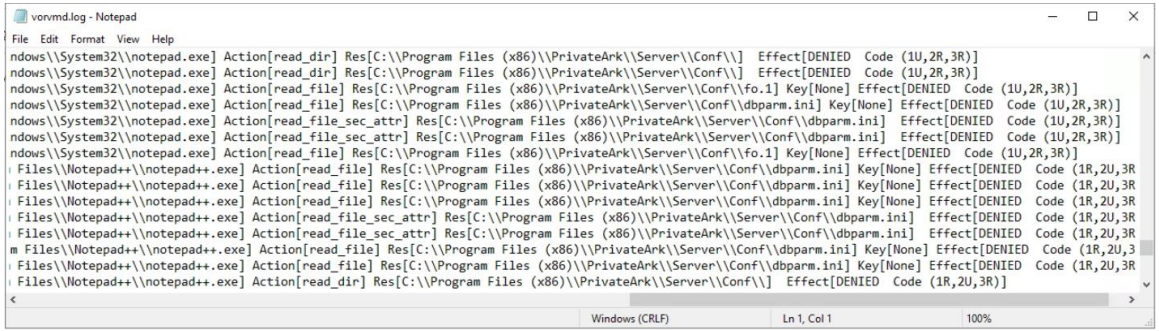
Thales will be continually adding new MFA providers to CipherTrust Transparent Encryption.
When the MFA providers pass compatibly testing, they will be added to this page.

Wdrożenie CTE wymaga posiada wspieranego systemu operacyjnego na którym instalowany jest agent (on-prem lub w chmurze)

- **MacOS nie jest wspierany 😐**
- **Matryca kompatybilności:** https://thalesdocs.com/ctp/cte/cte-cm/index.html

W budowie polityk (identyfikacji procesów, użytkowników, itp.) nieocenioną pomocą jest typ Learn Mode.

- **Uwaga**: pracę w trybie Learn Mode bez akcji „apply key” – możemy uszkodzić zaszyfrowany plik.



THALES

Tego raczej nie znajdziecie w dokumentacji.

Czy można się „wylogować z CTE i jak długo jestem „zalogowany”?

MFA authentication remains as long as user remains logged in. A user can always explicitly logout whenever intended.
There is also a voradmin command to set auto log out, specified in minutes. By default, it is 0, means no auto logout.

```
voradmin mfa set-auth-expiry <time in minutes, specify 0 to disable expiry>
```

Only admin can run this command. Admin can check its value using following command
```
voradmin mfa config
```

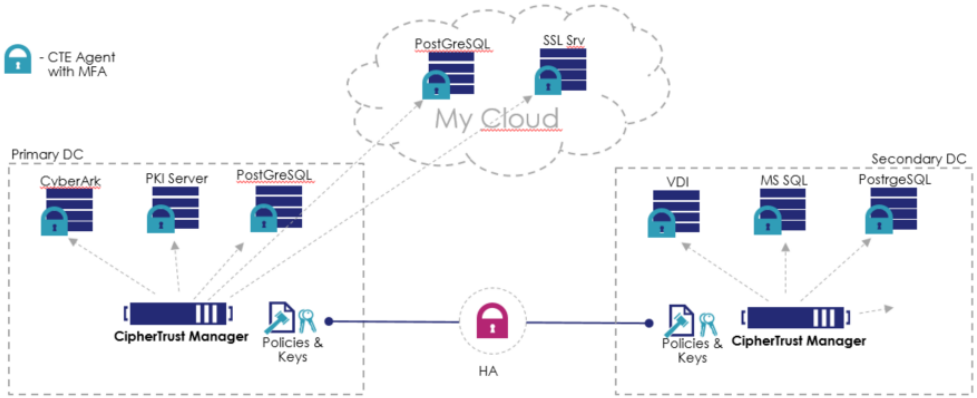
It displays all MFA settings.

CryptoPanel

podsumowanie

Podsumowanie i słowo o tym co do wyceny

- **CM jako „mózg” systemu oraz wymagana ilość licencji CTE**



- **produkty dostępne w kanale partnerskim**
- **licencja dożywotnia lub subskrypcja**
- **licencja demo do testów!**
- **zalecane zastosowanie HSM jako RoT**

Wycena:

- **2x CipherTrust Manager (16400 € netto / instancję)**
- **Nx CTE (5180 € netto / agenta)**
- **Opcja LDT: Mx Add-on CTE-LDT – (1250 € / instancja CTE)**

CryptoPanel

CryptoPanel

TEST WIEDZY #17

Ochrona wrażliwych plików (np. konfiguracyjnych) za pomocą szyfrowania ze wsparciem silnego uwierzytelniania

CryptoPanel #17 – bądź pierwszy, odbierz voucher!

- Zapraszamy do testu wiedzy z tematu: *„Ochrona wrażliwych plików (np. konfiguracyjnych) za pomocą szyfrowania ze wsparciem silnego uwierzytelniania.”*
- Uwaga: **5 najszybszych i poprawnych** odpowiedzi nagradzamy podwójną wejściówka do:

Multikino®

- Przy wypełnianiu formularza prosimy podać (aby móc zidentyfikować uczestnika!):
  - **Imię i Nazwisko**
  - **Adres e-mail**

Materiały

Oprogramowanie do pobrania lub wersja ewaluacyjna...

- W takim przypadku prosimy o kontakt z nami!

Dokumentacja:

- CipherTrust Manger: https://www.thalesdocs.com/ctp/cm/latest/
- CTE: https://www.thalesdocs.com/ctp/cte-con/cte/latest/user-manuals/index.html
- Matryca kompatybilności: https://www.thalesdocs.com/ctp/cte-con/cte/latest/comp-matrix/index.html
- Wspierane platformy: https://thalesdocs.com/ctp/cte/cte-cm/index.html

CryptoPanel