

# CryptoPanel

edycja #17

za chwilę zaczynamy...

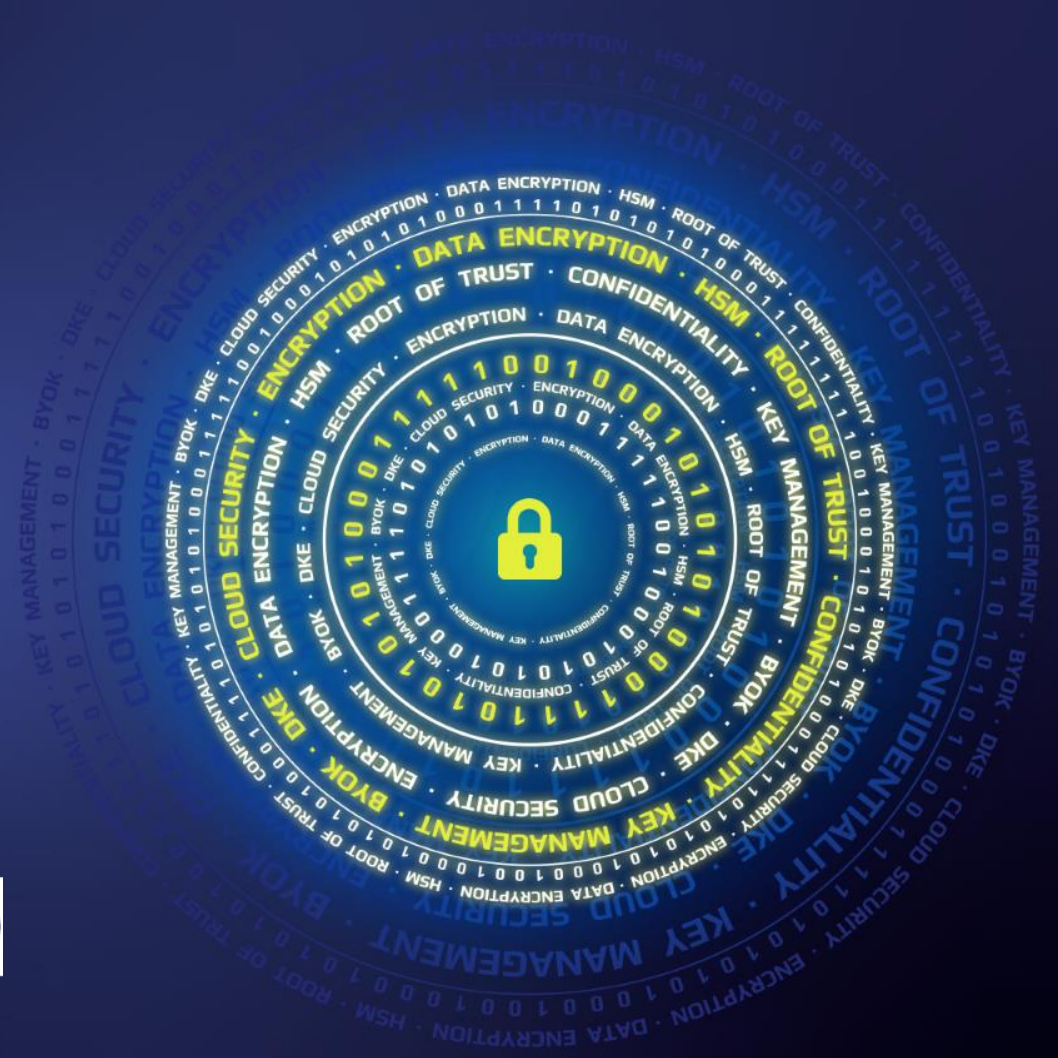


# CryptoPanel

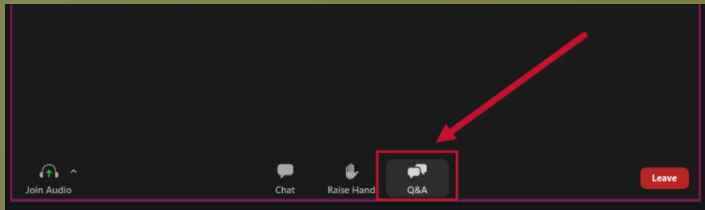
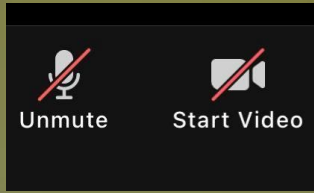


THALES

CLICO



# CryptoPanel



# CryptoPanel

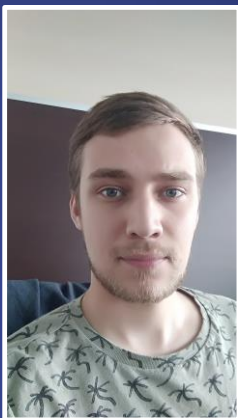
edycja #17

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



# CryptoPanel

dziś dyskutują



Patryk Jonczyk

Security Specialist

[Patryk.jonczyk@clico.pl](mailto:Patryk.jonczyk@clico.pl)

mob. +48 667 440 442



Jarosław Ulczok

Pre-sales Consultant

[Jaroslaw.Ulczok@thalesgroup.com](mailto:Jaroslaw.Ulczok@thalesgroup.com)

mob. +48 603 056 667



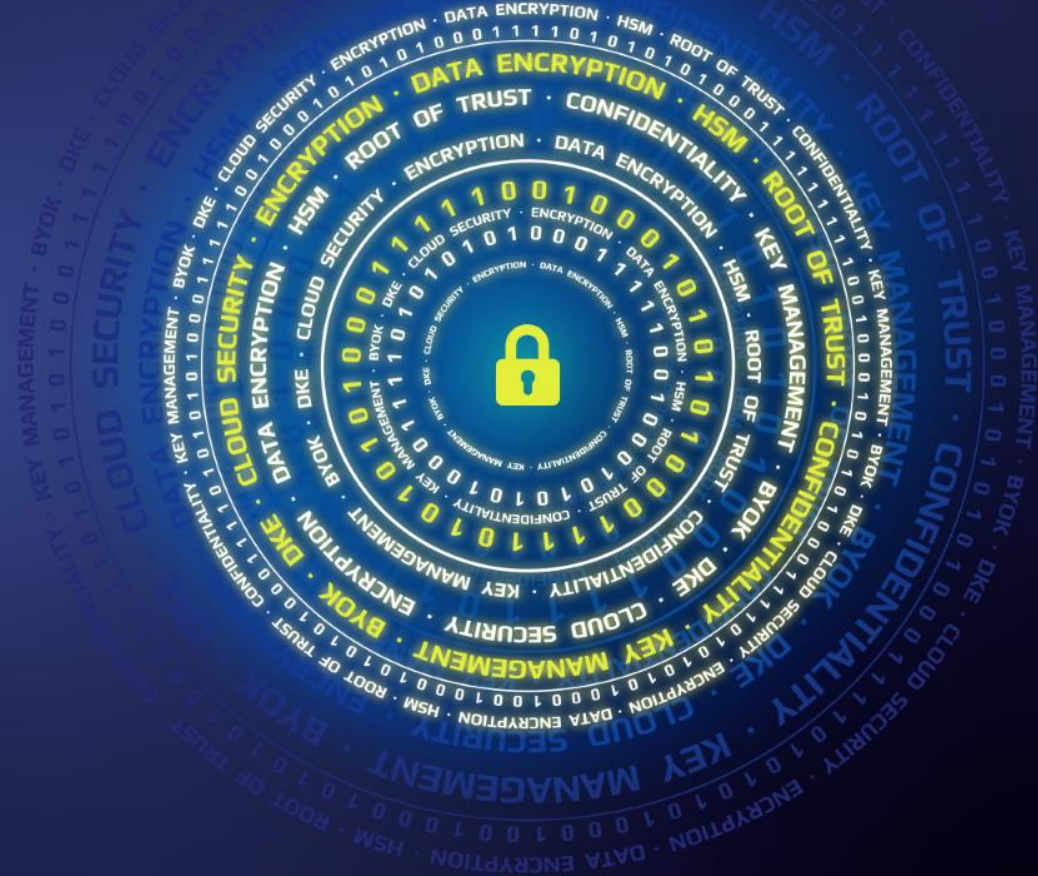
# CryptoPanel

## 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 część 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 przezroczyste 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 wymieniałeś CyberArk... 😊

**...to pokażemy co może znajdować się w pliku konfiguracyjnym...**

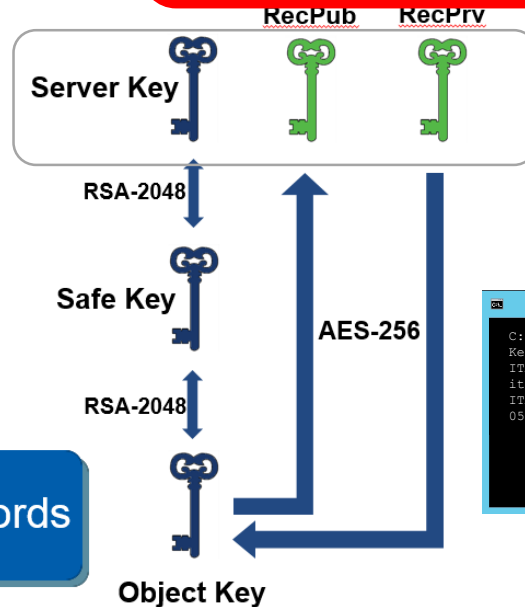
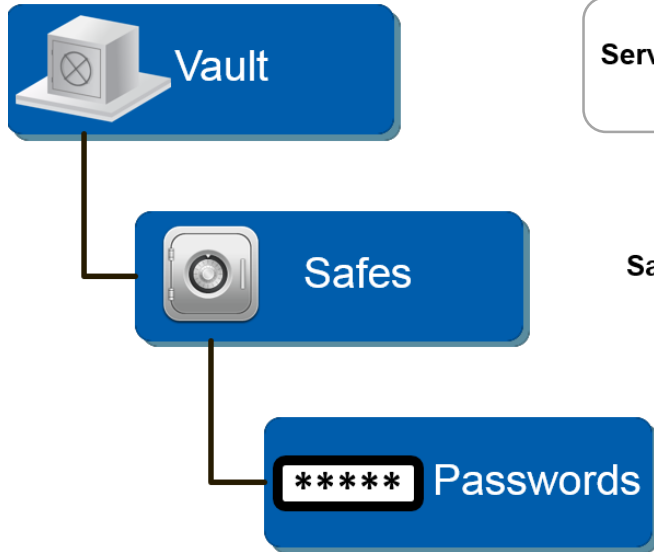
# CyberArk & HSM – znana integracja

## 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.

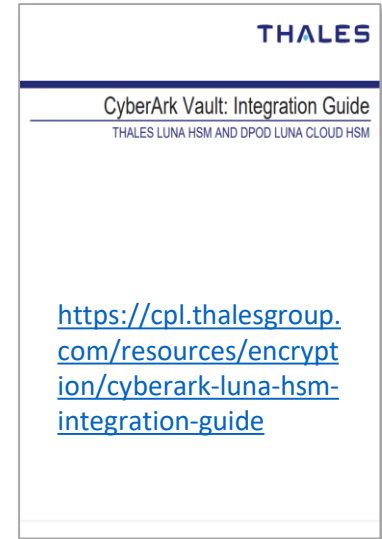


```
Administrator: Command Prompt
C:\Program Files (x86)\PrivateArk\Server>CAVaultManager GenerateKeyonHSM /Server
Key
TPADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 b
it, RSA (2048 bit), SHA1.
TPADM114I Successfully connected to Database, Database id 0.
05/24/2017 23:55:29 CHSRVK054I ChangeServerKeys process was successful.
```

# 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.

```
Administrator: Command Prompt
C:\Program Files (x86)\PrivateArk\Server>CAVaultManager.exe SecureSecretFiles /S
ecretType HSM /Secret alamakota
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 b
it, RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512 (Files Integrity).
CAVLT146I HSM secret was secured successfully.
C:\Program Files (x86)\PrivateArk\Server>_
```



```
AllowNonStandardFWAddresses=[10.7.7.1],Yes,3389:outbound/tcp,3389:inbound/tcp
```

```
*byULI:
```

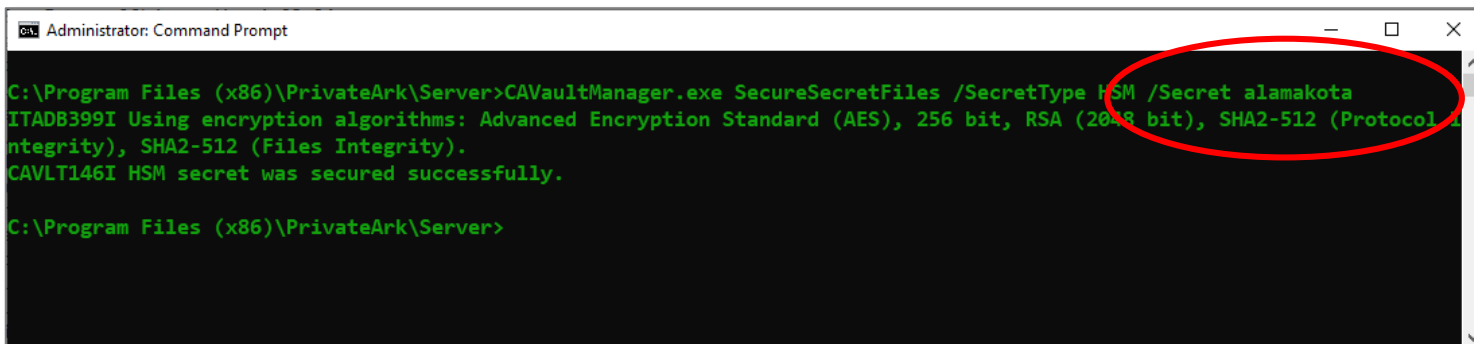
```
AllowNonStandardFWAddresses=[10.10.11.214],Yes,1792:inbound/tcp,1792:outbound/tcp
```

```
PKCS11ProviderPath="C:\Program Files\SafeNet\LunaClient\cryptoki.dll"
```

```
ComponentNotificationThreshold-BIProvider:Yes-30-1440:AppProvider:Yes-30-1440:OPMProv:
```

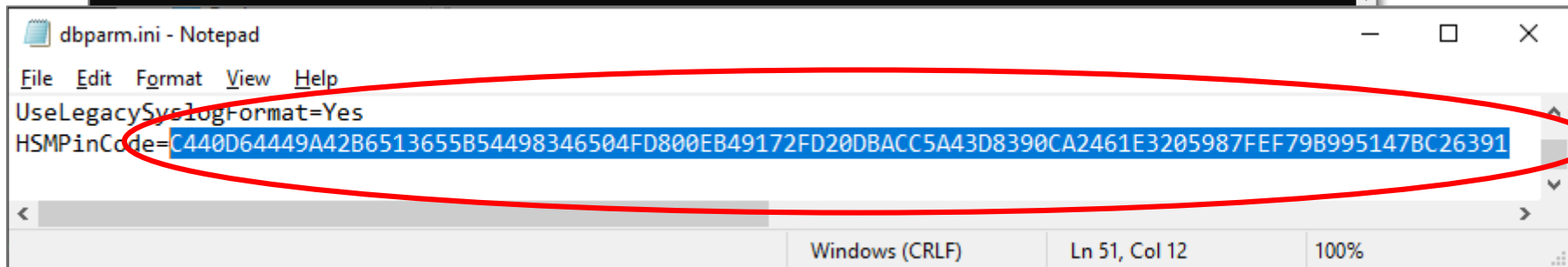
# CyberArk & HSM – znana integracja

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



```
Administrator: Command Prompt
C:\Program Files (x86)\PrivateArk\Server>CAVaultManager.exe SecureSecretFiles /SecretType HSM /Secret alamakota
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (2048 bit), SHA2-512 (Protocol 1
ntegrity), SHA2-512 (Files Integrity).
CAVLT146I HSM secret was secured successfully.

C:\Program Files (x86)\PrivateArk\Server>
```



```
dbparm.ini - Notepad
File Edit Format View Help
UseLegacySyslogFormat=Yes
HSMPinCode=C440D64449A42B6513655B54498346504FD800EB49172FD20DBACC5A43D8390CA2461E3205987FEF79B995147BC26391
Windows (CRLF) Ln 51, Col 12 100%
```

# CyberArk - tak, Admin - nie, CTE4STA - tak

Server Central Administration - Administration

Date	Time	Message
29/05/2023	08:32:37	ITAIGM03  DebugLevel 1 ACTIVATED for Class PE
29/05/2023	08:32:37	ITAIGM03  DebugLevel 1 ACTIVATED for Class PERF
29/05/2023	08:32:37	ITAIGM03  DebugLevel 2 ACTIVATED for Class PERF
29/05/2023	08:32:37	ITAIGM00  DebugLevel masking set
29/05/2023	08:32:37	ITADB518W MaxConcurrentUsersByClientID activated in dbparm.ini.
29/05/2023	08:32:37	ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, R
29/05/2023	08:32:38	ITADM114I Successfully connected to Database, Database id 0.
29/05/2023	08:32:38	ITATS319W Firewall contains external rules.
29/05/2023	08:32:39	ITAFW001I Firewall is open for client communication
29/05/2023	08:32:39	ITATP044W Security warning: Web server configuration file is not encrypted
29/05/2023	08:32:39	ITADB313I Server 13.0
29/05/2023	08:32:40	ITAQ5031I Object cach
29/05/2023	08:32:40	ITATS319W Firewall c

Task Manager - Performance

Name	Status
Microsoft Edge (4)	
Server Administration	
Server Central Administration	
Task Manager	

File Explorer - This PC > Local Disk (C:) > Program Files (x86) > PrivateArk > Server > Conf

Name	Modified
dbparm.ini	13.04.2023 06:21
dbparm.ini.good	13.04.2023 06:21
DBPARM.sample.ini	13.12.2022 22:28
License.xml	13.04.2023 06:08
license.xml.good	13.04.2023 06:08
PARagent.ini	13.04.2023 06:21
PARAGENT.sample.ini	13.12.2022 22:28
passparm.ini	13.04.2023 06:21
passparm.ini.good	13.04.2023 06:21
passparm.sample.ini	13.12.2022 22:28
tsparm.ini	13.04.2023 06:21
tsparm.ini.good	13.04.2023 06:21
Vault.ini	13.12.2022 22:28

Red arrows point from the text 'tak' to 'dbparm.ini' and 'DBPARM.sample.ini', and from 'nie' to 'dbparm.ini'. Another red arrow points from the text 'tak' to the 'dbparm.ini Properties' dialog box.

dbparm.ini Properties - Security

Object name: C:\Program Files (x86)\PrivateArk\Server\Conf\dbp

Group or user names:

- ALL APPLICATION PACKAGES
- ALL RESTRICTED APPLICATION PACKAGES
- SYSTEM
- Administrators (WINS2019S\Administrators)
- Users (WINS2019S\Users)

Change permissions, click Edit. [Edit...]

Permissions for Administrators	Allow	Deny
Full control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Modify	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read & execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced. [Advanced]



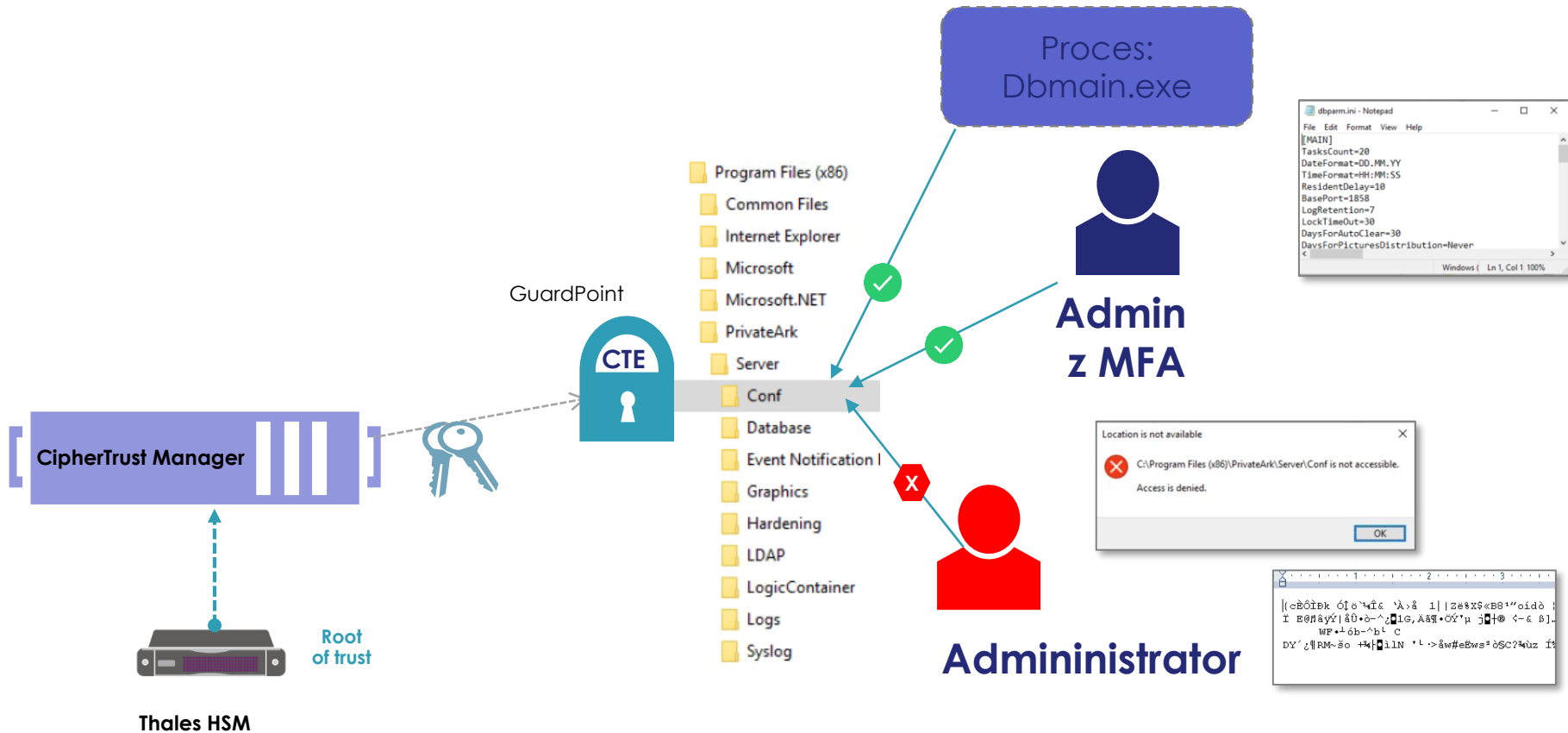
**Admin**  
**„STA4CTE”**  
**z MFA**

# 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

**THALES CipherTrust Manager**

Access Management

ValidSTA

Latest Connection Test  
Not tested

**GENERAL**

Name: ValidSTA

Description: Optional description of up to 250 characters

**CONNECTION**

OIDC Provider: `https://idp.eu.safenetid.com/auth/realms/MLUVSV3R05-STA/well-known/openid-configuration`

Client ID: 1417fc70-3240-40fc-aed1-e1704c3ef32c

Client Secret: \*\*\*\*\*

**PRODUCTS**

- CTE

**SafeNet Trusted Access**

Applications

Search applications

- Azure Conditional Auth...
- Azure Conditional Auth...
- CM\_clico\_JU\_PM\_PJ
- CTE\_clico\_JU\_PM\_PJ**

**CTE\_clico\_JU\_PM\_PJ**

Configure Assign

**CipherTrust Transparent Encryption Setup**

Configure your application with the information provided below. See [Help Documentation](#) for details.

CLIENT ID: 1417fc70-3240-40fc-aed1-e1704c3ef32c

ACCESS TYPE: Confidential

CLIENT SECRET: \*\*\*\*\*

AUTHORIZATION END POINT URL: `https://idp.eu.safenetid.com/auth/realms/MLUVSV3R05-STA/protocol/openid-connect/auth`

**Policies**

Applications Logon

- 1 CTE Policy** (New Policy Description)
- All 1 0 Scenario
- 2 OWA access (New Policy Description)

**CTE Policy**

Scope: All Users

Decision: Granted

Your policy applies to all users.

Authentication methods: OTP

Every access attempt



# Rozwiązanie – propozycja

wins2019s@

Live Data Transformation

File Header Supported

Secure Start

Multifactor Authentication

Domain Sharing

●

Unlock

Agent Lock

System Lock

Password Creation Method:

GENERATE

Regenerate Password

Client Profile

[Profile4OIDC](#)

Details

Microsoft Windows Server 2016/2019/2022

Upgrade on Reboot

NONE

Apply

GuardPoints

Client Settings

Membership

Challenge Response

Refresh GuardPoints

2 Total GuardPoints

0 Inactive

0 Disabled

1 Active

1 Unknown

Protected Path

Search by Protected Path

0 Selected 2 Results | 2 GuardPoints

Create GuardPoint

Status

Policy Name ↑

Protected Path

Type

SMB Connection

Efficient Storage

Client Group

Rekey Status

Enabled

LDT Progress

Native Domain

Processing

ProtectCARk

C:\Program Files (x86)\PrivateArk\Server

directory\_auto

N/A

No

-

N/A

Yes

N/A

root

Efficient Storage

No

Multifactor Authentication

CryptoPanel



# Rozwiązanie – propozycja

Policies >  
ProtectCArk

Restrict Update:  × Learn Mode:  ×

Security Rules Key Rules

0 Selected 3 results | 3 Security Rules

[+ Add Security Rule](#)

Order	Resource Set	User Set	ProcessSet	Action	Effect	Browsing	
<input type="checkbox"/> 1	INI	STAUsers		all_ops	permit,audit,applykey	Yes	...
<input type="checkbox"/> 2		Admins		read,f_rd_sec,f_r...	permit,audit	Yes	...
<input type="checkbox"/> 3				all_ops	deny,audit	Yes	...



# Rozwiązanie – propozycja

The screenshot shows a Windows File Explorer window open to the path `C:\Program Files (x86)\PrivateArk\Server`. The 'Conf' folder is selected. An error dialog box is displayed in the foreground with the following text:

Location is not available  
C:\Program Files (x86)\PrivateArk\Server\Conf is not accessible.  
Access is denied.  
OK

The File Explorer window also shows a list of files and folders:

Name	Date modified	Type	Size
Conf	13.04.2023 06:22	File folder	
Database	13.04.2023 06:21	File folder	
Event Notification Engine	13.04.2023 06:21	File folder	
Graphics	13.04.2023 06:21	File folder	
Hardening	13.04.2023 06:21	File folder	
LDAP	13.04.2023 06:21	File folder	
LogicContainer	13.04.2023 06:21	File folder	
Logs	29.05.2023 09:21	File folder	
Syslog	13.04.2023 06:21	File folder	
CACert	13.12.2022 22:28	Application	15 117 KB
CAVaultManager	13.12.2022 22:28	Application	13 815 KB
ChangeServerKeys	13.12.2022 22:28	Application	14 053 KB
dbmain	13.12.2022 22:28	Application	



**CipherTrust Transparent Encryption and Key Agent**

Authenticate to MFA  
CipherTrust Transparent Encryption system tray  
Go to Settings to activate Windows  
based product center

Local Disk (C:) > Program Files (x86) > PrivateArk > Server

Name	Date modified	Type	Size
Conf	13.04.2023 06:22	File folder	
Database	13.04.2023 06:21	File folder	
Event Notification Engine	13.04.2023 06:21	File folder	
Graphics	13.04.2023 06:21	File folder	
Hardening	13.04.2023 06:21	File folder	
LDAP	13.04.2023 06:21	File folder	



*You have successfully authenticated, access to GuardPoint is enabled.*

*Close the window to continue.*

*[Logout](#) to disable access to the GuardPoint.*

### 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

123 456

.....

Login



dbparm.ini - Notepad

```
File Edit Format View Help
[MAIN]
TasksCount=20
DateFormat=DD.MM.YY
TimeFormat=HH:MM:SS
ResidentDelay=10
BasePort=1858
LogRetention=7
LockTimeOut=30
DaysForAutoClear=30
DavsForPicturesDistribution=Never
```

Windows ( Ln 1, Col 1 100%



Authenticate

- Multifactor Authentication >
- Exit
- About...

# Pozostał jeszcze mały szczegół: dbmain.exe

Server Central Administration

Control View Administration

Date	Time	Message
 29/05/2023	09:17:17	ITADB324S Unable to open parameters file dbparm.ini.
 29/05/2023	09:17:17	ITADB369I Server terminated.

Profiles  
Profile4OIDC

Clients  
Policies  
Reports  
Settings  
Profiles  
PQS Services

CLIENT LOGGING CONFIGURATION

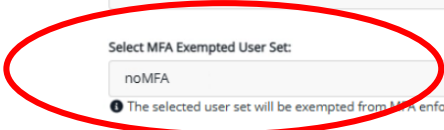
CLIENT SYSLOG CONFIGURATION


QUALITY OF SERVICE CONFIGURATION

MULTIFACTOR AUTHENTICATION















Select OIDC Connection:  
ValidSTA

Select MFA Exempted User Set:  
noMFA



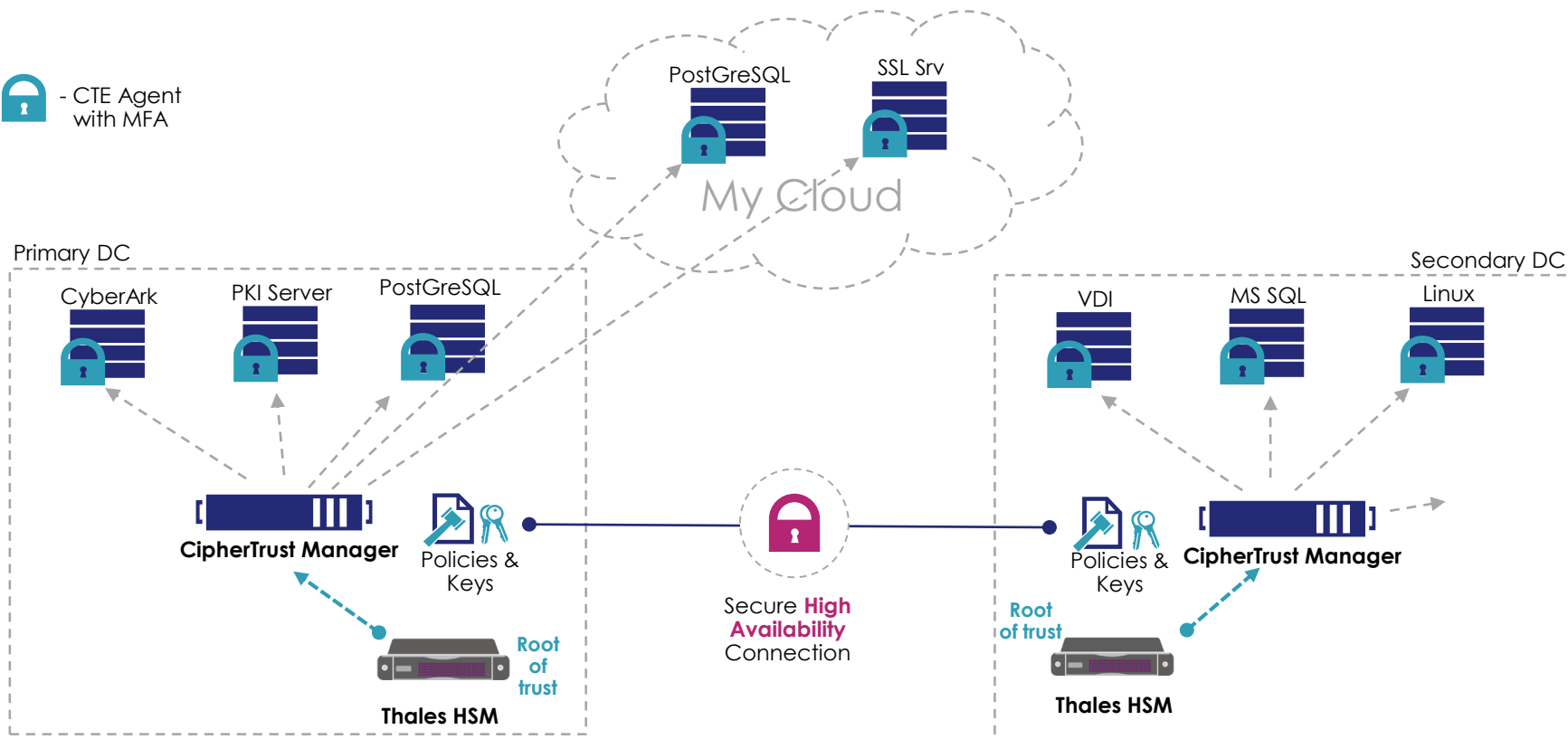
 The selected user set will be exempted from MFA enforcement. MFA will not be enforced on the users of this set.

# A jak to wygląda w logach?

<b>18:26:46</b> 2023-05-29	<b>STA4CTE</b>	 <b>Success</b>	 <b>CTE_clico_JU_PM_PJ</b> OIDC	<b>CTE Policy</b> 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.			
<b>18:24:48</b> 2023-05-29	<b>STA4CTE</b>	 <b>Success</b>	 <b>CTE_clico_JU_PM_PJ</b> OIDC	<b>CTE Policy</b> N/A	OTP	185.64.245.50	
<b>18:23:27</b> 2023-05-29	<b>CTE4STA</b>	 <b>Failure</b> Unknown user	 <b>CTE_clico_JU_PM_PJ</b> OIDC	<b>N/A</b> N/A		185.64.245.50	
<b>18:21:08</b> 2023-05-29	<b>Administrator</b>	 <b>Failure</b> Unknown user	 <b>CTE_clico_JU_PM_PJ</b> OIDC	<b>N/A</b> N/A		185.64.245.50	

# Proponowana architektura

 - CTE Agent with MFA





# „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>

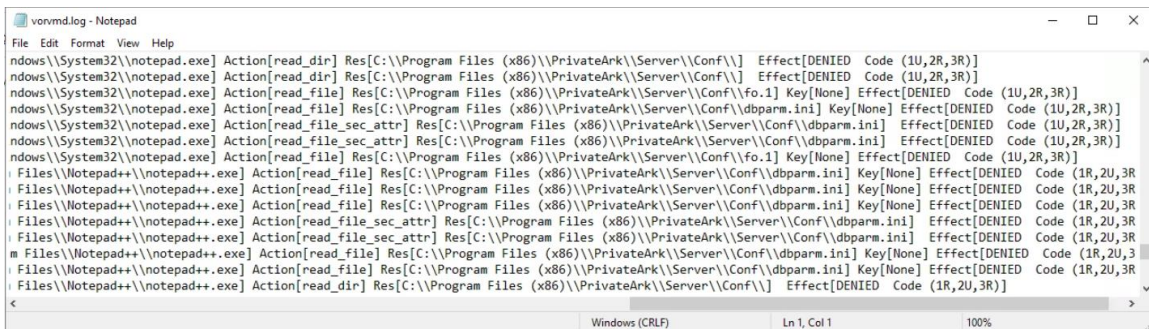
*Thales will be continually adding new MFA providers to CipherTrust Transparent Encryption. When the MFA providers pass compatibly testing, they will be added to this page.*

## 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.



```
vorvmd.log - Notepad
File Edit Format View Help
ndows\System32\notepad.exe Action[read_dir] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\] Effect[DENIED Code (1U,2R,3R)]
ndows\System32\notepad.exe Action[read_dir] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\] Effect[DENIED Code (1U,2R,3R)]
ndows\System32\notepad.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\fo.1] Key[None] Effect[DENIED Code (1U,2R,3R)]
ndows\System32\notepad.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Key[None] Effect[DENIED Code (1U,2R,3R)]
ndows\System32\notepad.exe Action[read_file_sec_attr] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Effect[DENIED Code (1U,2R,3R)]
ndows\System32\notepad.exe Action[read_file_sec_attr] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Effect[DENIED Code (1U,2R,3R)]
ndows\System32\notepad.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\fo.1] Key[None] Effect[DENIED Code (1U,2R,3R)]
Files\Notepad+\notepad+.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Key[None] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Key[None] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Key[None] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_file_sec_attr] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_file_sec_attr] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Key[None] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_file] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\dbparm.ini] Key[None] Effect[DENIED Code (1R,2U,3R)]
Files\Notepad+\notepad+.exe Action[read_dir] Res[C:\Program Files (x86)\PrivateArk\Server\Conf\] Effect[DENIED Code (1R,2U,3R)]
Windows (CRLF) Ln 1, Col 1 100%
```

# 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>
```

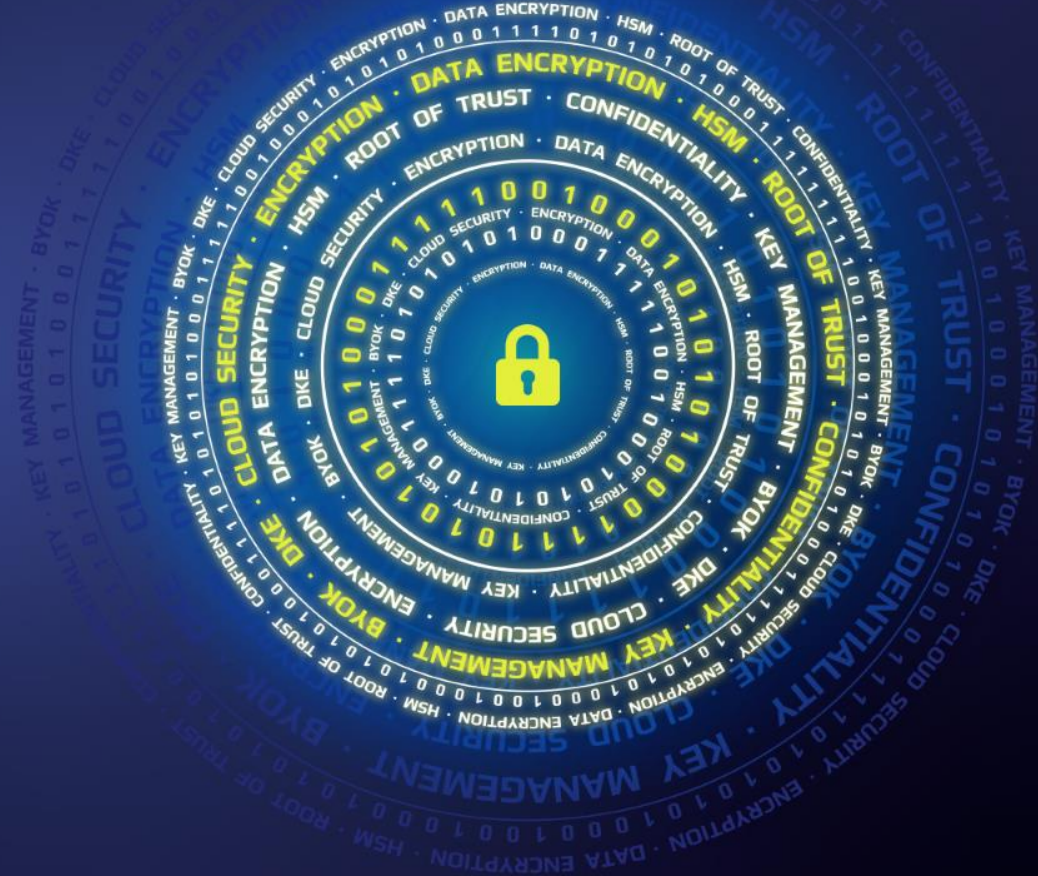
Only admin can run this command. Admin can check its value using following command

```
voradmin mfa config
```

It displays all MFA settings.



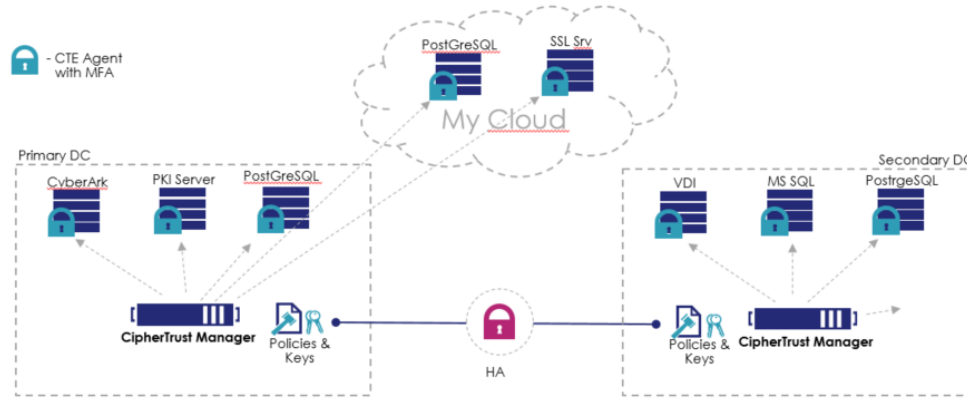
# CryptoPanel



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 wejściówką do:



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



## ▮ Oprogramowanie do pobrania lub wersja ewaluacyjna...

- W takim przypadku prosimy o kontakt z nami!

## ▮ Dokumentacja:

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