CryptoPanel

edycja #10

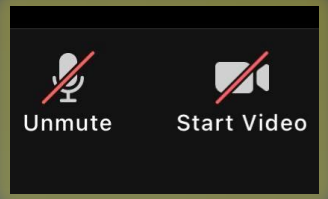
za moment zaczynamy...

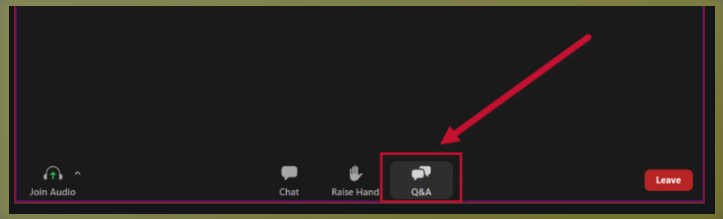
CryptoPanel

THALES

CLICO

CryptoPanel





CryptoPanel

dziś dyskutują

Joanna Rzepka

Channel Sales Manager
Joanna.rzepka@thalesgroup.com
mob. +48 600 537 666

Jarosław Ulczok

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

CryptoPanel

edycja #10

Podpisanie kodu certyfikatem jest jednym z elementów wpływających na bezpieczeństwo tego co tworzysz.

Jak podpisać kod, jakim certyfikatem, co z kluczem prywatnym?.

CryptoPanel

problem

co nas boli...

- Tworzymy kompleksowo oprogramowanie dla firmy przemysłu chemicznego
- Wykonujemy oprogramowanie autorskie szyte na miarę. Mamy także stałą ofertę produktów, które rozwijamy
- Główne platformy, dla których tworzymy oprogramowanie to: Android, iOS, Java, Windows (.Net)
- Obecnie podpisujemy część tworzonego kodu za pomocą dostępnych narzędzi developerski (jak **signtool** i **jarsigner**)
- Klucze i certyfikaty przechowujemy w plikach (PEM) na dedykowanej stacji. Mamy też certyfikaty na karcie inteligentnej

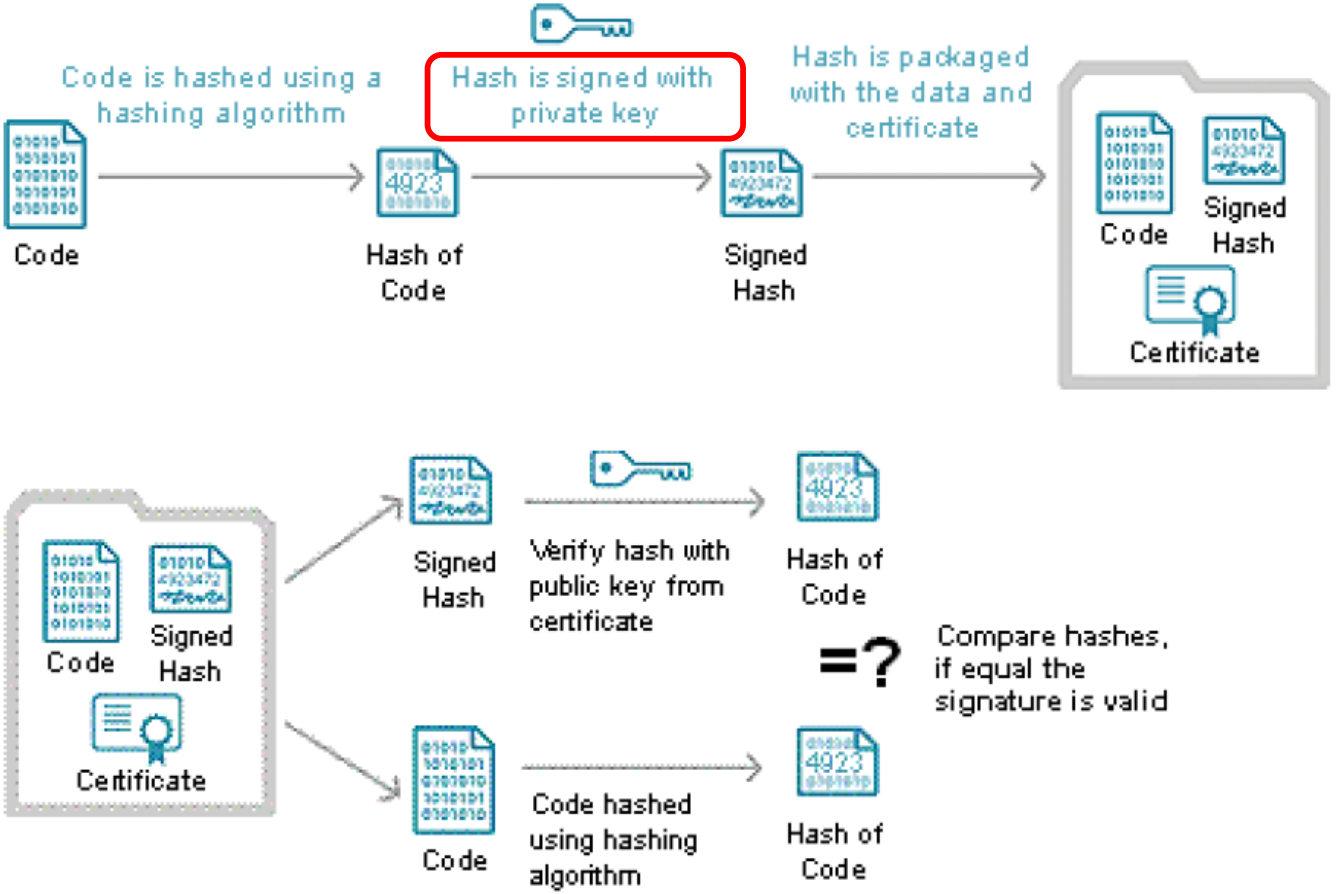
- …potrzebujemy większej ochrony podpisującego klucza prywatnego
  - kłopoty w przypadku kompromitacji
  - wymóg Zleceniodawcy
  - błędu operatora
- ...poszukujemy HSM do przechowywania certyfikatu EV do podpisywania kodu
- …chcemy na początek zintegrować HSM z **signtool** i **jarsigner**, potem **Install4J**
- …docelowo myślimy o kompleksowym rozwiązaniu (wszystkie platformy, wszystkie języki programowania)
- …docelowo także automatyzacja procesu, zamiast „ręcznej roboty”. Intensywnie wchodzimy w CI/CD.

CryptoPanel

rozwiązanie

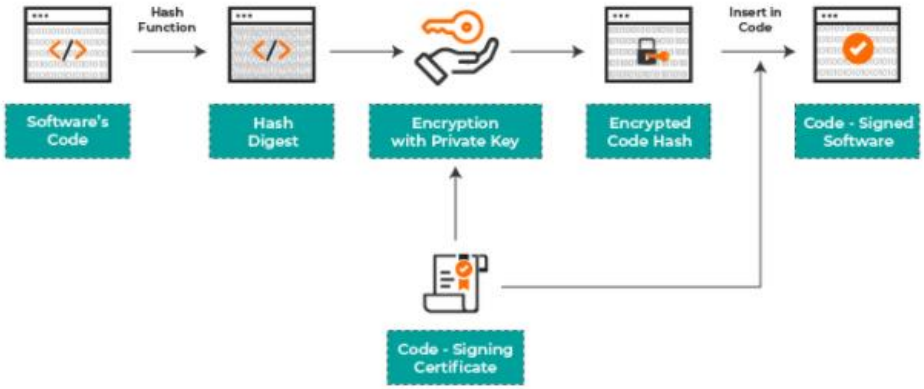
Na początek ...
po co nam CodeSigning?

Co to w ogóle jest „podpisywanie kodu”?



Co nam daje?

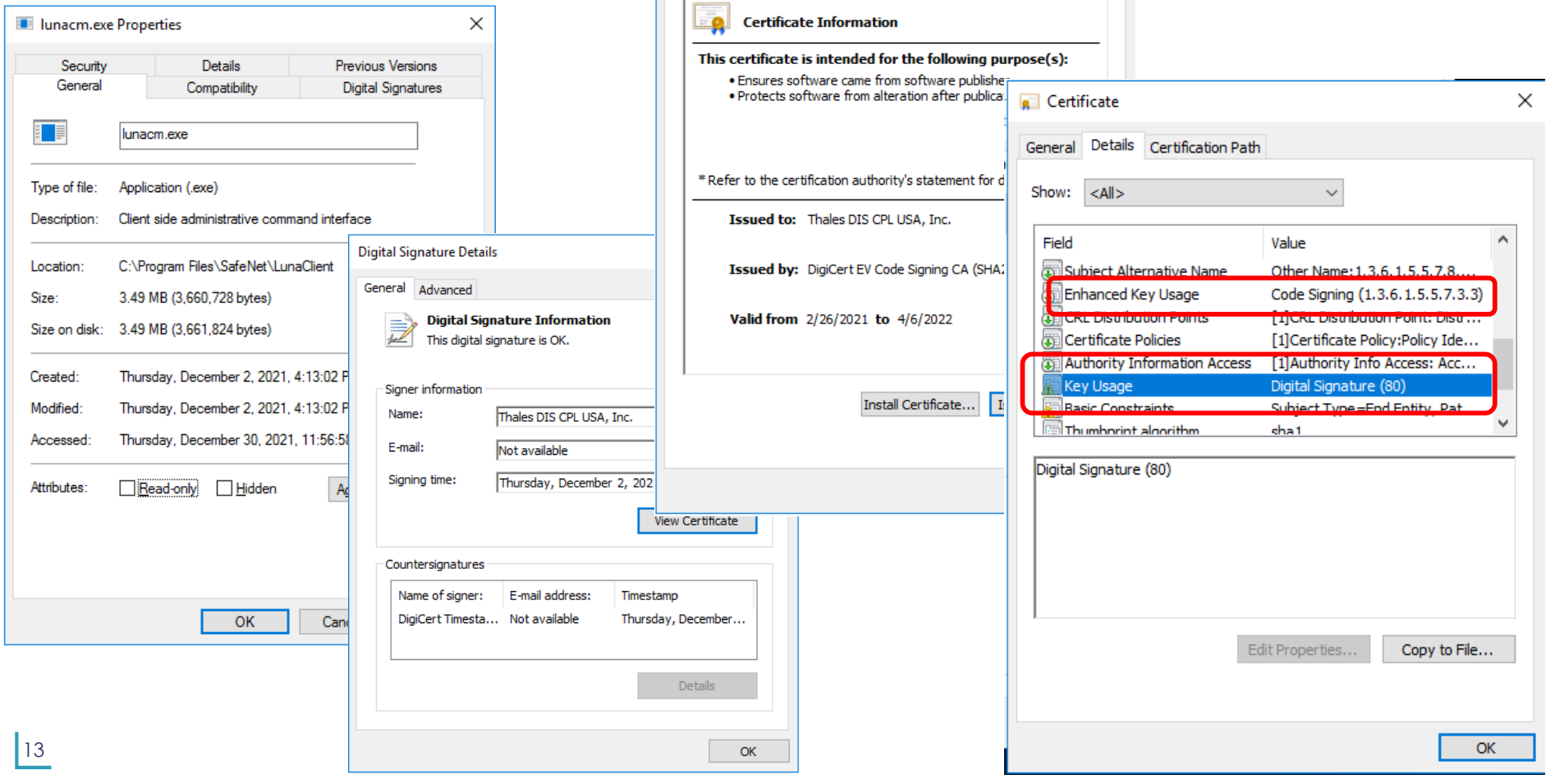
- Potwierdza tożsamość twórcy/dostawcy oprogramowania
- Gwarantuje, że oprogramowanie nie zostało zmienione po podpisaniu
- Pozwala programistom na dystrybucję na platformach, na których podpisywanie kodu jest obowiązkowe



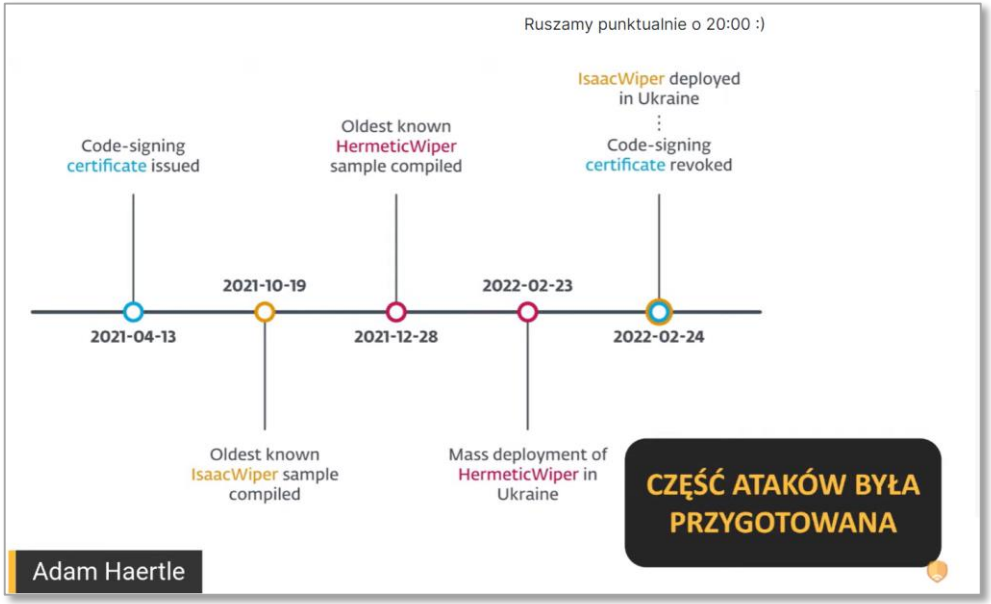
Proces wykorzystujący certyfikat cyfrowy wygenerowany przez **zaufane** źródło do **podpisywania** plików, takich jak pliki wykonywalne, skrypty, biblioteki DLL, itp.

THALES

Na ten przykład…



Czy jest to faktycznie potrzebne?



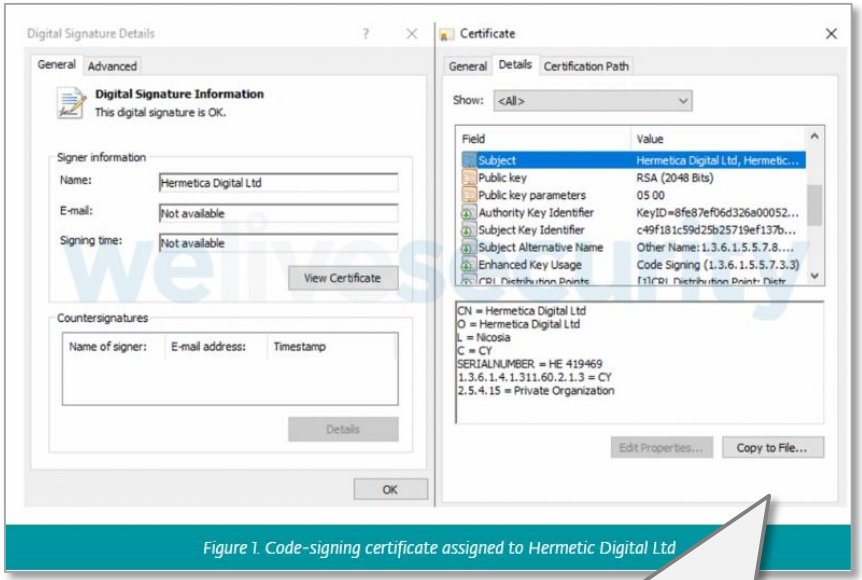


Figure 1. Code-signing certificate assigned to Hermetic Digital Ltd

According to a *report by Reuters*, it seems that this certificate was not stolen from Hermetica Digital. It is likely that instead the attackers **impersonated the Cypriot company** in order to get this certificate from DigiCert.

https://wideo.zaufanatrzeciastrona.pl/cyberwojna/watch

THALES

Aspekty bezpieczeństwa w kontekście podpisu kodu wykonywalnego

Jak to zrobić?

Wygeneruj parę kluczy w HSM

- Tak jest najbezpieczniej)alternatywa to import kluczy wygenerowanych przez dostawcę – mniej bezpiecznie)
- Wcześniej sprawdź jakie klucze obsługuje twój dostawca certyfikatu
- Sprawdź ponadto…

→

Wyeksportuj klucz publiczny

- Do pliku PEM, P12, itp..

→

Zbuduj żądanie podpisania certyfikatu (CSR) wraz kluczem publicznym

↓

Złóż CSR u dostawcy celem wydania certyfikatu do podpisywania kodu

→

Uzyskałeś certyfikat do podpisywania kodu

→

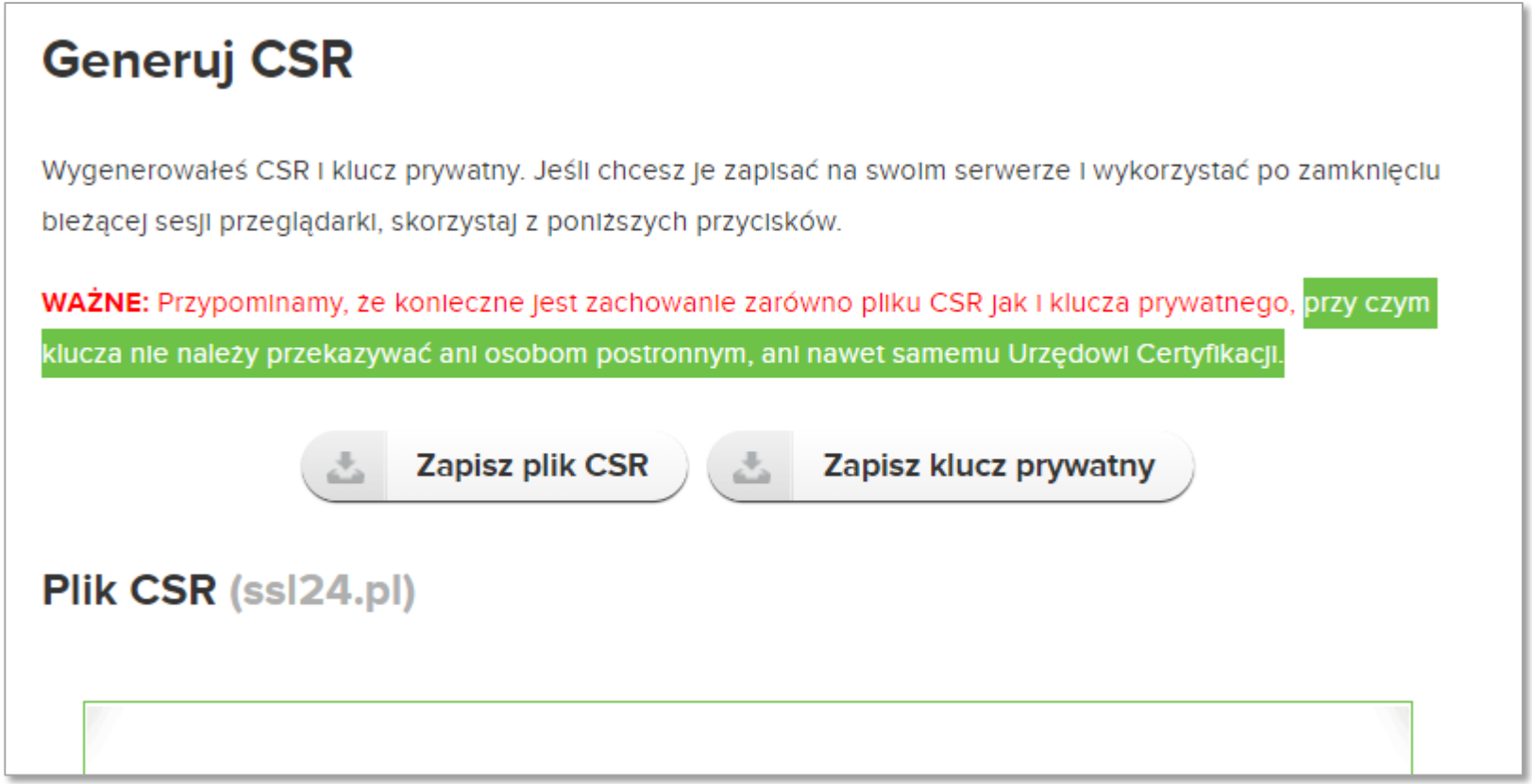
Zainstaluje certyfikat w HSM

→

Gotowe

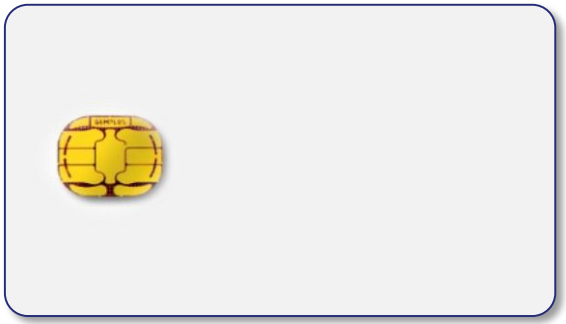
THALES

Po co w HSM jak można w pliku?



THALES

Po co w HSM jak można na karcie inteligentnej?



VS

„HSM to karta inteligentna na sterydach…"

Główna różnica?

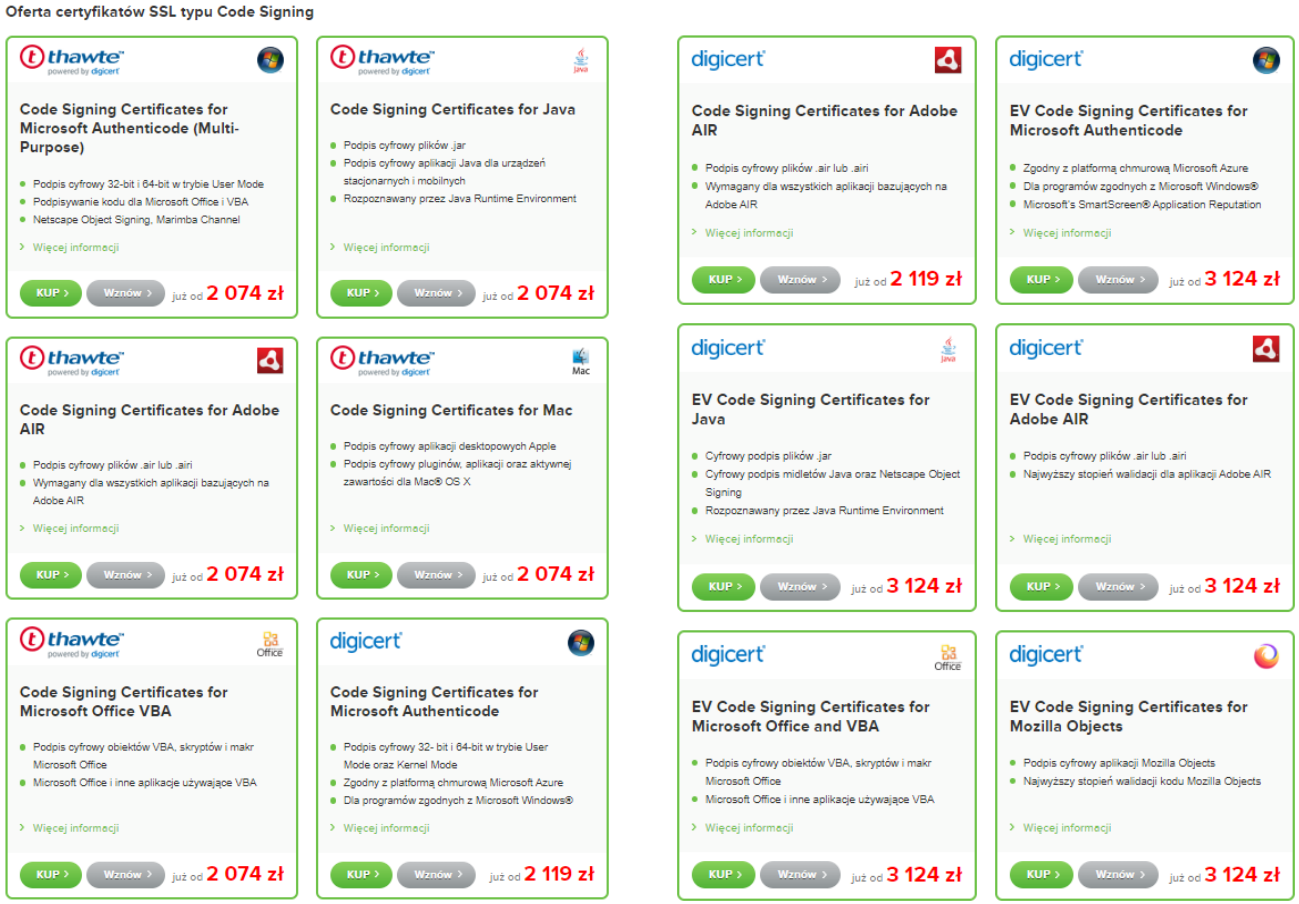
…poza:
pojemnością,
wydajnością,
certyfikacjami,
mechanizmami
ltd..

karta inteligentna nie dostarcza mechanizmu backupu klucza prywatnego

z definicji, każdy HSM wspiera backup materiału kryptograficznego, który chroni

THALES

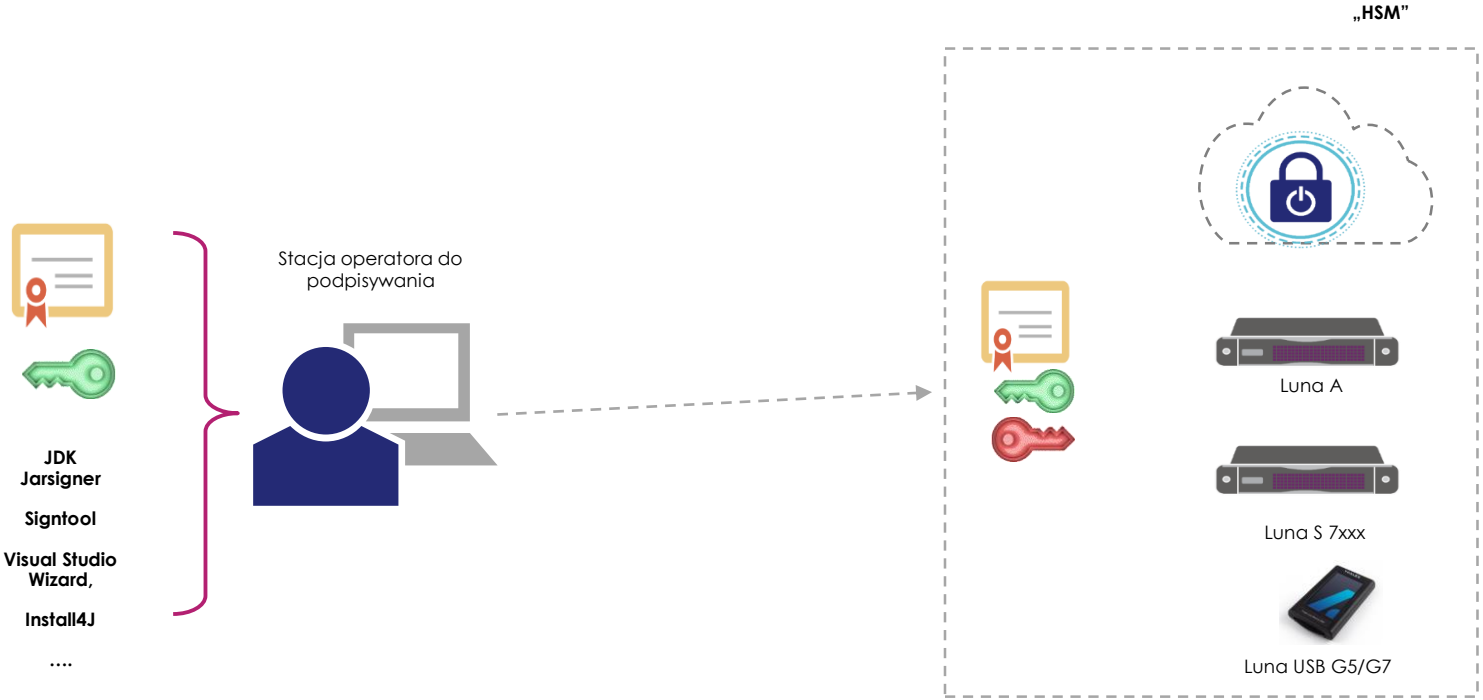
Samo ponowne „wydanie” certyfikatu może być kosztowne



THALES

Rozwiązanie…

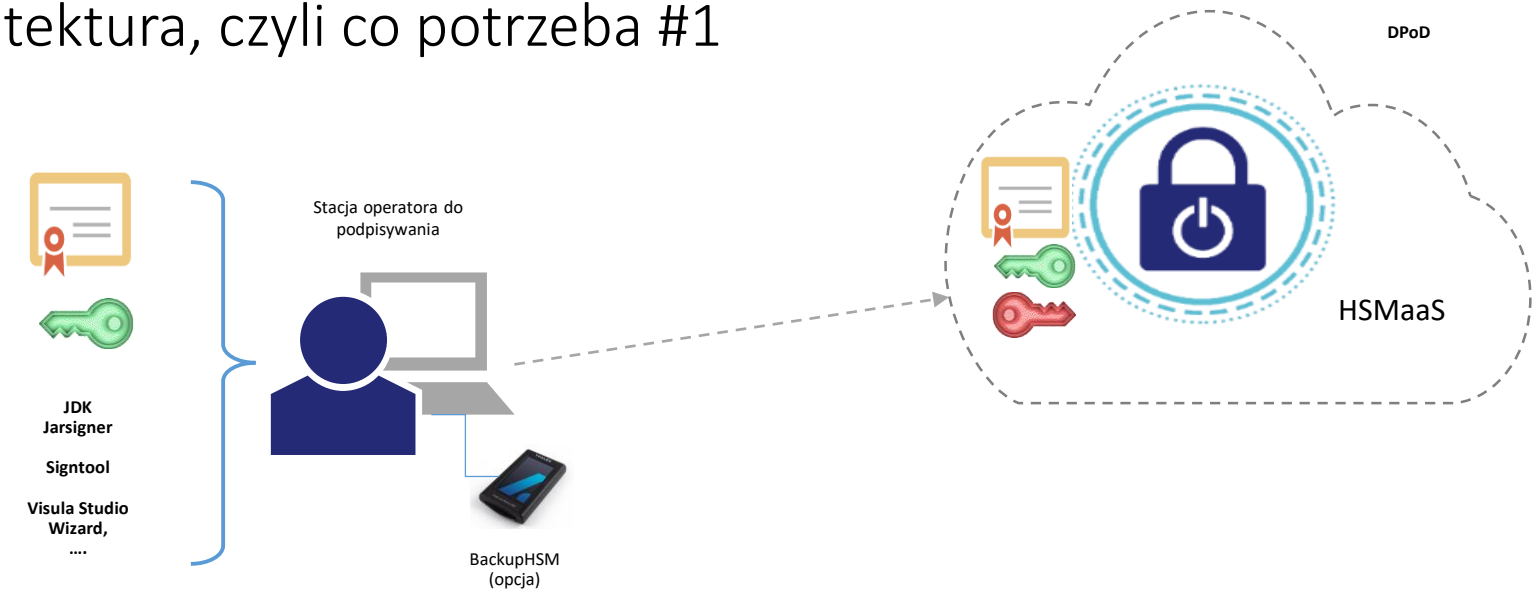
Rozwiązanie



CryptoPanel

podsumowanie

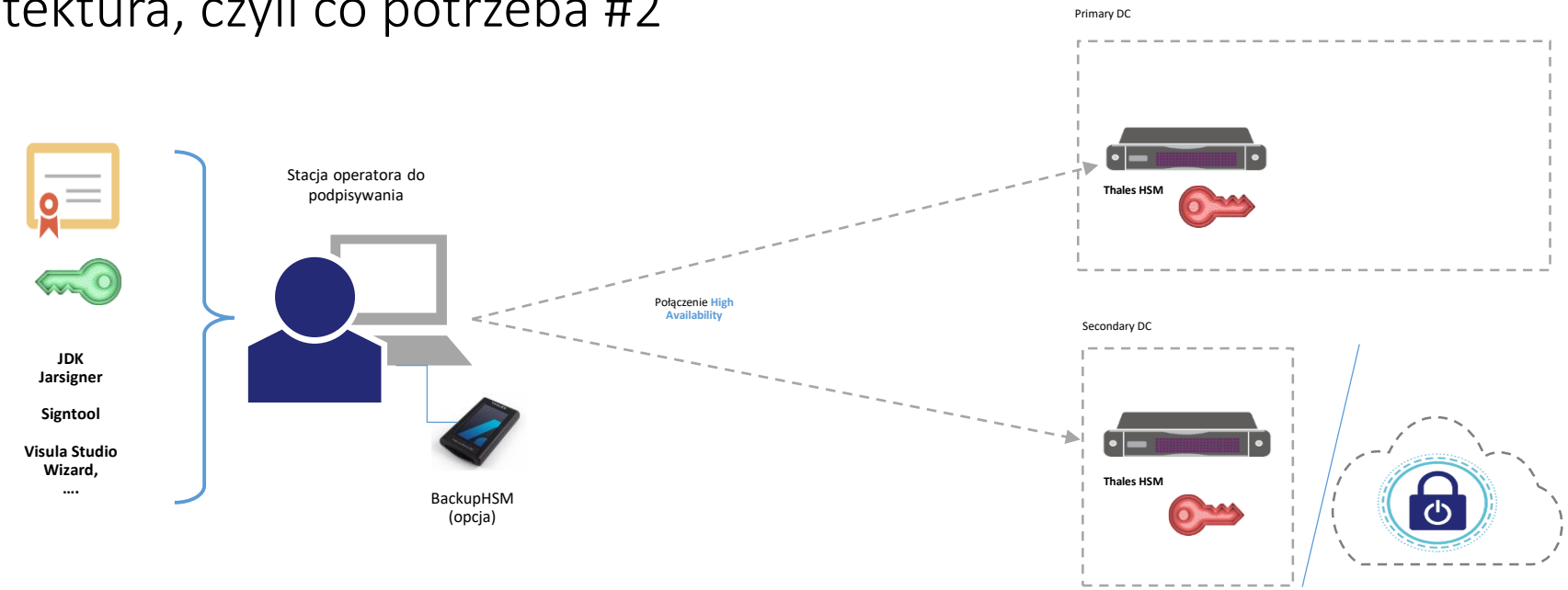
Architektura, czyli co potrzeba #1



- **produkty dostępne w polskim kanale partnerskim**
- **model licencjonowania subskrypcyjny**
- **subskrypcja demo na 30 dni**
- **Zalecane: BackupHSM lub DPoD BackupHSM**

Cena: 800€ za miesiąc (1x HSMaaS, 5 clientów, 100s/s, 100 obiektów)

Architektura, czyli co potrzeba #2



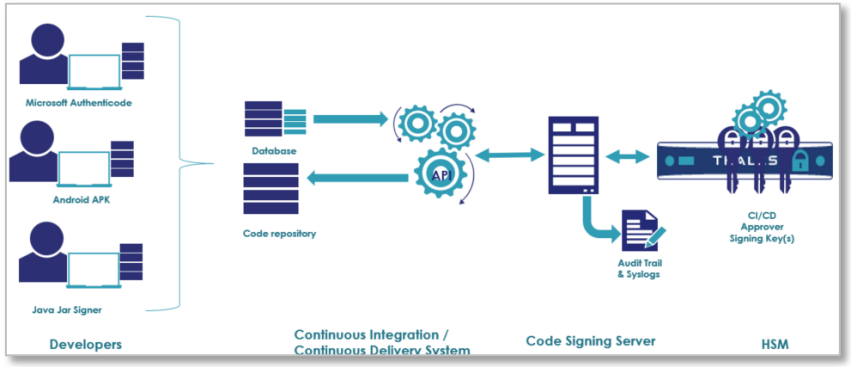
- **Produkty dostępne w polskim kanale partnerskim**
- **HSM to Thales Luna seria A7xx lub seria S7xx**
- **Model licencjonowania: per urządzenie, (plus licencja kliencka)**
- **Urządzenia do testów na 30 dni**

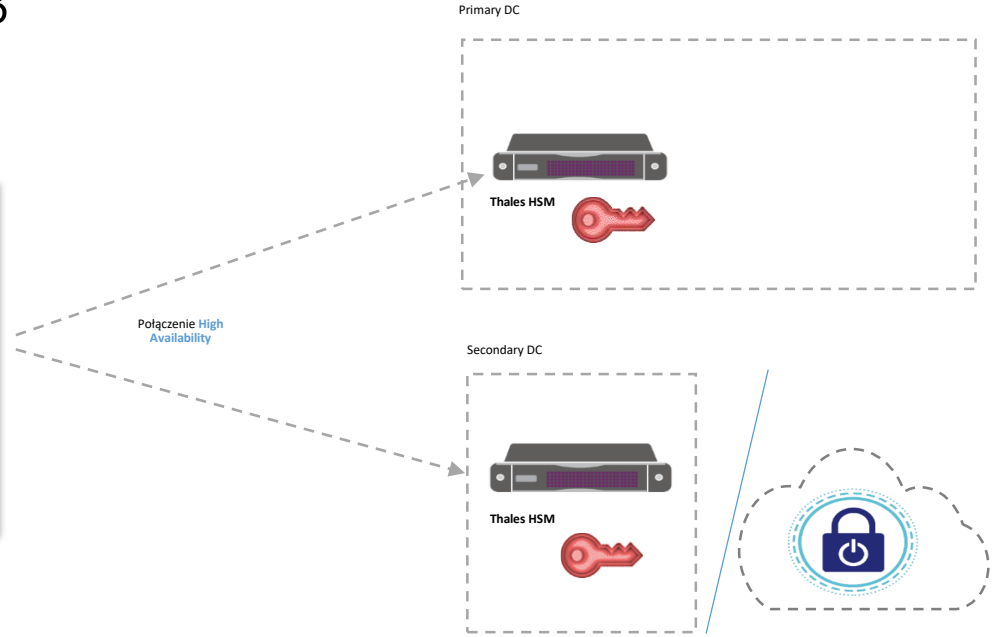
Ceny:

Luna A700 – około 20,000 € ze wsparciem na rok

Luna Client License: 1000€

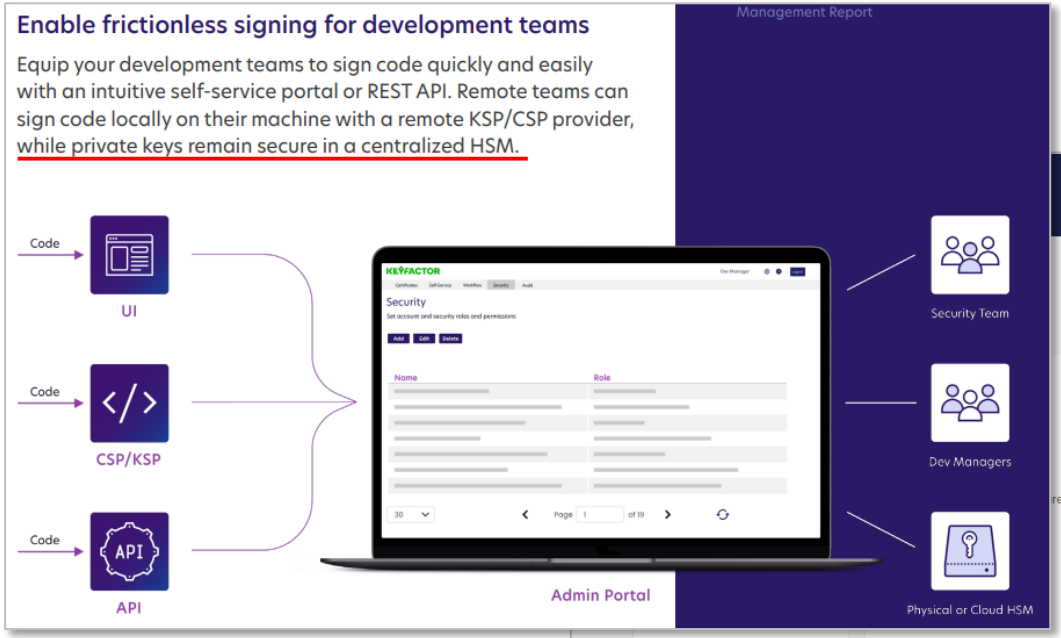
Architektura, czyli co potrzeba #3

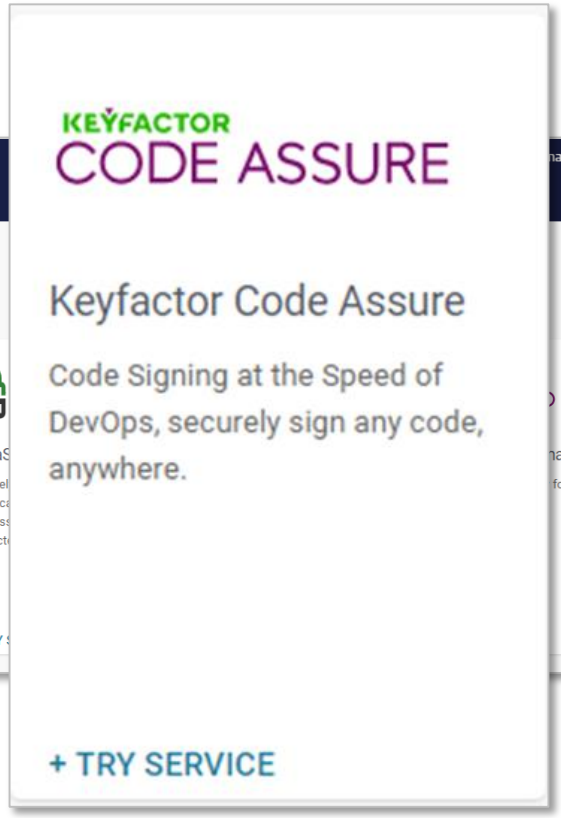




- **Produkty dostępne w kanale partnerskim**
- **HSM w tle to DPoD lub Luna**
- **Zapytaj o wycenę…**

Architektura, czyli co potrzeba #3





- **Produkty dostępne w kanale partnerskim**
- **HSM w tle to DPoD HSMaaS**
- **Zapytaj o wycenę…**

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

Jak zabezpieczyć certyfikat do podpisywania kodu (klucz prywatny) przed przypadkowy usunięciem?

- Programista/operator/aplikacja czasem się myli.

```
26: Maximum pin length : 255
28: Allow Key Management Functions : 1
29: Perform RSA signing without confirmation : 1
```

28	**Enable Key Management Functions** Always **1**. This capability allows cryptographic objects to be created, deleted, generated, derived, modified on the partition. See also **Cloning vs Key Management** at the bottom of this page.	**Allow Key Management Functions (destructive OFF-to-ON)** > **1** (default): The Crypto Officer can manage (create/delete, etc.) objects on the partition. The Crypto User is restricted to read-only operations. > **0**: Partition objects are read-only for both the CO and CU roles.

Choć sam kod jest podpisany to ten fakt nie gwarantuje, że kod jest bezpieczny. Tylko od systemu operacyjnego/uruchomieniowego czy aplikacji zależy jak dokładnie sprawdzany jest podpis kodu przed jego uruchomieniem lub wczytaniem.

- Np. czy system w czasie bootowania ma dostęp do listy CRLi lub usługi OCSP?

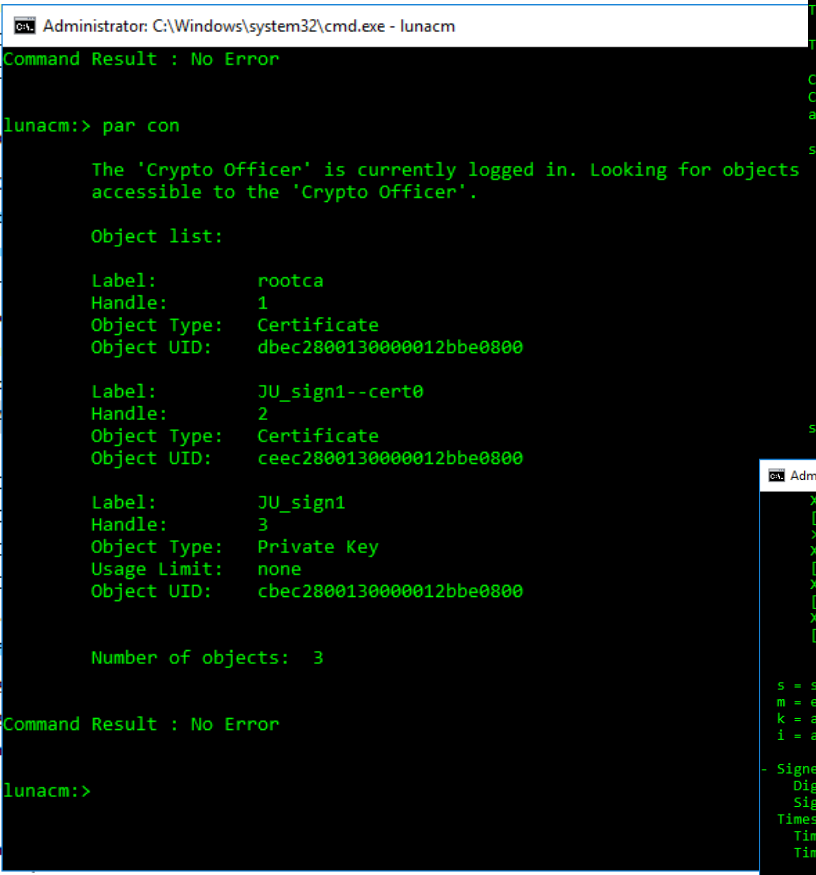
Nie wyłączajmy konieczności posiadania podpisu na komponentach systemu operacyjnego (np. W2019 i sterowniki)

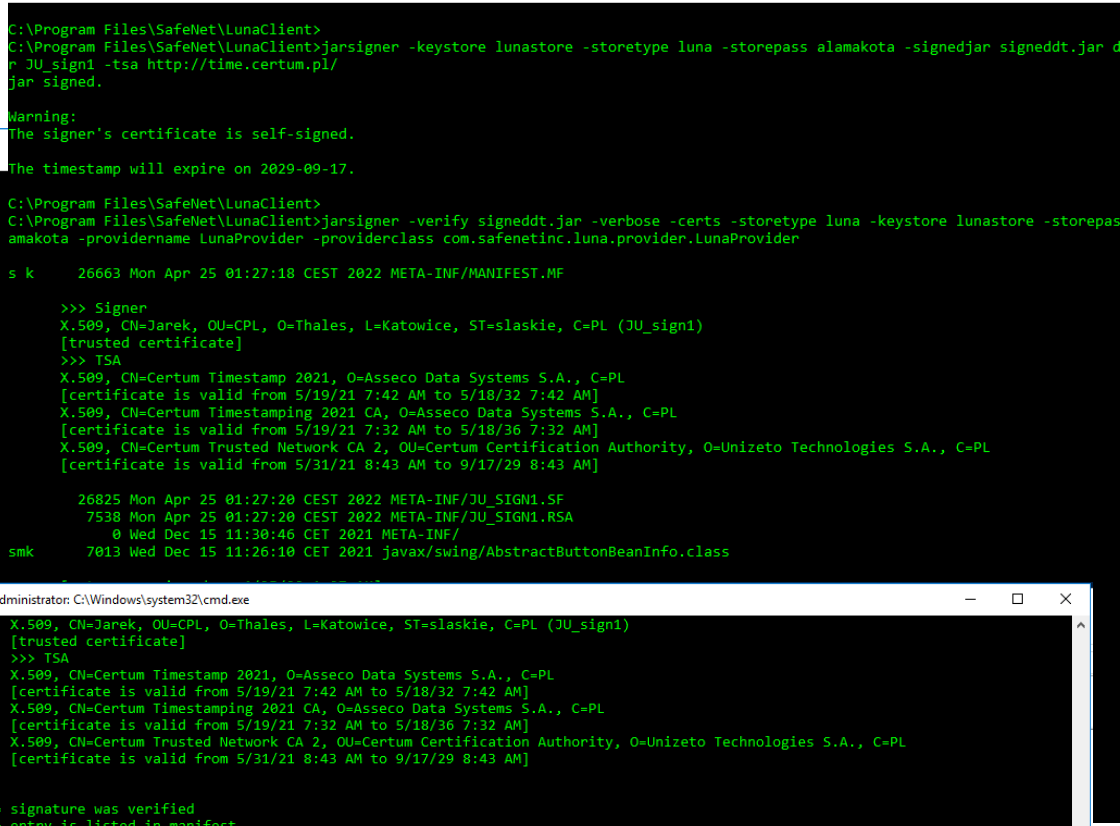
Kontroluj kto ma dostęp do możliwości podpisu kodu w Twoje firmie.

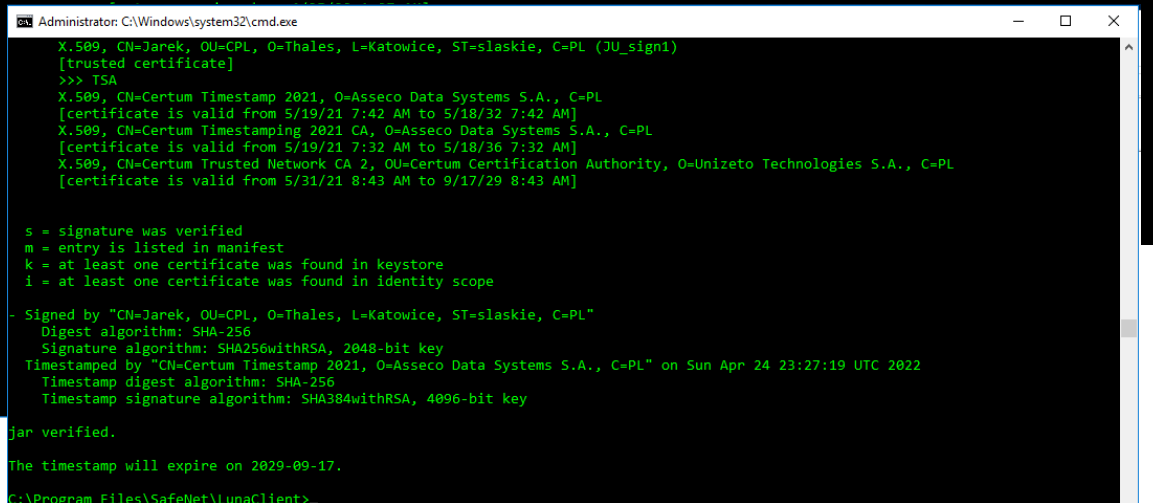
CryptoPanel

CryptoPanel

konkurs


Administrator: C:\Windows\system32\cmd.exe - lunacm
Command Result : No Error
lunacm:> par con
The 'Crypto Officer' is currently logged in. Looking for objects accessible to the 'Crypto Officer'.
Object list:
Label: rootca
Handle: 1
Object Type: Certificate
Object UID: dbec2800130000012bbe0800
Label: JU_sign1--cert0
Handle: 2
Object Type: Certificate
Object UID: ceec2800130000012bbe0800
Label: JU_sign1
Handle: 3
Object Type: Private Key
Usage Limit: none
Object UID: cbec2800130000012bbe0800
Number of objects: 3
Command Result : No Error
lunacm:>


C:\Program Files\SafeNet\LunaClient>
C:\Program Files\SafeNet\LunaClient>jarsigner -keystore lunastore -storetype luna -storepass alamakota -signedjar signeddt.jar d
r JU_sign1 -tsa http://time.certum.pl/
jar signed.
Warning:
The signer's certificate is self-signed.
The timestamp will expire on 2029-09-17.
C:\Program Files\SafeNet\LunaClient>
C:\Program Files\SafeNet\LunaClient>jarsigner -verify signeddt.jar -verbose -certs -storetype luna -keystore lunastore -storepas
amakota -providername LunaProvider -providerclass com.safenetinc.luna.provider.LunaProvider
s k 26663 Mon Apr 25 01:27:18 CEST 2022 META-INF/MANIFEST.MF
>>> Signer
X.509, CN=Jarek, OU=CPL, O=Thales, L=Katowice, ST=slaskie, C=PL (JU_sign1)
[trusted certificate]
>>> TSA
X.509, CN=Certum Timestamp 2021, O=Asseco Data Systems S.A., C=PL
[certificate is valid from 5/19/21 7:42 AM to 5/18/32 7:42 AM]
X.509, CN=Certum Timestamping 2021 CA, O=Asseco Data Systems S.A., C=PL
[certificate is valid from 5/19/21 7:32 AM to 5/18/36 7:32 AM]
X.509, CN=Certum Trusted Network CA 2, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
[certificate is valid from 5/31/21 8:43 AM to 9/17/29 8:43 AM]
26825 Mon Apr 25 01:27:20 CEST 2022 META-INF/JU_SIGN1.SF
7538 Mon Apr 25 01:27:20 CEST 2022 META-INF/JU_SIGN1.RSA
0 Wed Dec 15 11:30:46 CET 2021 META-INF/
smk 7013 Wed Dec 15 11:26:10 CET 2021 javax/swing/AbstractButtonBeanInfo.class


Administrator: C:\Windows\system32\cmd.exe
X.509, CN=Jarek, OU=CPL, O=Thales, L=Katowice, ST=slaskie, C=PL (JU_sign1)
[trusted certificate]
>>> TSA
X.509, CN=Certum Timestamp 2021, O=Asseco Data Systems S.A., C=PL
[certificate is valid from 5/19/21 7:42 AM to 5/18/32 7:42 AM]
X.509, CN=Certum Timestamping 2021 CA, O=Asseco Data Systems S.A., C=PL
[certificate is valid from 5/19/21 7:32 AM to 5/18/36 7:32 AM]
X.509, CN=Certum Trusted Network CA 2, OU=Certum Certification Authority, O=Unizeto Technologies S.A., C=PL
[certificate is valid from 5/31/21 8:43 AM to 9/17/29 8:43 AM]
s = signature was verified
m = entry is listed in manifest
k = at least one certificate was found in keystore
i = at least one certificate was found in identity scope
- Signed by "CN=Jarek, OU=CPL, O=Thales, L=Katowice, ST=slaskie, C=PL"
Digest algorithm: SHA-256
Signature algorithm: SHA256withRSA, 2048-bit key
Timestamped by "CN=Certum Timestamp 2021, O=Asseco Data Systems S.A., C=PL" on Sun Apr 24 23:27:19 UTC 2022
Timestamp digest algorithm: SHA-256
Timestamp signature algorithm: SHA384withRSA, 4096-bit key
jar verified.
The timestamp will expire on 2029-09-17.
C:\Program Files\SafeNet\LunaClient>