# CryptoPanel

## edycja #16


eIDAS i pieczęć kwalifikowana.
Jak zbudować lokalne środowisko dla pieczęci kwalifikowanej w oparciu o  modułu kryptograficznego Thales.

# CryptoPanel

dziś dyskutują i pokazują


## Piotr Wróbel

Regional Sales Manager
Piotr.Wrobel@thalesgroup.com
mob. +48 669 88 99 76

## Jarosław Ulczok

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

# CryptoPanel

## TEST WIEDZY #16


eIDAS i pieczęć kwalifikowana.
Jak zbudować lokalne środowisko dla pieczęci kwalifikowanej w oparciu o  modułu kryptograficznego Thales.

# CryptoPanel


problem

# co nas boli...

- Planujemy zakup pieczęci kwalifikowanej m.in na potrzeby masowego poświadczania dokumentów w firmie. Jest to jeden z elementów naszej cyfrowej transformacji.
- Nie wykluczamy użycia pieczęci w innych systemach dziedzinowych.
- Codziennie musimy podpisać około 1000 różnych dokumentów, w szczytowych okresach 5000. Maksimum zleceń jakie zaobserwowaliśmy to 1200 dokumentów do podpisu w ciągu godziny.
- Przewidujemy wzrost ilości dokumentów do poświadczania w przyszłości.
- Stworzyliśmy własne oprogramowanie do podpisywania dokumentów (zamierzamy dostosować je do wykorzystania pieczęci).

- W jakie rozwiązanie zainwestować?
- Jak uzyskać pieczęć na ternie RP?
- Jaka pieczęć będzie najlepsza dla naszego zastosowania?
- Co musimy kupić i jak wdrożyć aby pieczęć „była u nas”?
- Jakie wymagania musimy spełnić w tym celu?
- Ile to będzie kosztować?

- Posiadamy u siebie rozwiązanie klasy HSM, czy możemy je wykorzystać dla celów pieczęci kwalifikowanej?

# CryptoPanel


rozwiązanie

# Definicje eIDAS:

Regulacja eIDAS (**E**lectronic **ID**entification, **A**uthentication and trust **S**ervices) wprowadza:

## Electronic Signature (podpis elektoniczny)

- **Simple** - Electronic equivalent of a hand written signature such as a typed name at the bottom an email, scanned PDF document with a signature or a click of an I Accept button
- **Advanced** - Produced using encryption technology such as an HSM and can be accepted by other member states
- **Qualified** - An advanced electronic signature backed by a qualified certificate issued by a trust service provider whose credentials appear on the EU Trust list

## Seal (pieczęć)

- **A seal** is an electronic signature for a business or a organization

# To od początku: podpisy elektroniczny vs pieczęć?

- **Technicznie pieczęć kwalifikowana to nic innego jak certyfikat X.509 v3**
- **Zapewnia:**
  - **autentyczności** – pewności, że dokument pochodzi od danej organizacji, instytucji czy firmy,
  - **integralności** – pewności, że treść dokumentu nie została zmieniona.

**E-pieczęć i e-podpis – jaka jest różnica?**

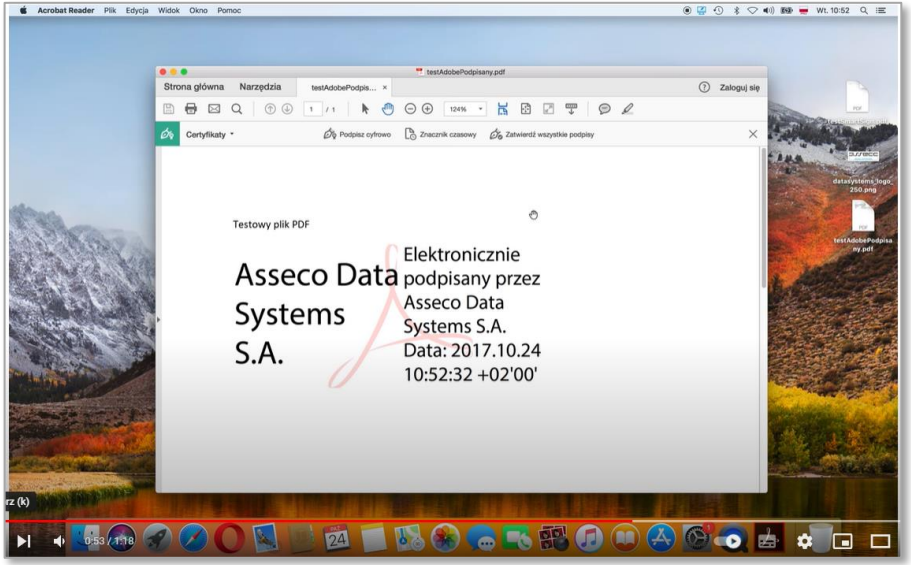
Najbardziej charakterystyczną cechą pieczęci elektronicznej jest to, że **korzystać z niej mogą osoby prawne**, a więc firmy, organizacje czy instytucje. W przypadku podpisu elektronicznego są to osoby fizyczne i służy on im jako podpis.

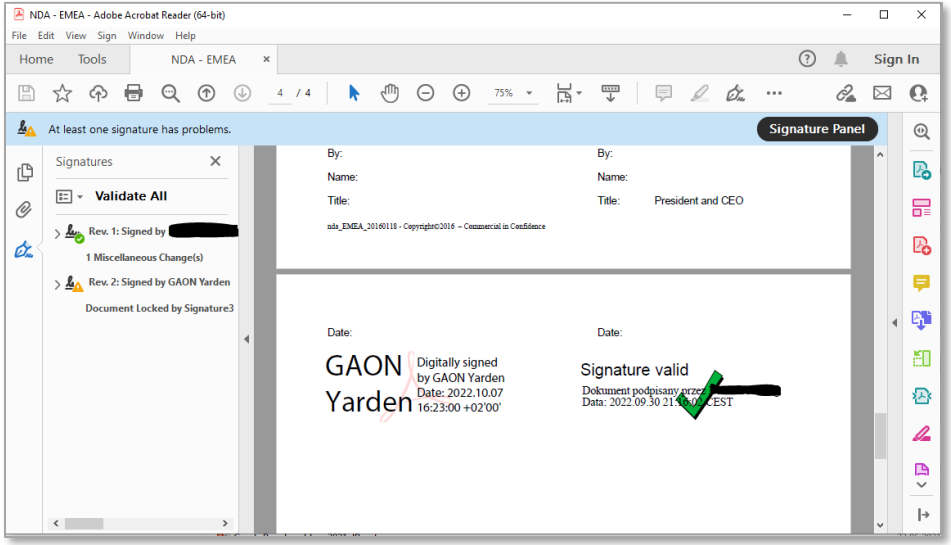
**Ważne**

Pieczęć elektroniczna **nie jest** odpowiednikiem podpisu elektronicznego osoby prawnej.

https://obserwatorium.biz/co-to-jest-pieczec-elektroniczna-i-czym-sie-rozni-od-podpisu.html

# Tak to wygląd w praktyce




https://www.youtube.com/watch?v=Az7Xp6V5IMc

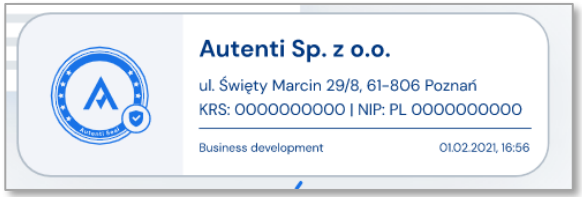


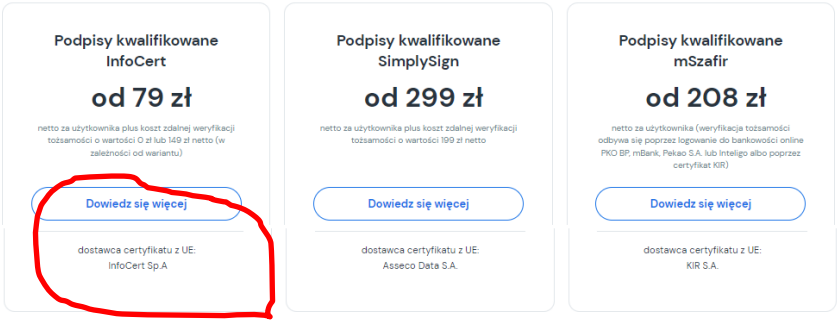
THALES

# Od kogo można uzyskać pieczęć w RP?

- Organ odpowiedzialny do certyfikowania kwalifikowanych dostawców usług zaufania w RP to Narodowe Centrum Certyfiakcji (NCCert)
- https://www.nccert.pl/


- W Polsce działają także podmioty oferujące pieczęć kwalifikowaną dostawców z obszaru EU.
- https://autenti.com/pl/



# Jakie „rodzaje” pieczęci można uzyskać (na przykładach)?

| | Pieczęć kwalifikowana na karcie | Kwalifikowana pieczęć chmurowa ECSigner | Pieczęć kwalifikowana chmurowa ECQSS Seal | Pieczęć kwalifikowana na własnym HSM |
|---|---|---|---|---|
| Ilość użytkowników mogących korzystać z usługi w tym samym czasie | 1 | 1 | Wiele | Wiele |
| Dla jakiej skali dokumentów jest dedykowane to rozwiązanie | Małej lub średniej | Małej lub średniej | Średniej, dużej lub masowej | Średniej, dużej lub masowej |
| Co jest potrzebne aby skorzystać z usługi | Karta z pieczęcią i aplikacja podpisująca desktop | Smartfon z aplikacją mobilną i aplikacja podpisująca desktop | Integracja własnego systemu (API) z usługą pieczęci i podpisywania w chmurze | Własny HSM z wygenerowaną pieczęcią oraz serwerowe oprogramowanie podpisujące |
| Dla jakiego rodzaju procesów | Półautomatycznych | Półautomatycznych | Półautomatycznych lub automatycznych | Półautomatycznych lub automatycznych |
| Dostęp do usługi w formie zdalnej | – | ✓ | ✓ | ✓ |
| Możliwość integracji z dowolnym systemem, portalem klienta - EZD, ERP za pomocą API | – | – | ✓ | ✓ |

EUROCERT

https://eurocert.pl/kwalifikowana-pieczec-elektroniczna-i-jej-rodzaje/

# Jakie „rodzaje” pieczęci można uzyskać?

## Kwalifikowana pieczęć elektroniczna

CenCert pieczęć elektroniczna kwalifikowana. Doskonałe narzędzie do uwierzytelniania dokumentów. Zapewnia autentyczność pochodzenia dokumentów. Przy podpisywaniu cyfrowych dokumentów bezpieczeństwo jest podstawą, którą mają zapewnić kolejne elektroniczne rozwiązania wymienione w rozporządzeniu eIDAS. Kwalifikowana pieczęć elektroniczna CenCert w pełni spełnia wymogi bezpieczeństwa.

Kwalifikowana pieczęć elektroniczna to nowoczesne narzędzie, które można stosować wszędzie tam, gdzie oczekujemy pewności co do zachowania integralności oraz autentyczności pochodzenia dokumentu z danej organizacji / firmy. Do składania pieczęci elektronicznej firma może upoważnić dowolne osoby.

Sortuj wg popularności

Wyświetlanie wszystkich wyników: 3


**Pieczęć kwalifikowana elektroniczna zestaw Token**
1.429,00 zł – 6.500,00 zł plus 23% VAT

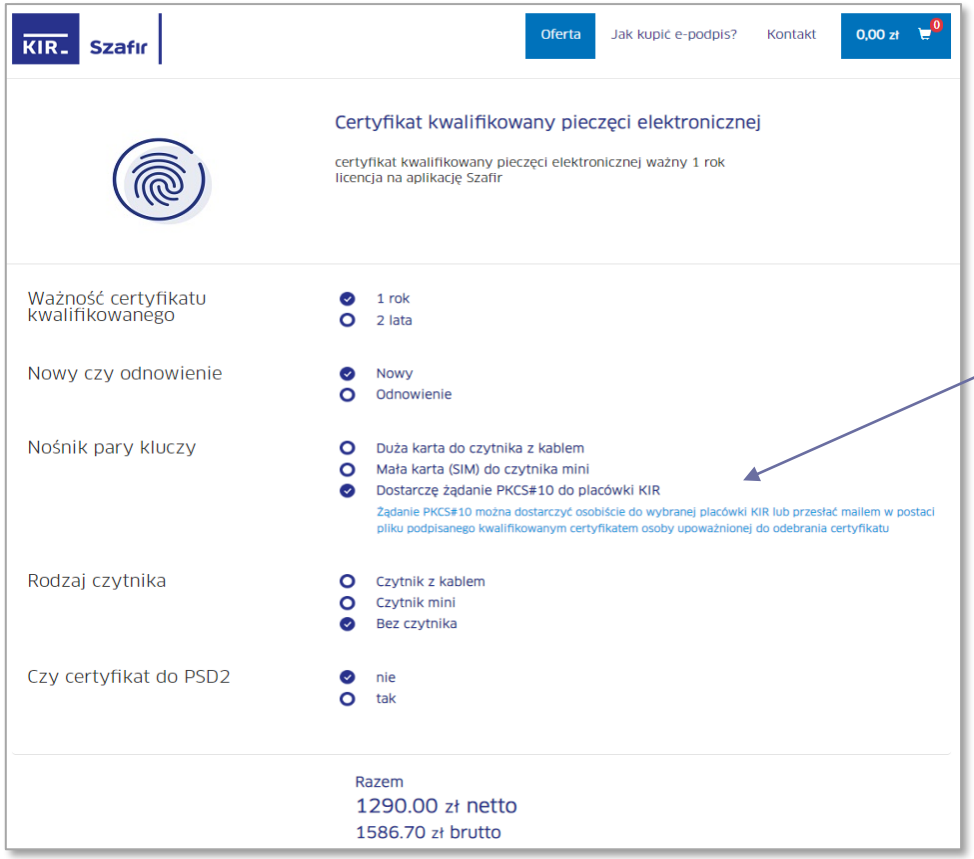
**Pieczęć kwalifikowana zestaw Standard**
1.429,00 zł – 6.500,00 zł plus 23% VAT


**Pieczęć kwalifikowana zestaw bez czytnika**
1.379,00 zł – 6.450,00 zł plus 23% VAT

https://www.cencert.pl/product-category/pieczec-elektroniczna/

**Uwaga**: choć na stronach CenCert nie jest to wymienione, to CenCert oferuje pieczęć kwalifikowaną wydawaną na własny HSM.

# Jakie „rodzaje” pieczęci można uzyskać?




https://szafir.kir.com.pl/eshop-web/items.html?id=191

Żądanie PKCS#10 może być wykorzystane do wydania pieczęci na własny HSM! Niepewność rozwiewa kontakt z dostawców usług zaufania.

# Jak wygląda procedura uzyskania pieczęci na HSM (EuroCert)?

10 lis 2022 16:58 [redacted]@eurocert.pl> napisał(a):

1. Upewniamy się czy klucz prywatny z pary kluczy wygenerowanej przez klienta pochodzi z HSM będącego urządzeniem QSCD w rozumieniu eIDAS. W tym celu:

1. Bierzemy udział w ceremonii generowania pary kluczy w HSM (zdalnie lub fizycznie), której wynikiem jest plik żądania certyfikacyjnego pkcs#10.
2. Dokonujemy oględzin urządzenia: nazwę, model, nr seryjne, tabliczki znamionowe, plomby itp.
3. Weryfikujemy dokumentację HSM: dowód zakupu, protokół odbioru od dystrybutora, protokół z odbioru urządzenia (plomby itp.), certyfikat QSCD, Common Criteria.

2. Sprawdzamy tozsamosc osoby reprezentującej klienta której zostanie przekazany certyfikat kwalifikowany.
3. Odbieramy od osoby reprezentującej plik żądania certyfikacyjnego w postaci pliku pkcs#10. Jest to plik zawierający klucz publiczny przedłożony do certyfikacji podpisany kluczem prywatnym. Zawiera podstawowe dane klienta, niekoniecznie pełne takie jak w certyfikacie. We wniosku o certyfikat zawarte są dane do certyfikatu oraz tzw. keyUsage (zastosowanie certyfikatu).
4. Weryfikujemy poprawność podpisu elektronicznego pod żądaniem certyfikacji aby potwierdzić kontrolę klienta nad kluczem prywatnym komplementarnym do klucza publicznego przedstawionego do certyfikacji.
5. Podpisujemy wniosek o wydanie certyfikatu zawierający dane do certyfikatu oraz akceptację warunków usługi i zgodę na przetwarzania danych osobowych.
6. Generujemy certyfikat i przekazujemy go osobie reprezentującej.

Tak polityki też oraz:

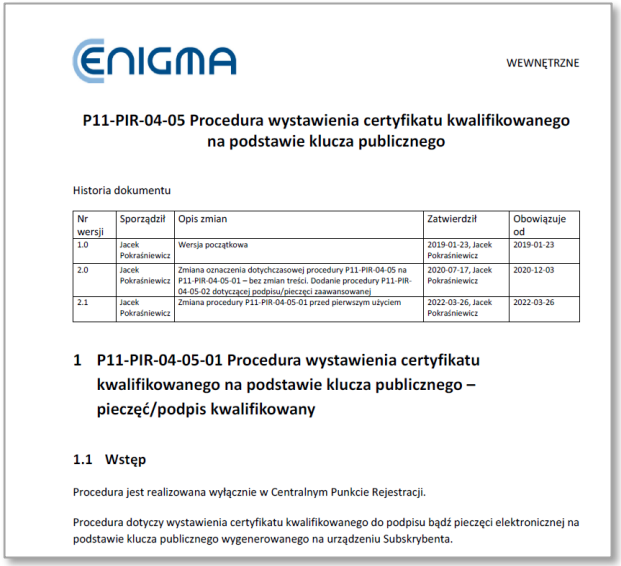
1) minimalną konfigurację ról: SO, AU i CO. W przypadku CO mającego możliwość bezpośredniego uzycia klucza (key owner) – weryfikujemy ustawienia uwierzytelniania (M z N) oraz
2) kontrolę CO nad kluczem prywatnym („control") – weryfikujemy poprzez weryfikację wspomnianego żądania CSR (PKCS#10) otrzymanego od CO generującego CSR w imieniu osoby reprezentującej organizację.
3) Kontrolę fizyczną nad urządzaniem.

czy w p. 2i3 sprawdzacie takze ustawieni HSM (polityki) tak bay były zgodne z wymaganiami. CC/eIDAS?



THALES

# Jak wygląda procedura uzyskania pieczęci ma HSM (CenCert)?



ENIGMA

WEWNĘTRZNE

**P11-PIR-04-05 Procedura wystawienia certyfikatu kwalifikowanego na podstawie klucza publicznego**

Historia dokumentu

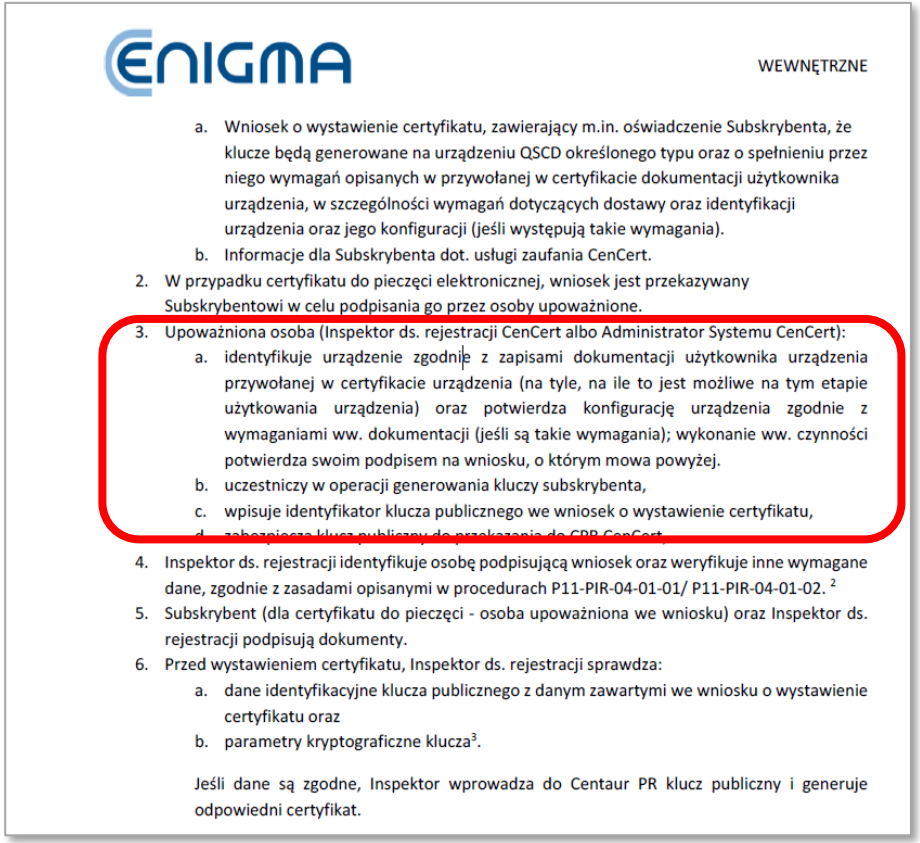
| Nr wersji | Sporządził | Opis zmian | Zatwierdził | Obowiązuje od |
|---|---|---|---|---|
| 1.0 | Jacek Pokraśniewicz | Wersja początkowa | 2019-01-23, Jacek Pokraśniewicz | 2019-01-23 |
| 2.0 | Jacek Pokraśniewicz | Zmiana oznaczenia dotychczasowej procedury P11-PIR-04-05 na P11-PIR-04-05-01 – bez zmian treści. Dodanie procedury P11-PIR-04-05-02 dotyczącej podpisu/pieczęci zaawansowanej | 2020-07-17, Jacek Pokraśniewicz | 2020-12-03 |
| 2.1 | Jacek Pokraśniewicz | Zmiana procedury P11-PIR-04-05-01 przed pierwszym użyciem | 2022-03-26, Jacek Pokraśniewicz | 2022-03-26 |

**1 P11-PIR-04-05-01 Procedura wystawienia certyfikatu kwalifikowanego na podstawie klucza publicznego – pieczęć/podpis kwalifikowany**

**1.1 Wstęp**

Procedura jest realizowana wyłącznie w Centralnym Punkcie Rejestracji.

Procedura dotyczy wystawienia certyfikatu kwalifikowanego do podpisu bądź pieczęci elektronicznej na podstawie klucza publicznego wygenerowanego na urządzeniu Subskrybenta.



ENIGMA

WEWNĘTRZNE

a. Wniosek o wystawienie certyfikatu, zawierający m.in. oświadczenie Subskrybenta, że klucze będą generowane na urządzeniu QSCD określonego typu oraz o spełnieniu przez niego wymagań opisanych w przywołanej w certyfikacie dokumentacji użytkownika urządzenia, w szczególności wymagań dotyczących dostawy oraz identyfikacji urządzenia oraz jego konfiguracji (jeśli występują takie wymagania).
b. Informacje dla Subskrybenta dot. usługi zaufania CenCert.

2. W przypadku certyfikatu do pieczęci elektronicznej, wniosek jest przekazywany Subskrybentowi w celu podpisania go przez osoby upoważnione.
3. Upoważniona osoba (Inspektor ds. rejestracji CenCert albo Administrator Systemu CenCert):
   a. identyfikuje urządzenie zgodnie z zapisami dokumentacji użytkownika urządzenia przywołanej w certyfikacie urządzenia (na tyle, na ile to jest możliwe na tym etapie użytkowania urządzenia) oraz potwierdza konfigurację urządzenia zgodnie z wymaganiami ww. dokumentacji (jeśli są takie wymagania); wykonanie ww. czynności potwierdza swoim podpisem na wniosku, o którym mowa powyżej.
   b. uczestniczy w operacji generowania kluczy subskrybenta,
   c. wpisuje identyfikator klucza publicznego we wniosek o wystawienie certyfikatu,
   d. zabezpiecza klucz publiczny do przekazania do CPR CenCert.
4. Inspektor ds. rejestracji identyfikuje osobę podpisującą wniosek oraz weryfikuje inne wymagane dane, zgodnie z zasadami opisanymi w procedurach P11-PIR-04-01-01/ P11-PIR-04-01-02. [2]
5. Subskrybent (dla certyfikatu do pieczęci - osoba upoważniona we wniosku) oraz Inspektor ds. rejestracji podpisują dokumenty.
6. Przed wystawieniem certyfikatu, Inspektor ds. rejestracji sprawdza:
   a. dane identyfikacyjne klucza publicznego z danym zawartymi we wniosku o wystawienie certyfikatu oraz
   b. parametry kryptograficzne klucza[3].

   Jeśli dane są zgodne, Inspektor wprowadza do Centaur PR klucz publiczny i generuje odpowiedni certyfikat.



THALES

# Uogólnijmy podejście do uzyskania pieczęci na własny HSM

**Wybierz dostawcę usług zaufania**

- Skontaktuj się z dostawcą.
- Sprawdź czy oferuje wydanie pieczęci na posiadane rozwiązanie HSM
- Równolegle sprawdź czy posiadasz HSM i środowisko zgodne z wymaganiami QSCD

**Zweryfikuj**

- Czy twój HSM może być skonfigurowany z wymaganiami QSCD
- Oraz wymaganiami dostawcy do wydania pieczęci

**Zbuduj środowisko do wydania i wykorzystania pieczęci**

**Zbuduj żądanie PKCS#10 zgodnie z procedurą dostawcy i złóż je u dostawcy celem wydania pieczęci**

**Uzyskałeś pieczęć**

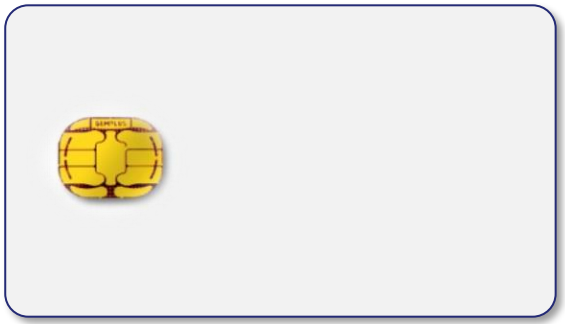
**Zainstaluje pieczęć w HSM**
**Wykonaj kopię zapasową**

**Gotowe**



THALES

# *„A po co w HSM jak można na karcie inteligentnej?”*



VS


*„HSM to karta inteligentna na sterydach…”*

## Główna różnica?

…poza:
pojemnością,
**wydajnością,**
certyfikacjami,
mechanizmami
Itd..

**karty inteligentne nie dostarczają mechanizmu backupu klucza prywatnego**

**z definicji, każdy HSM zapewnia backup materiału kryptograficznego, który chroni**



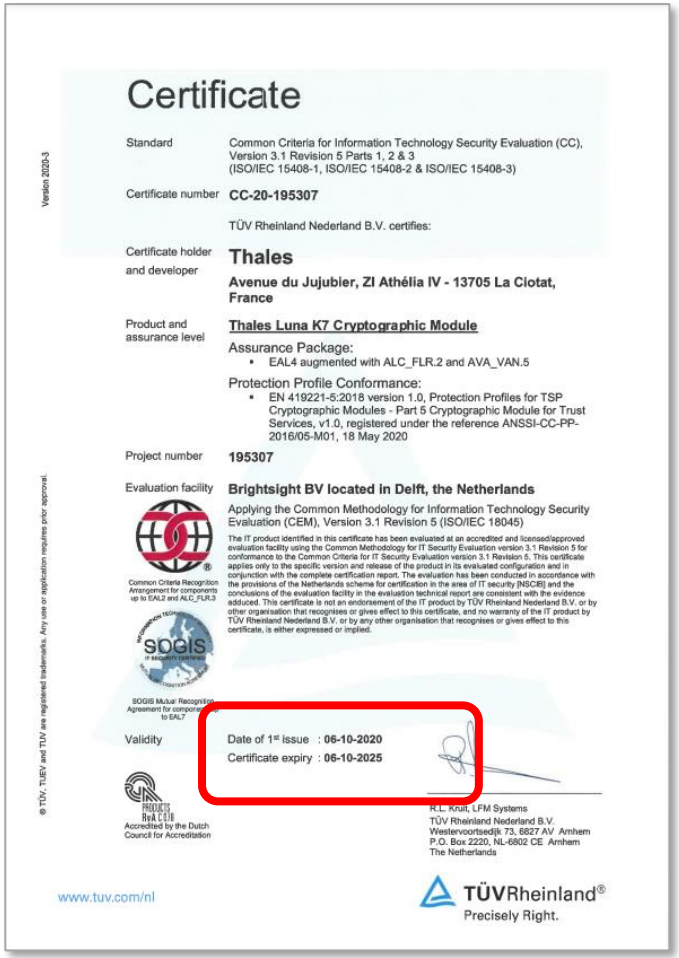
THALES

# A od strony technicznej: Luna 7 jako QSCD/QSealCD?

## Luna 7 posiada certyfikacje CC względem profilu:

| | |
|---|---|
| Product and assurance level | **Thales Luna K7 Cryptographic Module**<br>Assurance Package:<br>▪ EAL4 augmented with ALC_FLR.2 and AVA_VAN.5<br>Protection Profile Conformance:<br>▪ EN 419221-5:2018 version 1.0, Protection Profiles for TSP Cryptographic Modules - Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020 |

https://www.commoncriteriaportal.org/files/epfiles/CC-20-195307.pdf



Certificate

Standard: Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 Parts 1, 2 & 3 (ISO/IEC 15408-1, ISO/IEC 15408-2 & ISO/IEC 15408-3)

Certificate number: CC-20-195307

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer: Thales
Avenue du Jujubier, ZI Athélia IV - 13705 La Ciotat, France

Product and assurance level: Thales Luna K7 Cryptographic Module
Assurance Package:
▪ EAL4 augmented with ALC_FLR.2 and AVA_VAN.5
Protection Profile Conformance:
▪ EN 419221-5:2018 version 1.0, Protection Profiles for TSP Cryptographic Modules - Part 5 Cryptographic Module for Trust Services, v1.0, registered under the reference ANSSI-CC-PP-2016/05-M01, 18 May 2020

Project number: 195307

Evaluation facility: Brightsight BV located in Delft, the Netherlands
Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2 and ALC_FLR.3

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity: Date of 1st issue : 06-10-2020
Certificate expiry : 06-10-2025

Accredited by the Dutch Council for Accreditation

R.L. Kruit, LFM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.



Version 2020-3

# eIDAS: Luna K7 Cryptographic Module jako QSCD

https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD

| | |
|---|---|
| Name | Thales Luna K7 Cryptographic Module |
| Applicant | Thales |
| Remote QSCD | No |
| Qualified Signature Creation Device (QSigCD) | Yes |
| Issuer | TÜV Rheinland Nederland B.V. |
| Reference | CC-20-195307-eIDAS |
| URL | https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/02/eidas-certificate-luna-k7-20-195307-2.pdf en |
| Effective starting date | 06/10/2020 |
| Expiration date | 06/10/2025 |
| Art.30.3.(b) notified alternative certification method | https://www.tuv-nederland.nl/assets/files/general-files/2019/12/190724-trn-eidas-dutch-conformity-assessment-process---v5.0.pdf en |
| CC certification report(s) | |
| Reference: | NSCIB-CC-20-195307-CR |
| Issuer: | TÜV Rheinland Nederland B.V. |
| URL to report: | https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/10/cc-20-195307-certificate.pdf en<br>https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/10/nscib-cc-20-195307-cr.pdf en<br>https://www.tuv-nederland.nl/common-criteria/certificates.html en |
| URL to security target: | https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/10/st-002-010985-001_luna-pcie-hsm7_cc_securitytarget_revj.pdf en |
| Issuance date: | 06/10/2020 |



THALES

# eIDAS: Luna K7 Cryptographic Module jako QSealCD

| | |
|---|---|
| Qualified Seal Creation Device (QSealCD) | Yes |
| Issuer | TÜV Rheinland Nederland B.V. |
| Reference | CC-20-195307-eIDAS |
| URL | https://www.tuv-nederland.nl/assets/files/cerfiticaten/2021/02/eidas-certificate-luna-k7-20-195307-2.pdf en |
| Effective starting date | 06/10/2020 |
| Expiration date | 06/10/2025 |
| Art.30.3.(b) notified alternative certification method | https://www.tuv-nederland.nl/assets/files/general-files/2019/12/190724-trn-eidas-dutch-conformity-assessment-process---v5.0.pdf en |
| CC certification report(s) | |
| Reference: | NSCIB-CC-20-195307-CR |
| Issuer: | TÜV Rheinland Nederland B.V. |
| URL to report: | https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/10/cc-20-195307-certificate.pdf en<br>https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/10/nscib-cc-20-195307-cr.pdf en<br>https://www.tuv-nederland.nl/common-criteria/certificates.html en |
| URL to security target: | https://www.tuv-nederland.nl/assets/files/cerfiticaten/2020/10/st-002-010985-001_luna-pcie-hsm7_cc_securitytarget_revj.pdf en |
| Issuance date: | 06/10/2020 |
| Note(s) | |



THALES

# Luna 7 – konfiguracja jako QSCD/QSealCD

## Wymagania wstępne

- **Luna Network HSM wersja (SW/FW) 7.7.0 lub wyższa albo Luna PCIe HSM wersja 7.7.0 lub wyższa**
  - FW 7.7.1 i 7.7.2 też są „eidasowe!"
- **Luna HSM firmware version 7.7.0 lub wyższa**
- **Luna Client wersja 10.3 lub nowszy (Windows lub Linux)**
- **Backup HSM (G7) z FW 7.7.x lub  Backup HSM (G5) z FW 6.28.x**



THALES

# Luna 7 – konfiguracja jako QSCD/QSealCD

## Referencje :

### Dokumentacja do produktu Luna HSM:

- https://www.thalesdocs.com/gphsm/luna/7/docs/network/Content/CRN/Luna/firmware/7-7-0.htm
- Zawiera: przegląd produktów, instalacja i konfiguracja, podręcznik administrowania urządzeniem, konfiguracja klienta

### Przewodnik użytkownika Common Criteria

**DOW0006186 (KB0023049)** is
- "PART 1: PREPARATIVE PROCEDURES"

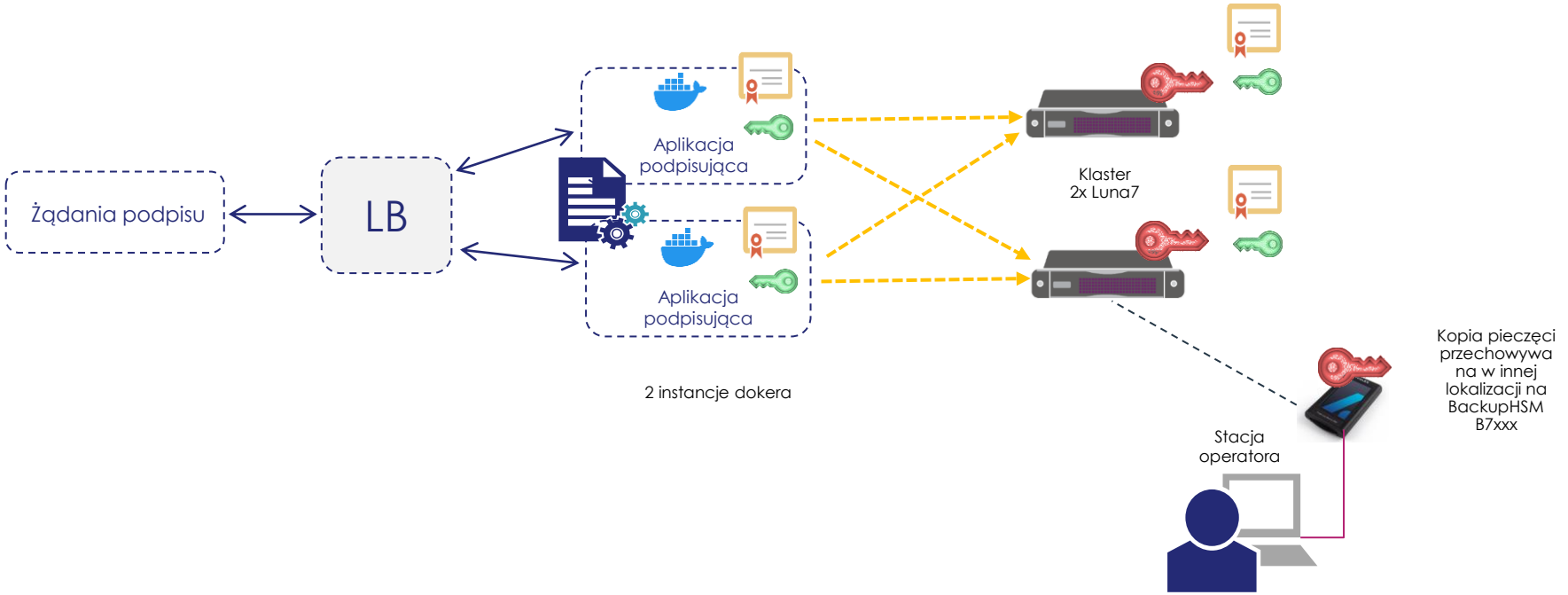
**DOW0006187 (KB0023050)** is
- "PART 2: OPERATIONAL GUIDANCE"

**DOW0006188 (KB0023051)** is
- "PART 3: EIDAS GUIDANCE"

**DOW0006189 (KB0023052)** is
- "PART 4 TOE INTEGRATION FOR USE IN COMPOSITE EVALUATION"

# Rozwiązanie

# Propozycja rozwiązania - architektura



# CryptoPanel


## podsumowanie

# I słowo o tym „*co potrzeba*”

- **Luna7 (A700) może być QSealCD do utrzymywania pieczęci kwalifikowanej**
- **Dla wymagających:**
  - Możliwość wdrożenia klastra HA/LB oraz
  - Kopia kluczy na wypadek DR (BackupHSM B7xx lub G5)

- **produkty dostępne w kanale partnerskim**
- **urządzenia demo do testów**

**BOM:**

- **2x Luna A700 – 2x 18k €**
- **2x Luna Client License - 2x 1k €**
- **1x Luna Backup HSM B700 – 1x 6k €**
- **Brak dodatkowych kosztów związanych z:**
  - Budową klastra,
  - Wsparciem ECC
  - „certyfikacją eIDAS”

# Nauczki i raczej nie znajdziecie w dokumentacji…

## Dedykowany HSM pod QSealCD czy nie dedykowany?

- Tak, bo…

## Jednoczesne przeznaczenie po inne zastosowania?

- **Raczej nie**, ponieważ…

## Czy można wykorzystać DPoD (HSMaaS) pod QSealCD?

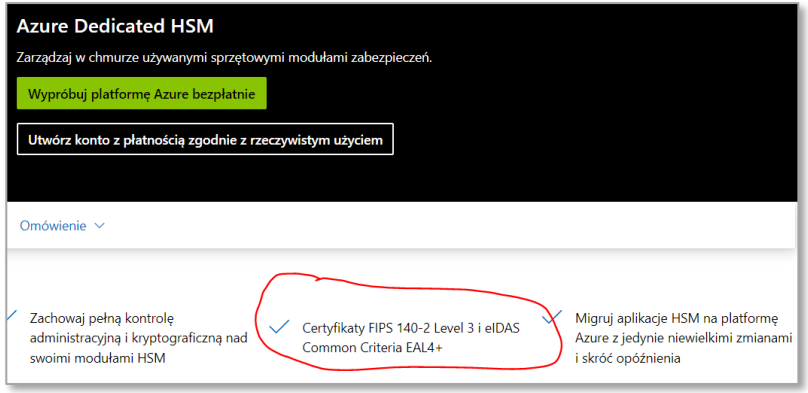
- Nie, choć może tak, ale nie…

# Nauczki i raczej nie znajdziecie w dokumentacji…

## Dedicated HSM z Microsoft jest QSealCD czy nie?

- To nasz Luna 7 Network HSM z certyfikacja CC i eIDAS

## A dlaczego nas pytacie? ☺ Wiecie co należy spełnić i powinniście pytać QTSP




W tym przypadku problem jest rodzaju prawnego. Ponieważ eIDAS rozpoznaje **lokalne** (użytkownik końcowy jest właścicielem QSCD) lub **zdalne użycie** QSCD.
Ponieważ Azure jest SP i nie jest QTSP, klient może potrzebować formalnego oświadczenia od Azure, np. że zapewniają tylko hosting, ale kontrola fizyczna i logiczne znajdują się w rękach użytkownika końcowego.

W przypadku zdalnego podpisywania (Remote Signing) - Azure HSM nie ma dziś (A.D. luty 2023) modułu SAM (do opracowania lub wdrożenia w FM)