LTV-Long-Term Validation of Signatures

Juliusz Horowski

Data:
13.06.2022

Proces uwierzytelniania podpisów

Certyfikat podpisującego

Nazwa powszechna: Marek Ernest Gosławski

Nazwa nadana: Marek Ernest

Nazwisko: Gosławski

Organizacja: Politechnika Poznańska

Kraj: PL

Numer (serialnumber): PNOPL-76060405172

Numer seryjny certyfikatu:
352846483643163967997463940013971990643743381 21

Wystawiony przez: COPE SZAFIR - Kwalifikowany

Wystawca certyfikatu zaufany

Certyfikat zweryfikowano pozytywnie

Ważny od: 30 października 2020, 09:00:00 (+02:00)
Ważny do: 30 października 2022, 09:00:00 (+02:00)

Certyfikat został zweryfikowany za pomocą:
- Certyfikat nie znajduje się na liście CRL
- Certyfikat nie znajduje się na liście OCSP

Elementy podpisu

Referencje
- 03_zweryfikowanie%20podpisu%20kwalifikowanego.txt
  md5: 1124fe18607b6964cebaa99c8ceb5ead
- #ID-d1f5ee34-5943-4d0f-bcaf-58934edc935c

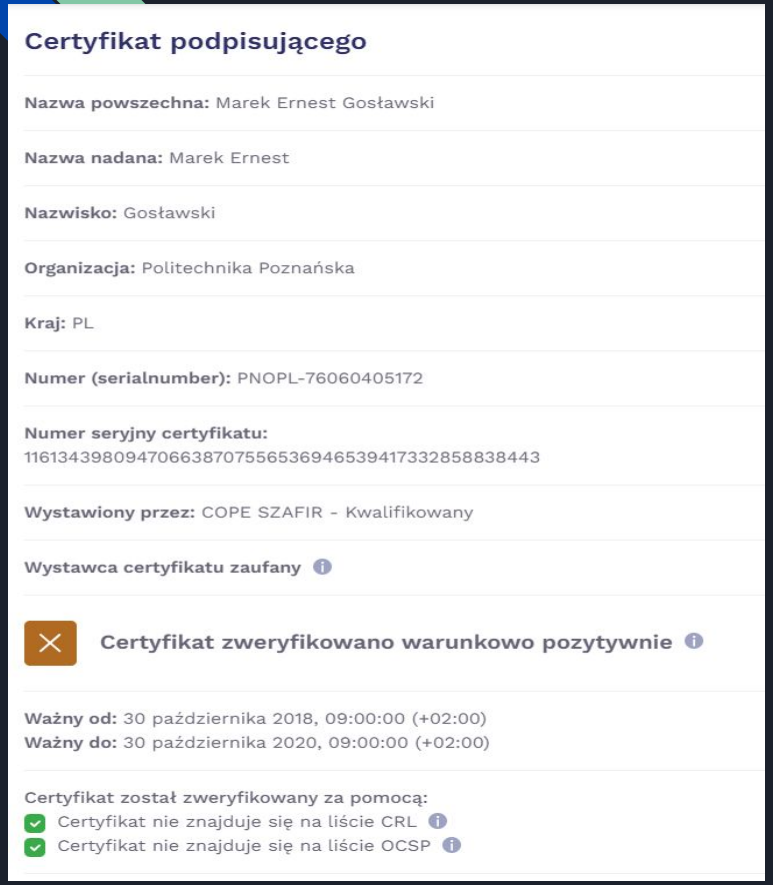
Wartość sygnatury

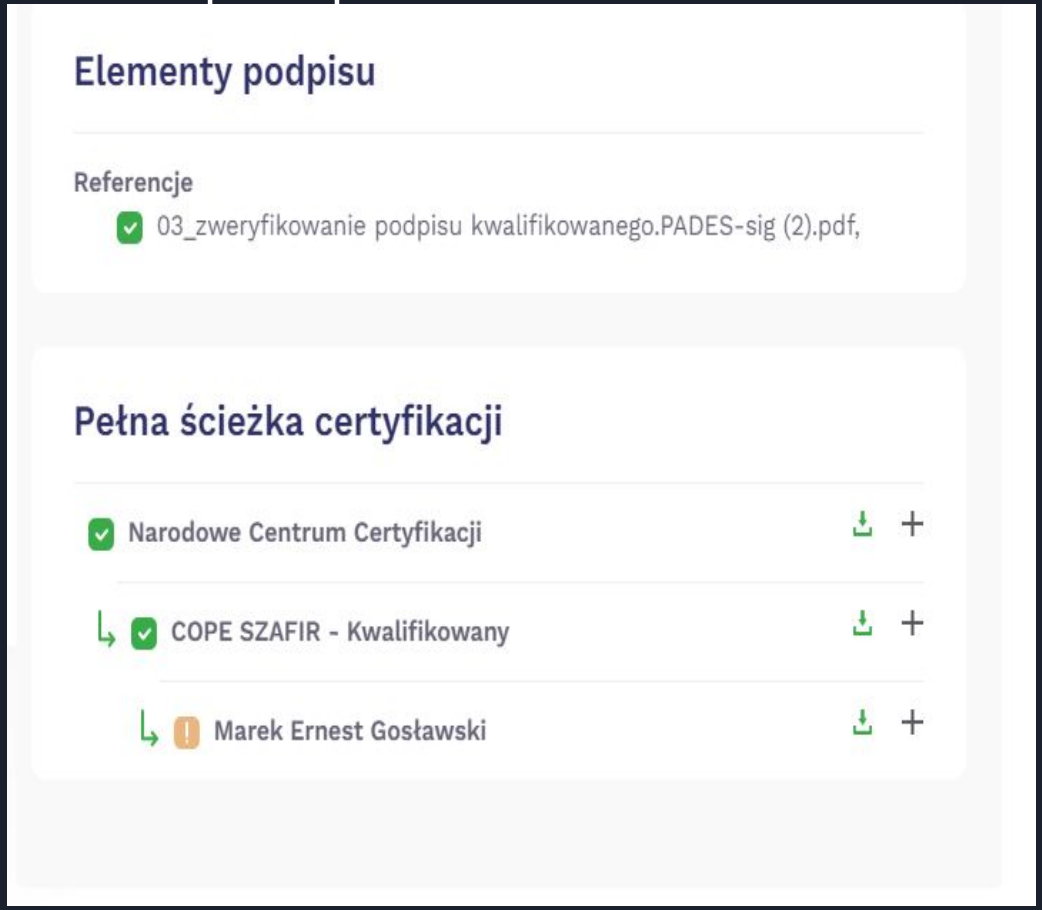
Wartość certyfikatu

Pełna ścieżka certyfikacji

- Narodowe Centrum Certyfikacji
  - COPE SZAFIR - Kwalifikowany
    - Marek Ernest Gosławski

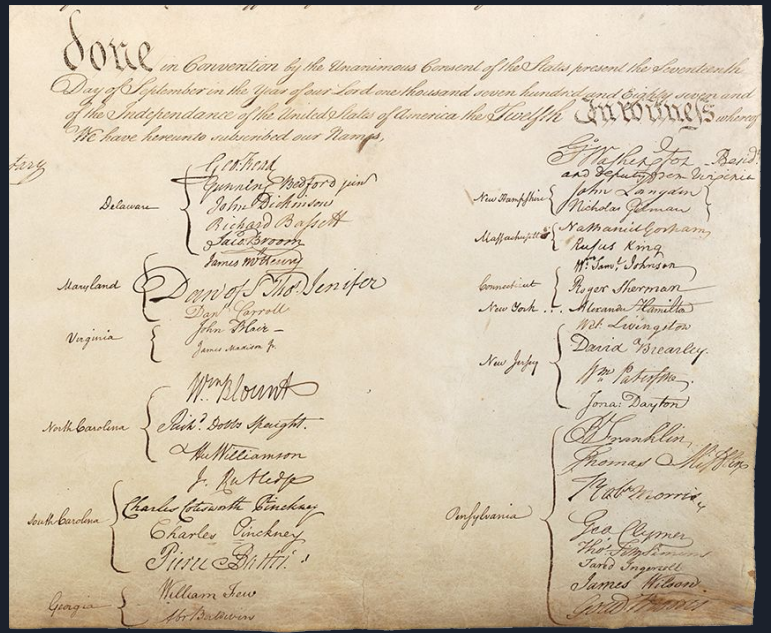
Proces uwierzytelniania podpisów





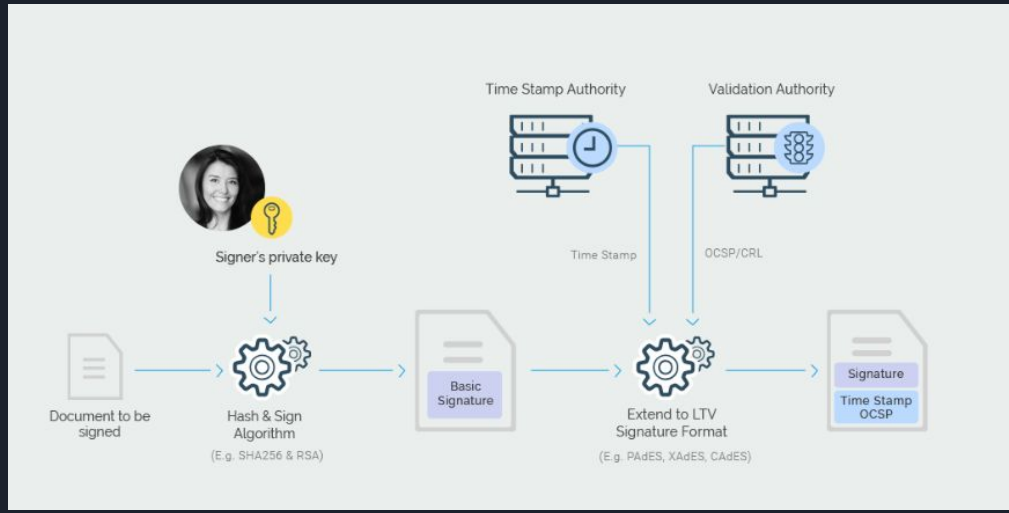
Problem przechowywania pliku w długim terminie

- kiedy podpisujemy się na papierze zakładamy że podpis jest na zawsze, a nie na np 2 lata
- Po upływie terminu certyfikatu nasz dokument nie przejdzie weryfikacji, i będzie potrzebny dodatkowy dokument.
- Dochodzi do tego koszt/czas na stworzenie nowego certyfikatu, podpisanie go ponownie dostarczenie wszystkim itp.



Na pomoc przychodzi LTV

- Long-Term Validation
- Pades(PDF Advanced Electronic Signatures)
- W celu przedłużenia wykorzystuje się znaczniki czasowe

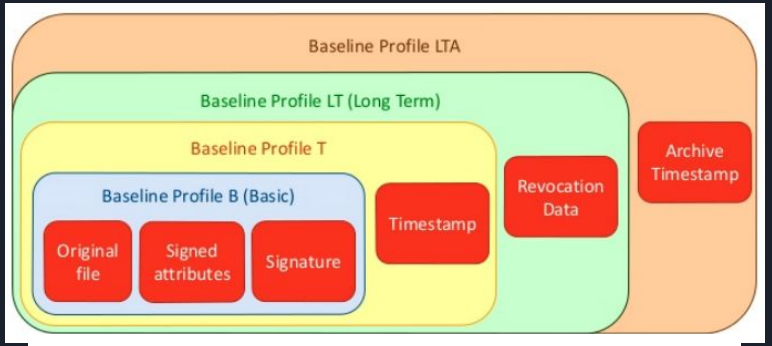


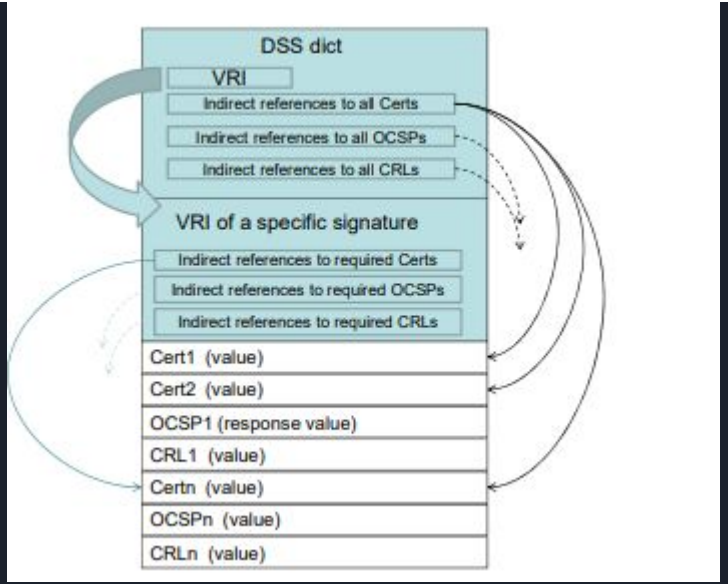
Pades

- Jest standardem rozszerzającym pdf i ISO 32000-1
- Po jego wykorzystaniu powstaje jeden, integralny dokument, który zawiera zarówno podpisaną treść jak i załączniki.
- W pliku może pojawić się wizualizacja, która wskazuje na to, że został on odpowiednio podpisany.
- Podpis w formacie PAdES uniemożliwia późniejszą zmianę i modyfikację danych w dokumencie.
- Jest to najprostszy sposób podpisania dokumentu zarówno w biznesie, jak i w administracji publicznej.

Pades- budowa

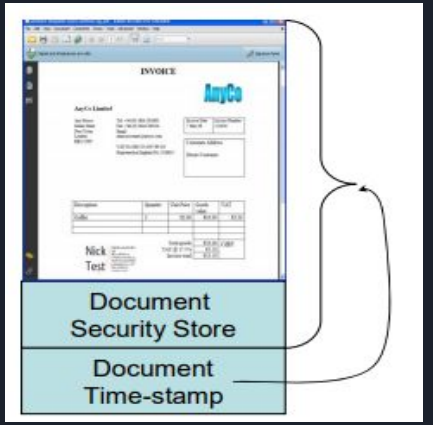
- Document Security Store
- Validation Related Information
- Różne profile wymagają różnych informacji
  - B-level- przeznaczone dla krótkoterminowych podpisów
  - T level- potwierdza że w danym momencie istniał dokument
  - LT level - dodaje VRI pozwala to na potwierdzenie dokumentu w długim terminie, do momentu daty ważności najwyższego certyfikatu
  - LTA level-dodaje dodatkowy timestamp i VRI dla TSA

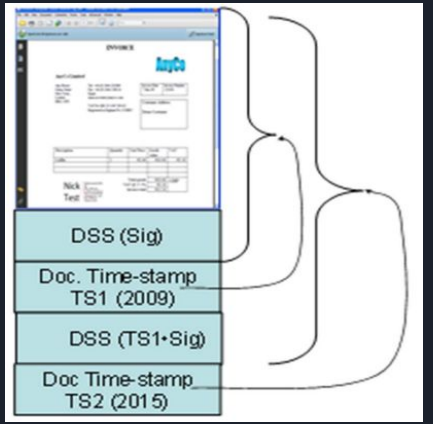




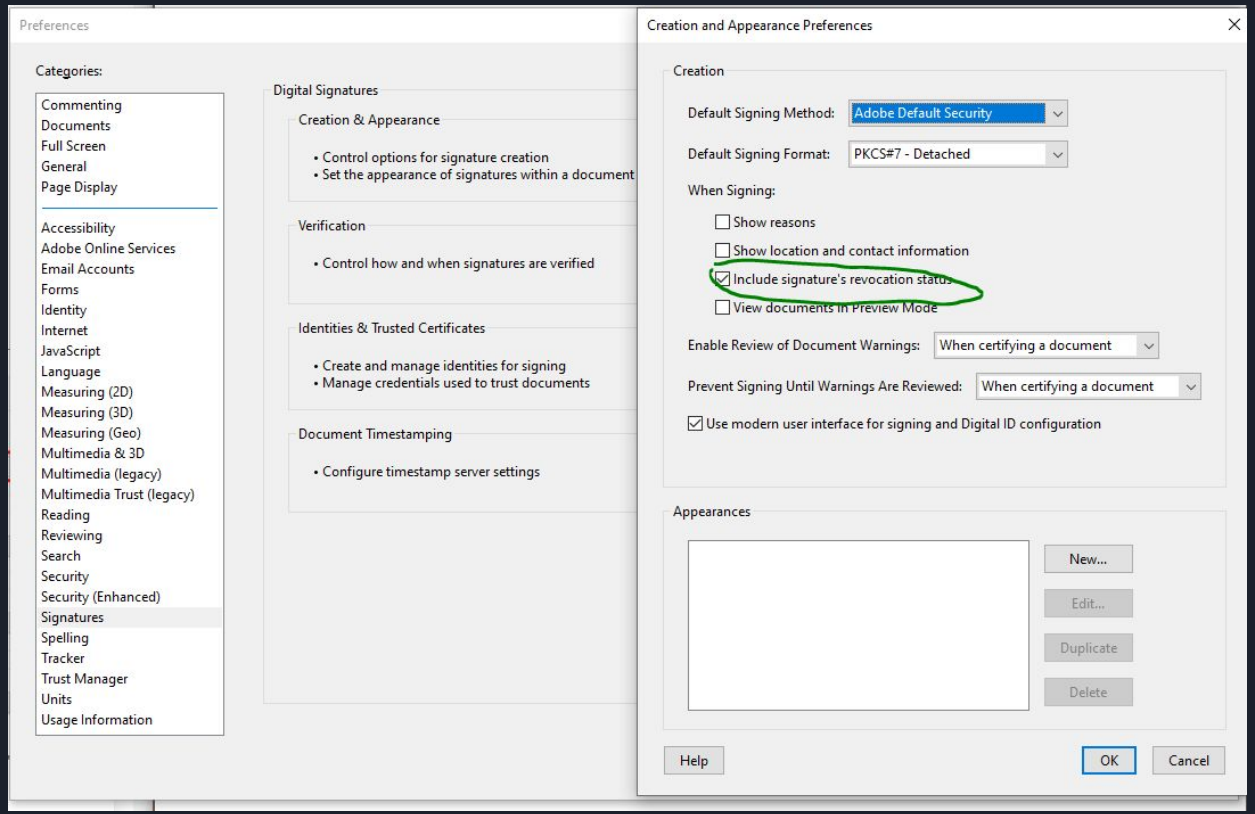
LTV- jak działa

- Przy pomocy document Time-stamp i TSA potwierdzamy że dokument w danym dniu był “potwierdzony”
- Sprawdzamy każdy krok certyfikacji za pomocą informacji zapisanych w pliku
- Możemy dalej przedłużać plik kiedy poprzedni podpis wygaśnie poprzez dodanie nowego Timestampu oraz VRI

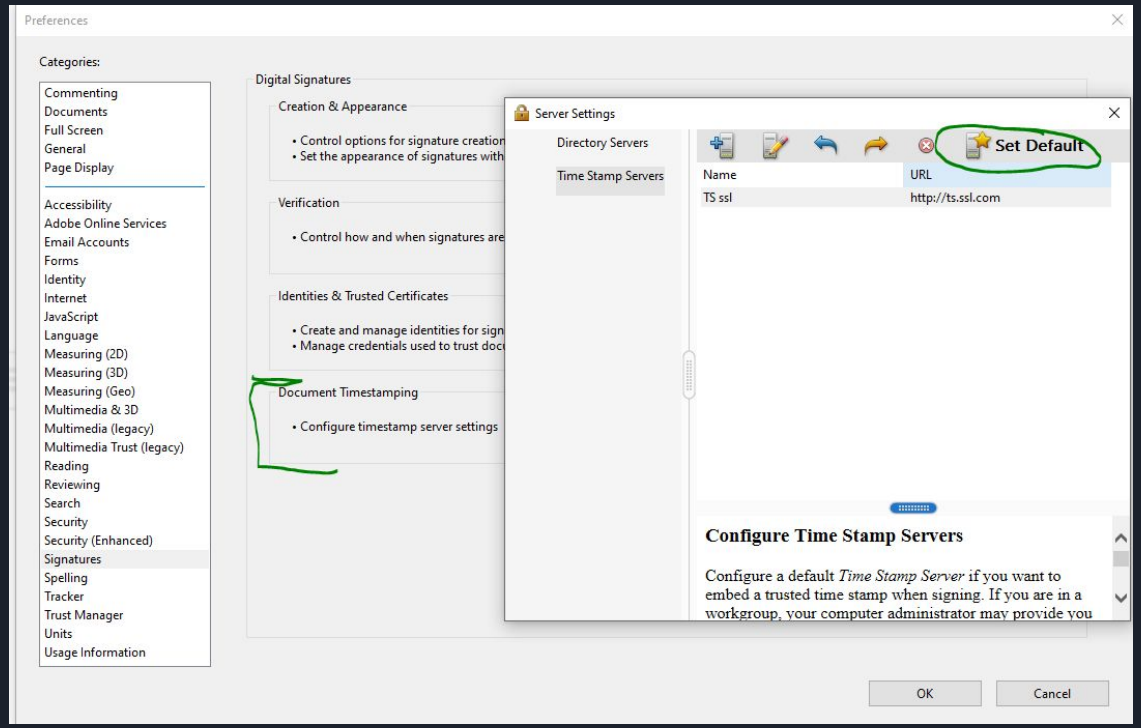


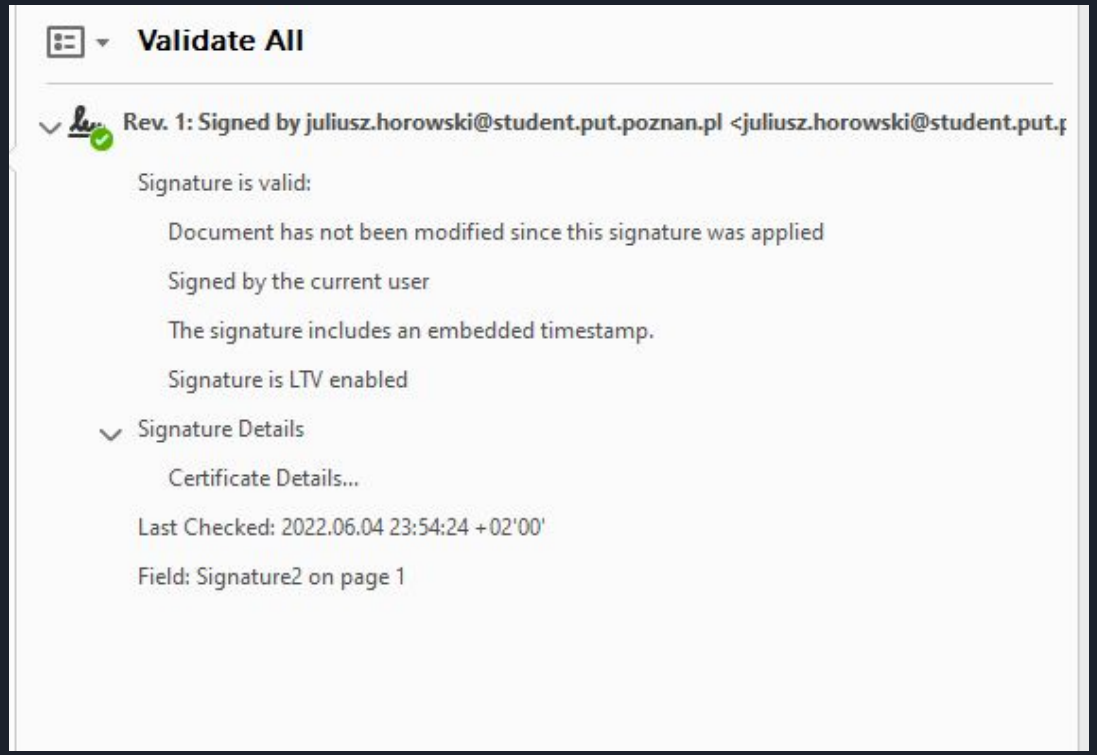


Jak dodać LTV - adobe reader



Jak dodać LTV - adobe reader




Validate All
Rev. 1: Signed by juliusz.horowski@student.put.poznan.pl <juliusz.horowski@student.put.p
Signature is valid:
Document has not been modified since this signature was applied
Signed by the current user
The signature includes an embedded timestamp.
Signature is LTV enabled
Signature Details
Certificate Details...
Last Checked: 2022.06.04 23:54:24 +02'00'
Field: Signature2 on page 1

Szczegóły podpisu

Certyfikat:

Numer seryjny	[redacted]
Wystawiony przez	EDU-CA
Właściciel (nazwa powszechna)	juliusz.horowski@student.put.poznan.pl
Status	Ważny
Czy kwalifikowany?	Tak

Podpis:

Data podpisania	2022-06-05 01:09:39 CEST
Status	Zgodny z dokumentem
Typ podpisu	PAdES

Zamknij

Rev. 2: Signed by Minister do spraw informatyzacji - pieczec podpisu zaufanego

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

Document has not been modified since this signature was applied

Signer's identity is valid

Signing time is from the clock on the signer's computer.

Signature is not LTV enabled and will expire after 2024/02/17 11:37:12 +02'00'

Signature Details

Last Checked: 2022.06.05 01:35:24 +02'00'

Field: Signature1 on page 1

Click to view this version

Rev. 2: Signed by Minister do spraw informatyzacji - pieczec podpisu zaufanego

Signature is valid:

Source of Trust obtained from European Union Trusted Lists (EUTL).

Document has not been modified since this signature was applied

Signer's identity is valid

The signature includes a timestamp embedded in the document.

Signature is LTV enabled

Signature Details

Last Checked: 2022.06.05 01:31:39 +02'00'

Field: Signature1 on page 1

Click to view this version

Signature Properties

Signature is VALID, signed by Minister do spraw informatyzacji - pieczec podpisu zaufanego.

Signing Time: 2022/06/05 01:28:41 +02'00'

Source of Trust obtained from European Union Trusted Lists (EUTL).

Reason: Opatrzono pieczęcią ministra właściwego do spraw informatyzacji w imieniu: JULIUSZ HOROWSKI, PESEL: 97091905358, PZ ID: travesom

Validity Summary

The document has not been modified since this signature was applied.

The certifier has specified that Form Fill-in, Signing and Commenting are allowed for this document. No other changes are permitted.

The signer's identity is valid.

The signature includes a timestamp embedded in the document. Timestamp time:
2022/06/05 01:31:39 +02'00'

Signature was validated as of the secure (timestamp) time:
2022/06/05 01:31:39 +02'00'

Źródła

ETSI TS 103 172 V2.2.2 (2013-04)

ETSI EN 319 142-1 V1.1.1 (2016-04)

ETSI TS 102 778-4 V1.1.1 (2009-07

https://www.cryptomathic.com/news-events/blog/pades-and-long-term-archival-lta

https://eideasy.com/eidas-digital-signature-profiles/

https://www.archives.gov/files/founding-docs/constitution-signatures.png