

Computer Security List r

Bartosz Michalak

29 April 2024

1 Task 2.2

Trusted profile is used to **confirm user's identity** in various electronic administrative systems as well as **signing documents** with trusted signature.

It may be used by anyone who has PESEL number and full or restricted legal capacity. It is valid for 3 years.

2 Task 2.3

I signed simple .txt file. It was signed by XAdES and returned as XML. We may check if the file is properly signed by clicking "ZOBACZ" option.

XAdES - signature is separate from the document.

PADES - built in PDF file (extends it).

3 Task 2.4

Certificate was issued by Trusted signature (Minister of Information Technology - trusted signature stamp).


Certificate revocation list (CRL) is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.

4 Task 2.5


We see that insides of document where changed.

Twój dokument został poprawnie podpisany

PODPISYWANIE PLIKÓW W FORMACIE XAdES




testForSign.txt



Wróć do początku

Właściciel podpisu: **BARTOSZ MICHALAK**

Data i godzina podpisu: **2024-04-28 23:06:39 CEST**

Status podpisu:  **Ważny**

Rodzaj podpisu: **Podpis zaufany**

Pobierz dokument ze swoim podpisem na dysk lokalny.

Plik będzie w formacie XML.

POBIERZ

Jak zobaczyć zawartość pobranego pliku XML ^

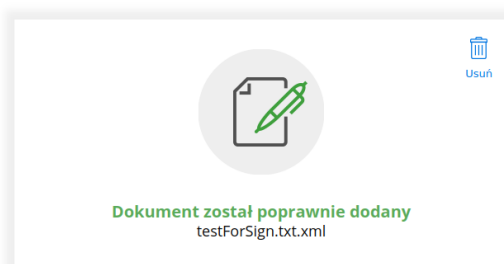
Skorzystaj z usługi jeszcze raz.

[Wróć do początku](#) , dołącz pobrany plik i kliknij przycisk **Zobacz dokument**.

Figure 1: Task 2.3 Document is signed

Możesz:

- podpisywać dokumenty – również te, które podpisał ktoś inny
- sprawdzić, czy inne osoby złożyły prawidłowy podpis
- zobaczyć podpisane dokumenty



Właściciel podpisu: **BARTOSZ MICHALAK**
Data i godzina podpisu: **2024-04-28 23:06:39 CEST**
Status podpisu: **Ważny**
Rodzaj podpisu: **Podpis zaufany**

**Jeśli chcesz zobaczyć zawartość dodanego dokumentu –
kliknij przycisk poniżej.**

W ten sposób pobierzesz dokument na dysk lokalny.

ZOBACZ DOKUMENT

Teraz możesz podpisać dodany dokument za pomocą podpisu
elektronicznego

PODPISZ

① **Rozmiar dokumentu:** maksimum 10 MB.

Rozszerzenie: .pdf, .txt, .rtf, .xps, .odt, .ods, .odp, .doc, .xls, .ppt, .docx, .xlsx, .pptx, .csv, .jpg, .jpeg, .tif, .tiff, .geotiff, .png, .svg, .wav, .mp3, .avi, .mpeg, .mp4, .m4a, .mpeg4, .ogg, .ogv, .zip, .tar, .gz, .gzip, .7z, .html, .xhtml, .css, .xml, .xsd, .gml, .rng, .xsl, .xslt, .TSL, .dwg, .dwt, .dxf, .dgn, .jp2.

Format podpisywania:

- **Dokument .pdf** podpiszesz w formacie PAdES
Jeśli chcesz podpisać .pdf w formacie XAdES - kliknij ten link.
- **Dokumenty inne niż .pdf** podpiszesz w formacie XAdES

[Sprawdź, czym się różnią formaty PAdES i XAdES.](#)

Zalecamy przeglądarki internetowe:

- Google Chrome od wersji 71.0.3
- Firefox od wersji 65.0.1
- Safari od wersji 12.0.2

Figure 2: Task 2.3 Menu

5 Task 2.6

If service is not on the TSL list it means that supervised/accredited by (in this case) the Polish state.

6 Task 2.7

Trusted Signature:

Figure 3: Task 2.3 Insides of signed XML file

Figure 4: Task 2.4 Proper file

Figure 5: Task 2.4 Signature

4

Certyfikat podpisującego

Nazwa powszechna: Minister do spraw informatyzacji - pieczęć podpisu zaufanego

Organizacja: Ministerstwo Cyfryzacji

Kraj: PL

Numer seryjny certyfikatu: 20892124217292921814138920212746575688618877

Wystawiony przez: Centrum Kwalifikowane EuroCert

Wystawca certyfikatu zaufany ⓘ



Certyfikat zweryfikowano pozytywnie ⓘ

Ważny od: 13 lutego 2024, 11:27:09 (+02:00)

Ważny do: 12 lutego 2027, 11:27:09 (+02:00)

Certyfikat został zweryfikowany za pomocą:



Certyfikat nie znajduje się na liście CRL ⓘ

SZCZEGÓŁY ▾

Figure 6: Task 2.4 Certificate

identity verification compared to personal or qualified signatures.

Personal Signature:

A personal signature is a more advanced form of electronic signature that requires identity confirmation through special authentication means, such as an SMS code or password.

Using a personal signature usually entails a higher level of trust and is applied to more demanding online transactions.

Qualified Signature:

Elementy podpisu

Referencje

- ✓ Podpisany dokument
- ✓ #SignedProps-3adfc304-08a4-4607-99bb-2f1c5b4c30b7

✓ Wartość sygnatury

✓ Wartość certyfikatu

Pełna ścieżka certyfikacji

- ✓ Narodowe Centrum Certyfikacji  +
- ↳ ✓ Centrum Kwalifikowane EuroCert  +
- ↳ ✓ Minister do spraw informatyzacji - pieczęć podpisu zaufanego  +

Figure 7: Task 2.4 Additional Info

	testForSign.txtCHANGE.xml md5: dcb35d1246f258f85dbadda2e4d7a607	
	Integralność:	Niezachowana - podpisane dane prawdopodobnie zostały zmodyfikowane po ich uwierzytelnieniu elektronicznym
	Podpisujący:	BARTOSZ MICHALAK
	Rodzaj uwierzytelnienia:	Podpis zaufany (Minister do spraw informatyzacji - pieczęć podpisu zaufanego)
	Deklarowany czas złożenia podpisu:	2024-04-28T23:06:39.259+02:00 ⓘ

Figure 8: Task 2.5 Modified document

A qualified signature is the most advanced form of electronic signature, legally equivalent to a traditional handwritten signature. To obtain a qualified signature, a qualified certificate issued by trusted certification authorities is required. A qualified signature provides the highest level of security, authenticity, and

	sec-lab4-testowy-osobisty-eDOApp.pdf md5: 6919e4599400c5509017558a58eaa443	
	Integralność:	Zachowana - podpisane dane nie zostały zmodyfikowane od czasu ich elektronicznego uwierzytelnienia
	Podpisujący:	ANNA STANISŁAWA LAUKS-DUTKA
	Rodzaj uwierzytelnienia:	Podpis osobisty
	Deklarowany czas złożenia podpisu:	2024-04-21 14:31:32+00:00 ⓘ

Figure 9: Task 2.6 Downloaded Document

legal significance.

Podpis	SHA384	PAdES-BASELINE-B
Podpisujący: ANNA STANISŁAWA LAUKS-DUTKA		
Deklarowany czas złożenia podpisu: 2024-04-21 14:31:32+00:00 ⓘ		
Rodzaj uwierzytelnienia: Podpis osobisty		
Podpisano dokument: sec-lab4-testowy-osobisty-eDOApp.pdf, rewizja 1 z 1		
Certyfikat podpisującego		
Nazwa powszechna: ANNA STANISŁAWA LAUKS-DUTKA		
Nazwa nadana: ANNA		
Nazwisko: LAUKS-DUTKA		
Kraj: PL		
Numer (serialnumber): PNOPL-81012816287		
Numer seryjny certyfikatu: 155514391784278870926230391426620553441		
Wystawiony przez: pl.ID Authorization CA		
Wystawca certyfikatu niezaufany ⓘ		

Figure 10: Task 2.6 Signature info

Wystawiony przez: pl.ID Authorization CA

Wystawca certyfikatu niezauwany ⓘ

✓

Certyfikat zweryfikowano pozytywnie ⓘ

Ważny od: 1 marca 2023, 08:00:26 (+02:00)

Ważny do: 2 marca 2033, 00:59:59 (+02:00)

Certyfikat został zweryfikowany za pomocą:

✓ Certyfikat nie znajduje się na liście OCSP ⓘ

SZCZEGÓŁY ✓

Elementy podpisu

Referencje

✓ sec-lab4-testowy-osobisty-eDOApp.pdf,

Pełna ścieżka certyfikacji

✓ pl.ID Root CA

↓ +

↳ ✓ pl.ID Authorization CA

↓ +

↳ ✓ ANNA STANISŁAWA LAUKS-DUTKA

↓ +

Figure 11: Task 2.6 More Info