E-DOWÓD

FUNKCJE I KONSTRUKCJA

Maciej Marciniak

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

CZYM JEST E-DOWÓD

E-dowód to dowód osobisty z warstwą elektroniczną.

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

ZASTOSOWANIA BIZNESOWE

- Identyfikacja i uwierzytelnienie,
- Elektroniczne podpisanie dokumentu,
- Potwierdzenie obecności obywatela (służba zdrowia, administracja),
- Możliwość odczytu danych zawartych warstwie wizualnej z warstwy elektronicznej,
- Możliwość przechowania dodatkowych danych do odczytu (np. numer ICE),

ZASTOSOWANIA BIZNESOWE CD.

- Dokument podróży zgodny z ICAO (np. przejście przez bramki lotniska),
- Możliwość zainicjowania kwalifikowanego podpisu serwerowego (innego dostawcy),
- Możliwość użycia w przyszłości w Urzędomatach np. ZUS, US,
- Dotychczasowa funkcjonalność dowodu bez warstwy elektronicznej pozostaje bez zmian.

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

UŻYCIE W E-USŁUGACH

- E-dowód umożliwia uwierzytelnienie na poziomie wysokim, przy czym Profil Zaufany na poziomie średnim,
- Stosowany w przypadku kiedy wymagane jest nie tylko uwierzytelnienie, ale podpis,
- Możliwe udostępnienie SDK dla zastosowań komercyjnych.

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

PRZECHOWYWANE DANE

- dane dotyczące osoby:
  - Nazwisko,
  - Imię i pozostałe imiona,
  - Nazwisko rodowe,
  - Imiona rodziców,
  - Data i miejsce urodzenia,
  - Płeć,
  - Zdjęcie (biometryczne)
  - PESEL,
  - Obywatelstwo.

PRZECHOWYWANE DANE

- dane dotyczące dowodu osobistego:
  - serię i numer dowodu osobistego,
  - Datę wydania,
  - Datę ważności,
  - Oznaczenie organu wydającego dowód osobisty.

PRZECHOWYWANE DANE

- dane dodatkowe:
  - Certyfikat uwierzytelniający oraz potwierdzający obecność (10 lat ważności),
  - Kontener danych własnych – pamięć FLASH.

ZAWARTOŚĆ CERTYFIKATU IDENTYFIKACJI

- Kraj (countryName) - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, 2 literowy kod zgodny z ISO 3166;
- Nazwa wyróżniająca (commonName) - pole obowiązkowe: Jest to połączenie pól „Imię/Imiona” + „ ” + „Nazwisko”;
- Nazwisko (Surname) - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Nazwisko”;
- Pierwsze Imię (givenName) – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Pierwsze imię”;
- Drugie Imię (givenName) – pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – „Drugie imię”;
- Numer seryjny (serialNumber) - pole obowiązkowe: numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

ZAWARTOŚĆ CERTYFIKATU DLA ZAAWANSOWANEGO PODPISU ELEKTRONICZNEGO

- Kraj (countryName) - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, 2 literowy kod zgodny z ISO 3166;
- Nazwa wyróżniająca (commonName) - pole obowiązkowe: Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko”;
- Nazwisko (Surname) - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Nazwisko”;
- Pierwsze Imię (givenName) – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Pierwsze imię”;
- Drugie Imię (givenName) – pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – „Drugie imię”;
- Numer seryjny (serialNumber) - pole obowiązkowe: numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

ZAWARTOŚĆ CERTYFIKATU DO POTWIERDZANIA OBECNOŚCI

- Kraj (countryName) - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, 2 literowy kod zgodny z ISO 3166;
- Nazwa wyróżniająca (commonName) - pole obowiązkowe: Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko”;
- Nazwisko (Surname) - pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Nazwisko”;
- Pierwsze Imię (givenName) – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Pierwsze imię”;
- Drugie Imię (givenName) – pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – „Drugie imię”;
- Numer seryjny (serialNumber) - pole obowiązkowe: numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

ZABEZPIECZENIA

FIZYCZNE

- Mikroteksty pozytywowe/negatywowe,
- Przejścia kolorystyczne,
- Linie giloszowe (UV),
- Kod w technice TLE.

CYFROWE

- Zgodne z ISO 15408,
- Poziom certyfikacji EAL4+,
- Numer CAN – zabezpieczenie przed nieuprawnionym odczytem,
- Dwa PINy stosowane wymiennie do operacji uwierzytelniania.

PLAN PREZENTACJI

- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

WYMAGANIA CZYTNIKA

- Deklaracja zgodności WE oraz oznaczenie CE dla czytnika,
- Połączenie ze stacja roboczą za pomocą złącza USB lub bezprzewodowo, lub poprzez inny port komunikacyjny zapewniający poprawną komunikację czytnika ze stacją roboczą,
- Interfejs bezstykowy zgodny z ISO 14443 1-4 Typ A oraz ISO 14443 1-4 Typ B; Obsługa protokołów T=0 oraz T=1,
- Obsługa extended APDU,
- Obsługa kart w formacie TD1 (85,6 mm x 54,0 mm x 1,25 mm) zgodnych z ICAO 9303-3 oraz anteny klasy 1 zgodnie z ISO 14443-1.

Źródło:
https://www.gov.pl/documents/4675785/0/Specyfikacja_wymagan_technicznych_dla_czytnika_kart_bez_pinpadu_-_inne.pdf/b572b797-095d-68ac-846b-1569bc81bcca

PLAN PREZENTACJI

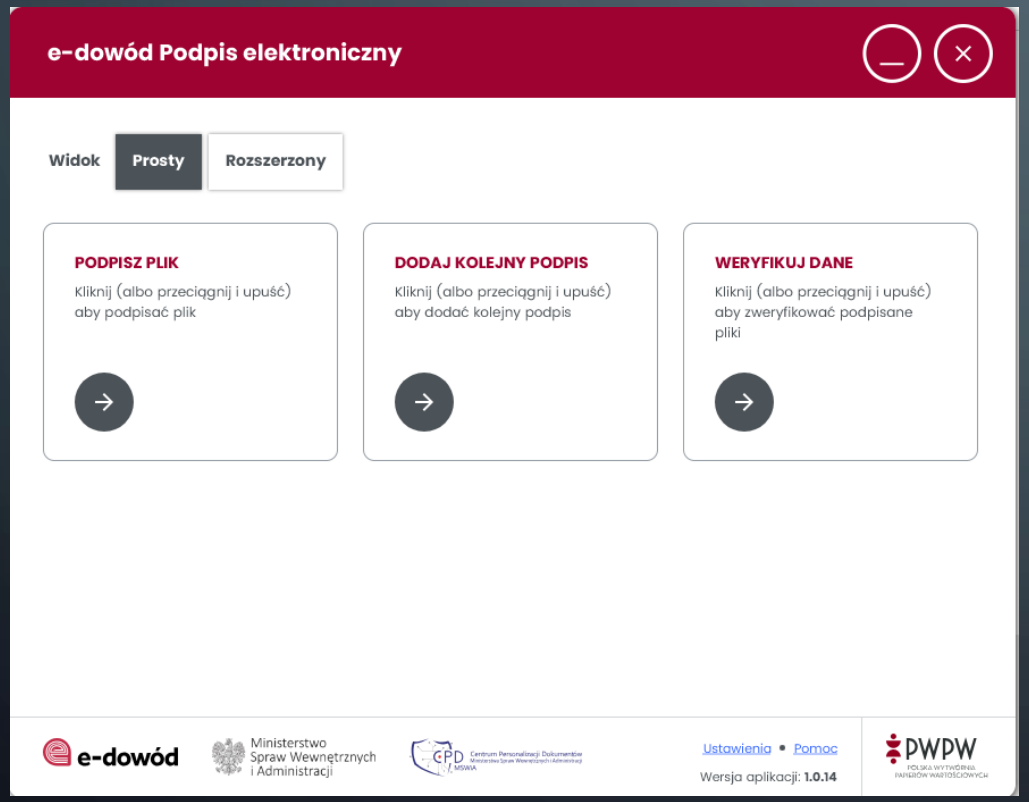
- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.

OPROGRAMOWANIE

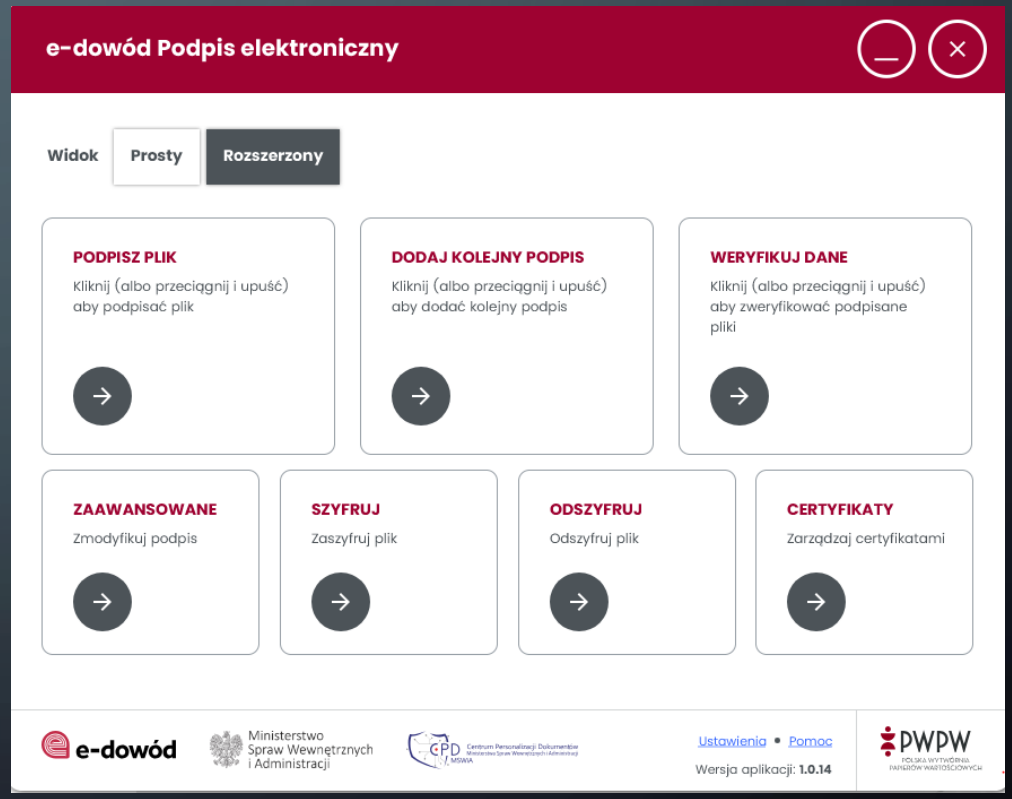
- E-dowód podpis elektroniczny – umożliwia podpisanie jednym lub wieloma podpisami plik, albo jego zweryfikowanie,
- E-dowód menadżer – pakiet programów do zarządzania e-dowodem:
  - E-dowód Monitor,
  - E-dowód Menedżer,
  - E-dowód Podaj CAN.

E-DOWÓD PODPIS ELEKTRONICZNY

WIDOK PROSTY

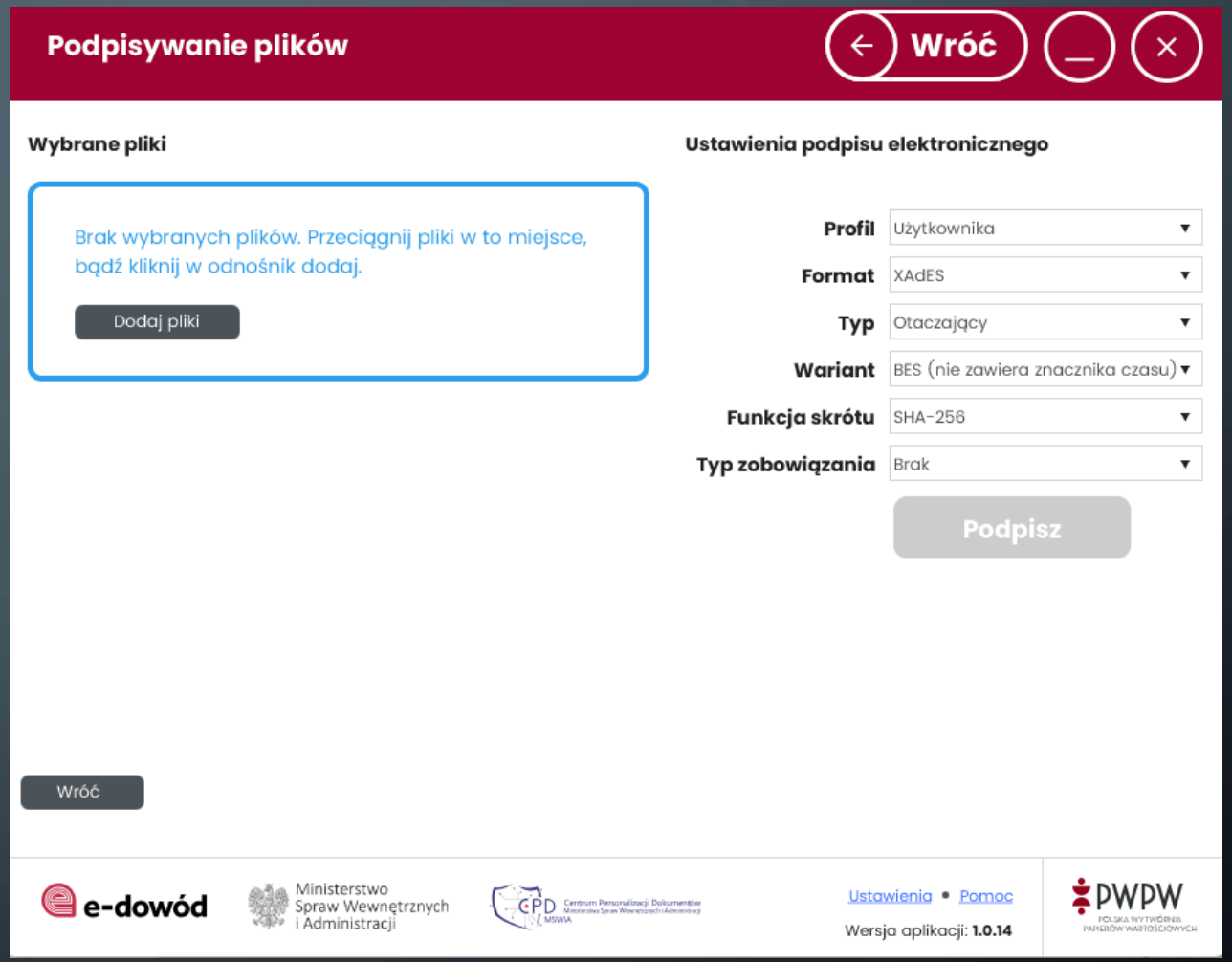


WIDOK ROZSZERZONY



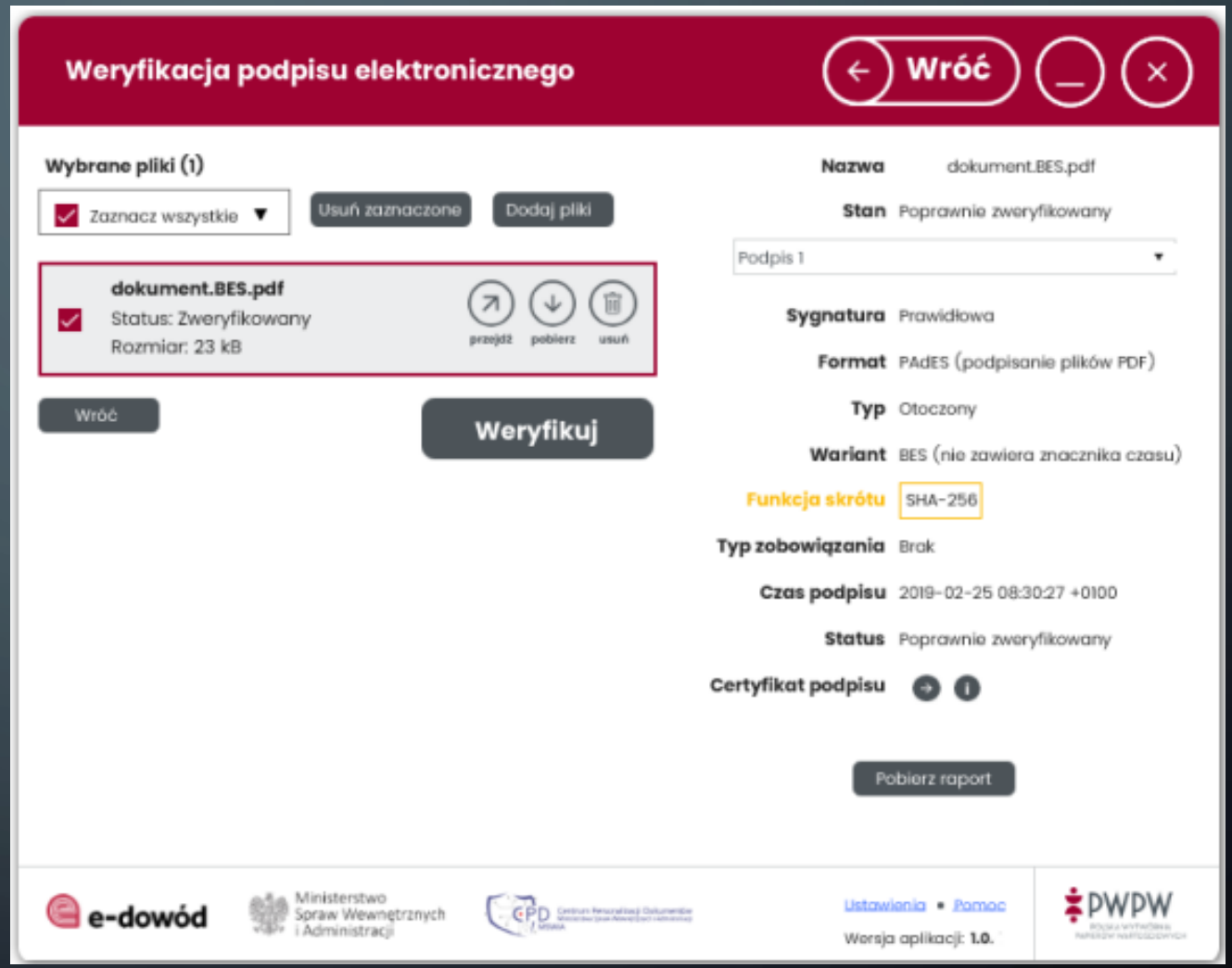
PODPISANIE PLIKU

- Wybór pliku przez przeciągnięcie lub menedżer plików,
- Wybór profili: podstawowy, użytkownika, e-deklaracje, e-puap, dokumenty prawne, podpis długoterminowy,
- Obsługiwane formaty: XAdES, PAdES, CAdES, ASiCE i ASiCS,
- Typ – zależy od formatu,
- Wariant – oznacza czy występuje znacznik czasu, czy nie
- Funkcja skrótu: SHA 256/384/512,
- Typ zobowiązania: dowód pochodzenia, potwierdzenie odbioru, dowód dostawy, dowód nadawcy, formalne potwierdzenie, potwierdzenie utworzenia,
- Kolejne podpisu zawierają jedynie: wariant, funkcje skrótu i zobowiązanie.



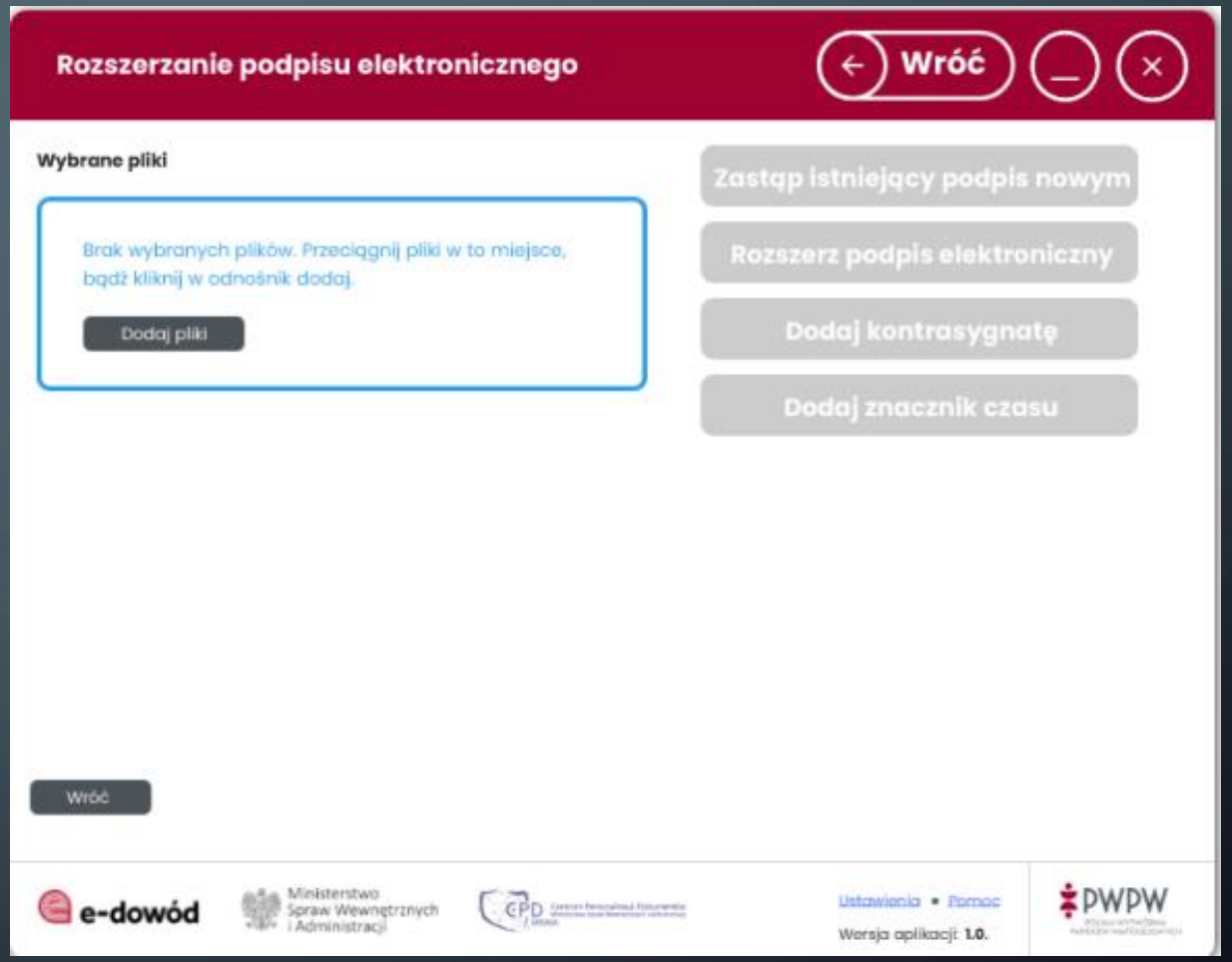
WERYFIKUJ DANE

- Wybór pliku przez upuszczenie lub menedżer plików,
- Możliwe stany weryfikacji: poprawnie zweryfikowany, negatywnie zweryfikowany, niekompletnie zweryfikowany, ostrzeżenia (brak list CRL, brak danych wystawcy),



OPCJE ZAAWANSOWANE

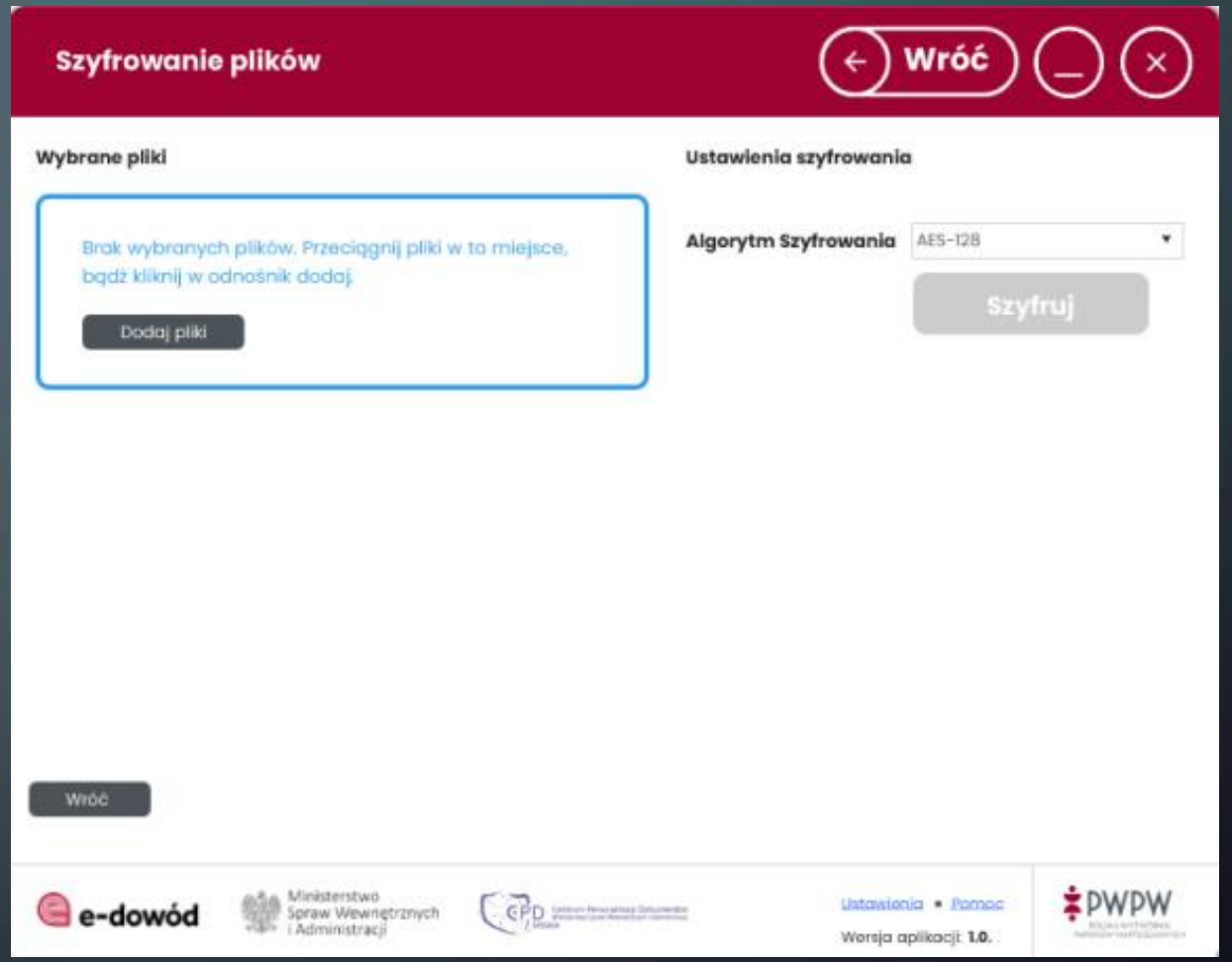
- Zastępowanie istniejących podpisów,
- Rozszerzenie o znacznik czasu,
- Dodaj kontrasygnatę oznacza, że do podpisu, przyporządkowanego do pliku dodany zostanie kolejny potwierdzający integralność treści.



SZYFROWANIE

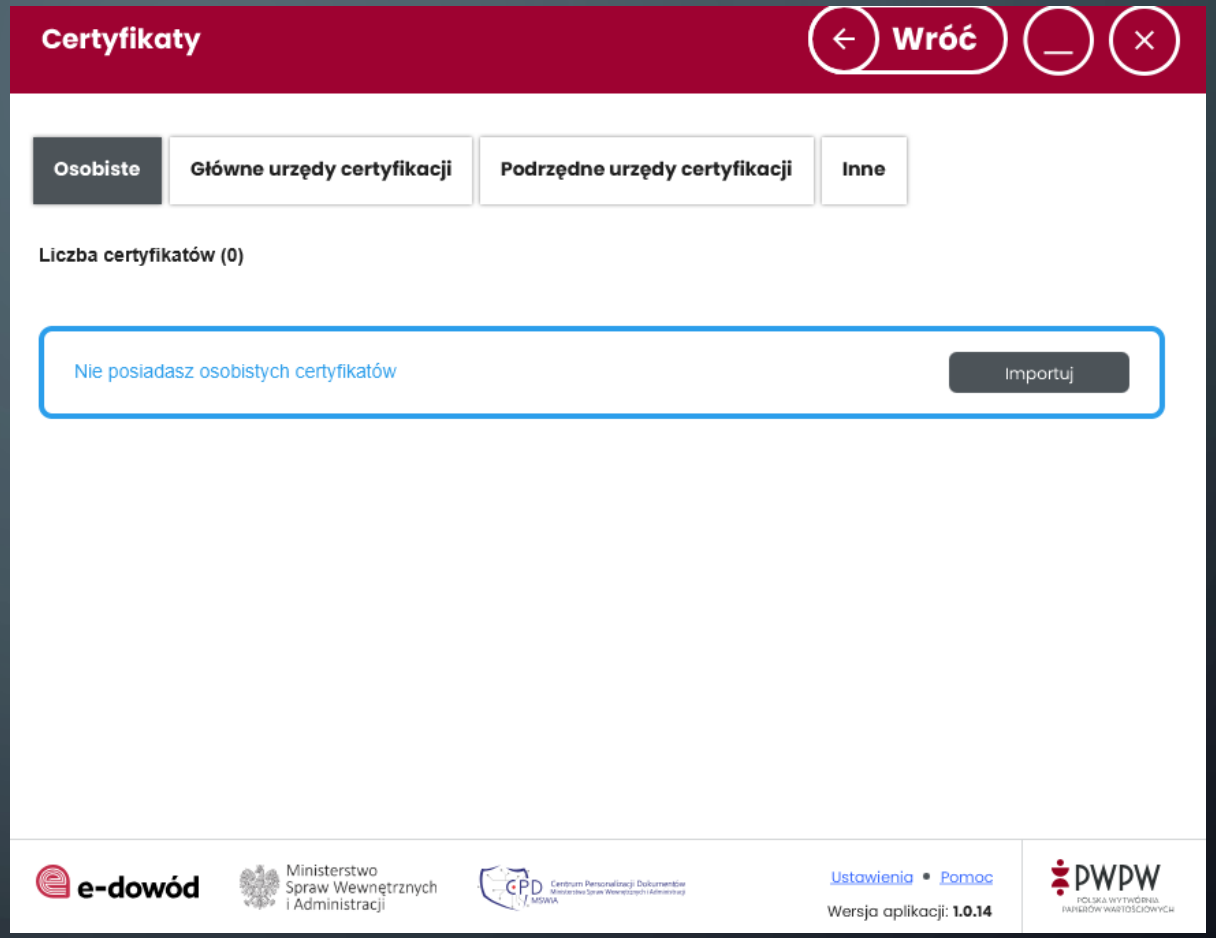
Do wyboru jest algorytm szyfrujący: AES128/3DES lub DES. Domyślnie plik szyfrowany jest kluczem publicznym właściciela e-dowodu, lecz istnieje możliwość dodawania certyfikatów odbiorcy.

Ekran odszyfrowania polega jedynie na wybraniu pliku i odpowiedniego certyfikatu (swojego lub nadawcy).



OKNO CERTYFIKATÓW

Umożliwia dodawanie certyfikatów własnych (osobistych), urzędów certyfikacji oraz w zakładce Inne certyfikatów odbiorców.



E-DOWÓD PODAJ CAN

Pozwala na rozpoczęcie komunikacji z e-dowodem. Numer CAN zabezpiecza przed nieupoważnionym połączniem bezstykowym.

Brak dostępnej instrukcji ;(

E-DOWÓD MENEDŻER

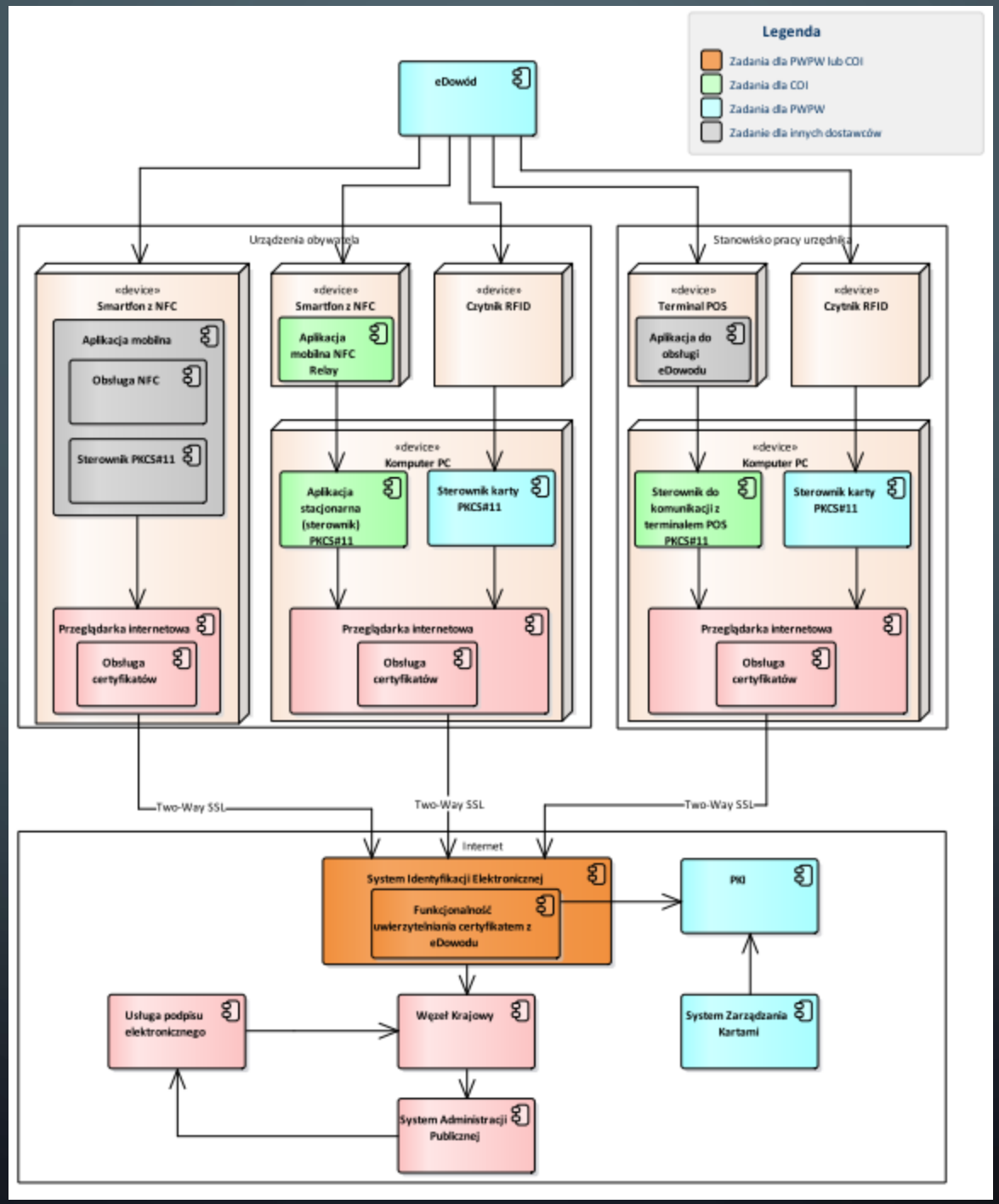
Brak dostępnej instrukcji ;(

UWAGI DO OPROGRAMOWANIA

- Według koncepcji e-dowodu miały powstać aplikacje mobilne pozwalające na komunikację zbliżeniową z kartą, lecz jeszcze nie powstały – brak informacji dlaczego, do końca 2019?
- Koncepcja NFC Relay – nie powstała, prawdopodobnie na popularne ataki hackerskie, informacja o powstaniu do końca 2019 roku,

PLAN PREZENTACJI

- Czym jest e-dowód,
- Zastosowania e-dowodów:
  - Zastosowania biznesowe,
  - Zastosowania w e-usługach,
- Przechowywane dane,
- Zabezpieczenia fizyczne i cyfrowe,
- Wymagania czytnika,
- Oprogramowanie,
- Infrastruktura aplikacji.


Legenda
Zadania dla PWPW lub COI
Zadania dla COI
Zadania dla PWPW
Zadanie dla innych dostawców
eDowód
Urządzenia obywatela
Stanowisko pracy urzędnika
«device»
Smartfon z NFC
Aplikacja mobilna
Obsługa NFC
Sterownik PKCS#11
Przeglądarka internetowa
Obsługa certyfikatów
«device»
Smartfon z NFC
Aplikacja mobilna NFC Relay
«device»
Czytnik RFID
«device»
Komputer PC
Aplikacja stacjonarna (sterownik) PKCS#11
Sterownik karty PKCS#11
Przeglądarka internetowa
Obsługa certyfikatów
«device»
Terminal POS
Aplikacja do obsługi eDowodu
«device»
Czytnik RFID
«device»
Komputer PC
Sterownik do komunikacji z terminalem POS PKCS#11
Sterownik karty PKCS#11
Przeglądarka internetowa
Obsługa certyfikatów
Two-Way SSL
Two-Way SSL
Two-Way SSL
Internet
System Identyfikacji Elektronicznej
Funkcjonalność uwierzytelniania certyfikatem z eDowodu
PKI
Usługa podpisu elektronicznego
Węzeł Krajowy
System Zarządzania Kartami
System Administracji Publicznej

DZIĘKUJE ZA UWAGĘ