



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 stacją 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_techicznych_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

The screenshot shows the 'e-dowód Podpis elektroniczny' application interface in the 'Widok Prosty' (Simple View) mode. The top navigation bar is dark red with the title 'e-dowód Podpis elektroniczny' and window control icons. Below the bar, there are two tabs: 'Prosty' (selected) and 'Rozszerzony'. The main content area contains three large white boxes, each with a red title and a right-pointing arrow button. The first box is titled 'PODPISZ PLIK' and contains the text 'Kliknij (albo przeciągnij i upuść) aby podpisać plik'. The second box is titled 'DODAJ KOLEJNY PODPIS' and contains 'Kliknij (albo przeciągnij i upuść) aby dodać kolejny podpis'. The third box is titled 'WERYFIKUJ DANE' and contains 'Kliknij (albo przeciągnij i upuść) aby zweryfikować podpisane pliki'. At the bottom, there is a footer with logos for 'e-dowód', the Ministry of Internal Affairs and Administration, CPD (Centrum Personalizacji Dokumentów), and PWPW (Polskie Wytyczne Papierów Wartościowych). It also includes links for 'Ustawienia' and 'Pomoc', and the version number 'Wersja aplikacji: 1.0.14'.

WIDOK ROZSZERZONY

The screenshot shows the 'e-dowód Podpis elektroniczny' application interface in the 'Widok Rozszerzony' (Extended View) mode. The top navigation bar is dark red with the title 'e-dowód Podpis elektroniczny' and window control icons. Below the bar, there are two tabs: 'Prosty' and 'Rozszerzony' (selected). The main content area contains seven white boxes arranged in two rows. The first row has three boxes: 'PODPISZ PLIK' (text: 'Kliknij (albo przeciągnij i upuść) aby podpisać plik'), 'DODAJ KOLEJNY PODPIS' (text: 'Kliknij (albo przeciągnij i upuść) aby dodać kolejny podpis'), and 'WERYFIKUJ DANE' (text: 'Kliknij (albo przeciągnij i upuść) aby zweryfikować podpisane pliki'). The second row has four boxes: 'ZAAWANSOWANE' (text: 'Zmodyfikuj podpis'), 'SZYFRUJ' (text: 'Zaszyfruj plik'), 'ODSZYFRUJ' (text: 'Odszyfruj plik'), and 'CERTYFIKATY' (text: 'Zarządzaj certyfikatami'). Each box contains a right-pointing arrow button. At the bottom, there is a footer with logos for 'e-dowód', the Ministry of Internal Affairs and Administration, CPD (Centrum Personalizacji Dokumentów), and PWPW (Polskie Wytyczne Papierów Wartościowych). It also includes links for 'Ustawienia' and 'Pomoc', and the version number 'Wersja aplikacji: 1.0.14'.

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.

Podpisywanie plików

[← Wróć](#) [-](#) [×](#)

Wybrane pliki

Brak wybranych plików. Przeciągnij pliki w to miejsce, bądź kliknij w odnośnik dodaj.

[Dodaj pliki](#)

Ustawienia podpisu elektronicznego

Profil

Format

Typ


Wariant


Funkcja skrótu


Typ zobowiązania

[Podpisz](#)

[Wróć](#)


 **e-dowód**

 **Ministerstwo
Spraw Wewnętrznych
i Administracji**

 **CPD** Centrum Personalizacji Dokumentów
Ministerstwa Spraw Wewnętrznych i Administracji

[Ustawienia](#) • [Pomoc](#)

Wersja aplikacji: **1.0.14**

 **PWPW**
POLSKA WYTYCZNA
PAPIERÓW WARTOŚCIOWYCH

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),

Weryfikacja podpisu elektronicznego

← **Wróć** [minus] [x]

Wybrane pliki (1)

Zaznacz wszystkie ▼ **Usuń zaznaczone** **Dodaj pliki**

dokument.BES.pdf
Status: Zweryfikowany
Rozmiar: 23 kB

przejdź pobierz usuń

Wróć **Weryfikuj**

Nazwa dokument.BES.pdf
Stan Poprawnie zweryfikowany

Podpis 1

Sygnatura Prawidłowa
Format PAdES (podpisanie plików PDF)
Typ Otoczony
Wariant BES (nie zawiera znacznika czasu)

Funkcja skrótu SHA-256

Typ zobowiązania Brak
Czas podpisu 2019-02-25 08:30:27 +0100
Status Poprawnie zweryfikowany

Certyfikat podpisu → ⓘ

Pobierz raport

e-dowód Ministerstwo Spraw Wewnętrznych i Administracji **CPD** Centrum Prasowania Dokumentów **Ustawienia** • **Pomoc** **PDPW** Powszechna Platforma Dokumentacji Wersja aplikacji: 1.0.

OPCJE ZAAWANSOWANE

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

The screenshot shows the 'Rozszerzanie podpisu elektronicznego' (Electronic Signature Extension) interface. At the top, there is a red header with the title and navigation buttons: a back arrow, 'Wróć' (Return), a minus sign, and a close 'X' button. Below the header, the main area is divided into two sections. On the left, under the heading 'Wybrane pliki' (Selected files), there is a blue-bordered box containing the text 'Brak wybranych plików. Przeciągnij pliki w to miejsce, bądź kliknij w odnośnik dodaj.' (No files selected. Drag files here, or click the add link.) and a 'Dodaj pliki' (Add files) button. On the right, there are four stacked buttons: 'Zastąp istniejący podpis nowym' (Replace existing signature with new), 'Rozszerz podpis elektroniczny' (Extend electronic signature), 'Dodaj kontrasygnatę' (Add counter-signature), and 'Dodaj znacznik czasu' (Add timestamp). At the bottom left of the main area, there is a 'Wróć' (Return) button. The footer contains logos for 'e-dowód', the Ministry of Internal Affairs and Administration, 'CPD' (Centralna Platforma Dokumentacji), 'Ustawienia • Pomoc' (Settings • Help), 'Wersja aplikacji: 1.0.' (Application version: 1.0.), and 'DWPW' (Digital Signature and Seal).

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).

The screenshot shows the 'Szyfrowanie plików' (File Encryption) screen. At the top, there is a red header with the title 'Szyfrowanie plików' and navigation buttons: a back arrow, 'Wróć' (Return), a minus sign, and a close 'X' button. The main area is divided into two sections: 'Wybrane pliki' (Selected files) and 'Ustawienia szyfrowania' (Encryption settings). The 'Wybrane pliki' section contains a blue-bordered box with the text 'Brak wybranych plików. Przeciągnij pliki w to miejsce, bądź kliknij w odnośnik dodaj.' and a 'Dodaj pliki' (Add files) button. The 'Ustawienia szyfrowania' section has a dropdown menu for 'Algorytm Szyfrowania' (Encryption algorithm) set to 'AES-128' and a 'Szyfruj' (Encrypt) button. At the bottom left, there is a 'Wróć' (Return) button. The footer contains logos for 'e-dowód', the Ministry of Internal Affairs and Administration, 'GPD' (Central Office for Register and Identification), 'Ustawienia • Pomoc' (Settings • Help), and 'Wersja aplikacji: 1.0.' (Application version: 1.0.). The PDPW logo is also present on the right.

OKNO CERTYFIKATÓW

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

The screenshot shows a mobile application interface for 'Certyfikaty'. At the top, there is a red header bar with the title 'Certyfikaty' and navigation icons: a back arrow, a 'Wróć' button, a minus sign, and a close 'X' button. Below the header, there are four tabs: 'Osobiste' (selected), 'Główne urzędy certyfikacji', 'Podrzędne urzędy certyfikacji', and 'Inne'. Under the 'Osobiste' tab, the text 'Liczba certyfikatów (0)' is displayed. A blue-bordered box contains the message 'Nie posiadasz osobistych certyfikatów' and an 'Importuj' button. The footer contains logos for 'e-dowód', the Ministry of Internal Affairs and Administration, 'CPD' (Centrum Personalizacji Dokumentów), 'Ustawienia • Pomoc', the version 'Wersja aplikacji: 1.0.14', and 'PDPW' (POLSKA WYTWÓRNIĄ PAPIERÓW WARTOŚCIOWYCH).

E-DOWÓD PODAJ CAN

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

Brak dostępnej instrukcji ;(

e-dowód Podaj CAN

CAN (Wprowadź numer CAN na klawiaturze komputera)

Zapamiętaj na tym komputerze

 **CAN (Card Access Number)** to 6-cyfrowy numer nadrukowany poziomo na dole dowodu osobistego. Numer ten jest kodem dostępu do twojego dowodu.

Dokument został wykryty w czytniku: **brak podłączonego czytnika**

   [Instrukcja](#) • [Pomoc](#)  POLSKA WYTWÓRNIA PAPIRÓW WARTOŚCIOWYCH

Wersja aplikacji: **3.0.26.543**

E-DOWÓD MENEDŻER

Brak dostępnej instrukcji ;(



The screenshot shows the 'e-dowód Menedżer' application window. The title bar is red with the text 'e-dowód Menedżer' and standard window control buttons (minimize, maximize, close). The main content area features a stylized cityscape background. In the center, there is a red 'X' icon between a document icon and a calculator icon, indicating a connection error. Below this, the text reads: 'Połączenie zerwane' and 'Umieść dowód na podłączonym czytniku'. At the bottom, there is a footer with logos and text: 'e-dowód', 'Ministerstwo Spraw Wewnętrznych i Administracji', 'CPD Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji', 'Instrukcja • Pomoc', 'Wersja aplikacji: 3.0.26.543', and 'PWPW POLSKA WYTIKARNA PRAWÓW WARTOŚCIOWYCH'.

e-dowód Menedżer

Połączenie zerwane
Umieść dowód na podłączonym czytniku

e-dowód

Ministerstwo Spraw Wewnętrznych i Administracji

CPD Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji

Instrukcja • Pomoc

Wersja aplikacji: 3.0.26.543

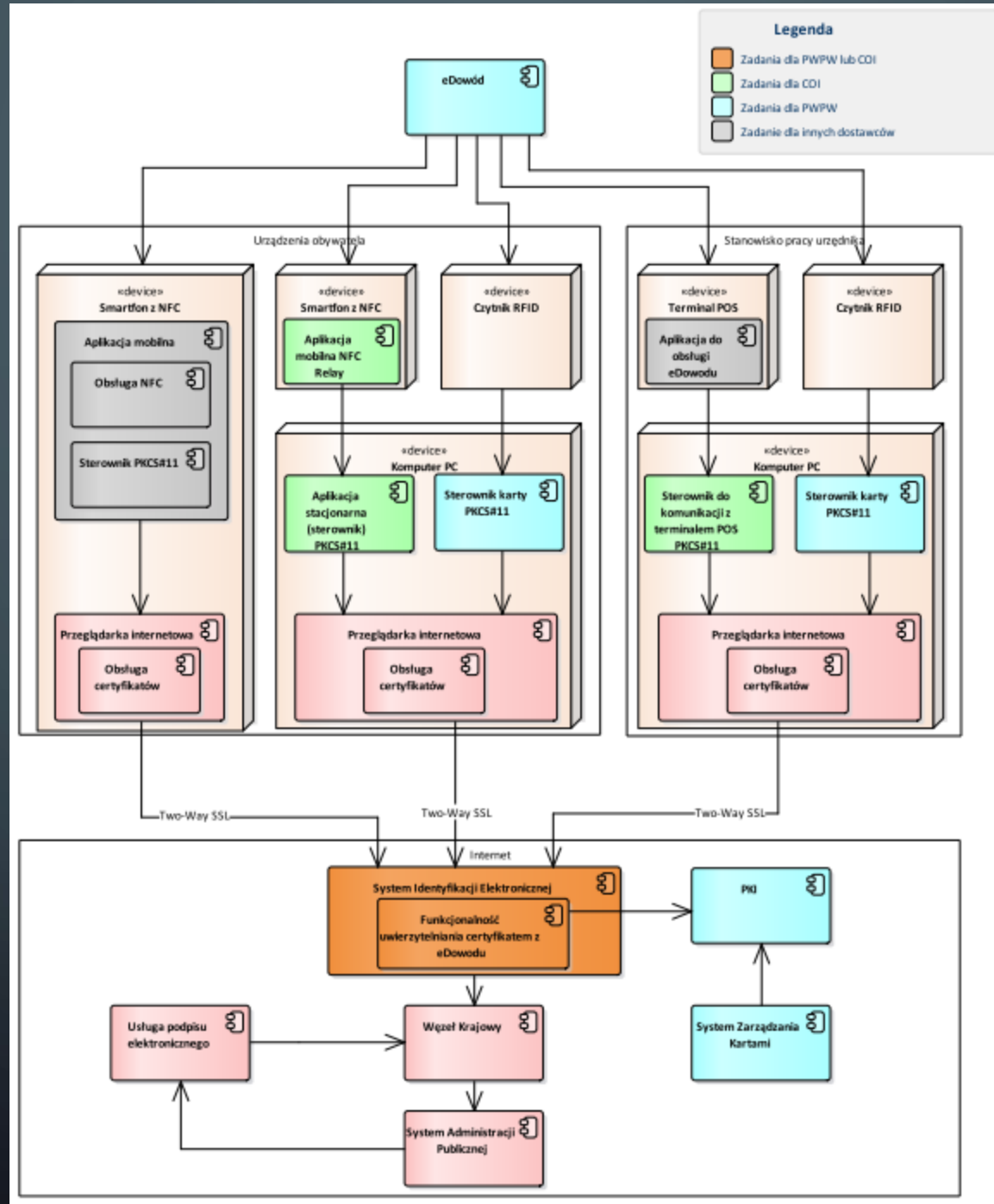
PWPW
POLSKA WYTIKARNA
PRAWÓW WARTOŚCIOWYCH

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.





DZIĘKUJE ZA UWAGĘ