mDokumenty

Anna Streżyńska

Minister Cyfryzacji
Warszawa, 05.04.2017

Główne cele projektu

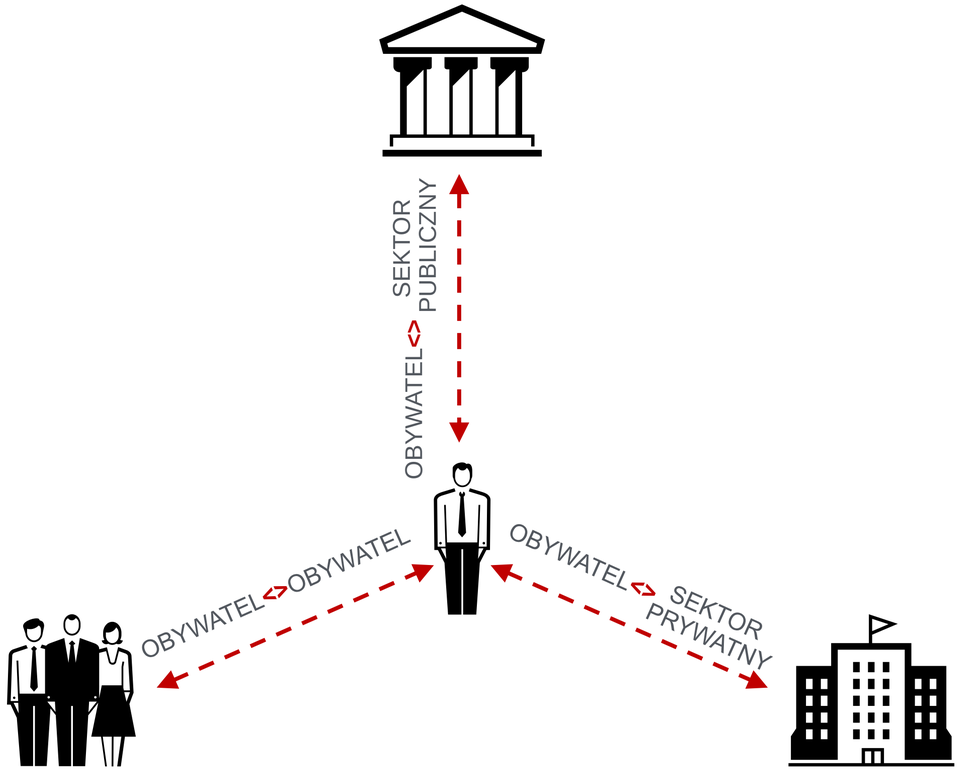
Ministerstwo Cyfryzacji

- Usługa dla obywateli
- Usługa dla administracji
- Obrót elektroniczny
- Oszczędności
- Ograniczenie ryzyk

Harmonogram i zakres etapów projektu

Wymiary działania mDokumentów

Dostępne relacje



Dostępne rodzaje dokumentów

Dokumenty z Systemu Rejestrów Państwowych

- Dowód osobisty
- Prawo jazdy
- Dowód rejestracyjny

Dokumenty z systemów dziedzinowych

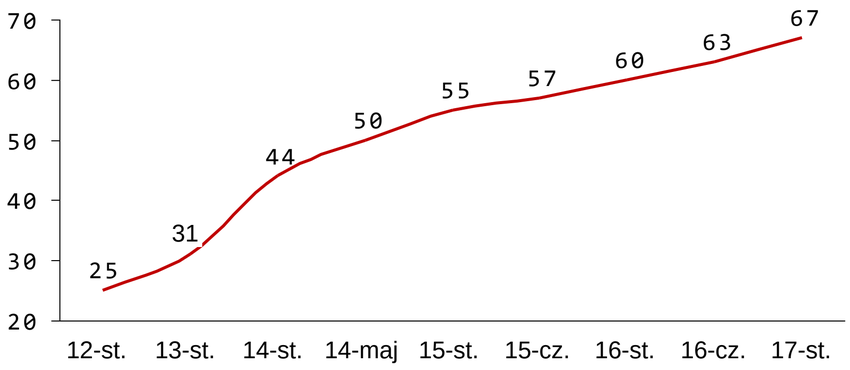
- Ubezpieczenie OC
- Legitymacja studencka
- Karta Dużej Rodziny
- Legitymacja emeryta
- Legitymacja szkolna

Dokumenty inne

- Karta miejska
- Karty lojalnościowe
- inne

Uwarunkowania technologiczne – podejście etapowe

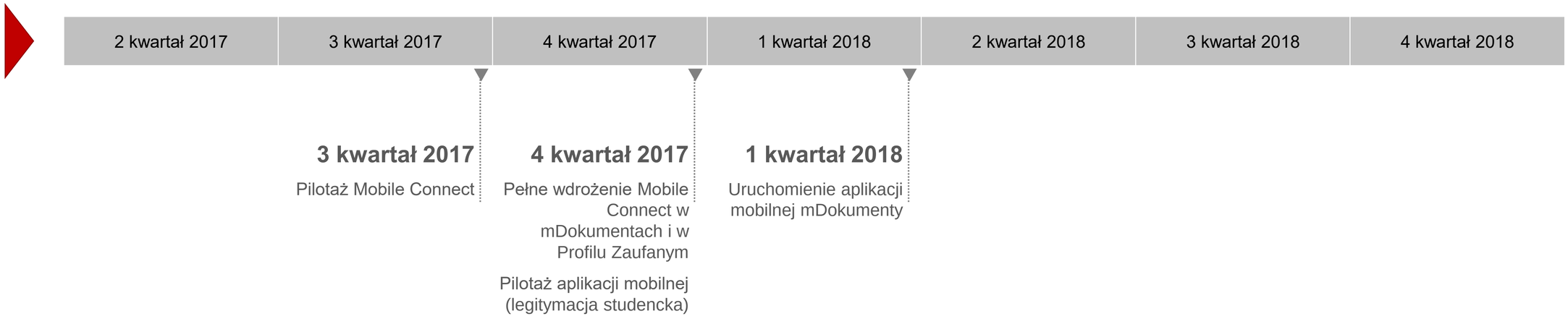
Penetracja smartfonów wśród klientów telefonii komórkowej w Polsce
[% wszystkich telefonów]



Źródło: EY

Mobile Connect	Alternatywna (tańsza niż sms) metoda uwierzytelnienia obywatela i autoryzacji jego transakcji na każdym telefonie w systemach administracji publicznej
Aplikacja na smartfon	Start od „lekkich dokumentów” - legitymacja szkolna, karta miejska – w związku z rosnącą popularyzacją smartfonów wśród klientów sieci komórkowych w Polsce

Harmonogram uruchamiania Mobile Connect i aplikacji mobilnej



Harmonogram wdrożenia projektu mDokumenty

11 maja 2017

Pilotaż usługi dla dowodu osobistego

4 kwartał 2017*

Pilotaż aplikacji mobilnej - wdrożenie usługi dla legitymacji studenckiej

1 kwartał 2018*

Uruchomienie aplikacji mobilnej
Usługa obywatel-obywatel
Legitymacja studencka
Karta miejska

3 kwartał 2018*

Wdrożenie usługi dla karty emeryta

Maj	Czerwiec	Lipiec	Sierpień	Wrzesień	4 kwartał 2017	1 kwartał 2018	2 kwartał 2018	3 kwartał 2018

Koniec lipca 2017

Pełne wdrożenie usługi dla dowodu osobistego.

4 kwartał 2017

Pełne wdrożenie usługi dla dokumentów kierowcy i pojazdu (prawo jazdy, ubezpieczenie OC, karta pojazdu, dowód rejestracyjny, badanie techniczne)

2 kwartał 2018*

Wdrożenie usługi dla karty dużej rodziny i legitymacji szkolnej

* Daty zaplanowane wstępnie

Etap 1

Główne założenia (1 z 4)

- **Bezpieczeństwo**: równie wiarygodny mechanizm prezentacji i potwierdzenia tożsamości albo posiadanych przez niego uprawnień, co tradycyjnie wykorzystywane metody okazywania dokumentów w formie papierowej i plastikowej
  - Wykorzystanie obecnych systemów dziedzinowych takich jak Źródło (SRP) czy Krajowy System Informacyjny Policji (KSIP) przez obecnych urzędników
  - Stworzenie nowej aplikacji z uwierzytelnieniem na bazie Profilu Zaufanego i wykorzystaniem dodatkowych zabezpieczeń dla pozostałych użytkowników, którzy nie posiadających dzisiaj uprawnień do systemów dziedzinowych

- **Opcjonalność**: nie zastępuje tradycyjnego dowodu osobistego czy innych dokumentów, lecz wprowadza nową, opcjonalną i dodatkową możliwość potwierdzania tożsamości i uprawnień Obywatela. Tym samym obowiązujące regulacje w tym zakresie zostaną jedynie uzupełnione o nowy, opcjonalny sposób potwierdzenia tożsamości, z wykorzystaniem mDokumentu

Główne założenia (2 z 4)

- **Funkcjonowanie obecnych procedur i uprawnień**: rozwiązanie nie ingeruje w obecne uprawnienia służb w zakresie legitymowania osób i potwierdzania przez ich tożsamości oraz nie zmienia stanu prawnego w tym zakresie

- **Prostota użycia**: proste i pewne oraz powszechnie stosowane mechanizmy jak SMS (jednorazowy kod) czy Profil Zaufany (rejestracja i logowanie strony weryfikującej)

- **Dopasowanie do strony weryfikującej**: Przewiduje się np. brak wykorzystania mechanizmów autoryzacyjnych (np. SMS) w kontaktach operacyjnych służb, w tym Policji

- **Etapowość**: Dowód Osobisty – II kw. 2017, IV 2017 - Ubezpieczenie Pojazdu / Dowód Rejestracyjny / Prawo Jazdy, 2018 – sektor prywatny oraz relacje obywatel do obywatela; kolejne dokumenty: np. legitymacja studencka

Główne założenia (3 z 4)

- **Finansowanie**: finansowanie z budżetu Ministerstwa Cyfryzacji (etap 1)

- **Re-użycie**: możliwość wykorzystania uprawnień i urządzeń dostępowych znajdujących się na stanie urzędów i instytucji dzięki minimalnym wymaganiom sprzętowym
  - Wykorzystanie obecnych systemów dziedzinowych (np. Źródło, CEPIK, KSIP) dla sieci zamkniętych
  - Wykorzystanie aplikacji internetowej wykorzystującej Profil Zaufany, a aktywacja usługi przez Obywatela na obywatel.gov.pl
  - Wnioskowanie o dostęp dla Instytucji czy Urzędnika w analogii do uzyskiwania dostępów i uprawnień na ePUAP lub CEIDG

- **Promowanie jednej metody logowania - Profil Zaufany**: w przypadku braku dostępu do systemu dziedzinowego (KSIP, Źródło, CEPIK) Strona Weryfikująca tworzy konto w panelu administracyjnym i uwierzytelnia się z użyciem Profilu Zaufanego

Główne założenia (4 z 4)

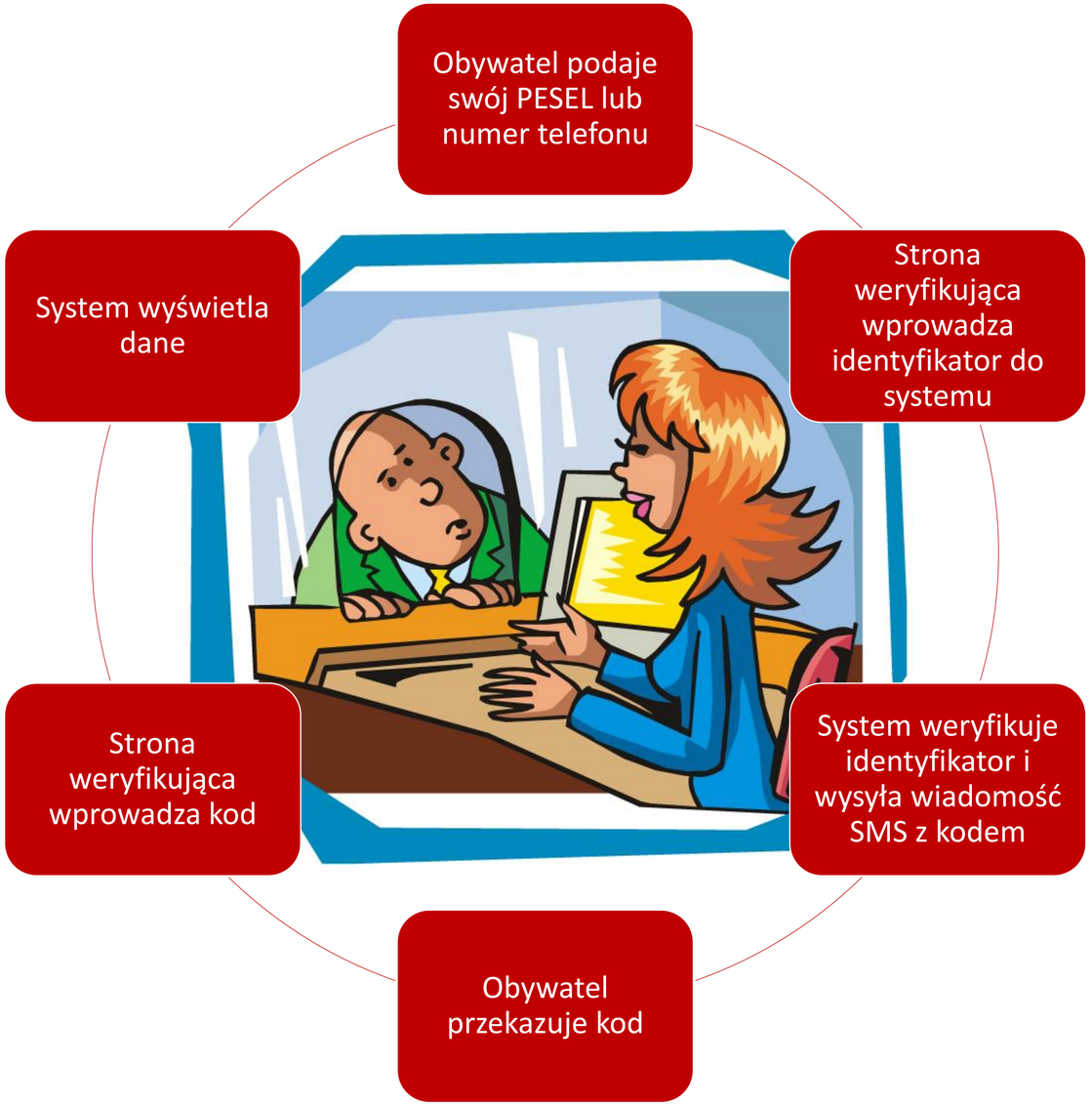
- **Brak przechowywania danych**: Nie przewiduje się przechowywania danych na urządzeniu dostępowym, więc nie zwiększa ryzyka masowej utraty danych. Kontrola fizyczna nad urządzeniem podczas realizacji czynności przez użytkownika w kontekście konkretnego obywatela będzie ograniczać przed dostępem osób niepowołanych

- **System działa na terenie kraju**: System nie będzie ograniczał prawa cudzoziemców do korzystania z posiadanych przez nich dokumentów wydanych przez organy innego państwa na terenie RP. Podobnie obywatele RP będą normalnie posługiwać się swoimi dokumentami poza granicami RP. System będzie funkcjonował jedynie na terenie kraju.

- **mDokument nie jest osobnym zbiorem danych osobowych**: umożliwia wyświetlenie w bezpieczny sposób danych z rejestrów państwowych dotyczących osoby lub rzeczy na wniosek strony weryfikującej

Proces weryfikacji

Proces weryfikacji (aplikacja internetowa z Profilem Zaufanym)



Uproszczony proces weryfikacji (np. system Policji)

Obywatel podaje swój PESEL lub numer telefonu

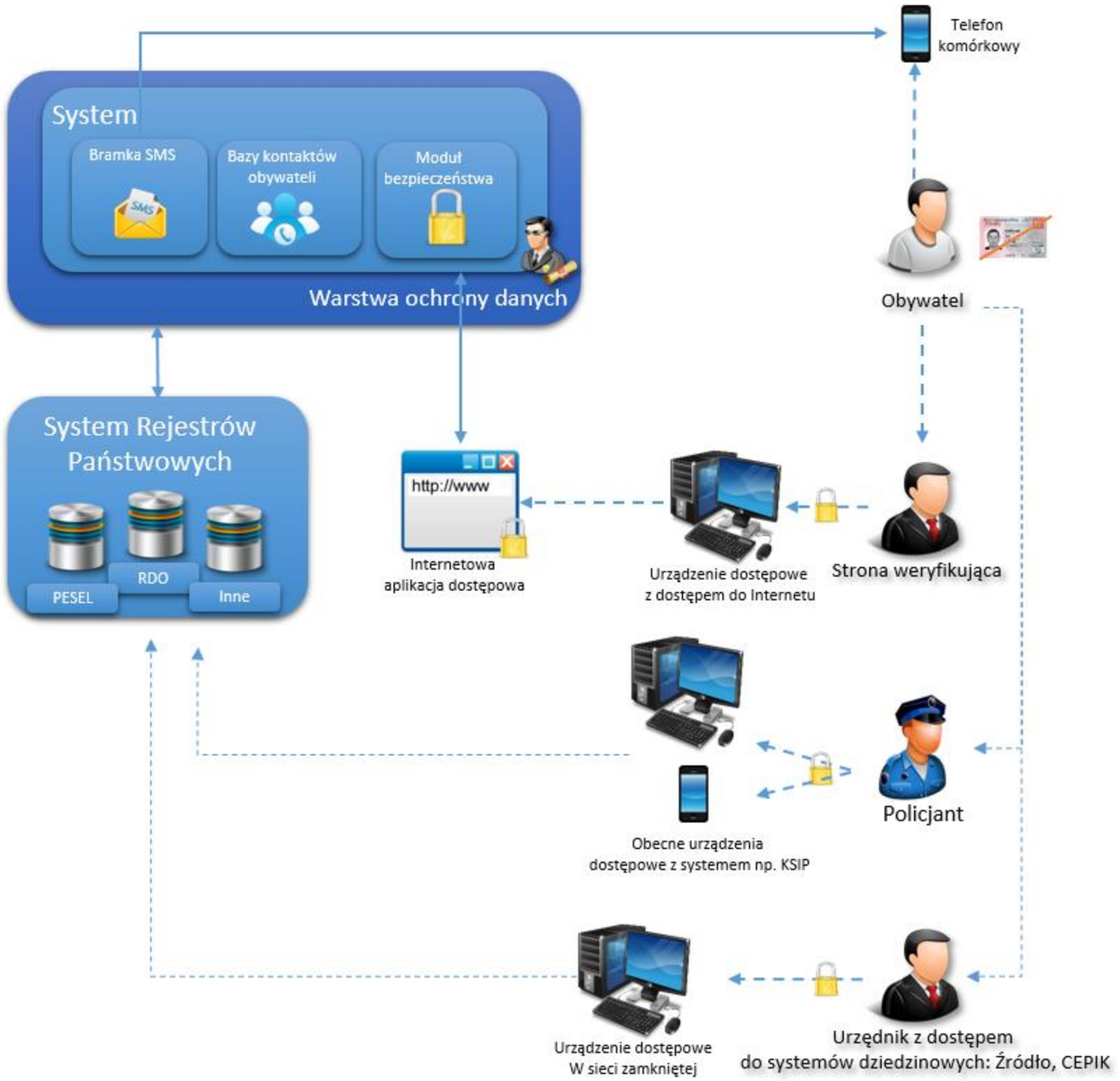
Policjant wprowadza identyfikator do systemu

System weryfikuje identyfikator

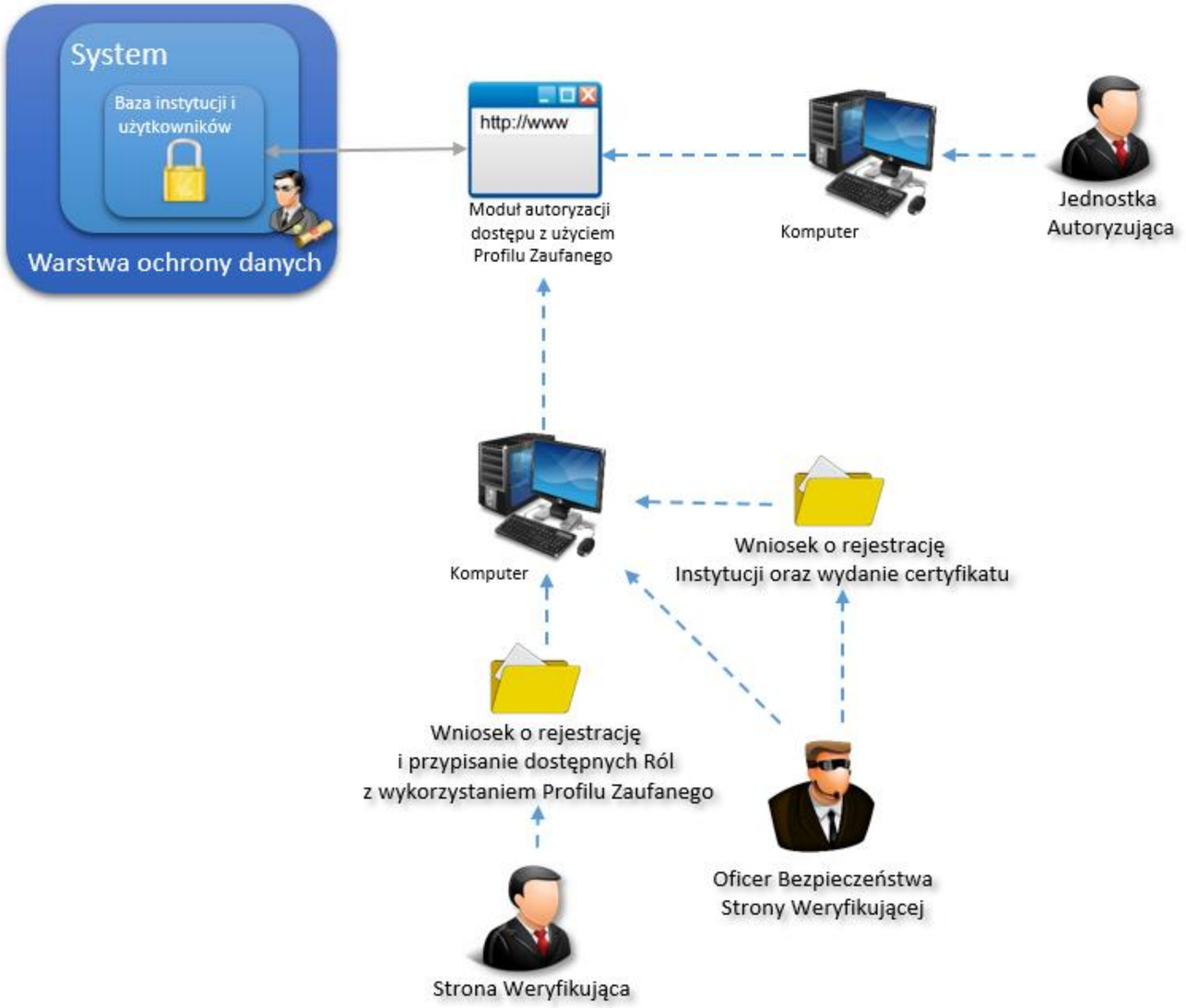
System wyświetla dane

Wizja architektury – etap 1

Prezentacja wizji architektury



Wizja architektury systemu autoryzacji



Założenia bezpieczeństwa

Założenia bezpieczeństwa (1 z 2)

- Obywatel musi aktywować sobie usługę mDokumenty na portalu obywatel.gov.pl
- Urzędnik , który ma dostęp do systemu dziedzinowego (np. CEPIK, Źródło, KSIP) uzyskuje dostęp do danych dokumentów obywatela przy zastosowaniu obecnie używanego certyfikatu dedykowanego dla systemu dziedzinowego i wydanych w nim uprawnień
- Urzędnik , który nie ma dostępu do systemu dziedzinowego uzyskuje dostęp do danych dokumentu po zalogowaniu się do aplikacji mDokumenty za pomocą swojego Profilu Zaufanego
- Strona Weryfikująca (np. patrol Policji) korzysta z Mobilnego Urządzenia (np. Mobilny Terminal Noszony)
- Mobilne Urządzenie działa na dedykowanym punkcie APN w sieci pakietowej operatora komórkowego obsługującego Stronę Weryfikującą (np. Policję)
- Dostęp urzędnika do danych dokumentu każdorazowo będzie wymagał autoryzacji obywatela przez podanie przez niego urzędnikowi jednorazowego kodu przesłanego w SMS na numer telefonu obywatela (nie dotyczy służb)

Założenia bezpieczeństwa (2 z 2)

- Procedury bezpieczeństwa i oficerowie bezpieczeństwa (Lokalny Administrator Systemu)
- Liczba prób (udanych lub nieudanych) pobrania danych dokumentów obywatela będzie limitowana w ciągu dnia, po jej przekroczeniu konto urzędnika zostanie zablokowane
- Połączenie z SRP.NET lub poprzez szyfrowane połączenie z internetem (dla aplikacji dostępowej)
- Preferowane wykorzystanie systemu Mobile Device Management (zarządzania uprawnieniami i aplikacjami na urządzeniu mobilnym z systemem dziedzinowym)
- Wykorzystanie SMS jako narzędzia zapasowego do bezpłatnego Mobile Connect
- Mapowanie ryzyk i mitygacja (m.in. na bazie doświadczenia z SRP)

Ministerstwo Cyfryzacji