# Model podpisu elektronicznego - wyzwania i szanse

**Prof. dr hab. Mirosław Kutyłowski**

**Wydział Informatyki Technicznej i Telekomunikacji,**

**Politechnika Wrocławska**

# Ewolucja

## Sytuacja 20 lat temu:

- **offline,**
- **karta kryptograficzna jako (jedyny) token umożliwiający złożenie podpisu**

## Sytuacja 2021:

- **dostępność online (nawet bez 5G)**
- **wiele urządzeń w rękach użytkownika**
- **olbrzymi wolumen operacji online**
- **dostępność dodatkowych usług zaufania**
- **rekomendacje epidemiologiczne**

# Ewolucja

## Sytuacja 20 lat temu:

- **podpis kwalifikowany jako Święty Graal**

## Sytuacja 2021:

- **podpis kwalifikowany wciąż traktowany jako Święty Graal**
- **używany głównie tam gdzie istnieje obowiązek prawny**

- **Ale … suwerenność danych i przesunięcie punktu ciężkości na podmiot danych wbrew architekturze X.509**

# Pieczęć elektroniczna

**luźne wymagania eIDAS: mutatis mutandis z odniesieniem do podpisów elektronicznych**

**Ze względu na skalę zagrożeń możemy potrzebować więcej:**

1. **kompletność zbioru wystawionych pieczęci elektronicznych (np. pozostawienie śladu po usuniętych fakturach, fałszowaniu doumentacji medycznej, …)**
2. **niezaprzeczalności sklonowania kluczy,**
3. **…**

# Podpis elektroniczny a pieczęć elektroniczna

- **Naturalnym głównym obszarem zastosowań podpisu cyfrowego jest pieczęć elektroniczna dla operacji masowych.**

- **Np: faktura, dokument bankowy, tytuł egzekucyjny, świadectwo uprawnień zawodowych, …**

- **Poziom zastosowania:  prawie zerowy, brak obowiązków prawnych**

# Konwersja postaci dokumentu

**Dokument elektroniczny powinien być transferowalny do wersji papierowej i vice versa z zachowaniem najważniejszych gwarancji dawanych przez różne formy podpisów**

**Motywacje:**

1. **okres trwałości dokumentu (+papier)**
2. **zaufanie osoby fizycznej (ślad papierowy w segregatorze) (+papier)**
3. **wykluczenie cyfrowe (+papier)**
4. **bezpieczeństwo epidemiologiczne (+elektronicznie)**
5. **koszt, efektywność obrotu (+elektronicznie)**

# Konwersja postaci dokumentu – jako usługa zaufania

- analogicznie np. do tradycji niemieckiej, osoby zaufania społecznego (nie tylko notariusze) pełniący funkcje potwierdzania konwertowanych dokumentów
- drukowana wersja podpisu elektronicznego (QR code) z najważniejszymi danymi
- distributed ledger do rejestrowania

# SSCD – dostępność

- **SSCD traktowany jako bariera do rozpowszechniania się podpisu elektronicznego**
- **nowy eIDAS ma zapewnić uniwersalne narządzie w postaci European Identity Wallet**
- **doświadczenie niemieckie z nPA:**
  - **podobna motywacja i nadzieje**
  - **nieznaczne zainteresowanie obywateli – bo koszt certyfikatów i tak pozostał zniechęcający**
- **“Podpis serwerowy”: kompromis wygody i bezpieczeństwa kosztem zdemontowania bezpieczeństwa**

# Lekcja estońska

**(wadliwa procedura generowania kluczy RSA)**

1. **Certyfikaty CC nie uchronią przed kompromitacją urządzeń SSCD**
2. **Urządzenie typu *czarnej skrzynki* trzeba jakoś monitorować**
3. **Efektywne rozwiązanie może być zaimplementowane na najwyższej warstwie systemu z podziałem odpowiedzialności na różne komponenty**

# Lekcja estońska

**Rozwiązanie:**

1. **Generowanie kluczy rozproszone pomiędzy serwer a urządzenie obywatela:** ani serwer ani urządzenie nie ma pełnego wpływu na tworzone klucze i zna tylko ich część
2. **Podpis z mediatorem:** łatwość zawieszenia, zablokowania w przypadku podejrzenia fraudu
3. **Linkowanie:** mechanizm wykrywania klonów urządzenia

**Wszystko dla podpisów RSA, które w istocie nie są podpisami RSA (moduł *n* ma 4 czynniki pierwsze)**

**(dla podpisów opartych na DLP byłoby to łatwiejsze)**

# Sole control

- **iluzja ochrony przez PIN**
- **fizyczna kontrola and SSCD – brak śladów użycia (lunch break attack)**
- **informacja zwrotna o wykonaniu podpisu możliwa jedynie w przypadku systemów z mediatorem**

**Estonia wdrożyła rozwiązanie umożliwiające pewnien niezależny zakres kontroli.**

# Dane do składania podpisu elektronicznego

*„dane służące do składania podpisu elektronicznego” oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego*

**Definicja wadliwa pod względem technicznym:**

1. **unikalność rozumiana jako cecha zabezpieczająca przed złożeniem podpisu przez osoby trzecie. Tak nie jest:**
   - **np dla klucza publicznego RSA istnieje więcej niż 1 odpowiadający mu klucz prywatny**

# Dane do składania podpisu elektronicznego

*„dane służące do składania podpisu elektronicznego” oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego*

**Definicja wadliwa pod względem technicznym:**

2. **pod definicję podpadają losowe klucze efemeryczne (np z ECDSA)**

3. **random padding - też (już wbrew sensowi technicznemu)**

# Dane do składania podpisu elektronicznego

***„dane służące do składania podpisu elektronicznego” oznaczają unikalne dane, których podpisujący używa do składania podpisu elektronicznego***

**Naprawdę chodzi o dane WARUNKUJĄCE MOŻLIWOŚĆ ZŁOŻENIA PODPISU**

# Podpis zaawansowany a kwalifikowany

- **Podpis kwalifikowany traktowany jako najwyższa postać podpisu zaawansowanego.**
- **Tymczasem jest to postać bazowa pod względem bezpieczeństwa ale o największych skutkach prawnych.**

# Podpis zaawansowany a kwalifikowany

***Zaawansowany podpis elektroniczny musi spełniać następujące wymogi:***

***a) jest unikalnie przyporządkowany podpisującemu;***

***b) umożliwia ustalenie tożsamości podpisującego;***

***c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą; oraz***

***d) jest powiązany z danymi podpisanymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.***

# Podpis zaawansowany a kwalifikowany

*„kwalifikowany podpis elektroniczny” oznacza*

*zaawansowany podpis elektroniczny,*

*który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego*

*i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego;*

**Brzmi to jak podpis zaawansowany z dwoma dodatkowymi wymaganiami**

**w istocie warunki te są (bazowym) sposobem na realizację wymagań wobec podpisu zaawansowanego**

# Podpis zaawansowany a kwalifikowany

***“opiera się na kwalifikowanym certyfikacie podpisu elektronicznego”,***
**Głównie sposób realizacji dla:**

***a) jest unikalnie przyporządkowany podpisującemu;***

***b) umożliwia ustalenie tożsamości podpisującego;***

**(związek klucza publicznego I prywatnego  z osobą fizyczną atestowany przez CA)**

# Podpis zaawansowany a kwalifikowany

***“składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego”***

**Głównie sposób realizacji dla:**

***c) jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą***

**(ochrona klucza prywatnego poprzez kwalifikowane urządzenie SSCD – certyfikowane urządzenie o minimalnych cechach zapewniających te własności)**

# Podpis zaawansowany - perspektywy

**Usunięcie “single-point-of-failure” – np. tożsamość certyfikowana u źródła danych a nie przez pośrednika na podstawie dokumentu tożsamości**

**Sekwencja czasowa i ślady cyfrowe – np. w distributed ledger czy choćby w niemanipulowalnym archiwum**

**Kontrola użycia – wsparcie zabezpieczenia obrotu dokumentów z rozliczalnością**

# Podpis zaawansowany - perspektywy

**Rejestry – w KRS jest adres pocztowy podmiotu,**

**zaś potrzebny jest**

**klucz publiczny do weryfikacji pieczęci elektronicznej podmiotu**

**i/lub certyfikat dla osoby reprezentującej**

# Podpis a RODO

Zaawansowany podpis elektroniczny to dane osobowe:

***„dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować,***

**zaawansowany podpis odpowiada możliwemu do zidentyfikowania podpisującemu – więc podpis to dane osobowe**

# Podpis a RODO

Walidacja to przetwarzanie danych osobowych:

***„walidacja” oznacza proces weryfikacji i potwierdzenia ważności podpisu elektronicznego lub pieczęci.***

**Nawet przy zachowawczej interpretacji przetwarzania danych osobowych:**

**walidacja jest przetwarzaniem danych osobowych –**

**bo tworzone są dodatkowe dane osobowe “podpis X jest ważny”**

# Uprawnienia do przeprowadzenia walidacji

- **Dostęp do podpisu nie oznacza zgody na przeprowadzenie walidacji czy innej formy przetwarzania.**

- **Walidacja legalna, gdy istnieje:**
  - **interes prawny**
  - **obowiązek prawny**
  - **zgoda podpisującego**
  - **…**

- **Zgoda nie może być domyślna**

# Uprawnienia do przeprowadzenia walidacji

**Pragmatyczne rozwiązania:**

**opcja 1: zgoda na przetwarzanie zaszyta w formacie podpisu**

**opcja 2: validation token – rozwiązanie techniczne kontrolujące możliwość walidacji**

# Uprawnienia do przeprowadzenia walidacji

**Pragmatyczne rozwiązania:**

**opcja 1: zgoda na przetwarzanie zaszyta w formacie podpisu**

**opcja 2: validation token – rozwiązanie techniczne kontrolujące możliwość walidacji**

**opcja 3: wywołania procedur walidacji poprzez podpisującego**

# Validation token - przykład 1: designated verifier

**Podpis wiadomości *M* przeznaczonej dla osoby z kluczem publicznym *P*:**

- ***d* = opis praw do użycia podpisu wskazujący na posiadacza klucza *P***
- ***c:= $Enc_P(x)$ dla losowego x***
- ***w schemacie DSA: zamiast e:=Hash(M,r) mamy***
  ***e:= Hash(M,r,d,x)***
- ***podpis dla M zawiera oprócz standardowych składników również***
  ***d,c***

# Validation token - przykład 1: designated verifier

***Weryfikacja podpisu wymaga***

- **odzyskania *x* poprzez deszyfrowanie *c* i obliczenia *Hash(M,r,d,c,x)***

- ***nie da się sprawdzić prawidłowości hasza bez użycia argumentów, tj. między innymi***

***c oraz x***

# Validation token  - przykład 1: designated verifier

***Wskazana osoba może przekazać d oraz x osobom trzecim umożliwiając przeprowadzenie testu podpisu ale:***

- ***pozostawia  ślad,  że odszyfrowała c i zdradziła x osobie trzeciej***

***Z kolei osoba trzecia***

- ***nie może twierdzić, że nie była świadoma braku uprawnień***

# Validation token  - przykład 2: wskazywanie uprawnionych osób wg potrzeby

*Można przekształcić standardowy podpis poprzez dodatkowe metadane, tak aby*

*podpisujący mógł tworzyć dowolną liczbę różnych tokenów dla różnych odbiorców*

# Skany podpisów – pułapka RODO

***„dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;***

**Podpis na dokumencie papierowym – to nie są “dane biometryczne”**

**Skan tego dokumentu – to są “dane biometryczne” (RODO!)**

**Podpis zaawansowany – to nie są “dane biometryczne”**

# Dziękuję za uwagę