Instytut Autostrada Technologii i Innowacji

Cybersecurity Academy, 30.06.2016

EIDAS i techniczne perspektywy identyfikacji elektronicznej

Prof. Mirosław Kutyłowski
Katedra Informatyki, WPPT

www.iati.pl

1 lipca 2016

- Wejście w życie Regulacji eIDAS:
- obowiązki w zakresie obsługiwania systemów zagranicznych
- obowiązki w zakresie własnych systemów i ochrony interesów obywateli

Sytuacja w obrocie elektronicznym

- rozpad systemu zaufania opartego na tradycyjnych metodach
- rosnąca mobilność
- zagrożenia dla systemu finansowego w Polsce wg banków:
- 1) cybersecurity
- 2) ...

Ataki

- sfałszowane dokumenty papierowe
  - faktury z prawie prawdziwą treścią
  - wrogie przejęcie z wykorzystaniem KRS
  - przejmownie własności nieruchomości (czynności u notariusza)
  - ...
- filozofia ataku:
  idealne podrobienie jest niemożliwe, ale liczy się krótkookresowy efekt i nieodwracalne efekty zwykłej weryfikacji

Dokument dualny

TEZA:

Obrót powinien być oparty o dokumenty, które można REPREZENTOWAĆ

- w postaci elektronicznej

  oraz

- w postaci fizycznego wydruku

Element spinający różne reprezentacje: pieczęć elektroniczna

Dokument dualny

Pieczęć elektroniczna (electornic seal):

- kryptografia: podpis cyfrowy
- hardware: (dość) bezpieczne urządzenie
- reprezentacja: ciąg cyfr, może być drukowany za pomocą kodu dwuwymiarowego

Dokument dualny

Zalety

- weryfikacja telefonem, skanerem ...
- masowe przetwarzanie
- niezależność od innych technik, np.. druków ścisłego zarachowania

Dokument dualny

Wady

- liczba danych „wciąganych” do podpisu jest ograniczona
- brak europejskiej standaryzacji
- jak każdy podpis elektorniczny umożliwia niekontrolowane rozpowszechnianie „oryginałów”

Dokument dulany – pola zastosowań

- Zaświadczenia (bezpieczniejsze w praktyce niż papierowe oryginały)
- Wydruki dokumentów bankowych
- Faktury
- Istotne pisma (np. informacja o zmianie konta bankowego firmy)

Dokument dualny – wyzwania

- standaryzacja
- urządzenia do generowania dokumentów
- oprogramowanie do weryfikacji

Szansa rynkowa w Polsce:

- liczba fraudów
- relatywnie dobrze zorganizowany system bankowy
- opóźnienia w administracji publicznej

Dokument dualny – co mamy

Prototyp, Piotr Lipiak, student Pwr:

generator dokumentów

- pola krytyczne
- pola niekrytyczne
- reprezentacja graficzna pól krytycznych
- Generowanie pieczęci cyfrowej w postaci kodu 2D

Samorozpakowujący się system:

- skonfigurowany system
- plug-and-play na dedykowanej maszynie
- np: Raspberry Pi w skrzynce na klucz

„Dowód osobisty na smartfonie”

Ministerstwo Cyfryzacji

Jaka koncepcja?

- „linki” na telefonie
- weryfikacja online w rejestrach (np.. CEPIK, PESEL,...)

„Dowód osobisty na smartfonie”

Zalety

- aktualna informacja o statusie
- nośnik nie musi być bezpieczny
- racjonalizacja – np. brak obowiązku noszenia prawa jazdy

„Dowód osobisty na smartfonie”

Wady:

- kolejna prowizorka (tak jak Zaufany Profil)
- wyłącznie pasywna rola – brak możliwości użycia do zdalnego uwierzytelniania
- niewielka wartość dodana (np. Policja i tak sprawdza online prawo jazdy w CEPIK)
- otwarcie drogi dla nielegalnego obrotu danymi osobowymi

Symulowalność – techniczna ochrony danych osobowych

ZASADA:

powinno unikać się generowania danych elektornicznych, które mogą być weryfikowane w sposób niekontrolowany

PRZYKŁAD:
dane takie jak wizerunek właściciela dokumentu przekazywane niepodpisane ale poprzez bezpieczny i uwierzytelniony kanał ustanowiony z chipem z dokumentu tożsamości

Dokument tożsamości w PL – stan na dziś

- solidny paszport biometryczny
- dowód osobisty zabezpieczony wyłącznie graficznie – z możliwością fałszerstw (przeróbki treści)

Dokument tożsamości w PL – potrzeby minimalne

- warstwa elektroniczna na poziomie paszportu biometrycznego

- np. zastosowanie najnowszej wersji standardu ICAO:

  - zabezpieczenie hasłem (PACE)
  - silne uwierzytelnienie dokumentu i jego treści (CAM)
  - sprawdzenie uprawnień terminala (TA)

Koncepcja eID

Identity based dla bezpiecznej komunikacji:

- dokument cyfrowy dla Alicji szyfrujemy jej PESELem, dla firmy jej NIPem, dla isntytucji jej REGONem
- deszyfrowanie kluczem prywatnym odbiorcy

Identity based

- Zaleta: wystarczy wiedzieć KOMU wysyłam
- Zaleta: szczelna implementacja zasady ochrony danych osobowych, poufności korespondencji, przetwarzania w chmurze
- Wady: jak to zrobić?

Identity based

Realizacja (analiza Marty Mularczyk, studentka Pwr)

- mRSA (Tsudik i inni):
  – wspólny moduł RSA dla wszystkich użytkowników
  – Key Generation Center
  – klucz szyfrujący za pomocą funkcji haszującej
  – klucz deszyfrujący dzielony pomiędzy użytkownika i serwer (np.. EPUAP, KIR,...)

Identity based

Zalety

- możliwość częstego odświeżania kluczy deszyfrujących u użytkownika
- możliwość współpracy z wieloma serwerami

Techniczne subtelności:
atak multyplikatywny: kłopot gdy e dzieli e1*e2

Scenariusz

(Krzysztof Kozłowski, student PWr)

1) Klient łączy się ze stroną banku

2) na stronie wyświetla się kod autoryzacyjny 2D – kryptogram mRSA za pomocą ID based

3) telefon klienta odszyfrowuje kod (kamera telefonu obserwuje ekran!)

4) klient wprowadza kod, który widzi na ekranie telefonu

E-IDAS token

- specyfikacja niemiecka, sygnowana również przez francuski urząd
- silne oparcie o Pseudonymous Signature

wersja protokołu uwierzytelniania Okamoto

Pseudonymous Signature

Zalety:

- brak konieczności certyfikatów

- Anonimizacja: do każdego sektora inna tożsamość (możliwe zastosowania do wireless authentication i klasycznego podpisywania dokumentów)

Pseudonymous Signature

Wady:

- wystawca zna klucze prywatne obywatela
- Możliwość tworzenia tokenów do pełnej deanonimizacji – wymiana między „służbami”
- Złamanie 2 tokenów daje możliwość kreowania nowych użytkowników

Pseudonymous Signature

Rozwiązania (ACISP 2016):

- ~~wystawca zna klucze prywatne obywatela~~
- ~~Możliwość tworzenia tokenów do pełnej deanonimizacji – wymiana między „służbami”~~
- Złamanie 2 tokenów daje możliwość kreowania nowych użytkowników – pozostaje problemem

(ciężkie rozwiązania: whitelists, certyfikaty, certificate of health,...)

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

e-IDAS

-

Instytut Autostrada Technologii i Innowacji

Dziękuję za uwagę

www.iati.pl

Dokument tożsamości w PL – stan na dziś

- solidny paszport biometryczny
- dowód osobisty zabezpieczony wyłącznie graficznie – z możliwością fałszerstw (przeróbki treści)