Weryfikacja podpisu elektronicznego – jak to robić poprawnie

dr inż. Jacek Pokraśniewicz

ENIGMA Systemy Ochrony Informacji Sp. z o.o.

Plan prezentacji

- Co to jest podpis - przypomnienie
- Podpis „zwykły” a podpis „bezpieczny”
- Jak zweryfikować *bezpieczny* podpis elektroniczny
- Kiedy *bezpieczny* podpis jest ważny – archiwalna forma podpisu, konserwacja podpisów
- Propozycja serwera weryfikacji podpisów

Podpis

Dokument

Niniejszym przekazuję 10 zł na zbożny cel

Podpis Jana Kowalskiego

89473CB91E79134E82743

Podpis Stanisława Nowaka

309488E2438700C41234D

Dokument

Niniejszym przekazuję 100 zł na zbożny cel

Podpis Jana Kowalskiego

A2CB7939E9173BC80134

Podpis Stanisława Nowaka

7B02419348253948B8093

- Podpis jest składany przy użyciu klucza prywatnego (karty elektronicznej zawierającej klucz prywatny)
- Podpis jest weryfikowany przy użyciu wskazanego w nim certyfikatu; certyfikat zawiera dane osoby, która złożyła podpis (np. imię, nazwisko, adres, PESEL)
- Dany podpis „pasuje” tylko do jednego, konkretnego dokumentu i do jednego klucza, którym został złożony
  - podpis może być przesyłany i składowany niezależnie od dokumentu

Podpis „zwykły”

- Znany od wielu lat, stosowany w Polsce co najmniej od początku lat 90. (pionierskie działania ENIGMA SOI)
- Główna funkcja – **silne uwierzytelnienie**
  - odbiorca wie, że wiadomość (dokument) nie została sfałszowana, ale nie ma możliwości udowodnienia tego w sądzie
- W niektórych systemach – **niezaprzeczalność** (możliwość prowadzenia dowodu), na podstawie szczegółowych umów pomiędzy stronami określających zasady odpowiedzialności

Bezpieczny podpis elektroniczny

- Wprowadzony ustawą z dnia 18 IX 2001 r.
- Zapewnia niezaprzeczalność
- Technologicznie, na niskim poziomie, realizowany tak jak podpis zwykły
  - te same operacje matematyczne co przy podpisie zwykłym
- Istotne różnice w interpretacji

Podpis *zwykły* a podpis *bezpieczny*

- Podpis zwykły - uwierzytelnienie lub niezaprzeczalność w zamkniętych systemach
  - zamknięte środowisko, małe prawdopodobieństwo celowych nadużyć
- Podpis *bezpieczny* – niezaprzeczalność jako usługa publiczna
  - znaczące prawdopodobieństwo celowych nadużyć
  - konieczność precyzyjnego określenia w przepisach, kiedy podpis ma wartość dowodową i zakresu odpowiedzialności podmiotów w przypadkach brzegowych
- **Inne procedury weryfikacji**

Weryfikacja podpisu zwykłego (1)

- Po otrzymaniu podpisanego dokumentu, odbiorca:
  - weryfikuje podpis matematycznie
  - sprawdza ważność certyfikatu
    - data weryfikacji musi być zawarta w *okresie ważności* certyfikatu
    - certyfikat nie może być unieważniony
  - Unieważnienie certyfikatu weryfikuje się na podstawie „aktualnej” listy unieważnionych certyfikatów CRL
    - przyjmuje się (za X.509) że lista CRL jest aktualna, jeśli nie nastąpiła jeszcze data planowego wystawienia następnej listy CRL

Weryfikacja podpisu zwykłego (2)

- W przypadku unieważnienia certyfikatu występuje określony czas propagacji informacji o tym unieważnieniu
  - nie jest określone czy podpis jest wtedy ważny - kto odpowiada za działania wynikające z przyjęcia ważności potencjalnie nieważnego podpisu
  - ze względu na zakres zastosowań (uwierzytelnienie) ta niepewność nie jest zazwyczaj szkodliwa

Weryfikacja *bezpiecznego* podpisu – podejście „naiwne” (1)

- Po otrzymaniu podpisanego dokumentu, odbiorca:
  - weryfikuje podpis matematycznie
  - sprawdza ważność certyfikatu -
    - data weryfikacji musi być zawarta w okresie ważności certyfikatu
    - certyfikat nie może być unieważniony
  - Unieważnienie certyfikatu weryfikuje się na podstawie „aktualnych” list unieważnionych certyfikatów CRL i zaświadczeń certyfikacyjnych ARL
    - przyjmuje się (za X.509) że listy ARL i CRL są aktualne, jeśli nie nastąpiła jeszcze data planowego wystawienia następnej listy ARL/CRL

Weryfikacja „bezpiecznego” podpisu – podejście „naiwne” (2)

- W przypadku unieważnienia certyfikatu występuje określony czas propagacji informacji o tym unieważnieniu (np. 1 godzina)
  - podpis jest nieważny (nie stanowi dowodu) od momentu unieważnienia certyfikatu
  - weryfikacja podpisu po unieważnieniu certyfikatu, a przed otrzymaniem informacji o tym unieważnieniu (CRL) da wynik niezgodny z rzeczywistością (*podpis poprawie zweryfikowany*, gdy tym czasem on jest już nieważny - nie stanowi dowodu)
  - odpowiedzialność za szkody wynikające z działań podjętych na skutek błędnej weryfikacji podpisu ponosi odbiorca (bo to on wykonał działania, a dokument od nadawcy nie jest podpisany – nadawca może się go z łatwością wyprzeć)
    - oraz ewentualnie – wtórnie – dostawca oprogramowania, jeśli ono działa niepoprawnie

Weryfikacja *bezpiecznego* podpisu – wniosek

- Weryfikacja *bezpiecznego* podpisu elektronicznego **nie** odbywa tak samo jak weryfikacja podpisu zwykłego
- Zastosowanie oprogramowania realizującego weryfikację zwykłego podpisu do weryfikowania podpisu *bezpiecznego* w niektórych sytuacjach (ściśle zależnych od nadawcy) prowadzi do błędnych wyników
- Do weryfikacji *bezpiecznych* podpisów elektronicznych może służyć tylko oprogramowanie posiadające *deklarację zgodności* z wymaganiami określonymi dla *bezpiecznego urządzenia do weryfikacji podpisów elektronicznych*
  - wymagania na cechy „bezpiecznego urządzenia” i ich spełnianie przez konkretne oprogramowanie odbiorca (użytkownik/audytor) powinien kontrolować

Weryfikacja *bezpiecznego* podpisu – podejście bezpieczne (wstęp)

- Po otrzymaniu podpisanego dokumentu, odbiorca:
  - weryfikuje podpis matematycznie (ew. ***podpis negatywnie zweryfikowany***)
  - sprawdza datę certyfikatu - data weryfikacji musi być zawarta w okresie ważności certyfikatu
  - zapewnia sobie dowód istnienia podpisu w określonym czasie
    - znacznik czasu
  - sprawdza ważność certyfikatu - certyfikat nie może być unieważniony …

Weryfikacja *bezpiecznego* podpisu – podejście bezpieczne (CRL/ARL)

- Unieważnienie certyfikatu weryfikuje się na podstawie „aktualnych” list unieważnionych certyfikatów CRL i ARL
  - lista CRL/ARL jest aktualna jeśli dowodzi, że w czasie istnienia podpisu certyfikat (zaświadczenie certyfikacyjne) był ważny
  - taki dowód zapewnia jedynie lista CRL/ARL wystawiona **po** (możliwym do udowodnienia) momencie, w którym istniał już podpis
    - w praktyce – po momencie wynikającym z posiadanego znacznika czasu
- Wniosek – na listy CRL/ARL trzeba czekać (np. 1 dzień roboczy).
  - przed otrzymaniem tych list podpis powinien mieć status weryfikacji ***niekompletnie zweryfikowany***
  - zwrócenie przez oprogramowanie weryfikujące jakiegokolwiek innego statusu jest wprowadzaniem w błąd i narażanie na ryzyko odbiorcę dokumentu
- Po otrzymaniu odpowiednio nowych list CRL/ARL podpis otrzymuje status ***poprawnie zweryfikowany***

Weryfikacja bezpiecznego podpisu – postać archiwalna podpisu

- Bezpieczny podpis elektroniczny, który ma status ***poprawnie zweryfikowany*** może zmienić status na ***negatywnie zweryfikowany***
  - „niezabezpieczony” *bezpieczny* podpis elektroniczny
    - traci ważność po upływie ważności zaświadczenia certyfikacyjnego (są wystawiane na 5 lat)
    - może być niemożliwy do zweryfikowania po upływie ważności certyfikatu (są wystawiane na 1-2 lata) – w chwili weryfikacji nowe listy CRL nie mogą być użyte, bo nie zawierają już informacji o ew. unieważnieniu certyfikatu
- Należy przygotować *postać archiwalną podpisu*
  - podpis wraz z kompletem informacji pozwalających na jego weryfikację (listy CRL/ARL), oznakowane czasem
  - postać archiwalna pozwala na utrzymanie statusu podpisu ***poprawnie zweryfikowany*** również po przeterminowaniu certyfikatu i zaświadczenia certyfikacyjnego

Weryfikacja *bezpiecznego* podpisu – konserwacja postaci archiwalnej

- Postać archiwalną podpisu pozwala na jego weryfikację w dowolnym terminie, pod warunkiem że wciąż jest ważny „najbardziej zewnętrzny” znacznik czasu
- Znacznik czasu przestaje być ważny po przeterminowaniu lub unieważnieniu zaświadczenia certyfikacyjnego dla kwalifikowanego podmiotu świadczącego usługi w zakresie znakowania czasem (zaśw. wydawane na 5 lat)
  - przed utratą ważności tego znacznika czasu trzeba podpis *konserwować* – co oznacza ponowne znakowanie czasem
  - konserwację podpisu trzeba powtarzać cyklicznie dopóki jest istotne dla użytkownika utrzymywanie ważności podpisów pod dokumentem

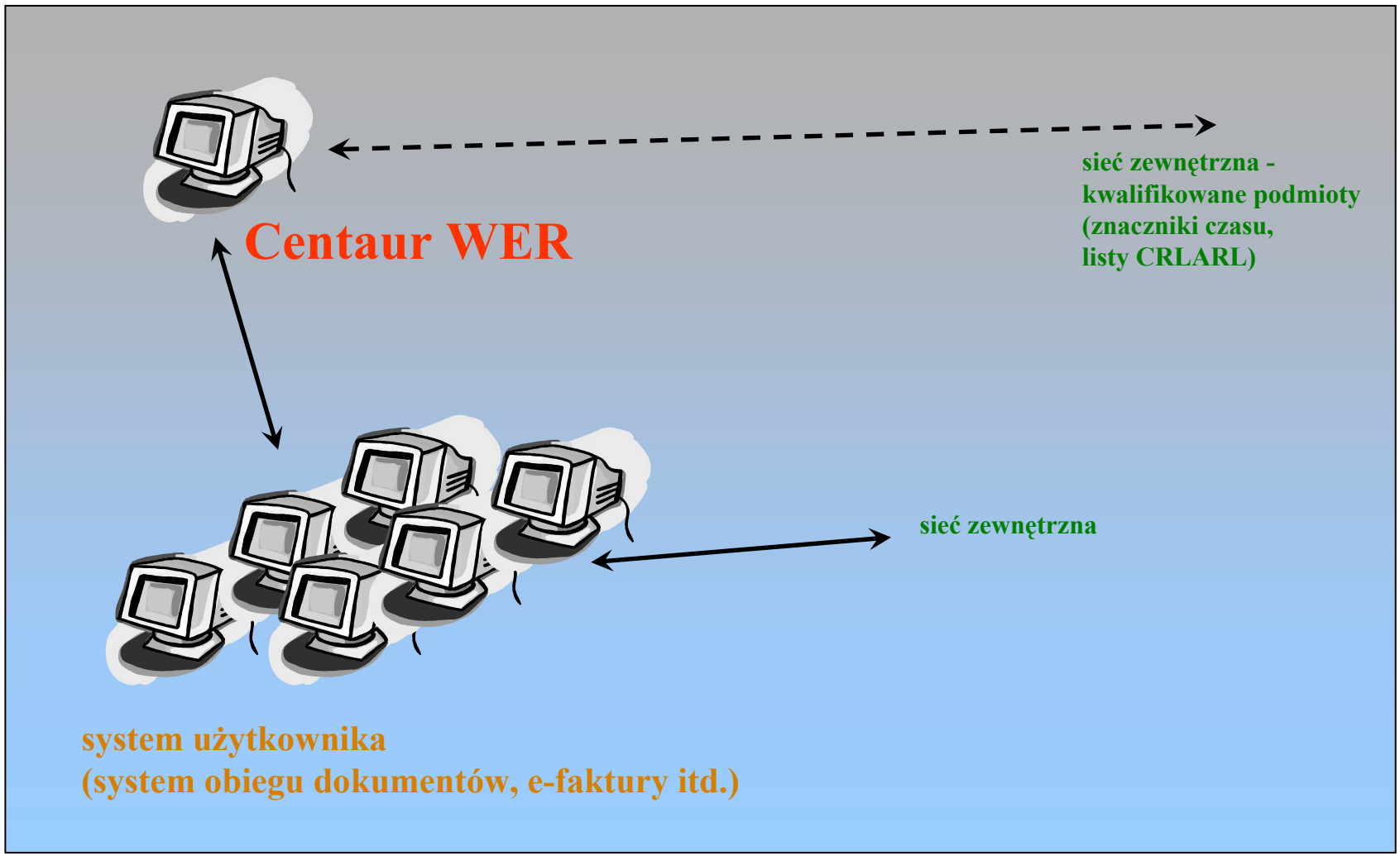
Weryfikacja *bezpiecznego* podpisu – inne problemy

- W systemach publicznych nadawca może przysłać dokument podpisany z podpisem w różnych formatach, np.:
  - PKCS#7/CMS
    - z podpisem wewnątrz wiadomości
    - z podpisem odłączonym
    - bez kodowania/z kodowaniem S/MIME
  - XML
- Odbiorca publiczny powinien te formaty rozumieć

Weryfikacja *bezpiecznego* podpisu – podsumowanie

- Operacja dość skomplikowana
- Procedury działania istotnie różne od sytuacji *zwykłego* podpisu elektronicznego
- Niezbędne wspomaganie oprogramowaniem, ściśle opartym na funkcjonujących w kraju przepisach dotyczących podpisu elektronicznego

Weryfikacja *bezpiecznego* podpisu – propozycja systemu



Centaur WER

- Serwer weryfikacji bezpiecznych podpisów elektronicznych
- Podstawowe cechy
  - obsługuje wiele formatów podpisów (PKCS#7 – podpis w dokumencie i odłączony, S/MIME, XML)
  - realizuje praktycznie wszystkie potrzeby aplikacji posługujących się dokumentami podpisanymi elektronicznie – w zakresie weryfikacji podpisu
  - interfejs Web Services – łatwe dołączenie do systemów pisanych w różnych językach programowania

Centaur WER – model działania (1)

- Aplikacja użytkownika (np. system obiegu dokumentów czy system e-faktur) otrzymuje dokument – *być może* podpisany elektronicznie i przesyła go do Centaur WER
  - jeśli dokument nie jest podpisany żadnym ze znanych formatów podpisów – otrzymuje komunikat (i dalej go przetwarza jako dokument niepodpisany)
  - jeśli dokument jest podpisany – aplikacja otrzymuje zazwyczaj status weryfikacji podpisu *niekompletnie zweryfikowany*

Centaur WER – model działania (2)

- Centaur WER zapisuje otrzymany dokument w swojej bazie danych i niezależnie od pracy aplikacji podejmuje wysiłki w celu doprowadzenia do poprawnej weryfikacji dokumentu (znakuje go czasem, pobiera niezbędne informacje z sieci itd.)
- Po jakimś czasie aplikacja pyta ponownie o ten dokument, otrzymuje status ***poprawnie zweryfikowany***, na życzenie otrzymuje również postać archiwalną podpisów pod dokumentem

Centaur WER – model działania (podsumowanie)

- System obiegu dokumentów nie musi rozumieć formatów podpisów elektronicznych ani umieć je weryfikować, konserwować itd.
- Długotrwały proces weryfikacji dokumentu odbywa się całkowicie poza systemem o.d. i go nie obciąża
  - przy czym dokument o statusie *niekompletnie zweryfikowany* w wielu przypadkach może być procedowany, a przed podjęciem ostatecznej decyzji na podstawie dokumentu sprawdza się ostatecznie jego status
- Podpisy są przekształcane przez Centaur WER do postaci archiwalnej, umożliwiającej zachowanie ich ważności w czasie
  - co ok. 2-3 lata podpisy powinny być konserwowane

ENIGMA Systemy Ochrony Informacji Sp. z o.o.

Zapraszamy do współpracy

jacek.pokrasniewicz@enigma.com.pl

www.enigma.com.pl