Bezpieczeństwo i podpis elektroniczny

Paweł Radziński - p.radzinski@abg.com.pl

Spis treści

Uwagi ogólne

Niniejszy wykład traktuje zagadnienia dotyczące bezpieczeństwa wysokopoziomowo, bez techniczno-matematycznych szczegółów

Bardzo ważną a często pomijaną kwestią jest jakość stosowanego generatora liczb pseudolosowych.

Skróty kryptograficzne

- Ang. *cryptographic hash*, także „odcisk palca".
- Główne cechy:
- Skrót nie ujawnia niczego o wiadomości.
- Drobna zmiana we wiadomości powoduje bardzo dużą zmianę w wynikowym skrócie. Teoretycznie zmiana 1 bitu wiadomości to zmiana połowy bitów skrótu.
- Praktycznie niemożliwe jest „podrobienie" skrótu, czyli znalezienie 2 wiadomości mających ten sam skrót (możliwość podmiany).

Skróty kryptograficzne c.d.

- Przykłady skrótów:
- MD-5 128 bitów (zupełnie niebezpieczny),
- SHA-1 160 bitów
- SHA-224/256/384/512 określane łącznie jako SHA-2 - nowsze i bardziej bezpieczne

Przykładowe zastosowania:

- weryfikacja integralności,
- skrót hasła,
- podpis elektroniczny

Algorytmy asymetryczne

Cechy:

- Para kluczy (publiczny i prywatny) powiązanych ze sobą.
- Klucz publiczny może znać każdy i nie powinno to zmniejszać bezpieczeństwa.
- Poznanie klucza prywatnego na podstawie publicznego to konieczność rozwiązania jakiegoś bardzo skomplikowanego obliczeniowo problemu.
- Różnica w stosunku do algorytmów symetrycznych, gdzie jest **jeden tajny** klucz.
- Przykłady: RSA (Rivest, Shamir, Adleman); DSA (Digital Signature Algorithm)

Algorytmy asymetryczne c.d.

- **Szyfrowanie** kluczem **publicznym**

  Tylko posiadacz klucza prywatnego może odszyfrować skierowaną do siebie wiadomość.

- **Podpis** kluczem **prywatnym**

  Praktycznie każdy mający dostęp do klucza publicznego może zweryfikować prawidłowość podpisu.

Algorytmy asymetryczne c.d.

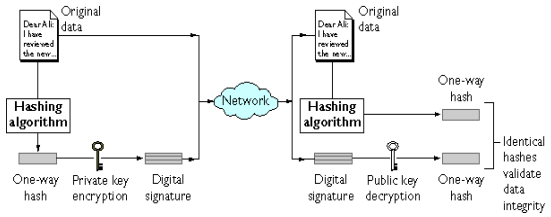
Algorytmy asymetryczne są dużo wolniejsze od symetrycznych, dlatego zazwyczaj stosuje się rozwiązania hybrydowe. Klucz algorytmu symetrycznego jest szyfrowany algorytmem asymetrycznym (np. klucz sesyjny w TLS/SSL).

Szczególne zastosowania podpisu:

- znakowanie czasem
- certyfikaty X.509.

Podpis elektroniczny

Zasada działania podpisu elektronicznego:



Kluczowa rola:

- jakości algorytmu haszującego (funkcji skrótu),
- jakości asymetrycznego algorytmu szyfrowania/deszyfrowania.

Podpis elektroniczny w sensie prawnym

- Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.
- Ustawa wprowadza też też pojęcie "bezpiecznego podpisu elektronicznego" (w prawie unijnym jest to *advanced eletronic signature*)

PKI i certyfikaty

PKI (ang. *Public Key Infrastructure*) vel Infrastruktura Klucza Publicznego

PKI to zespół rozwiązań technicznych (sprzęt, oprogramowanie) i **organizacyjnych**.

Najistotniejszą częścią PKI są certyfikaty X.509.

Certyfikat to sposób na **powiązanie klucza publicznego** (zatem pośrednio także prywatnego) **z informacją o tożsamości** jego posiadacza. Jest on podpisany przez **trzecią stronę** (urząd/centrum certyfikacji).

PKI i certyfikaty c.d.

Certyfikat zawiera zazwyczaj:

- nazwę posiadacza (to może być też np. numer IP serwera)
- okres ważności
- numer seryjny unikalny w zbiorze certyfikatów od danego wystawcy
- informację o możliwych zastosowaniach klucza prywatnego
- nazwę wystawcy certyfikatu (trzeciej strony)
- informację o źródle informacji o odwołaniu certyfikatu
- wiele innych (teoretycznie także zdjęcie bądź „fizyczny” odcisk palca).

PKI i certyfikaty c.d.

Wiele z wyżej wymienionych informacji znajduje się w tzw. rozszerzeniach. Zapewniają one (nomen omen) rozszerzalność standardu.

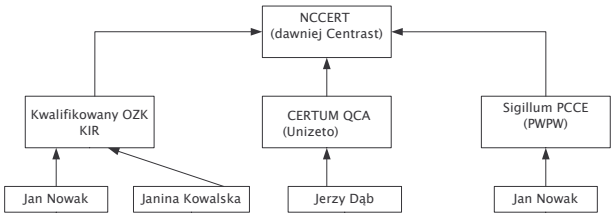
Integralną i najistotniejszą częścią certyfikatu jest podpis złożony przez urząd certyfikacji (trzecia strona) jego kluczem prywatnym.

Z kolei certyfikat urzędu może być podpisany przez urząd wyższego rzędu i tak dalej... aż do urzędu, któremu trzeba zaufać, bo on sam sobie podpisuje swój certyfikat. Jest to tzw. root.

PKI i certyfikaty c.d.

Certyfikaty od „najniższego" do „roota" tworzą tzw. ścieżkę certyfikacji.

Przykład struktury dla tzw. podpisu kwalifikowanego w Polsce.



PKI i certyfikaty c.d.

Informacje o odwołaniu certyfikatu.

- Listy CRL (ang. Certificate revocation list) – lista numerów seryjnych odwołanych certyfikatów podpisana przez wystawcę
- OCSP (ang. Online Certificate Status Protocol) – pytanie o konkretny certyfikat, mniejszy ruch w sieci.

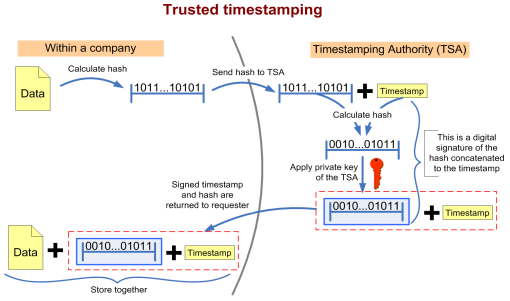
PKI i certyfikaty c.d.

Ze względu na rozwiązania przyjęte w polskim prawie rozróżniamy 2 rodzaje certyfikatów:

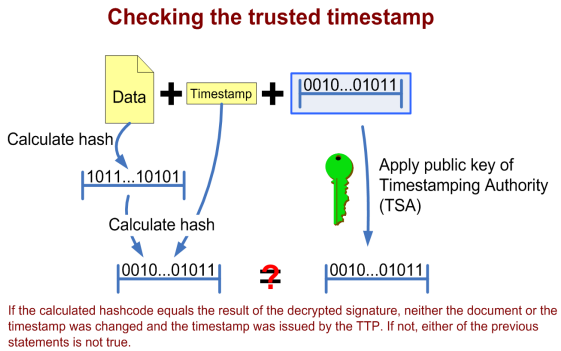
- Kwalifikowane. Podpis nimi złożony przy spełnieniu dodatkowych warunków określonych w ustawie o podpisie elektronicznym ma skutki prawne równoważne podpisowi odręcznemu.
- Niekwalifikowane, czyli cała reszta. Wykorzystywane do podpisu niekwalifikowanego, szyfrowania, logowania, TLS.

Znakowanie czasem

Znakowanie czasem polega na podpisaniu przez zaufaną trzecią stronę skrótu kryptograficznego znakowanych danych i daty.



Znakowanie czasem – weryfikacja



XML Signature

- Podpis dokumentu XML-owego:
  - zapisany w postaci struktury XML-owej,
  - umieszczany w elemencie `Signature`:
    - w osobnym dokumencie (*detached signature*),
    - dołączonym do podpisywanego dokumentu (*enveloped signature*),
    - zawierającym podpisywane dane (*enveloping signature*).
- Możliwości XML Signature:
  - podpisywanie fragmentów dokumentu XML,
  - podpisywanie zasobów zewnętrznych (dostępnych poprzez URL)
  - podpisy wielokrotne.

XML Signature – przykład 1. (*detached*)

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm=
      "http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <SignatureMethod Algorithm=
      "http://www.w3.org/2000/09/xmldsig#dsa-sha1"/>
    <!-- w URI znajduje się wskazanie na podpisywane dane - tu zewnętrzne -->
    <Reference URI="http://przyklad.pl/pliki/do-podpisu.xml">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#base64"/>
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <DigestValue>60NvZvtdTB+7UnlLp/H24p7h4bs=</DigestValue>
    </Reference>
  </SignedInfo>
  <!-- zaszyfrowany skrót z SignedInfo - podpis  -->
  <SignatureValue>OsH9AljTNL...</SignatureValue>
  <KeyInfo><KeyValue><DSAKeyValue>
    <P>imup6lm...</P><Q>xDve3j7...</Q><G>NlugAf...</G>
    <Y>W7dOmH/v...</Y>
  </DSAKeyValue></KeyValue></KeyInfo>
</Signature>
```

Źródło: Kazienko, P., *Co tam panie w XML-u?*, Software 2.0, 6/2003

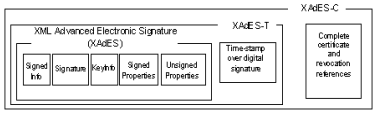
XML Signature – przykład 2. (*enveloped*)

```
<?xml version="1.0" encoding="UTF-8"?>
<Document>
  <Content>
    ...
  </Content>
  <ds:Signature>
  <ds:SignedInfo>
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
      </ds:Transforms>
    </ds:Reference>
  </ds:SignedInfo>
    ....
  </ds:Signature>
</Document>
```


XML Signature – XAdES

XadES – XML Advanced Electronic Signature

Rodzina zaawansowanych formatów podpisu XML zawierających informacje pozwalające na przedłużenie ważności podpisu. Zgodność z Dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.



XML Encryption

- Cel: zagwarantowanie poufności danych w XML.
- Szyfrować można zarówno cały plik XML jak i jego części.

```
<purchaseOrder>
  <Order>
  <Item>book</Item>
    <Id>123-958-74598</Id>
    <Quantity>12</Quantity>
  </Order>
  <Payment>
    <CardId>123654-8988889-9996874</CardId>
    <CardName>visa</CardName>
    <ValidDate>12-10-2004</ValidDate>
  </Payment>
</purchaseOrder>
```


XML Encryption – przykład 1.

Przykład zaszyfrowania całego pliku.

```
<EncryptedData xmlns='http://www.w3.org/2001/04/xmlenc#'
  Type='http://www.isi.edu/in-notes/iana/assignments/media-types/text/xml'>
  <CipherData>
    <CipherValue>A23B45C56</CipherValue>
  </CipherData>
</EncryptedData>
```

XML Encryption – przykład 2.

Przykład zaszyfrowania zawartości elementu.

```
<PurchaseOrder>
  <Order>
  <Item>book</Item>
  <Id>123-958-74598</Id>
  <Quantity>12</Quantity>
  </Order>
  <Payment>
    <CardId>
      <EncryptedData Type='http://www.w3.org/2001/04/xmlenc#Content'
        xmlns='http://www.w3.org/2001/04/xmlenc#'>
      <CipherData>
        <CipherValue>A23B45C564587</CipherValue>
      </CipherData>
    </EncryptedData></CardId>
    <CardName>visa</CardName>
    <ValidDate>12-10-2004</ValidDate>
  </Payment>
</PurchaseOrder>
```


Czytniki i karty

- Klucz prywatny którym składany jest podpis znajduje się na karcie inteligentnej.
- Klucz nie opuszcza tej karty, podpis jako przekształcenie matematyczne jest wyliczany na karcie.
- Jest sporo rodzajów czytników i kart.
- Najpopularniejszym sposobem dostępu do czytników i kart jest PKCS#11 (ang. Public Key Encryption Standard) – standard pochodzący z firmy RSA Security. Dostawca czytnika i karty zapewnia bibliotekę PKCS#11 i dzięki temu możemy nie przejmować się różnicami.

Bibliografia

Ogólne pojęcia z dziedziny bezpieczeństwa:

- http://www.ssh.com/support/cryptography/index.html
- http://ipsec.pl/leksykon/
- http://kryptografia.prv.pl/

Podpis elektroniczny, XML Signature, XML Encryption:

- XML-Signature Syntax and Processing – http://www.w3.org/TR/xmldsig-core/
- XML Encryption Syntax and Processing – http://www.w3.org/TR/xmlenc-core/
- http://www.w3.org/TR/XAdES/
- Dokumenty ETSI (European Telecommunications Standards Institute) – http://www.etsi.org
- ETSI TS 101 733 – Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats
- ETSI TS 101 903 – XML Advanced Electronic Signatures (XadES)
- http://xml.apache.org/security/index.html

Bibliografia – akty prawne

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. 2001 nr 130 poz. 1450)

Rozporządzenie z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. 2002 nr 128 poz.1094).

Dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (OJ L 13 z dn. 19.01.2009, str. 12).