•Podpis elektroniczny

Wiosna 2016

Bezpieczeństwo korespondencji elektronicznej

- Ochrona przed modyfikacją (integralność),
- Uniemożliwienie odczytania (poufność),
- Upewnienie adresata, iż podpisany nadawca jest faktycznie autorem otrzymanej korespondencji (autentyczność),
- O integralności i autentyczności świadczy podpis, natomiast poufność gwarantuje szyfrowanie/kryptografia.

Operacja podpisywania wiadomości podpisem elektronicznym jest:

- Niepodrabialna
- Autentyfikowalna
- Jednorazowa
- Nieprzerabialna
- Jednoznaczna

Art. 5 ust. 2 Ustawy z dnia 18.09.2001 o podpisie elektronicznym (z 2001 r. Dz.U. Nr 130, poz. 1450).

- „Art. 78. §2. Oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne formie pisemnej."
- „dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej"

Decyzja Komisji Europejskiej 2003/511/EC z 14 lipca 2003 r.

Przyjmująca normy i standardy techniczne określające zalecane wymagania dla kwalifikowanych certyfikatów i dla bezpiecznych urządzeń służących do składania podpisu elektronicznego.

Podpis elektroniczny

- jest jednoznacznie przyporządkowany podpisującemu
- umożliwia identyfikację podpisującego
- stworzony jest za pomocą środków, które podpisujący może mieć pod swoją wyłączną kontrolą
- jest powiązany z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest wykrywalna.

Podpis elektroniczny

„dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji (nowelizacja: uwierzytelnianie) osoby składającej podpis elektroniczny....”- „jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna....”

Źródło: Ustawa o podpisie elektronicznym (z 18 września 2001 roku).

Podpis cyfrowy

- przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę; asymetryczne podpisy cyfrowe mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

- http://www.certum.pl/pl/dokumentacja/slownik/

Ustawa o podpisie elektronicznym

- Podpisana 11 października 2001 roku
- Ustawa wyróżnia dwa rodzaje podpisów:
  - **podpis zwykły** (do weryfikacji nie jest potrzebny kwalifikowany certyfikat – skutki prawne zależnie od podpisanej przez strony umowy)
  - **bezpieczny** (zrównany z podpisem własnoręcznym – rodzi skutki prawne bez konieczności wcześniejszego podpisania umowy pomiędzy stronami).

Dwa rodzaje podpisu elektronicznego

- **Zwykły -** spełnia dodatkowe wymogi dotyczące uwierzytelniania składającego oraz bezpieczeństwa samej technologii
- **Kwalifikowany** – zaawansowany podpis oparty o kwalifikowany certyfikat, złożony za pomocą bezpiecznego urządzenia do składania podpisów pozostającego pod wyłączną kontrolą składającego podpis. Tylko kwalifikowany podpis ma moc prawną równą podpisowi odręcznemu.

Kwalifikowany podpis elektroniczny

- podpis złożony za pomocą certyfikatu kwalifikowanego oraz bezpiecznego urządzenia do składania podpisu (SSCD). Jest równoważny podpisowi odręcznemu i przyporządkowany do osoby, która go składa.
- Certyfikat kwalifikowany wydawany jest odpłatnie wyłącznie osobom fizycznym. Służy do podpisywania dokumentów przekazywanych drogą elektroniczną.

Inne pojęcia podpisu ustawy 2001

- **„podpis elektroniczny"** to dane w postaci elektronicznej, służące wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, do identyfikacji osoby składającej podpis
- **„bezpieczny podpis elektroniczny”** podpis przypisany osobie go składającej.
- **podpis elektroniczny znakowany czasem,** który nie tylko identyfikuje podpisującego, ale również jednoznacznie określa czas złożenia podpisu.

Podpis elektroniczny: rząd przyjął projekt ustawy

- Podpis zwykły to podpis niekwalifikowany, zgodny z dotychczas obowiązującym prawem.
- Podpis zaawansowany będzie połączony z kwalifikowanym certyfikatem lub certyfikatem innego rodzaju
- Pieczęć elektroniczna ma służyć uwierzytelnianiu wiarygodności dokumentów i będzie mieć zastosowanie przy wydawaniu elektronicznych zaświadczeń z rejestrów.
- Podpis zaawansowany, będą mogły składać osoby fizyczne i prawne. dane w postaci elektronicznej, opatrzone przez osobę fizyczną posługującą się tym rodzajem podpisu, będą umożliwiały wywołanie skutków prawnych w relacji z podmiotami publicznymi.
- Podpis kwalifikowany/bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu.

•http://www.podatki.biz/artykuly/16_10318.htm

Pojęcia wg projektu ustawy nowelizującej 1/2

- „zaawansowany podpis elektroniczny" „kwalifikowany podpis elektroniczny" „podpis urzędowy" „pieczęć elektroniczna" oraz „podpis elektroniczny znakowany czasem"
- „podpis elektroniczny" to dane w postaci elektronicznej dołączone do innych danych elektronicznych lub z nimi logicznie powiązane i służące jako metoda uwierzytelnienia.
- Zaawansowany podpis to taki, który przyporządkowany jest wyłącznie podpisującemu, umożliwia jego identyfikację, a także jest utworzony za pomocą środków pozostających pod wyłączną kontrolą podpisującego. Ujętą odrębnie formą zaawansowanego

Pojęcia wg projektu ustawy nowelizującej 2/2

- kwalifikowany podpis elektroniczny. Taki podpis jest weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu oraz składany za pomocą specjalnego, bezpiecznego urządzenia
- podpis urzędowy to wariant zaawansowanego podpisu elektronicznego, składanego przez podpisującego będącego osobą fizyczną przy pomocy danych służących do składania podpisu elektronicznego zawartych w dokumencie tożsamości.
- Pieczęć elektroniczna z kolei jest podpisem składanym przez podpisującego niebędącego osobą fizyczną.
- oświadczenie woli złożone w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu jest równoważne z oświadczeniem woli złożonym w formie pisemnej.

elektroniczna platforma usług administracji publicznej - ePUAP”

podpis potwierdzony profilem zaufanym ePUAP - podpis złożony przez użytkownika konta ePUAP, do którego zostały dołączone informacje identyfikujące zawarte w profilu zaufanym ePUAP, a także:

a) jednoznacznie wskazujący profil zaufany ePUAP osoby, która wykonała podpis,

b) zawierający czas wykonania podpisu,

c) jednoznacznie identyfikujący konto ePUAP osoby, która wykonała podpis,

d) autoryzowany przez użytkownika konta ePUAP,

e) potwierdzony i chroniony podpisem systemowym ePUAP;

USTAWA z dnia 17 lutego 2005 r.

Profil Zaufany – projekt MSWiA

- bezpłatny podpis elektroniczny do kontaktów obywateli z administracją
- zdalne załatwianie spraw w urzędach bez konieczności wykupywania kwalifikowanego podpisu elektronicznego,
- W tym celu należy założyć konto na stronie Elektronicznej Platformy Usług Administracji Publicznej - epuap.gov.pl
- Potwierdzenie osobiste z dowodem

Certyfikat (certyfikat klucza publicznego)

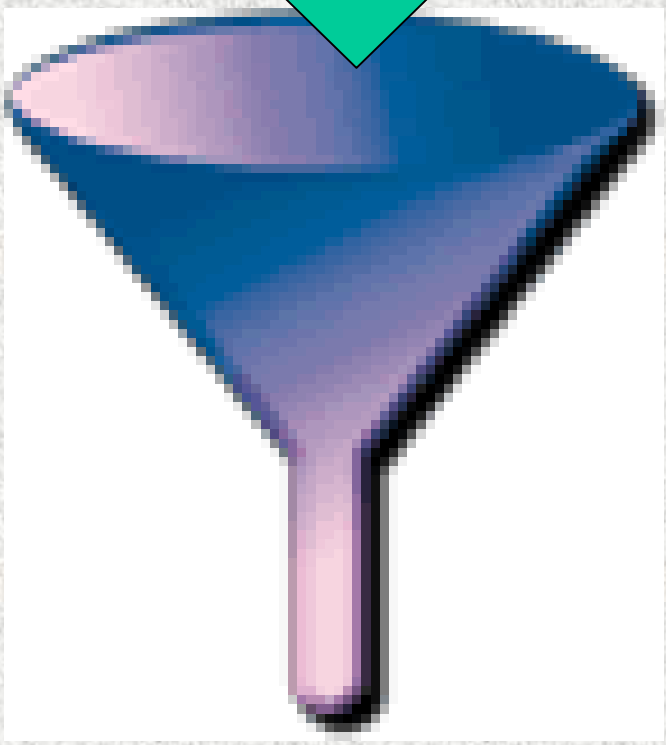
- wiadomość, która zawiera co najmniej nazwę lub identyfikator organu wydającego certyfikaty, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez organ wydający.

•http://www.certum.pl/pl/dokumentacja/slownik/

Słabość certyfikatów

- Fałszywe lub skompromitowane (złamane) certyfikaty podważają sens stosowania jakiegokolwiek szyfrowania w trakcie wymiany danych przez Sieć.
- Warto sprawdzić, czy podczas teoretycznie bezpiecznego połączenia nie jest wykorzystywany certyfikat wydany przez złamany certyfikat, np. wydany przez Comodo.
- Narzędzie aprawdzenia: filippo.io/Badfish.

Dowolny tekst, z którego obliczany jest „skrót”



(skrót:) **8376594048959**

Algorytmy typu Hash

- HMAC
- MD 2, 4, 5
- SHA-1
- MD5

Podpis elektroniczny inaczej

- Musi być związany wyłącznie z osobą, która go używa,
- Musi być trudny lub niemożliwy do podrobienia,
- Musi być ściśle powiązany z danymi, do których został dołączony,
- Musi uniemożliwić podpisanemu zaprzeczenie złożenia podpisu

Procedura

1. Abacki i Babacki mają dwie pary kluczy – do szyfrowana para A, do podpisu – para B.
2. Abacki szyfruje swój list adresowany do Babackiego, kluczem publicznym z pary (A) kluczy Babackiego.
3. Abacki podpisuje swój list (zaszyfrowany lub nie), adresowany do Babackiego, poprzez dołączenie do listu obliczonego „skrótu” (robi to automat) i następnie szyfruje podpis swoim kluczem prywatnym (z pary B).
4. Abacki do szyfrowania podpisu wykorzystuje swój klucz prywatny z pary kluczy B (pamiętajmy, że do szyfrowania całego listu zastosował publiczny klucz z pary kluczy A Babackiego).
5. W efekcie adresat – Babacki - otrzymuje zaszyfrowany list, do którego dołączony jest zaszyfrowany podpis/„skrót” Abackiego.

Procedura c.d.

4. Babacki odszyfrowuje list swoim prywatnym kluczem A.
5. Babacki odszyfrowuje podpis korzystając z publicznego klucza B Abackiego.
6. Korzystając z tej samej metody co Abacki, Babacki oblicza jeszcze raz „skrót” otrzymanego od Abackiego listu.
7. Porównuje „skróty” - odszyfrowany z obliczonym. Identyczność skrótów dowodzi, że list nie został po drodze zmieniony.
8. Zwróćmy uwagę na zmianę funkcji kluczy asymetrycznych w podpisywaniu skrótu!

Procedura - koniec

Dzięki szyfrowaniu mamy zapewnioną poufność korespondencji (nikt jej po drodze nie odczyta), dzięki certyfikatowi jej autentyczność (list wysłała osoba, która się pod nim podpisała), a dzięki podpisowi (skrótowi) jego integralność (list dotarł do nas w niezmienionej postaci).

Procedura podpisu inaczej

nadawca

- Elektroniczny dokument
- Obliczanie funkcji skrótu
- Skrót
- Szyfrowanie Skrótu kluczem prywatnym nadawcy
- Podpis elektroniczny

odbiorca

- Elektroniczny dokument z podpisem nadawcy
- Odszyfrowanie podpisu kluczem publicznym nadawcy
- Obliczanie funkcji skrótu
- Porównanie obliczonego z otrzymanym skrótem

Po co certyfikaty?

- W operacji szyfrowania, klucz publiczny gwarantuje wyłącznie to, że wiadomość zaszyfrowana tym kluczem będzie odczytana przez jego właściciela – posiadającego odpowiadający klucz prywatny.
- W operacji odszyfrowania skrótu (podpis), klucz publiczny gwarantuje to, że odszyfrowany skrót jest identyczny z tym, który wysłał właściciel tego klucza (szyfrował skrót odpowiadającym mu kluczem prywatnym).
- Bez certyfikatu - brak gwarancji, że właściciel klucza publicznego jest osobą, za którą się podaje.

Certyfikaty

Certyfikat jest ciągiem danych (wiadomością), który zawiera co najmniej nazwę lub identyfikator urzędu wydającego certyfikaty, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu i jest podpisany przez urząd CA

http://www.certum.pl/pl/dokumentacja/pc/index.html

Certyfikat

CA wydając certyfikat subskrybentowi potwierdza tożsamość subskrybenta oraz fakt, iż będący w jego posiadaniu klucz publiczny w rzeczywistości należy do niego. Dzięki temu strona ufająca, po otrzymaniu podpisanej wiadomości jest w stanie zidentyfikować właściciela certyfikatu, który podpis ten złożył oraz ewentualnie rozliczyć go z działań, które podjął lub do których się zobowiązał.

http://www.certum.pl/pl/dokumentacja/pc/index.html

Certyfikat

- CA – Najważniejszy element PKI (Public Key Infrastructure)
- Certyfikat – odpowiednio zaszyfrowany identyfikator cyfrowy. Służy on do potwierdzenia tożsamości osoby, która z niego korzysta
- Certfikat wydawany (generowany) jest przez urząd certyfikacji (CA- Certificate Authority) *np. www.certum.pl*
- Można utworzyć lokalne CA, na potrzeby firmy

standard certyfikatów jest X.509 v.3, m.in.:

- *Wersja* – określa wersję certyfikatu,
- *Numer seryjny* – identyfikator certyfikatu, niepowtarzalny w ramach danego ośrodka,
- *Sygnatura* – opisuje identyfikator algorytmu wykorzystywanego do obliczenia podpisu elektronicznego złożonego na certyfikacie,
- *Wystawca* – nazwa ośrodka wydającego certyfikat (to pole musi być zawsze wypełnione),
- *Okres ważności* – przedział czasu, w jakim obowiązuje certyfikat,
- *Podmiot* – nazwa właściciela certyfikatu

C.Adams, S.Lloyd, *Podpis elektroniczny klucz publiczny,* Wydawnictwo Robomatic, Wrocław 2002.

Usługi certyfikacyjne

- rejestracja i wydanie certyfikatu,
- odnowienie certyfikatu,
- unieważnienie certyfikatu,
- weryfikacja statusu certyfikatu.

Źródło: http://www.certum.pl/pl/dokumentacja/pc/index.html

Pozostałe usługi certyfikacyjne:

- oznaczanie wiarygodnym czasem (ang. Time Stamping Authority),
- notariat elektroniczny (ang. Notary Authority),
- skarbiec elektroniczny (ang. Electronic Vault),
- kurier elektroniczny (ang. Delivery Authority)

są usługami niezaprzeczalności, które mogą być świadczone niezależnie od CA

Usługi świadczone przez CA

- Certyfikat poczty elektronicznej
- Certyfikat serwera WWW
- Certyfikat serwera SSL
- Identyfikator cyfrowy do kreowania podpisów elektronicznych
- Certyfikaty programistów
- Certyfikaty VPN

Infrastruktura klucza publicznego
PKI
(Public Key Infrastructure)

PKI tworzą wszystkie elementy (ludzie, sprzęt, oprogramowanie oraz komunikacja) służące sprawnemu, godnemu zaufania, operowaniu kluczami kodowymi. Innymi słowy PKI służy do zarządzania cyfrowymi certyfikatami i kluczami szyfrującymi dla osób, programów i systemów

Usługi świadczone na rzecz Ministra Gospodarki

- Certyfikacja podmiotów świadczących kwalifikowane usługi certyfikacyjne polegająca na wytwarzaniu i wydawaniu zaświadczeń certyfikacyjnych oraz publikacji rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne na terytorium kraju,
- prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, w imieniu ministra właściwego do spraw gospodarki

Kwalifikowani dostawcy usług zaufania (2016)

Podstawowy zestaw do składania bezpiecznego podpisu elektronicznego

- certyfikat kwalifikowany zapisany na karcie kryptograficznej,
- oprogramowanie do składania podpisu
- czytnik kart dołączany do komputera przez port USB. Można kupić zestaw bez czytnika. To opcja dla osób, które mają czytnik np. w notebooku.

Ceny

PODMIOT KWALIFIKOWANY	CENCERT	KIR S.A.	MOBICERT	PWPW	CERTUM
E-PODPIS WAŻNY ROK	282,9	301,35	bd.	301,35	301,35
E-PODPIS WAŻNY 2 LATA	338,25	366,54	293,97	366,54	366,54
ODNOWIENIE NA ROK	110,7	158,67	bd.	bd.	121,77
ODNOWIENIE NA 2 LATA	153,75	202,95	147,6	bd.	170,97

Wszystkie ceny brutto (z VAT 23%)

•CHIP.PL GRUDZIEŃ 2012

Koszty

- Koszt zestawu z czytnikiem oraz certyfikatem ważnym rok wynosi od 230 do 245 zł. Zestawy bez czytnika – ok. 200 zł.
- Certyfikat na dwa lata ok. 50 zł
  Odnowienie certyfikatu na kolejny rok kosztuje 90-95 zł, a 105-130 zł
  na kolejne dwa lata.

•lipiec 2012, www.pcworld.pl

SSL

- Narzędzie do zabezpieczenia transmisji danych.
- Pierwszy krok do realizacji wytycznych GIODO dotyczących gromadzenia i przetwarzania danych osobowych
- Certyfikaty SSL – ich zadanie to ochrona komunikacji między przeglądarką internetową użytkownika a serwerem.

Certyfikaty SSL 1/3

- Certyfikaty klasy EV (extended validation) mają najwyższy poziom zabezpieczeń.
- Wyróżnia je przede wszystkim zielony pasek adresu w oknie przeglądarki, a stosują je głównie banki oraz instytucje finansowe. **Zapewnia poufność, integralność i autentyczność**

Certyfikaty SSL 2/3

- Certyfikaty SSL klasy OV, czyli tzw. organization validation, przeznaczone dla dużych sklepów internetowych, serwisów biznesowych czy serwerów baz danych. Łatwo można sprawdzić kto jest właścicielem domeny.
  - **Zapewnia poufność, integralność i autentyczność w ograniczonym zakresie**
- Najtańsze certyfikaty klasy domain validation (DV), które weryfikują domeny.
  - **Zapewnia poufność, integralność nie autentyczność**
- To idealne rozwiązanie dla forów internetowych, małych portali czy nawet blogów.

Certyfikaty SSL 3/3

- certyfikaty wildcard oraz multidomain. Pierwsze oprócz domeny głównej obejmują również subdomeny, natomiast drugie przeznaczone są do szyfrowania pojedynczym certyfikatem połączeń do wielu różnych domen.

PCWorld, II. 2013

ePUAP: Elektroniczna Platforma Usług Administracji

- scentralizowany system informatyczny udostępniony przez MSWiA, który pozwala jednostkom administracji publicznej i innym instytucjom publicznym świadczenie usług drogą elektroniczną. Dla petenta oznacza to możliwość składania urzędowych dokumentów przez Internet.
- **Profil Zaufany** – potwierdzenie tożsamości niemal na prawach podpisu elektronicznego

Profil zaufany (PZ) 1/2

- jest bezpłatną metodą potwierdzania tożsamości osoby w systemach elektronicznej administracji
- Nie jest równoważny podpisowi elektronicznemu i nie można nim podpisywać umów cywilnoprawnych czy dokumentów ubezpieczeniowych przekazywanych do ZUS.

Profil zaufany (PZ) 2/2

- Profil zaufany może mieć każda osoba fizyczna bez ponoszenia dodatkowych opłat za wydanie certyfikatu służącego do składania podpisu elektronicznego.
- Użycie PZ nie wymaga dodatkowego urządzenia (czytnik) ani oprogramowania.
- Do jego założenia wymagane jest podanie adresu e-mail, na który wysyłane będą kody autoryzacyjne.
- W systemie ePUAP pełnią one podobną funkcję jak kody jednorazowe stosowane w bankowości elektronicznej.

Profil Zaufany

- **Podpisywanie dokumentów przekazywanych online do urzędów**
- **Dowody osobiste i dane osobowe:** wniosek o dowód dla siebie lub dziecka (serwis ePUAP), sprawdzenie ważności dowodu (serwis ePUAP), zgłoszenie utraty lub zniszczenia dokumenty (serwis ePUAP), sprawdzanie danych w Rejestrze Dowodów Osobistych lub PESEL (serwis obywatel.gov.pl)
- **Wyjazd za granicę:** EKUZ, czyli Europejska Karta Ubezpieczenia Zdrowotnego (serwis ePUAP)
- **Kierowcy i pojazdy:** wydanie wtórnika prawa jazdy, zawiadomienie o zbyciu pojazdu (serwis ePUAP)
- **Odpisy aktów z Urzędu Stanu Cywilnego:** m.in. akty urodzenia, małżeństwa, zgonu (serwis ePUAP)
- **Szukanie pracy:** zgłoszenie do Urzędu Pracy (serwis praca.gov.pl)
- **Wybory:** dopisanie do listy wyborców (serwis ePUAP)
- **Indywidualna interpretacja podatkowa** (serwis Krajowej Informacji Podatkowej)
- **Zaświadczenie o niekaralności** (serwis Krajowego Rejestru Karnego)
- **Karta Dużej Rodziny** (serwis Ministerstwa Rodziny, Pracy i Polityki Społecznej - Emp@tia)
- **Rejestracja działalności gospodarczej** (serwis CEIDG)
- **Usługi ZUS:** np. zwolnienie z powodu choroby dziecka lub innego domownika, rehabilitacja po zwolnieniu lekarskim, zaświadczenie płatnika składek ZUS dla Pracodawców zatrudniających do 21 pracowników, oświadczenie o osiąganiu przychodu dla pracujących Emerytów i Rencistów i wiele innych (serwis PUE ZUS)