Podpis elektroniczny
Zagadnienia prawne i techniczne

Pracownia Informatyki Prawniczej

Rok akademicki 2008-09

Nota:

Niniejsza prezentacja stanowi uzupełnienie wykładu prezentowanego na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego w ramach przedmiotu „Informatyka prawnicza i technologie informacyjne”.

7. Podpis elektroniczny

7.1. Podstawowe regulacje prawne dotyczące podpisu elektronicznego

- Ustawa z dnia 18 września 2001 r. **o podpisie elektronicznym.** (Dz. U. Nr 130, poz .1450)

- Ustawa modelowa o handlu elektronicznym - UNCITRAL - 1996

- Ustawa modelowa o podpisie elektronicznym - UNCITRAL - 2001

- Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U.UE L z dnia 19 stycznia 2000 r.)

- Decyzja Komisji Europejskiej z dnia 6 listopada 2000 r. w sprawie minimalnych kryteriów jakie powinny zostać wzięte pod uwagę przez Państwa Członkowskie przy wyznaczaniu organów zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady w sprawie wspólnotowych ram w zakresie podpisu elektronicznego (2000/709/WE)(Dz.U.UE L z dnia 16 listopada 2000 r.)

7. Podpis elektroniczny

7.1. Podstawowe regulacje prawne dotyczące podpisu elektronicznego

- Ustawa z dnia 18 września 2001 r. **o podpisie elektronicznym.** (Dz. U. Nr 130, poz .1450)

Dz.U.02.128.1094 **rozp.** **2002.08.07**

Określenie 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.03.229.2282 **rozp.** **2003.12.16**

Obowiązkowe ubezpieczenie odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.

Dz.U.02.128.1099 **rozp.** **2002.08.06**

Sposób prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzór tego rejestru oraz szczegółowy tryb postępowania w sprawach o wpis do rejestru.

Dz.U.02.128.1101 **rozp.** **2002.08.09**

Określenie szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym.

7. Podpis elektroniczny

7.2. Uniwersalność podpisu elektronicznego

Ustawa z dnia 18 września 2001 r.
o podpisie elektronicznym

Art. 5 ust. 2.

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.

7. Podpis elektroniczny

7.2. Uniwersalność podpisu elektronicznego

Projekt ustawy o podpisach elektronicznych (marzec 2008)

Art. 5. 1. Zaawansowany podpis elektroniczny (podpis zaawansowany) weryfikowany przy pomocy certyfikatu wywołuje skutek prawny, jeżeli został złożony w okresie ważności tego certyfikatu.

W przypadku złożenia podpisu elektronicznego w okresie zawieszenia certyfikatu skutek prawny następuje z chwilą uchylenia zawieszenia.

2. Podpis zaawansowany zapewnia integralność danych opatrzonych tym podpisem w ten sposób, że rozpoznawalne są wszelkie ich zmiany oraz jednoznacznie wskazuje na certyfikat wykorzystywany do weryfikacji tego podpisu.

3. Dane w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym (podpis kwalifikowany) wywołują skutki złożenia oświadczenia woli w formie pisemnej.

4. Podpis łączny wywołuje skutki reprezentacji łącznej na zasadach określonych przez właściwe przepisy, umowę albo statut.

5. Ilekroć przepisy przewidują złożenie podpisu elektronicznego innego niż podpis kwalifikowany, złożenie przez podpisującego podpisu kwalifikowanego jest równoznaczne ze złożeniem podpisu elektronicznego, o których mowa w tych przepisach.

7. Podpis elektroniczny

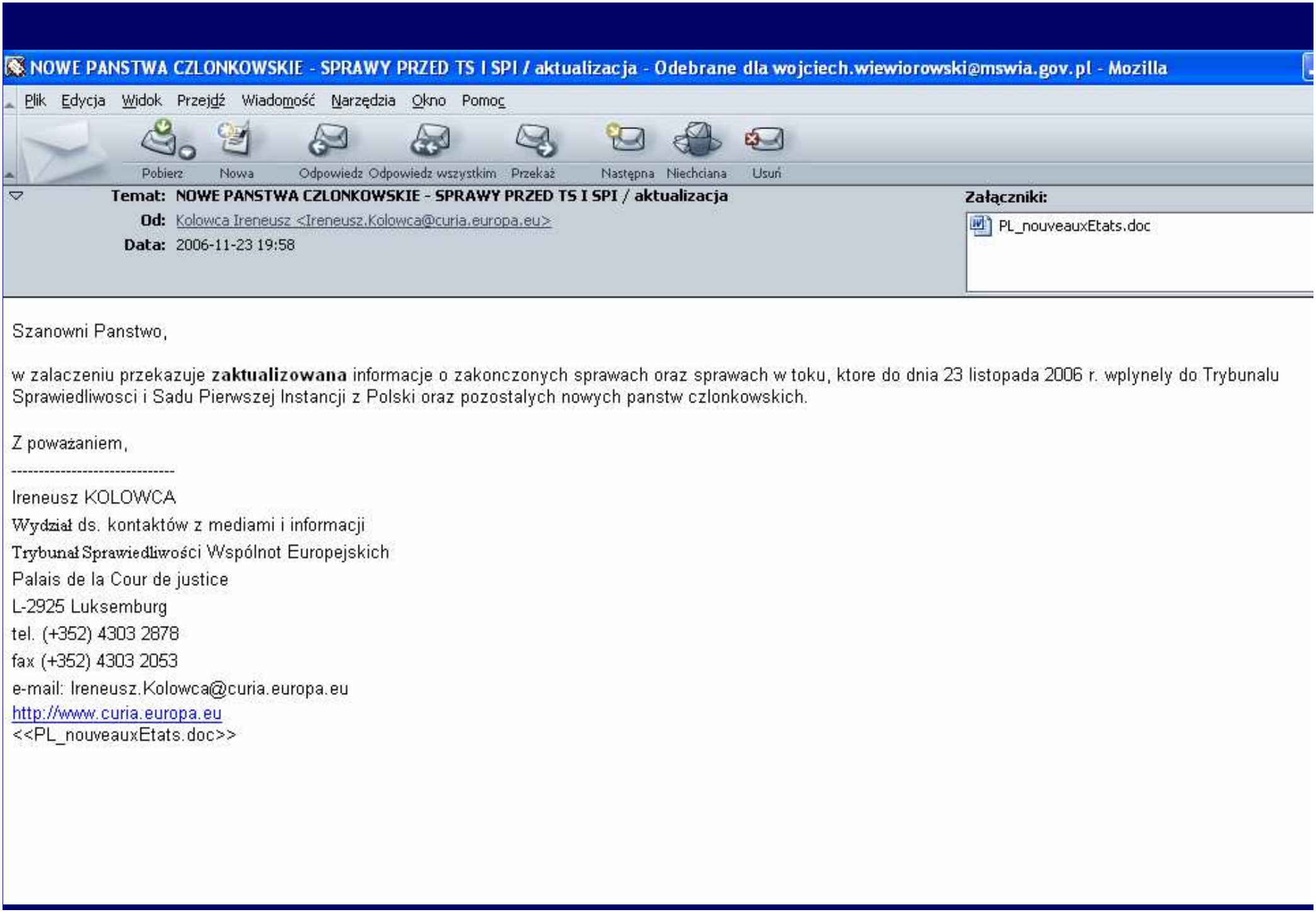
7.3. Rodzaje podpisu elektronicznego

Podpis elektroniczny (zwykły) - aktualnie obowiązująca treść

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,

Podpis elektroniczny (zwykły) - projekt zmiany (stan listopad 2008)

dane w postaci elektronicznej dołączone do innych danych lub z nimi logicznie powiązane i służące jako metoda uwierzytelnienia.


NOWE PANSTWA CZLONKOWSKIE - SPRAWY PRZED TS I SPI / aktualizacja - Odebrane dla wojciech.wiewiorowski@mswia.gov.pl - Mozilla
Plik Edycja Widok Przejdź Wiadomość Narzędzia Okno Pomoc
Pobierz Nowa Odpowiedz Odpowiedz wszystkim Przekaż Następna Niechciana Usuń
Temat: NOWE PANSTWA CZLONKOWSKIE - SPRAWY PRZED TS I SPI / aktualizacja
Od: Kolowca Ireneusz <Ireneusz.Kolowca@curia.europa.eu>
Data: 2006-11-23 19:58
Załączniki:
PL_nouveauxEtats.doc
Szanowni Panstwo,
w zalaczeniu przekazuje zaktualizowana informacje o zakonczonych sprawach oraz sprawach w toku, ktore do dnia 23 listopada 2006 r. wplynely do Trybunalu Sprawiedliwosci i Sadu Pierwszej Instancji z Polski oraz pozostalych nowych panstw czlonkowskich.
Z poważaniem,

Ireneusz KOLOWCA
Wydział ds. kontaktów z mediami i informacji
Trybunał Sprawiedliwości Wspólnot Europejskich
Palais de la Cour de justice
L-2925 Luksemburg
tel. (+352) 4303 2878
fax (+352) 4303 2053
e-mail: Ireneusz.Kolowca@curia.europa.eu
http://www.curia.europa.eu
<<PL_nouveauxEtats.doc>>

Maluchy mile widziane! W godzinach od 18.30 do 21.00 będzie zapewniona opieka i zabawa w sali Jana Sobieskiego, tuż obok nas no i razem z nami.

Bardzo prosimy o potwierdzenie obecności oraz ilości osób do dnia 20 sierpnia 2006 na telefon: Ania [redacted] Jarek [redacted]

Ania i Jarek Panasiuk

7. Podpis elektroniczny

7.3. Rodzaje podpisu elektronicznego

Podpis elektroniczny (zwykły)

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,

Kwalifikowany podpis elektroniczny (bezpieczny)

Podpis elektroniczny, który:

a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,
b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna,

7. Podpis elektroniczny

7.3. Rodzaje podpisu elektronicznego wg projektu ustawy o podpisach elektronicznych

Zaawansowany podpis elektroniczny

podpis elektroniczny przyporządkowany wyłącznie podpisującemu i umożliwiający jego identyfikację, utworzony za pomocą środków, które podpisujący ma pod wyłączną kontrolą i powiązany z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana tych danych jest wykrywalna.

Kwalifikowany podpis elektroniczny

zaawansowany podpis elektroniczny, weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu, złożony za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego.

Podpis urzędowy

zaawansowany podpis elektroniczny składany przez osobę fizyczną, weryfikowany przy pomocy ważnego certyfikatu urzędowego.

Pieczęć elektroniczna

zawansowany podpis elektroniczny składany przez podpisującego niebędącego osobą fizyczną za pomocą bezpiecznego urządzenia do składania podpisu elektronicznego, weryfikowany przy pomocy ważnego certyfikatu systemowego.

7. Podpis elektroniczny

7.4. Podpisujący - Ważna proponowana zmiana

Podpisującym ma być osoba, która działa w imieniu własnym albo w imieniu innych osób fizycznych, osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, posiadająca urządzenie do składania podpisu elektronicznego.

7. Podpis elektroniczny

7.5. Podpis elektroniczny a podpis własnoręczny

Funkcja identyfikacyjna

Funkcja finalizacyjna

Funkcja ostrzegawcza

Funkcja dowodowa

Przypisany do konkretnej osoby

Niemożliwy do podrobienia

Prosty w weryfikacji

Niemożliwy do odrzucenia

Jest funkcją zawartości dokumentu

Wpisany w cały dokument

Może być przesyłany i zachowywany niezależnie od dokumentu

7. Podpis elektroniczny

7.6. Kogo identyfikujemy ? Co umożliwiamy ? Co uwierzytelniamy ?

Autentykacja – ustalenie danych osoby,

Autoryzacja – umożliwienie działania w systemie,

Niezaprzeczalność – zaufana strona trzecia,

Podpis urzędowy – planowane rozwiązanie
Bezpieczny, ale opatrzony jedynie urzędowym certyfikatem, a nie certyfikatem kwalifikowanym. Z zasady służy jedynie do kontaktu z podmiotami władzy publicznej.

7. Podpis elektroniczny

7.7. Certyfikacja

Certyfikat (obecne brzmienie) - elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby,

(Projekt) *- zaświadczenie elektroniczne, za pomocą którego dane do weryfikacji podpisu elektronicznego są przypisywane podpisującemu, umożliwiając jego identyfikację. Jeżeli podpisującym jest osoba fizyczna certyfikat może zawierać jej dane biometryczne.*

Kwalifikowany certyfikat (obecne brzmienie) - certyfikat spełniający warunki określone w ustawie o podpisie elektronicznym, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne

(Projekt) *- certyfikat podpisującego będącego osobą fizyczną, spełniający wymogi określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne w zakresie podpisu elektronicznego (podmiot kwalifikowany).*

7. Podpis elektroniczny

7.8. Podmioty certyfikujące

Kwalifikowany podmiot świadczący usługi certyfikacyjne - podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne

Podmiotem świadczącym usługi certyfikacyjne może być:

1) przedsiębiorca w rozumieniu przepisów o swobodzie działalności gospodarczej,

2) inna osoba prawna,

3) Narodowy Bank Polski oraz organ władzy publicznej

Narodowy Bank Polski oraz organy władzy publicznej nie mogą świadczyć usługi wydawania certyfikatów kwalifikowanych a usługi certyfikacyjne świadczą na zasadach niezarobkowych.

Podmiot kwalifikowany nie może wydawać certyfikatów kwalifikowanych w stosunkach prawnych, w których jest stroną, chyba że jest to niezbędne do wykonywania umowy z odbiorcą usług certyfikacyjnych.

7. Podpis elektroniczny

7.9. Inne rodzaje certyfikatów

Projekt nowej ustawy o podpisach elektronicznych wprowadza do obrotu nowe rodzaje certyfikatów

Certyfikat systemowy

certyfikat przyporządkowany podpisującemu składającemu pieczęć elektroniczną.

Certyfikat urzędowy

certyfikat wystawiony zgodnie z przepisami podpisu urzędowego wydawany wraz z dokumentem tożsamości lub innymi dokumentami identyfikacyjnymi na zasadach określonych w odrębnych przepisach

Certyfikat atrybutów

zaświadczenie elektroniczne powiązane z certyfikatem kwalifikowanym określające, w szczególności uprawnienia osoby wskazanej w certyfikacie.

7. Podpis elektroniczny

7.10. Kryptografia symetryczna

Ten sam klucz używany do kodowania i odkodowywania

- algorytmy strumieniowe i blokowe

Zalety

- *szybkie*
- *jeden klucz*

Wady

- *bezpieczeństwo klucza*
- *różne klucze dla różnych adresatów*
- *duża ilość kluczy do przechowywania*
- *nieuczciwy partner może fałszować nasze dokumenty*

7. Podpis elektroniczny

7.10. Kryptografia symetryczna

Przykład 1 - szyfr podstawieniowy

A = B

B = C

C = D

VOJXFSTZUFU HEBOTLJ

UNIWERSYTET GDANSKI

7. Podpis elektroniczny

7.11. Kryptografia asymetryczna

Klucz publiczny i klucz prywatny

Klucz publiczny - przypisany do osoby ale dostępny dla każdego

Klucz prywatny - przypisany do osoby ale dostępny tylko dla niej

Zalety

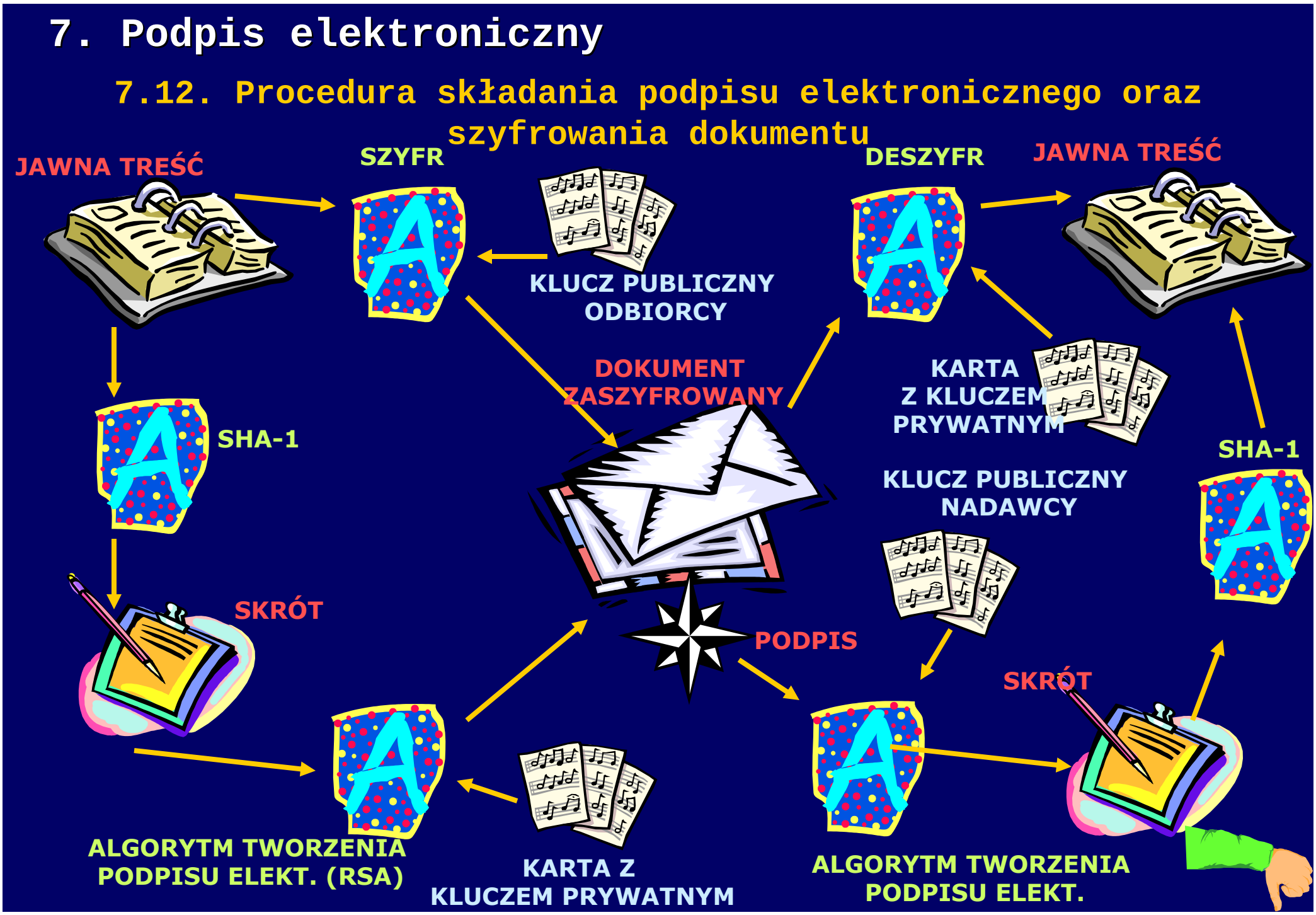
- *zawsze używamy jednej pary kluczy*
- *łatwiejsza ochrona klucza*
- *mniejsza liczba kluczy w obrocie*

Wady

- *mała szybkość szyfrowania*

7. Podpis elektroniczny

7.12. Procedura składania podpisu elektronicznego oraz szyfrowania dokumentu



7. Podpis elektroniczny

7.12. Procedura składania podpisu elektronicznego oraz szyfrowania dokumentu

Wyposażenie użytkownika

Aby składać bezpieczne podpisy elektroniczne należy posiadać:

- **kwalifikowany certyfikat klucza publicznego:**
- **kartę kryptograficzną**
- **czytnik kart kryptograficznych**
- **oprogramowanie**

***) Szczegółowy opis procedury w: P.Rawa, „Podpis elektroniczny w Administracji – aspekty praktyczne", prezentacja Klub KIR w Łodzi 10.IV.2006 r.**

http://www.kir.com.pl/aktualnosci.nsf/e4b4521fa74f550dc12568ce002cbadf/b16a06bfd375b712c125714c004df763?OpenDocument

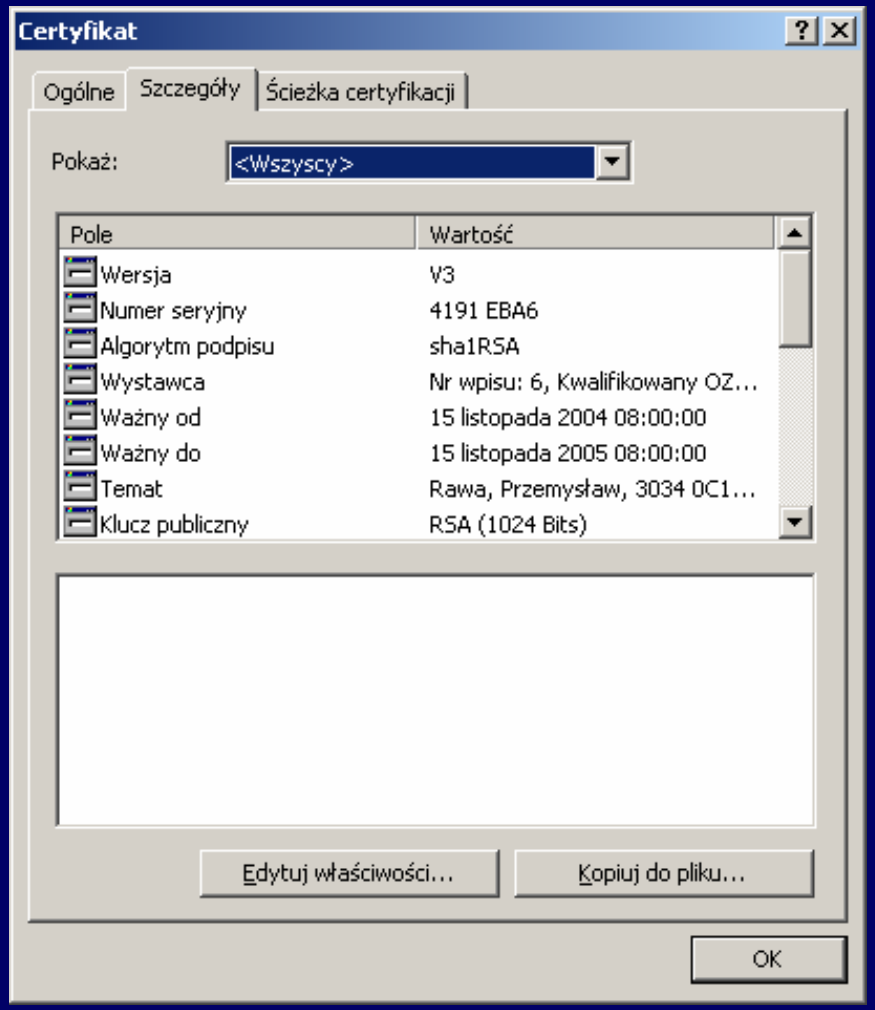
7. Podpis elektroniczny

7.12. Procedura składania podpisu elektronicznego oraz szyfrowania dokumentu

Dane identyfikujące:

- •Imię i nazwisko
- •Nazwa firmy
- •Adres firmy
- •NIP lub PESEL

- **Dane służące do weryfikacji podpisu**
- **Zakres zastosowania**
- **Poświadczenie trzeciej zaufanej strony**



***) Szczegółowy opis procedury w: P.Rawa, „Podpis elektroniczny w Administracji – aspekty praktyczne”, prezentacja Klub KIR w Łodzi 10.IV.2006 r.**

http://www.kir.com.pl/aktualnosci.nsf/e4b4521fa74f550dc12568ce002cbadf/b16a06bfd375b712c12571c004df763?OpenDocument

7. Podpis elektroniczny

7.12. Procedura składania podpisu elektronicznego oraz szyfrowania dokumentu

Wyposażenie użytkownika – karta kryptograficzna

Karta posiada certyfikat bezpieczeństwa: ITSEC E3 high, jako jeden spośród trzech dopuszczonych przez Ustawę.

*) Szczegółowy opis procedury w: P.Rawa, „Podpis elektroniczny w Administracji – aspekty praktyczne”, prezentacja Klub KIR w Łodzi 10.IV.2006 r.

http://www.kir.com.pl/aktualnosci.nsf/e4b4521fa74f550dc12568ce002cbadf/b16a06bfd375b712c12571c004df763?OpenDocument

7. Podpis elektroniczny

7.12. Procedura składania podpisu elektronicznego oraz szyfrowania dokumentu

- Czytnik kart kryptograficznych
  - Pośredniczy w przekazywaniu danych pomiędzy kartą, a oprogramowaniem
  - Różna sposoby podłączenia czytnika do komputera:
    - USB
    - Port szeregowy
    - PCMCIA

*) Szczegółowy opis procedury w: P.Rawa, „Podpis elektroniczny w Administracji – aspekty praktyczne”, prezentacja Klub KIR w Łodzi 10.IV.2006 r.

http://www.kir.com.pl/aktualnosci.nsf/e4b4521fa74f550dc12568ce002cbadf/b16a06bfd375b712c125714c004df763?OpenDocument

7. Podpis elektroniczny

7.12. Procedura składania podpisu elektronicznego oraz szyfrowania dokumentu

- **Oprogramowanie**
  - **Aplikacja SafeDevice - aplikacja do składania i weryfikacji bezpiecznych podpisów (część bezpiecznego urządzenia do składania i weryfikacji podpisów)**
    - **Prezentuje podpisywany dokument**
    - **Prezentuje zawartość certyfikatu użytkownika i odbiorcy**
    - **Sprawdza ważność certyfikatu na listach unieważnionych i zawieszonych certyfikatów**
    - **Posiada deklarację zgodności zgodną z normą PN-EN 45014**

***) Szczegółowy opis procedury w: P.Rawa, „Podpis elektroniczny w Administracji – aspekty praktyczne”, prezentacja Klub KIR w Łodzi 10.IV.2006 r.**

http://www.kir.com.pl/aktualnosci.nsf/e4b4521fa74f550dc12568ce002cbadf/b16a06bfd375b712c12571 4c004df763?OpenDocument

7. Podpis elektroniczny

7.13. Infrastruktura Klucza Publicznego

certyfikat - elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby,

zaświadczenie certyfikacyjne - elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu i które umożliwiają identyfikację tego podmiotu lub organu,

kwalifikowany certyfikat - certyfikat spełniający warunki określone w ustawie, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne, spełniający wymogi określone w ustawie,

7. Podpis elektroniczny

7.13. Infrastruktura Klucza Publicznego

usługi certyfikacyjne - wydawanie certyfikatów, znakowanie czasem lub inne usługi związane z podpisem elektronicznym,

podmiot świadczący usługi certyfikacyjne - przedsiębiorcę w rozumieniu przepisów ustawy z dnia 19 listopada 1999 r. - Prawo działalności gospodarczej Narodowy Bank Polski albo organ władzy publicznej, świadczący co najmniej jedną z usług, o których mowa w pkt 13,

kwalifikowany podmiot świadczący usługi certyfikacyjne - podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,

7. Podpis elektroniczny

7.13. Infrastruktura Klucza Publicznego

Lista podmiotów świadczących usługi certyfikacyjne (stan na dzień 10 kwietnia 2008 r.) - na różowo podmioty wykreślone w 2006 r.)

REJESTR PODMIOTÓW KWALIFIKOWANYCH
ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE

Wpisy uszeregowane pod kątem nazw podmiotów wpisanych do rejestru - uszeregowanych alfabetycznie

Numer wpisu	Nazwa podmiotu	Rodzaj świadczonych usług	Czas dokonania wpisu
6.	KRAJOWA IZBA ROZLICZENIOWA Spółka Akcyjna	Wydawanie kwalifikowanych certyfikatów	21 marca 2003 r., godz. 13:00:00
		Znakowanie czasem	13 września 2005 r., godz. 1:16:00
3.	POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH Spółka Akcyjna	Wydawanie kwalifikowanych certyfikatów	14 lutego 2003 r., godz. 15:00:00
5.	POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH Spółka Akcyjna	Znakowanie czasem	14 marca 2003 r., godz. 15:00:00
4.	TP INTERNET Spółka z ograniczoną odpowiedzialnością	Wydawanie kwalifikowanych certyfikatów	14 lutego 2003 r., godz. 15:30:00
7.	TP INTERNET Spółka z ograniczoną odpowiedzialnością	Znakowanie czasem	17 sierpnia 2004 r., godz. 13:30:00
1.	UNIZETO TECHNOLOGIES Spółka Akcyjna	Wydawanie kwalifikowanych certyfikatów	31 grudnia 2002 r., godz. 12:00:00
		Wydawanie kwalifikowanych certyfikatów atrybutów	13 września 2007 r., godz. 10:00:00
2.	UNIZETO TECHNOLOGIES Spółka Akcyjna	Znakowanie czasem	24 stycznia 2003 r., godz. 12:00:00
		Weryfikowanie statusu certyfikatów w trybie on-line	17 października 2006 r., godz. 12:00:00
		Walidacja danych	17 października 2006 r., godz. 12:00:00
		Poświadczenie odbioru i przedłożenia	17 października 2006 r., godz. 12:00:00
		Poświadczenie depozytowe	5 stycznia 2007 r., godz. 10:00:00
		Poświadczenie rejestrowe i repozytoryjne	5 stycznia 2007 r., godz. 10:00:00

7. Podpis elektroniczny

7.13. Infrastruktura Klucza Publicznego

Projekt nowej ustawy przewiduje utrzymanie krajowego urzędu certyfikacyjnego (czyli tzw. **roota centralnego**). Obowiązek posiadania roota nie wynika bezpośrednio z dyrektywy. Model krajowej infrastruktury klucza publicznego z centralnym rootem upraszcza rozpoznawanie zaufanych certyfikatów za granicą przez wskazanie tylko tego roota zamiast wielu lokalnych certyfikatów samopodpisanych.

Zakłada się wszakże, że oprócz rejestru wprowadzona zostanie czytelna maszynowo lista certyfikatorów.

7. Podpis elektroniczny

7.14. Procedura certyfikacji

Zabezpieczony zbiór dokumentów związanych ze świadczeniem usług certyfikacyjnych

Polityka certyfikacji

Notarialne poświadczenie tożsamości występującego o certyfikat

Kwalifikowany podmiot świadczący usługi certyfikacyjne

Lista zawieszonych certyfikatów

Lista unieważnionych certyfikatów

Warunki użycia certyfikatu

Pisemna zgoda na stosowanie danych zawartych w certyfikacie do weryfikacji podpisu elektronicznego

Pisemne potwierdzenie zapoznania się z warunkami użycia certyfikatu

Pisemna umowa

Kwalifikowany certyfikat

Lista wydanych certyfikatów

Podmiot występujący o kwalifikowany certyfikat

Przykładowy cennik usług

Pracownia Informatyki Prawniczej

Rok akademicki 2008-09

7. Podpis elektroniczny – aspekty prawne

7.15. Znakowanie czasem i data pewna

Art. 7 ust. 2

Znakowanie czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego.

Art. 7 ust. 3

Uważa się, że podpis elektroniczny znakowany czasem przez kwalifikowany podmiot świadczący usługi certyfikacyjne został złożony nie później niż w chwili dokonywania tej usługi. Domniemanie to istnieje do dnia utraty ważności zaświadczenia certyfikacyjnego wykorzystywanego do weryfikacji tego znakowania.

7. Podpis elektroniczny – aspekty prawne

7.15. Znakowanie czasem i data pewna

Usługa polegająca na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę,

Ustawodawca odniósł [...] definicję [znakowania czasem, o której mowa w art. 3 pkt 16 ustawy z 2001 r. o podpisie elektronicznym] jedynie do danych w postaci elektronicznej, które są opatrzone podpisem. Tak więc, mimo iż z technicznego punktu widzenia nie stanowi problemu znakowanie czasem danych, które nie były podpisane elektronicznie, taka usługa nie jest objęta powyższą definicją.

7. Podpis elektroniczny – aspekty prawne

7.15. Znakowanie czasem i data pewna

- Podpis elektroniczny zaświadcza, kto podpisał dany plik
- Natomiast znacznik czasu wystawiony do podpisanej wiadomości informuje, że była ona podpisana przed momentem oznakowania czasem i od tej pory nie dokonywano w niej jakichkolwiek zmian
- Podmiot odpowiedzialny za oznaczanie dokumentów czasem jest nazywamy urzędem znacznika czasu (TSA)
- Protokół znacznika czasu (TSP) został zdefiniowany w standardzie RFC 3161 w 2001 r. przez IETF

- Pierwszym krokiem do oznakowania czasem jest stworzenie skrótu binarnego dokumentu.
- Następnie tworzony jest plik z żądaniem uzyskania znacznika czasu (TSQ)
- Tak utworzone zapytanie przesyłane jest do wskazanego urzędu TSA, w postaci jawnej lub zaszyfrowanej
- Po otrzymaniu pliku z żądaniem mechanizm TSA sprawdza poprawność formatu zapytania.

- Następnie serwer TSA odczytuje aktualną wartość czasu z pewnego źródła czasu i generuje znacznik czasu (*token*) dla danego obiektu.
- Znacznik czasu zawiera unikatowy identyfikator, wartość czasu oznaczenia, dopuszczalny błąd czasu
- Do klienta, który zlecił oznaczenie czasem, odsyłana jest podpisana cyfrowo przez TSA wiadomość.

***) Szczegółowy opis procedury w: K.Ryłko, „Datowanie dokumentów elektronicznych - Urząd znacznika czasu" , CSO Nr 3 z 14.IX.2006 r.,**
wersja elektroniczna: http:///www.idg.pl/artykuly//52790.html

7. Podpis elektroniczny – aspekty prawne

7.16. Akredytacja i uznawanie certyfikatów zagranicznych

Art. 4. *1. Certyfikat, w szczególności certyfikat kwalifikowany, wydany przez podmiot świadczący usługi certyfikacyjne mający siedzibę na obszarze Europejskiego Obszaru Gospodarczego (EOG) jest równoważny certyfikatowi wydanemu na podstawie (…) ustawy [o podpisach elektronicznych.*

2. Certyfikaty wydawane jako kwalifikowane przez podmioty świadczące usługi certyfikacyjne, mające siedzibę w kraju nienależącym do EOG, uznaje się za certyfikaty kwalifikowane w rozumieniu ustawy, jeżeli:

1) podmiot świadczący usługi certyfikacyjne, który wydał certyfikat spełnia wymogi dyrektywy 1999/93/WE i jest akredytowany w określonym w tej dyrektywie systemie akredytacji jednego z państw członkowskich UE lub krajów EOG, albo

2) podmiot świadczący usługi certyfikacyjne, mający siedzibę na obszarze UE, spełniający wymogi dyrektywy (…) udzielił gwarancji na ten certyfikat, albo

3) certyfikat lub podmiot świadczący usługi certyfikacyjne, uznawane są na podstawie umowy dwustronnej lub wielostronnej, zawartej pomiędzy UE i państwami trzecimi albo pomiędzy UE i organizacjami międzynarodowymi.

7. Podpis elektroniczny – aspekty prawne

7.16. Akredytacja i uznawanie certyfikatów zagranicznych

[Z uzasadnienia projektu ustawy o podpisach elektronicznych]

Wprowadzona zmiana art. 4 precyzuje warunki, jakie spełnione zostać muszą dla zrównania pod względem prawnym certyfikatów wydawanych przez podmiot zagraniczny z certyfikatami polskimi. Przepis w nowym brzmieniu rozróżnia uznawanie certyfikatów z państw Europejskiego Obszaru Gospodarczego obowiązanych do stosowania Dyrektywy 99/93/WE oraz tzw. krajów trzecich. Uszczegółowione zostały skutki udzielenia gwarancji za certyfikat zagraniczny. Wprowadzenie precyzyjnych uregulowań w zakresie uznawania zagranicznych podpisów elektronicznych sprzyjać będzie rozwojowi konkurencji na krajowym rynku usług certyfikacyjnych, gdyż możliwe będzie wykorzystywanie certyfikatów wydanych w innych państwach europejskich.