

# Podnoszenie wiarygodności informacji w sieci – usługa pozyskiwania certyfikatów

Piotr Grzybowski  
Radosław Radzikowski



# Agenda

- Wprowadzenie
- Usługa SCS
- Usługa TCS
- Kierunki rozwoju

# Wprowadzenie

- 1994 – Netscape Communications Corporation wprowadza SSL
  - transakcje finansowe w sieci
- PCT (ang. Private Communicating Technology) - Microsoft
- 1996 - IETF (ang. Internet Engineering Task Force) wprowadza TLS
- Elektroniczne certyfikaty
  - CA
  - Serwerowe
  - Osobiste

# Usługa SCS

- Do czego służy usługa SCS ?

Usługa SCS (ang. Server Certificate Service) jest usługą podpisania przez urząd certyfikujący uznany jako zaufany w całej sieci Internet, certyfikatu wygenerowanego przez jednostkę

- Dla kogo jest przeznaczona ?

Usługa jest przeznaczona dla wszystkich instytucji o naukowym profilu działalności, które wykorzystują elektroniczne certyfikaty przy świadczeniu usług w sieci Internet (tj. dla providerów usług)

# CA Roots (SCS)

- GlobalSign Root CA, ważny do 2014 r.
  - Internet Explorer 5.01+, SGC-enabled: “128-bit”, Netscape 4.5+, ActiveX codesigning, Windows 2000+, Pocket PC 2000+, Mac OS 9+, Firefox, Mozilla, Safari, Opera
- GTE CyberTrust Global Root, ważny do 2018 r.
  - Internet Explorer 5.01+, Netscape 4.5+, Java code signing, client auth, Windows 2000+, Pocket PC 2000+, Mac OS 9+, Firefox, Mozilla, Safari, Opera, urządzenia mobilne
- Baltimore CyberTrust Root, ważny do 2025 r.
  - IE 6, NS 6, Windows 2000+, urządzenia mobilne
- Baltimore Mobile Device Root, ważny do 2022 r.
  - Urządzenia mobilne

# Umowa TERENA - PCSS

- Usługa świadczona jest na podstawie umowy pomiędzy PCSS (podpisana 2008) a TERENA gdzie PCSS występuje jako NREN
  - PCSS odpowiada za weryfikację wniosków składanych przez uprawnione instytucje
  - Usługa obejmuje dowolną ilość certyfikatów
  - Odpłatność dokonywana jest ryczałtem
- TERENA na podstawie umowy z CA Root pośredniczy przy świadczeniu usługi
  - aktualnie podpisana jest umowa z GlobalSign

# Zadania PCSS

- Wyznaczenie RA (ang. Registration Authority) administratorów odpowiedzialnych za proces weryfikacji wniosków o podpisanie certyfikatów
- Przygotowanie oraz podpisanie umowy z każdą uprawnioną instytucją, która może składać wnioski
  - weryfikacja organizacji (nazwa...)
  - weryfikacja osób składających wnioski
  - weryfikacja przynależności domen do organizacji
- Umieszczenie elektronicznego formularza do składania wniosków na stronie <https://scs.pionier.gov.pl>
- Prowadzenie oraz przechowywanie dokumentacji dotyczącej wniosków

# Współpraca PCSS z MANami

- Wsparcie MANów w realizacji usługi jest niezbędne ze względu na:
  - dużą liczbę potencjalnych instytucji wnioskujących
  - różny poziom umiejętności i wiedzy technicznej związanej z certyfikatami
  - potrzebę upowszechniania w regionie informacji na temat usługi SCS

# Procedura podpisywania certyfikatów (1)

- Wymagania formalne dla instytucji wnioskującej
  - Podpisanie umowy z NREN, która m.in. będzie zawierać:
    - nazwiska osób uprawnionych do podpisywania wniosków (wnioskujący)
    - listę domen dla których będą składane wnioski o podpisanie certyfikatu
    - dokumenty potwierdzające status instytucji (np. wypis RIN, KRS)

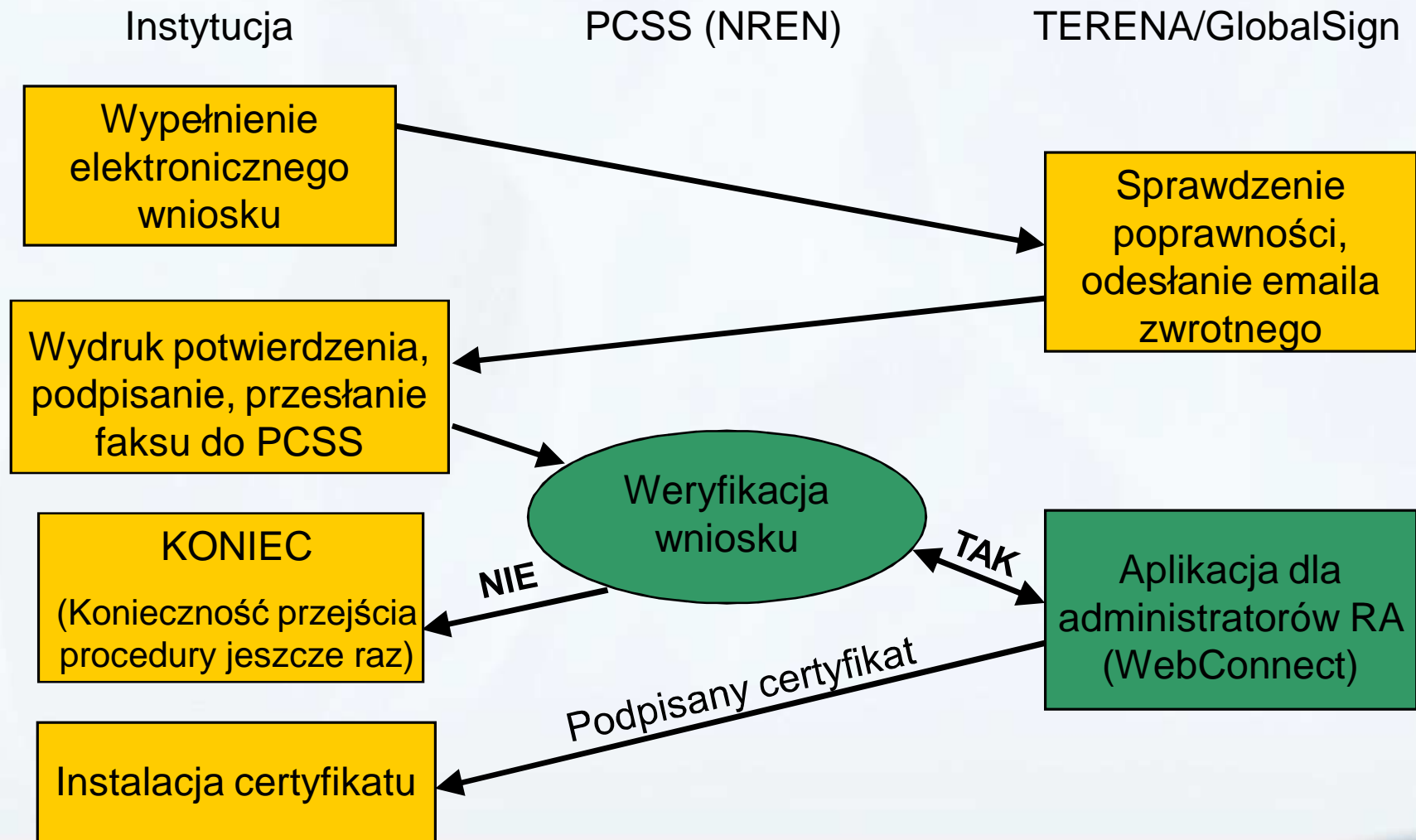
# Procedura podpisywania certyfikatów (2)

- Pozyskiwanie certyfikatu dla instytucji
  1. Wypełnienie wniosku na stronie www
    - określenie rodzaju certyfikatu (web server, email server)
    - określenie ważności certyfikatu (1,2,3 lata)
    - wprowadzenie wcześniej wygenerowanego certyfikatu do podpisania
    - wprowadzenie danych kontaktu technicznego usługi na adres którego zostanie wysłany podpisany certyfikat
    - wprowadzenie danych nt. instytucji oraz danych osobowych wnioskującego
    - zatwierdzenie wprowadzonych danych
    - email zwrotny wysyłany do wnioskującego

# Procedura podpisywania certyfikatów (3)

2. Przesłanie do PCSS potwierdzenia złożenia wniosku
  - wydruk zwrotnego emaila,
  - podpisanego przez uprawnioną osobę wnioskującą,
  - przesłanie faksem lub emailem w pliku pdf (skan)
3. Weryfikacja danych po stronie PCSS (RA Administratorzy)
  - pozytywna – zatwierdzenie wniosku
  - negatywna – informacja do wnioskodawcy o powodach
4. Instytucja (administrator) otrzymuje podpisany certyfikat drogą emailową lub informację o odrzuceniu wniosku
  - kontakt techniczny instaluje certyfikat dla usługi w instytucji

# Schemat procedury



# WebConnect

- WebConnect – aplikacja przeznaczona dla RA Administratorów
- Podstawowe funkcje
  - zatwierdzanie wniosków o podpisanie certyfikatów
  - odwoływanie ważności certyfikatów
  - zawieszanie ważności certyfikatów (nie zalecana)
  - określanie statusu wybranych certyfikatów

# Statystyki SCS

- Liczba podpisanych certyfikatów: 425
  - 413 – aktywnych
  - 12 – unieważnionych
- Podział ze względu na rodzaj
  - TLS – 317
  - TLS emailserver - 108
- Liczba podpisanych umów: 38

# Statystyki SCS

Uniwersytet Warszawski	87	Uniwersytet w Białymstoku	7
Uniwersytet Mikołaja Kopernika w Toruniu	57	Akademia Ekonomiczna w Katowicach	5
Politechnika Śląska	40	Uniwersytet Śląski	5
PCSS	37	Warszawski Uniwersytet Medyczny	5
Politechnika Wrocławska	27	Instytut Włókiennictwa w Łodzi	4
Politechnika Rzeszowska	21	Szkola Główna Gospodarstwa Wiejskiego w Warszawie	4
Politechnika Białostocka	20	Uniwersytet Rzeszowski	4
Uniwersytet Opolski	20	AWF Katowice	3
Politechnika Radomska	14	Instytut Techniki Gorniczej KOMAG	3
NASK	13	Uniwersytet Warmińsko Mazurski	3
Politechnika Świętokrzyska	9	Śląski Uniwersytet Medyczny	2
Politechnika Warszawska	9	Politechnika Łódzka	2
Uniwersytet Przyrodniczy we Wrocławiu	8	Biblioteka Kórnicka PAN	1
Akademia Medyczna we Wrocławiu	7	PFBN	1
Akademia Techniczno Humanistyczna w Białymstoku	7		

# Usługa TCS

- TCS (ang. TERENA Certificate Service)
- Zmiana dotychczasowego CA
  - nowy dostawca usług dla TERENA – Comodo
- Podpisana umowa TERENA – PCSS (PIONIER) 2009
- Podobne zasady korzystania z usługi

## Usługa TCS c.d.

- Dodatkowe rodzaje certyfikatów
  - wildcard
  - eScience – (zgodne z IGTF) serwerowe i personalne
  - podpisywanie kodu
  - personalne – potwierdzanie nadawcy maila
- Etapowe wprowadzanie usługi
  - przeniesienie do nowego CA istniejących cert.
  - wprowadzenie nowych cert.: multidomain oraz eScience serwerowe

# Kierunki rozwoju

- Uruchomienie TCS - pierwszy etap
- Przeniesienie cert. do nowego CA
- Podpisanie umów na nową usługę
- Wygaszenie usługi SCS
- Wprowadzenie kolejnych certyfikatów usługi TCS

**Dziękuję za uwagę**