

Wdrożenie infrastruktury klucza publicznego (PKI) dla użytkowników sieci PIONIER

Ireneusz Tarnowski

Wrocławskie Centrum Sieciowo-Superkomputerowe
Poznań, 4 listopada 2009

Plan wystąpienia

PKI – Infrastruktura Klucza Prywatnego

Zastosowania certyfikatów X.509

Jak to działa:

podpis elektroniczny

szyfrowanie

znakowanie czasem

Projekt **Pionier PKI**:

informacje ogólne

cel projektu

zakres działania

etapy prac

przyjęte założenia

wyniki projektu

Usługa TCS

Podsumowanie

PKI – Infrastruktura Klucza Prywatnego

Definicja:

Ogół zagadnień technicznych, operacyjnych i organizacyjnych umożliwiających realizację różnych usług ochrony informacji przy zastosowaniu kryptografii klucza publicznego i certyfikatów klucza publicznego

Budowa PKI:

- ✓ Urząd Rejestracji (RA) - weryfikacja danych użytkownika, a następnie jego rejestracja
- ✓ Urząd Certyfikacji (CA) - wydawanie certyfikatów cyfrowych
- ✓ Repozytoria kluczy, certyfikatów oraz List Unieważnionych Certyfikatów (CRL)

Zastosowania certyfikatów X.509

- ✓ Certyfikaty w infrastrukturze gridów obliczeniowych
- ✓ Certyfikaty w eduroam
- ✓ Certyfikaty w sieciach VPN
- ✓ Certyfikaty w serwerach WWW (SSL)
- ✓ Certyfikaty w serwerach poczty elektronicznej
- ✓ Certyfikaty indywidualne (pracownicy, studenci)
- ✓ Certyfikaty do podpisywania kodu oprogramowania
- ✓ Certyfikaty atrybutów
- ✓ Znacznik czasu
- ✓ DNSSEC
- ✓ Uwierzytelnianie w sieci XMPP

Jak to działa (1)

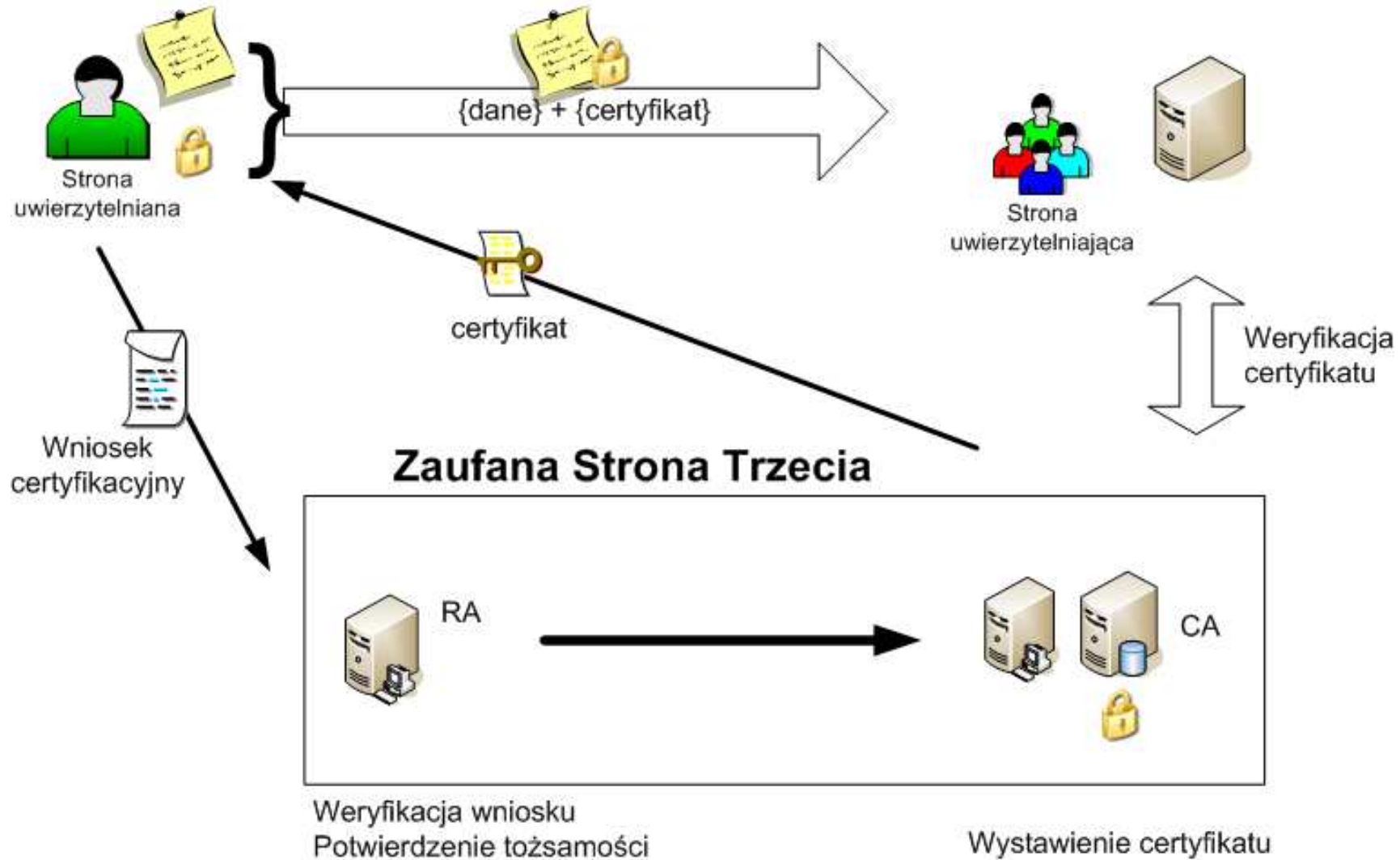
W uwierzytelnianie na podstawie certyfikatów zaangażowane są trzy strony:

- **strona uwierzytelniana**, posiadająca certyfikat wystawiony przez urząd certyfikacji (CA)
- **strona uwierzytelniająca**, uznająca zaufanie CA
- **urząd certyfikacji**, wystawiający certyfikaty (tzw. **Zaufana Strona Trzecia**)

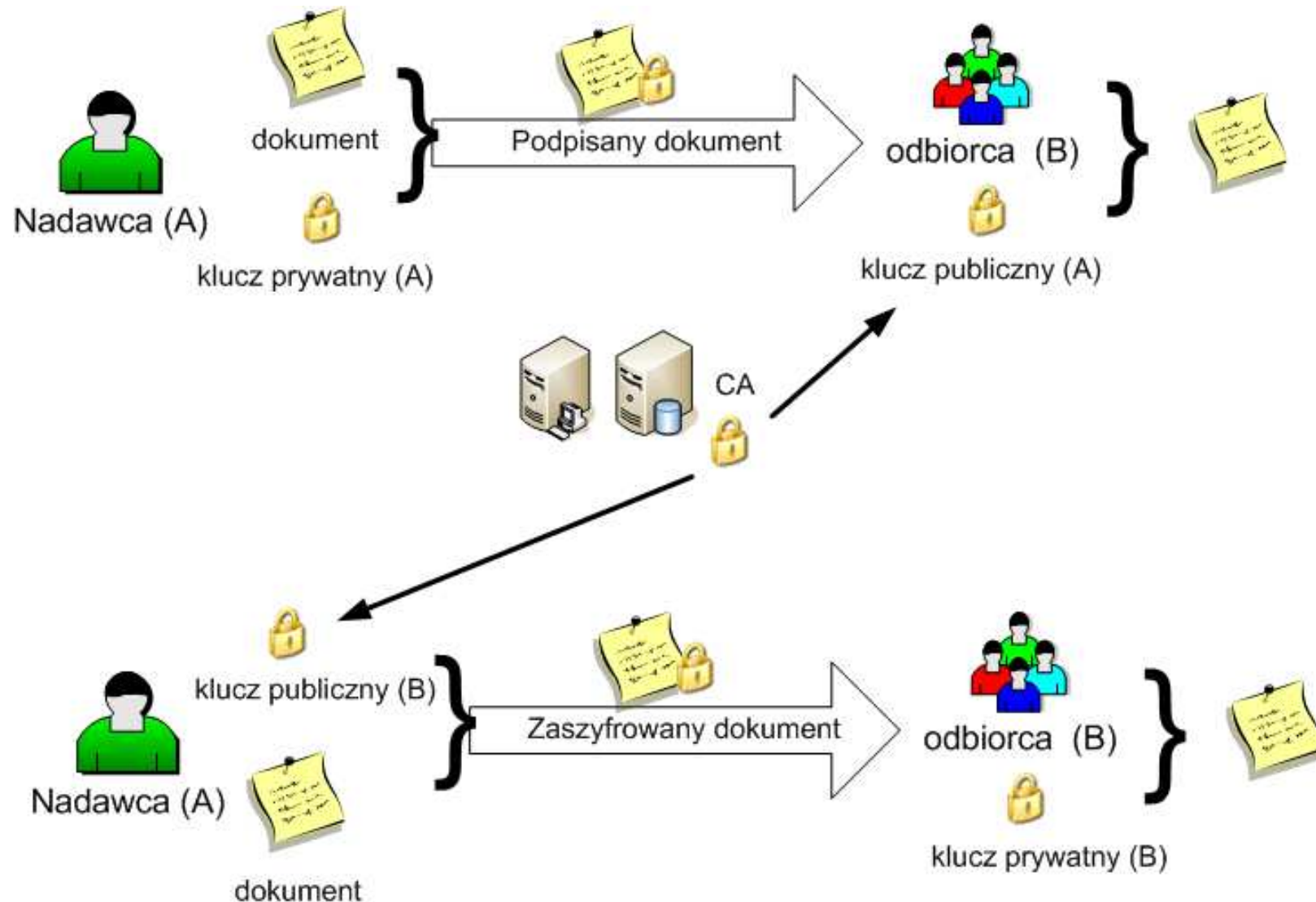
Strona uwierzytelniająca ufa wszystkim mającym ważny certyfikat wystawiony przez uznane za zaufane .

Podstawą działania są **relacje zaufania** między podmiotami.

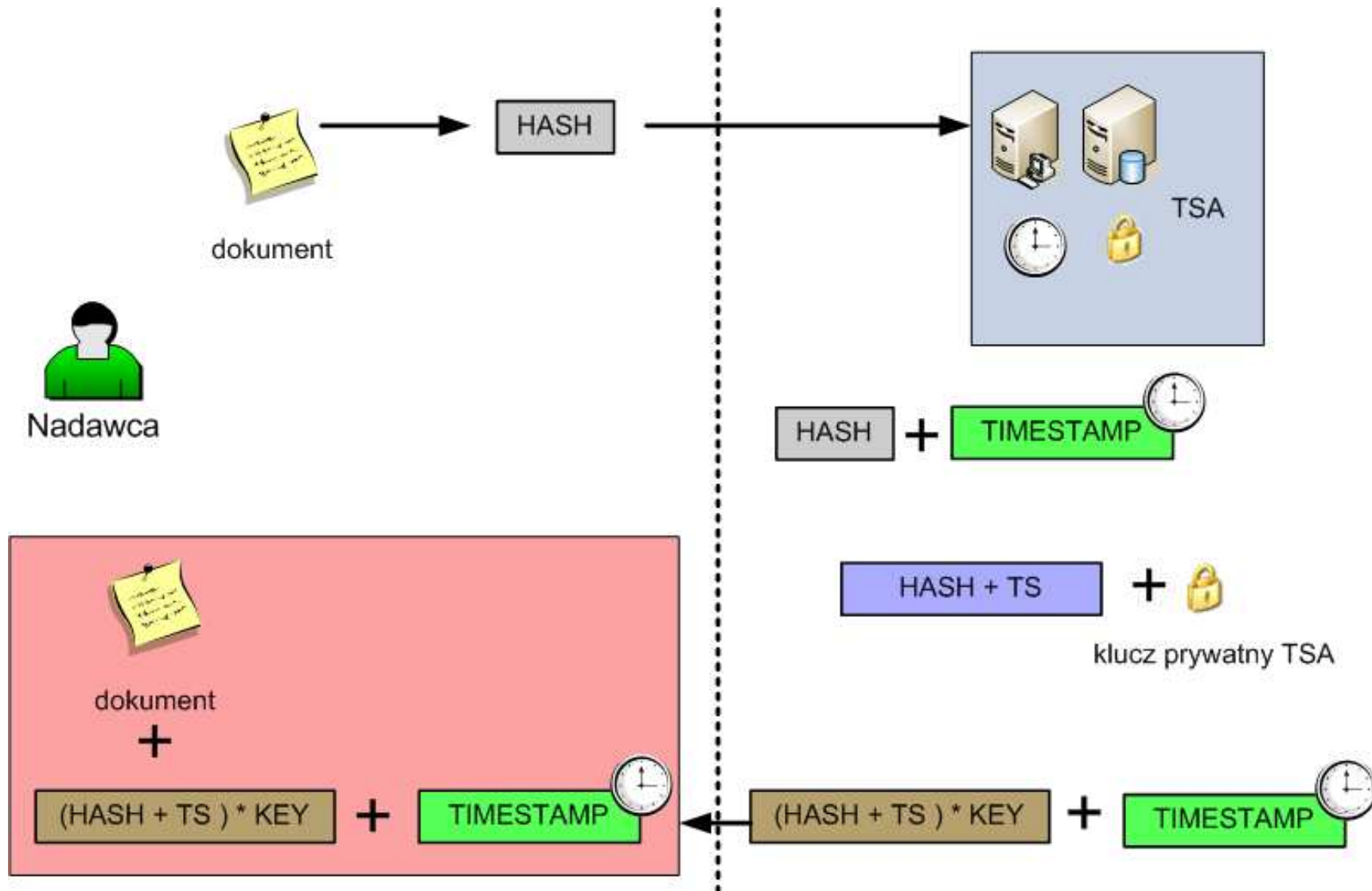
Jak to działa (2)



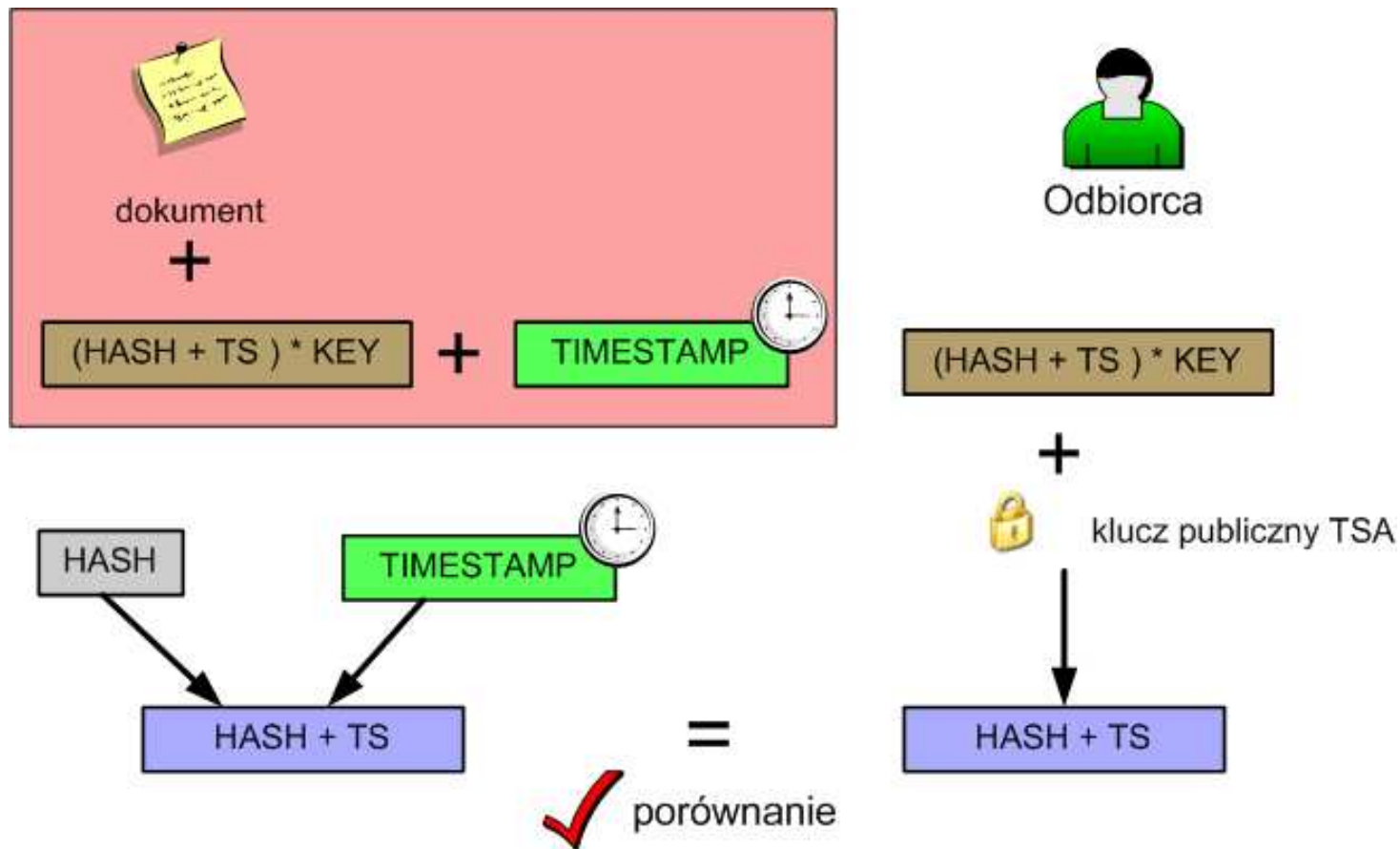
Jak to działa – podpis, szyfrowanie



Jak to działa – znakowanie czasem (1)



Jak to działa – znakowanie czasem (2)



Projekt **Pionier PKI** - informacje ogólne

czas realizacji:

12 miesięcy (1.05.2009 – 30.04.2010)

wykonawcy:

- Wrocławskie Centrum Sieciowo-Superkomputerowe, Wrocław
- Poznańskie Centrum Sieciowo-Superkomputerowe, Poznań
- UCI, Uniwersytet Mikołaja Kopernika, Toruń
- CK, Politechnika Śląska, Gliwice

odbiorcy:

- Pionier PKI będzie świadczyło usługi dla wszystkich użytkowników podłączonych do sieci PIONIER (bezpośrednio lub za pośrednictwem MAN'ow),
- CA wchodzące w skład Pionier PKI nie będzie obsługiwało użytkowników spoza Polski;

ogólnopolski zasięg oddziaływania

Projekt **Pionier PKI** - cel projektu

Projekt **wdrożenia infrastruktury klucza publicznego dla użytkowników sieci PIONIER** ma na celu opracowanie struktury zaufanych centrów certyfikacji dla sieci PIONIER oraz opracowanie jednolitych procedur wystawiania certyfikatów.

- ✓ Projekt ma charakter pilotażowo-wdrożeniowy
- ✓ Projekt ma określić polityki certyfikacji (CP) oraz procedury postępowania certyfikacyjnego
- ✓ Projekt ma dać szkielet Pionier PKI (podstawowa struktura) oraz narzędzia do uruchomienia/tworzenia własnego CA i przyłączenia do Pionier PKI

Projekt **Pionier PKI** - zakres działania

Zadania Pionier PKI:

wystawianie certyfikatów użytkownikom usług obliczeniowych

wystawianie certyfikatów użytkownikom i uczestnikom krajowych i międzynarodowych projektów

wystawianie certyfikatów pracownikom i użytkownikom usług udostępnianych w ramach sieci PIONIER oraz przez uczelnie:

- eduroam

- sieci VPN

- bezpieczny dostęp do usług WWW

- poczta elektroniczna

- systemy biblioteczne

wystawianie certyfikatów dla serwerów usług

Projekt **Pionier PKI** - etapy prac

Zadania dzielą się na:

- ✓ **analityczne** (analiza potrzeb oraz stanu obecnego)
- ✓ **badawczo-rozwojowe** (określenie podstaw teoretycznych dla całego projektu, zdefiniowanie struktury ośrodków CA/RA, ich obszary działania, przestrzenie nazw, powiązania funkcyjne oraz zakresy kompetencji)
- ✓ **wdrożeniowe** (uruchomienie centrów certyfikacyjnych tworzących infrastrukturę klucza publicznego: Root-CA, CA oraz RA)
- ✓ **zadania dokumentacyjne** (raporty z wyników analiz, badań oraz testów oprogramowania, dokumenty zawierające polityki certyfikacji oraz procedury postępowania certyfikacyjnego)

Projekt **Pionier PKI** - przyjęte założenia

Wspólna polityka certyfikacji (CP)

Jednolite procedury dotyczące wystawiania certyfikatów (CPS)

Struktura - tworzone rozwiązanie będzie złożone z:

- nadrzędnego centrum certyfikacji (Root-CA)
- pośrednich centrów certyfikacji (Sub-Root-CA). Sub-Root-CA będzie ustanawiać poziomy zaufania oraz ograniczać zastosowania certyfikatów.
- sieci podległych centrów certyfikacji (CA)
- sieci urzędów rejestracyjnych odpowiedzialnych za weryfikację wniosków o wydanie certyfikatu (RA). RA zostaną rozlokowane możliwie blisko potencjalnych użytkowników.

Pilotażowe włączenie ośrodków certyfikujących (CA) spoza zakresu terytorialnego Root-CA.

Możliwość włączania CA spełniających założenia przyjętych polityk - rozbudowa sieci PKI.

Projekt Pionier PKI - elementy CP (1)

- klucze prywatne dla certyfikatów końcowych muszą mieć długość co najmniej **2048 bitów**, klucze prywatne dla CA muszą mieć długość co najmniej **4096 bitów**,
- nie ograniczać od góry długości klucza (mimo wiedzy, że przy zbyt długich kluczach mogą występować kłopoty po stronie aplikacji klienckich),
- nie dopuszcza się używania algorytmów **MD5**, **używanie algorytmu SHA-1 zostanie** ograniczone czasowo, zalecanym algorytmem jest **SHA-2**,
- czas ważności certyfikatu nie może być dłuższy niż 3 lata ,
- niektóre CA będą mogły ustalić w swoich politykach krótszy czas ważności certyfikatu, np. 13 miesięcy (może to być konieczne, by zachować zgodność polityki z wymaganiami organizacji zewnętrznych)
- czas ważności certyfikatu Root CA oraz Sub-Root CA to 20 lat,

Projekt **Pionier PKI** - elementy CP (2)

- ochrona sprzętowa kluczy prywatnych CA, Root-CA,
- każda polityka musi mieć swój OID, OID powinien być publikowany w certyfikacie,
- informacja o odbiorcy usługi (użytkownikowi końcowym) musi być podana w dokumencie Polityki (CP) dla każdego CA oraz Root CA,
- CA wchodzące w skład Pionier PKI nie będzie obsługiwało organizacji wirtualnych,

Projekt **Pionier PKI** - wyniki projektu (1)

Infrastruktura PKI – uruchomienie usług Root-CA, Sub-Root-CA, sieć CA, sieć RA

Usługa TSP - Usługa znakowania czasem

Oprogramowanie CA - platforma programowa umożliwiająca uruchomienie kolejnego CA zgodnego z wymaganiami procedur i polityk

trwają testy oprogramowania: EJBCA, OpenCA, OpenXPKI

Portal informacyjny

Projekt **Pionier PKI** - wyniki projektu (2)

OCSP - uruchomienie usługi pozwalającej na sprawdzenie statusu certyfikatu on-line (OCSP, ang. Online Certificate Status Protocol). System OCSP powinien być dla użytkownika przezroczysty wobec infrastruktury sieci centrów certyfikacji (jeden system informacyjny powiązany z wszystkimi centrami).

TRS - jednolity system zgłoszeń problemów wynikających z użytkowania systemu (ang. TRS, Ticket Request System)

Dokumentacja projektu - instrukcje ułatwiające instalację oraz konfigurację oprogramowania dla nowego CA, szczegółowe instrukcje pracy w ramach PKI (instrukcja użytkownika, administratora)

Promocja rozwiązania, szkolenia użytkowników - działania o charakterze informacyjnym, wewnątrz ośrodków uczestniczących w projekcie, jak również podczas konferencji krajowych.

Usługa TCS

TCS (ang. *TERENA Certificate Service*) - usługa pozyskiwania certyfikatu wydanego przez zaufany urząd certyfikacyjny realizowana w ramach TERENA

TCS ma działać od roku 2010 jako kontynuacja usługi SCS (trzymiesięczny okres przejściowy)

zakres zastosowań:

- certyfikaty dla serwerów (gridy, WWW, poczta)
- certyfikaty osobiste (uwierzytelnianie w gridzie, podpisywanie poczty)
- certyfikaty do podpisywania kodu oprogramowania

zaleta:

CA zarejestrowane w systemach operacyjnych oraz przeglądarkach jako zaufane

wada:

konieczność korzystania z istniejących profili certyfikatów i brak wpływu na zawartość poszczególnych profili.

Podsumowanie

Po osiągnięciu celów projektu ...

1. Zwiększenie bezpieczeństwa użytkowników poprzez mechanizmy kryptografii klucza publicznego
2. Użytkownicy sieci PIONIER będą mieli możliwość korzystania ze struktury zaufanych CA w zastosowaniu do swoich usług
3. Użytkownicy (jednostki) będą mogli włączać się do struktury PKI uzyskując status zaufania

Wdrożenie infrastruktury klucza publicznego (PKI) dla użytkowników sieci PIONIER

Ireneusz Tarnowski

Wrocławskie Centrum Sieciowo-Superkomputerowe
Poznań, 4 listopada 2009