

Organizacja wymiany dokumentów elektronicznych w ramach współpracy międzynarodowej

Międzyzdroje, 9 czerwca 2006 r.



ООО «Top-Cross», Rosja

Sergej Murugow



Unizeto Technologies S.A., Polska

Ała Stoliatrowa-Myć, Jerzy Pejaś

Agenda

- **Warunki niezbędne dla wzajemnego uznania rozwiązań PKI.**
- **Rozwiązania i obszar ich zastosowania.**
- **Prawne i techniczne problemy uznawania podpisanych dokumentów elektronicznych.**
- **Koncepcja rozwiązania technicznego przy wymianie międzynarodowej dokumentów elektronicznych.**

Elementy niezbędne

dla wzajemnego uznania rozwiązań PKI

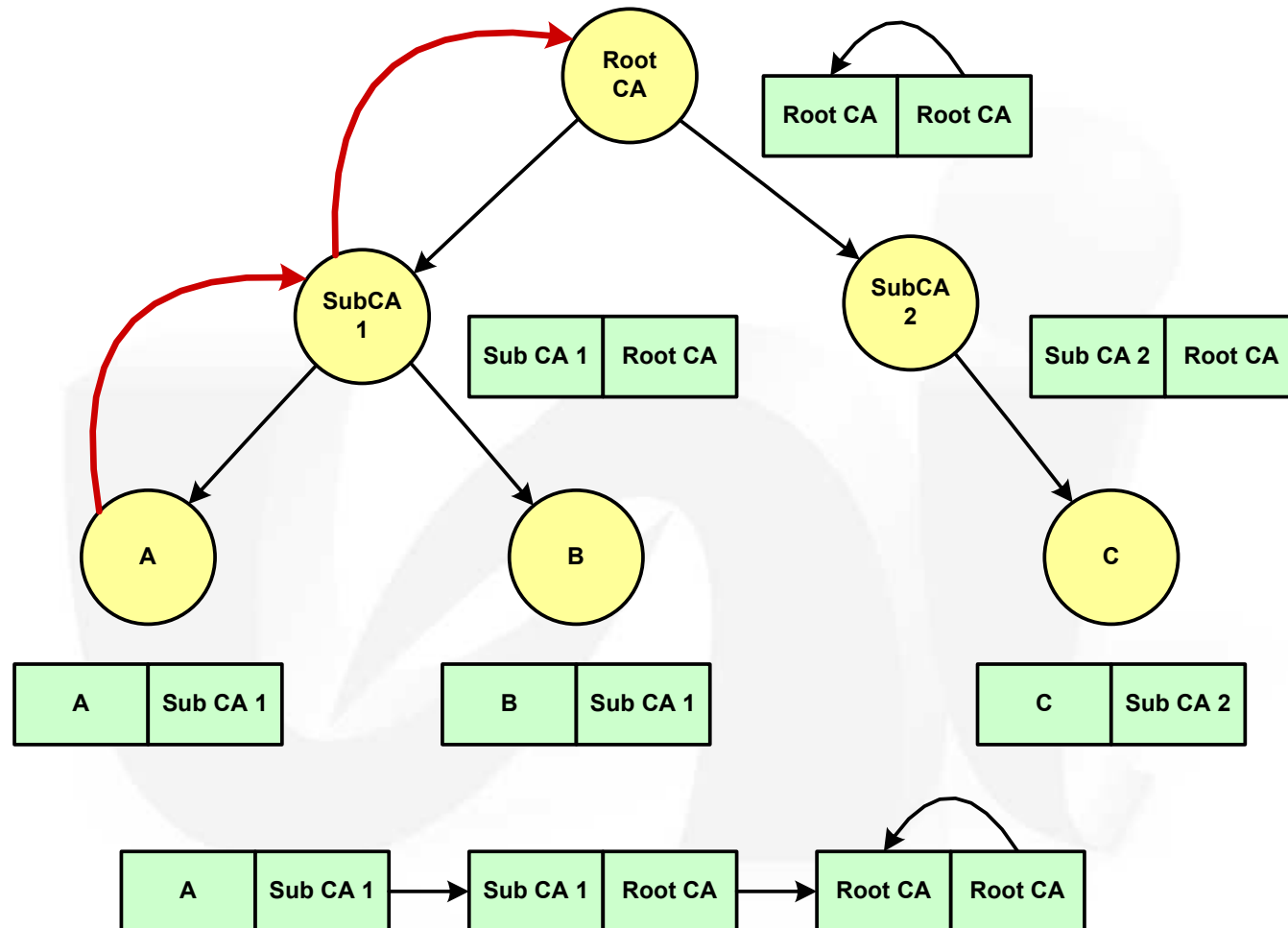
- Zgodność rozwiązań z normami prawnymi
- **Wzajemne zaufanie do stosowanych rozwiązań**
- Zgodność rozwiązań technicznych z odpowiednimi standardami międzynarodowymi (zaleceniami)
- Usługi roamingu w PKI

Podstawowe modele zaufania

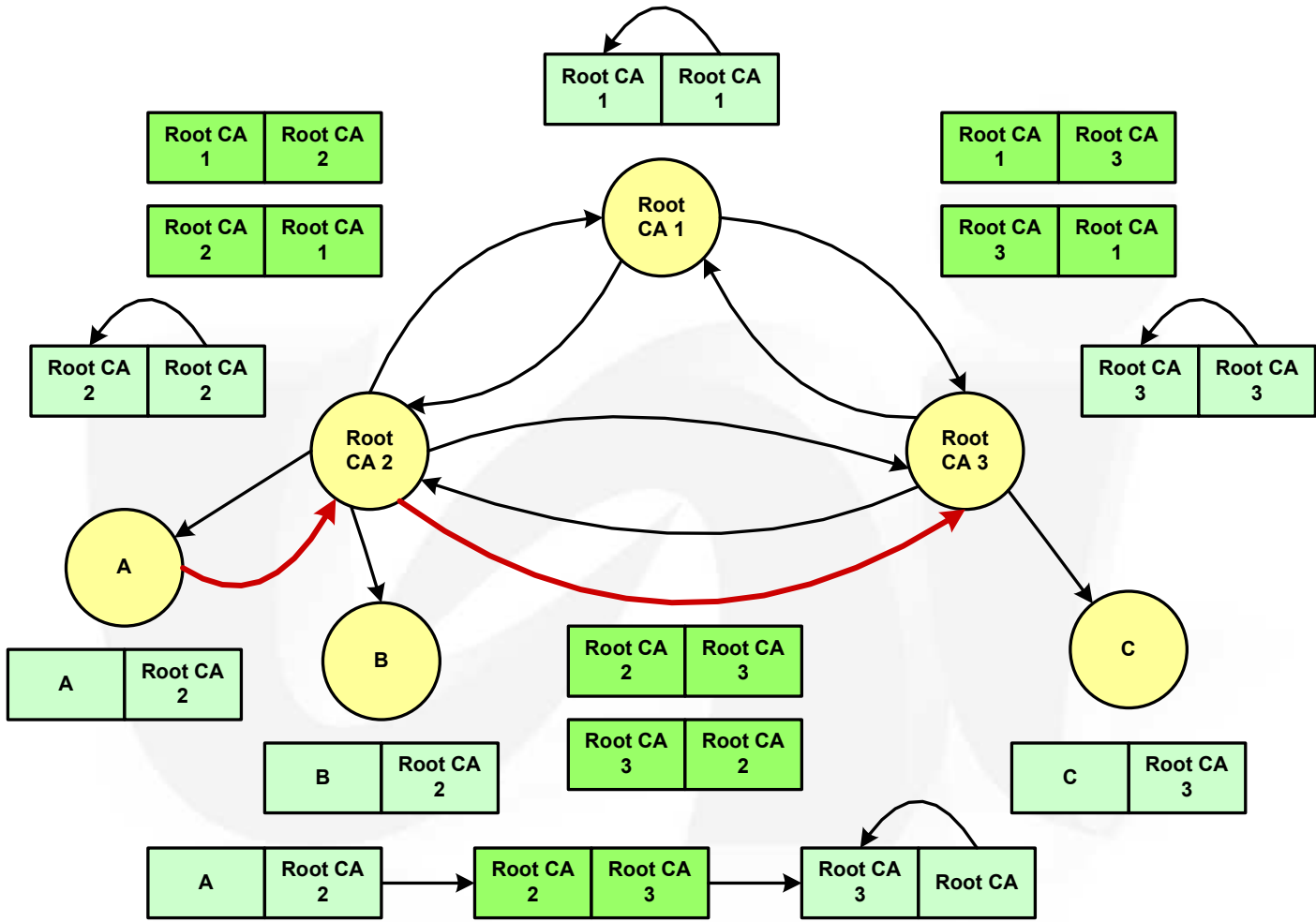
Zdeterminowane modele zaufania

- model hierarchiczny(ang. hierarchical model)
- model sieciowy
- model pomostowy(ang. trust lists)
- listy zaufania (ang. brigade model)

Model hierarchiczny

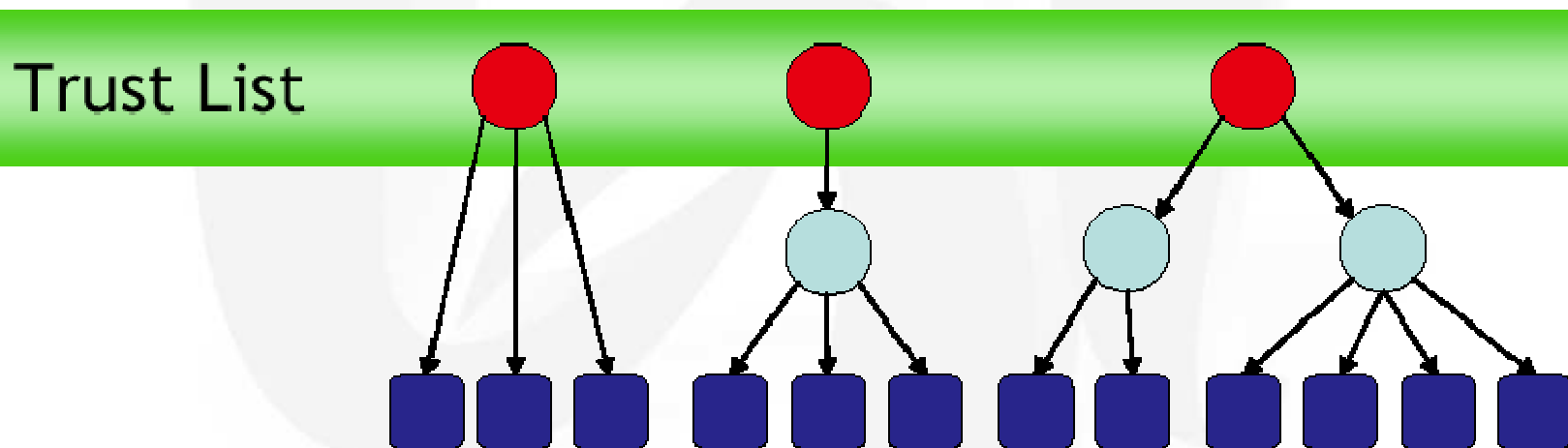


Model sieciowy

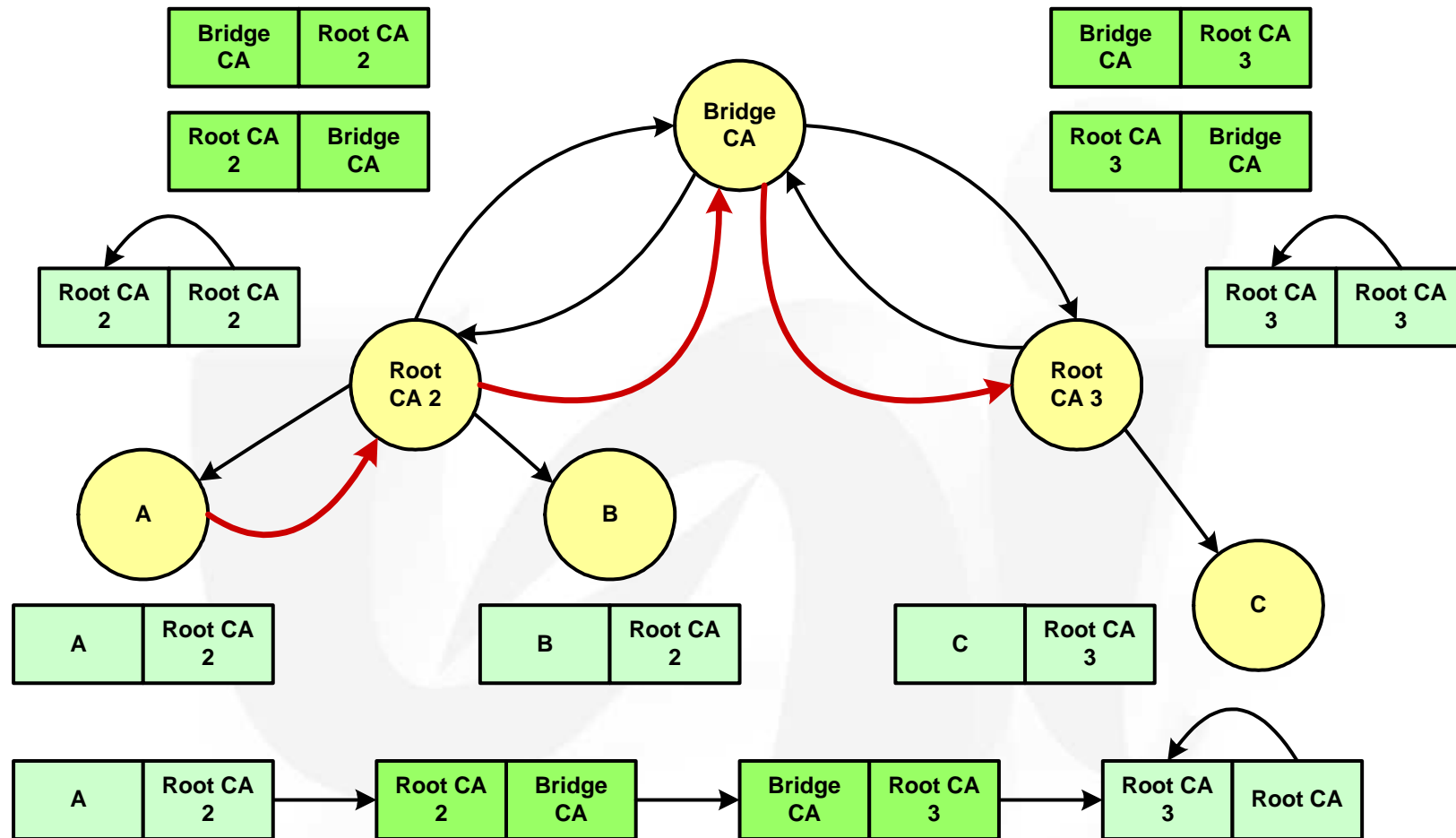


Listy zaufania (ang. trust list)

- Modele hierarchiczne obsługiwane są przez typowe oprogramowanie, modele sieciowe wymagają specjalizowanego oprogramowania
- Listy zaufania pozwalają na zarządzanie wieloma hierarchicznymi modelami CA



Model pomostowy



Realizowane modele pomostowe

- <http://europa.eu.int/idabc> Bridge/Gateway CA – projekt realizowany do 2009 roku, wspierany przez Komisję Europejską w ramach programu ramowego eEurope
W projekcie udział bierze 9 państw: Belgia, Włochy, Niemcy, Finlandia, Czechy, Estonia, Słowacja, Słowenia, Islandia
- www.bridge-ca.org European Bridge-CA – projekt realizowany przez TeleTrust (Niemcy); jest punktem wyjścia do realizacji projektu Bridge/Gateway CA
- Projekt - «Certyfikaty dostępu do usług elektronicznych» (Access Certificates for Electronic Services, ACES, <http://hydra.gsa.gov/aces/>), zainicjowany w 1996 roku Administracją publiczną USA

European Bridge-CA

- **European Bridge-CA jest pierwotnym punktem wymiany zaufania do certyfikatów CA**
- **European Bridge-CA przechowuje certyfikaty partnerskich CA w centralnie zarządzanej i cyfrowo podpisanej liście statusu usług zaufania (ang. trust-service status list, TSL)**

Lista TSL jest udostępniana wszystkim organizacjom afiliowanym w sieci Bridge-CA

- **Podpis Bridge-CA jest wiarygodny, zaś umieszczenie CA na liście jest jednocześnie gwarancją zaufania do tego CA oraz potwierdzeniem jego interoperacyjności**

Listy statusu usług zaufania

- Listy TSL mogą być przydatne w wielu zastosowaniach i środowiskach, gwarantując osiągnięcie szeroko rozumianej interoperacyjności oraz spełnienie różnych wymagań funkcjonalnych i pewności działania
- TSL jest istotnym elementem ustanowienia zaufania w procesie składania i weryfikacji *podpisów elektronicznych*
- Listy zaufania zostały znormalizowane w specyfikacji ETSI TS 102 231

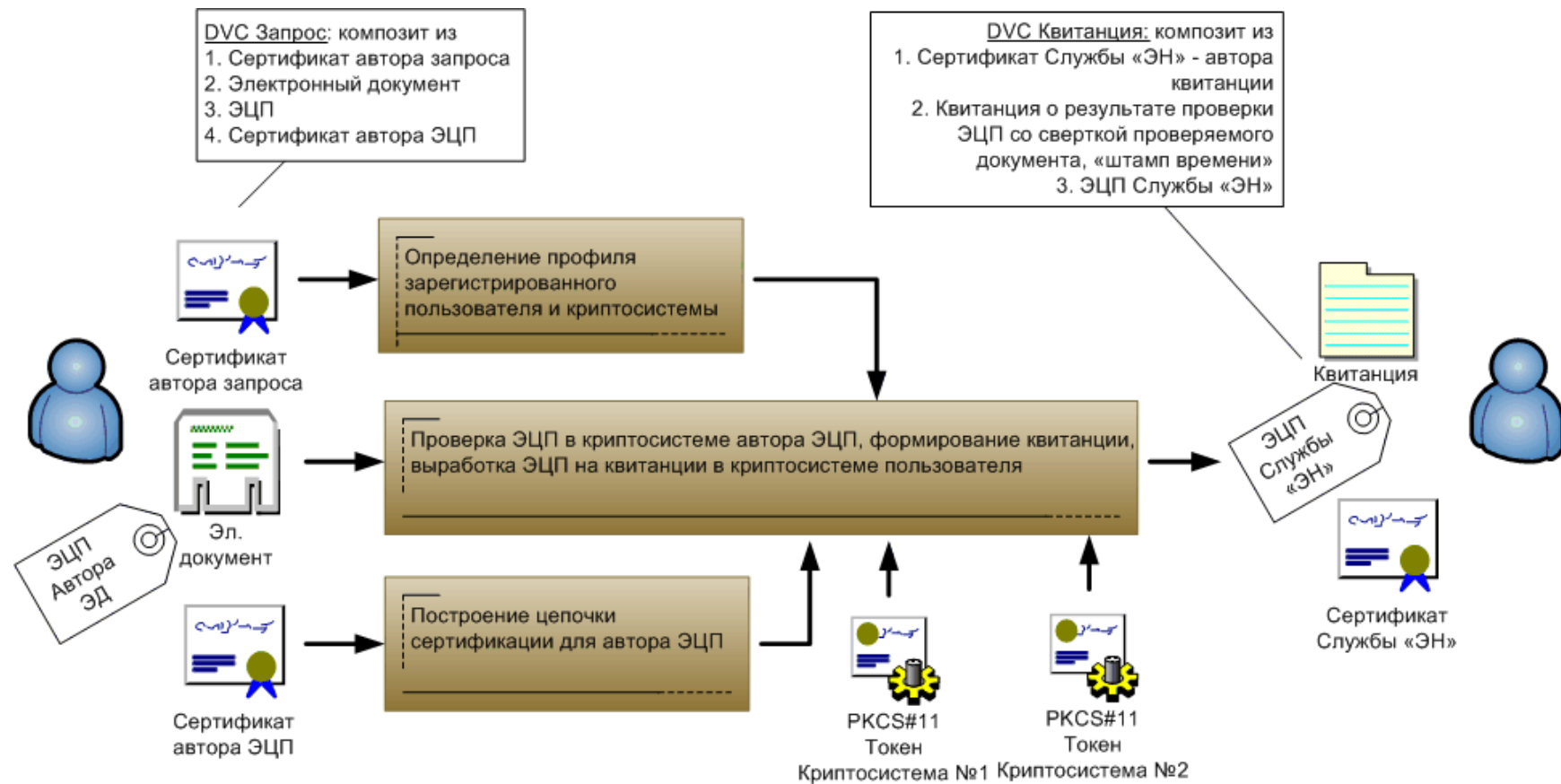
Prawne i techniczne problemy uznawania dokumentów elektronicznych opatrzonych podpisem elektronicznym

- **Zadania międzynarodowej integracji wymagają stworzenia warunków dla wymiany bezpiecznymi dokumentami elektronicznymi**
- **Podmioty wymiany informacyjnej znajdują się w strefach w których stosują lokalne ustawodawstwo określające wzajemnie wykluczające się algorytmy kryptograficzne**
- **Konieczność stworzenia możliwości prawnego uznania i technicznych możliwości weryfikacji podpisanych dokumentów elektronicznych**

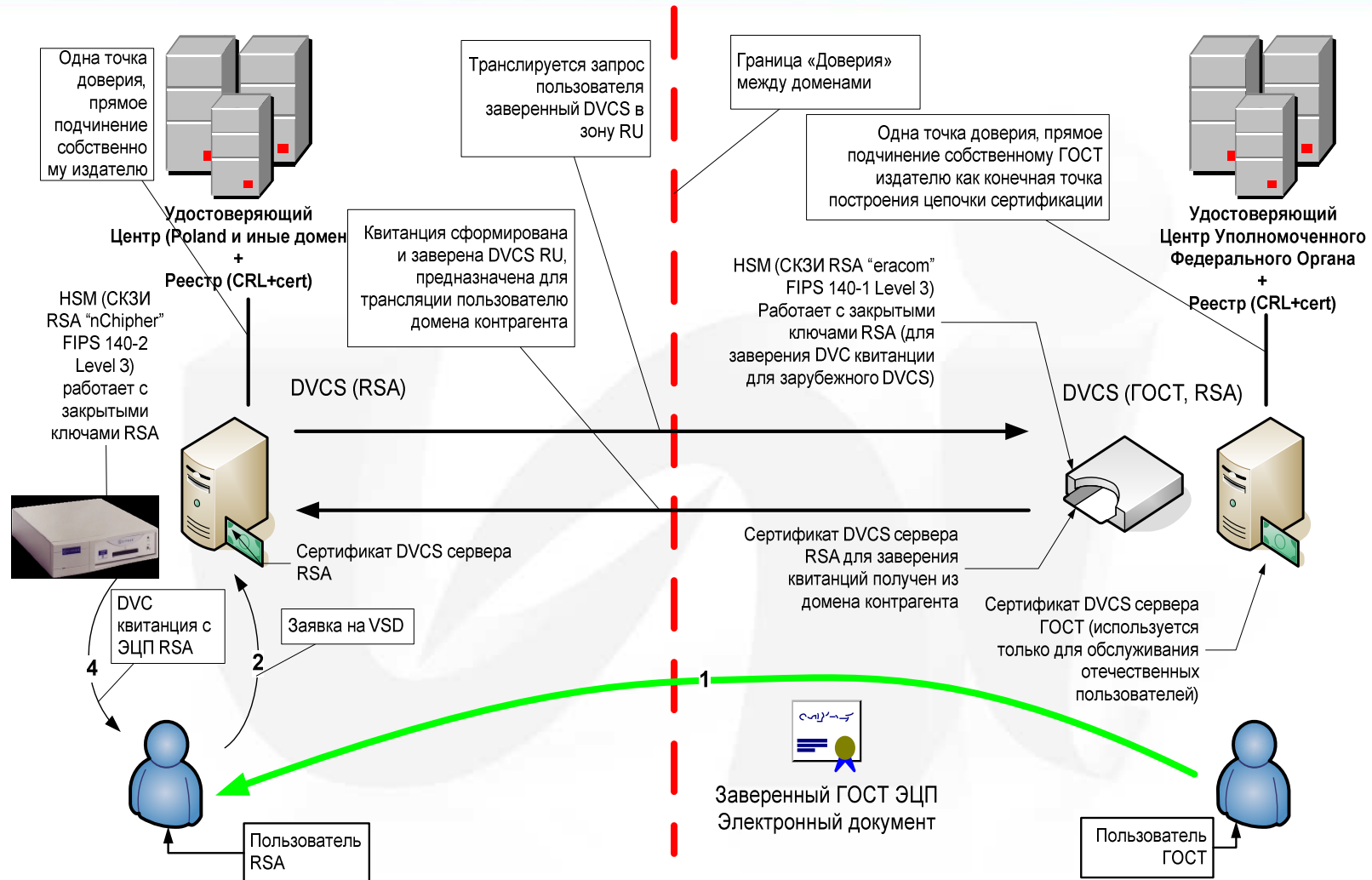
Koncepcja rozwiązania

- Problem może być rozwiązany z wykorzystaniem usług PKI opartych na międzynarodowej normie (zalecenie) RFC 3029-Data Validation and Certification Server
- Uruchomienie usługi «elektronicznego notariatu» w strukturze UFO FR jako zaufanej trzeciej strony da możliwość zrealizowania procedury centralnej weryfikacji podpisu elektronicznego zgodnie z algorytmami kryptograficznymi uczestnika wymiany informacyjnej przy spełnieniu wymogów bezpieczeństwa
- Usługa proCertum DVCS firmy Unizeto Technologies S.A., współpracuje z usługami proCertum OCSP oraz proCertum TSA, stwarza możliwość klientom sprawdzenie podpisu elektronicznego wykonanego zgodnie z polską ustawą o podpisie elektronicznym
- Wynik weryfikacji będzie w postaci poświadczenie elektronicznego zawierającego znacznik czasu oraz podpis urzędu poświadczającego zgodnie z ustawodawstwem odpowiedniego kraju

Schemat rozwiązania



Schemat współpracy



Techniczne cechy rozwiązania

Operacje kryptograficzne wykonywane w PKCS#11 tokenach dla:

ООО «Top Cross», Rosja.

1. Dla zagranicznych algorytmów kryptograficznych RSA:
 - HSM FIPS 140-1 bezpieczny moduł ProtectServer Orange (PSO-rus), producent ООО «ФИННЕТ-СЕРВИС» (<http://www.fnts.ru>) na licencji «Eracom Technologies AG».
 - Network Security Services (NSS) © 1998-2004 The Mozilla Organization. Dany token jest częścią projektu Mozilla.
2. CeXToken © 2005 ООО «Крипто Экс» (<http://www.cryptorex.ru>). Token zawierający biblioteki kryptograficzne posiadające certyfikat ФАПСи/ФСБ, w których realizowane są rosyjskie standardy ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11;

Techniczne cechy rozwiązania

Wykonanie operacji kryptograficznych w PKCS#11 tokenach dla:

Unizeto Technologies S.A. Polska

1. Dla algorytmów kryptograficznych RSA:
 - HSM FIPS 140-2 bezpieczny moduł nShield producent nCipher (<http://www.ncipher.com>)
2. Dla zagranicznych algorytmów kryptograficznych ГОСТ:
 - Weryfikacja podpisu elektronicznego przy wykorzystaniu bibliotek kryptograficznych BouncyCastle

Charakterystyki rozwiązania technicznego

- Omawiane rozwiązanie techniczne daje możliwość wyboru algorytmów kryptograficznych prawnie obowiązujących w danej strefie
- Żądanie i poświadczenie wysyła się z wykorzystaniem protokołu TLS (SSL) z wzajemnym uwierzytelnieniem stron informacyjnej wymiany co zabezpiecza przed wglądem przesyłania informacji
- Automatyczne przedłużenie poświadczeń poprzez zbudowanie wzajemnie powiązanych poświadczeń, które dają możliwość wywnioskować o ważności pierwotnego podpisu elektronicznego po wygaśnięciu ważności certyfikatu kluczy
- Rozwiązanie związane z budowaniem ścieżek certyfikacji zostało przetestowane przez producentów zgodnie z metodyką National Institute of Standards and Technology (NIST).

Literatura

- [PKCS#1] RFC 2437, B. Kaliski, J. Staddon, “PKCS #1: RSA Cryptography Specifications Version 2.0”, October 1998.
- [ГОСТ 28147-89] Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Издательство стандартов, 1996.
- [ГОСТ Р 34.10-94] Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Издательство стандартов, 1994.
- [ГОСТ Р 34.10-2001] Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной подписи. Издательство стандартов, 2001.
- [ГОСТ Р 34.11-94] Информационная технология. Криптографическая защита информации. Функция хэширования. Издательство стандартов, 1994.

Literatura

- [PKCS#11] PKCS #11 v2.20: Cryptographic Token Interface Standard. RSA Laboratories, 28 June 2004.
- [RFC 3280] R. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile”, April 2002.
- [ТК-ИОК-ЭН] «Автоматизированная Система «Электронный Нотариус» «ТК-ЭН» (версия 1.0) Описание применения» , ООО «Топ Кросс», Москва, 2005 г.
- [DVCS] C. Adams, P. Sylvester, M. Zolotarev, R. Zuccherato, “Internet X.509 Public Key Infrastructure. Data Validation and Certification Server Protocols”, RFC 3029, February 2001.
- [TSL] ETSI TS 102 231 Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust Service Provider status information, Technical Specification
- [PKI] Lectures on *Public Key Infrastructure and its Application on .NET platform*, Microsoft Information Security and Technology Training Center, Moscow Engineering Physics Institute (State University), 2004

WYKORZYSTANE ROZWIĄZANIA



ООО «Топ Кросс»
Rosja
www.top-cross.ru
E-mail: info@top-cross.ru



Unizeto Technologies S.A.
Polska
www.unizeto.pl
E-mail: szczecin@unizeto.pl

Pytania?...