

Wdrożenie infrastruktury klucza publicznego w firmie Polkomtel S.A.

Mateusz Kantecki
Polkomtel S.A.

Agenda

- Wymagania biznesowe
- Architektura rozwiązania
- O czym warto pamiętać wdrażając PKI
- Q&A

Agenda

- Wymagania biznesowe
- Architektura rozwiązania
- O czym warto pamiętać wdrażając PKI
- Q&A

Cel projektu

- Podniesienie poziomu bezpieczeństwa infrastruktury IT
- Wprowadzenie podpisu elektronicznego wewnątrz firmy
- Integracja systemów kontroli dostępu do systemów informatycznych i pomieszczeń
- Wdrożenie dla wszystkich pracowników firmy

Zastosowania PKI

- Autoryzacja pracowników w oparciu o wielofunkcyjną kartę mikroprocesorową
 - Logowanie do sieci
 - Kontrola dostępu do pomieszczeń
 - Identyfikator
- Szyfrowanie i podpisywanie danych
 - Poczta (S/MIME)
 - Szyfrowanie danych (Encrypted File System)
 - Podpisywanie wewnętrznych dokumentów
- Kontrola dostępu do sieci LAN
 - Autoryzacja w sieci Wireless poprzez certyfikat X509v3
 - Autoryzacja dostępu do sieci przewodowej (802.1x)
 - VPN

Zarządzanie kartami

- Delegacja procesu wystawiania certyfikatów poza IT
 - HR
 - Wnioski elektroniczne
- Centralne zarządzanie SO PIN
- Możliwość automatyzowanego odblokowania karty przez użytkownika

Zautomatyzowane wystawianie certyfikatów

- Dla użytkowników i komputerów
- Minimalny zaangażowanie użytkownika w proces wystawiania certyfikatów
- Elastyczna polityka zautomatycznego wystawiania / odświeżania dla różnych wzorców certyfikatów

Archiwizacja wybranych kluczy prywatnych

- Klucze użytkownika
 - ✓ Szyfrowanie e-poczty (S/MIME)
 - ✓ Szyfrowanie danych (Encrypted File System)
- Wymagana autoryzacja N z M przy odzyskiwaniu kluczy prywatnych użytkownika

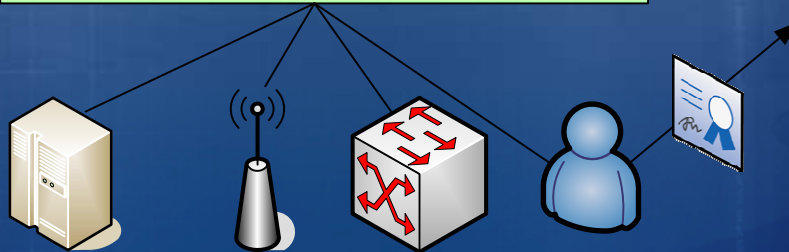
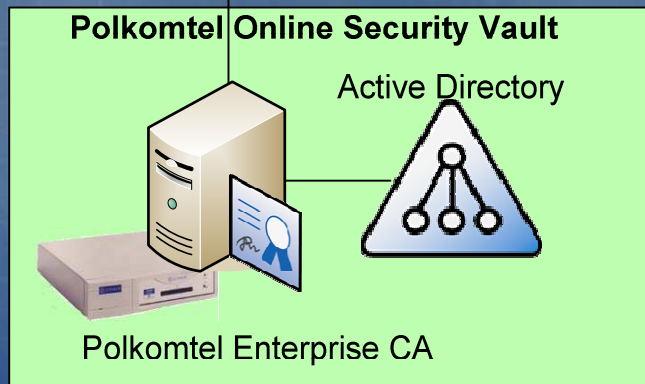
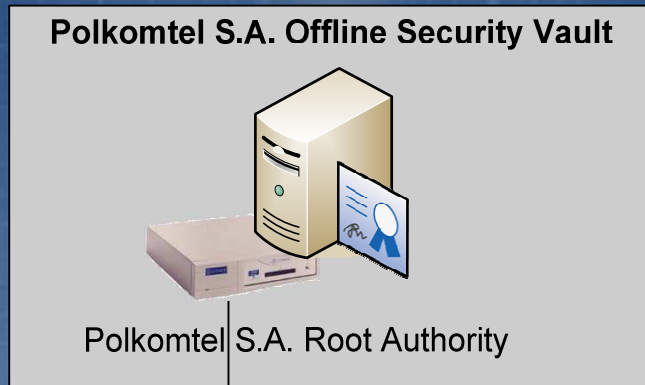
Plus+

Microsoft

Agenda

- Wymagania biznesowe
- Architektura rozwiązania
- O czym warto pamiętać wdrażając PKI
- Q&A

Hierarchia CA



Zautomatyzowany proces wystawiania certyfikatów

- Użytkownik otrzymuje pierwszy certyfikat w dziale HR (SmartCard logon)
- Automatycznie wystawiane certyfikaty
 - do szyfrowania - EFS
 - do podpisywania - S/MIME
- Automatycznie odnawianie certyfikatów
 - Logowanie
 - S/MIME
 - EFS
- Obniżenie kosztów utrzymania PKI

Zarządzanie kartami

- Dane na temat kart składowane są w bazie danych
 - Numer seryjny
 - SO PIN
 - Właściciel
- System zarządzania kartami
 - Odblokowanie karty
 - Zmiana PIN'u
 - Kasowanie zawartości karty

Archiwizacja wybranych kluczy prywatnych

- Archiwizowane klucze
 - ✓ Szyfrowanie e-poczty (S/MIME)
 - ✓ Szyfrowanie danych (EFS)
 - ✗ Podpisywanie e-poczty (S/MIME)
 - ✗ Podpisywanie dokumentów ('podpis elektroniczny')
- Archiwizacja kluczy składowanych na karcie mikroprocesorowej (CSP)
- Autoryzacja N z M przy odzyskiwaniu kluczy prywatnych użytkownika

Monitorowanie PKI

- MOM Management Pack dla MS PKI
- Skrypty monitorujące, uruchamiane w regularnych odstępach czasu
 - Status urzędów CA
 - Dostępność CRL
 - Automatyczne powiadamianie o wygasaniu certyfikatów
 - Użytkowników
 - Urzędzeń
- Automatyczne powiadamianie o wszelkiego typu błędach poprzez SMS/GSM

Agenda

- Wymagania biznesowe
- Architektura rozwiązania
- O czym warto pamiętać wdrażając PKI
- Q&A

„Beyond IT”

- Projekt wymaga udziału wielu działów
- Karty mikroprocesorowe
 - Integracja z systemem kontroli dostępu
 - Wygląd karty
- Aspekty legislacyjne
 - Czym jest podpis elektroniczny (niekwalifikowany)
 - Polityka wykorzystania certyfikatów

Root CA: klucz prywatny

- Długość klucza
 - Root CA: 2048/ 4096
- Ochrona dostępu do klucza CA
 - Moduł HSM
 - Chrysalis-ITS Luna CA3
 - Algorithmic Research
 - AEP
 - Eracom
 - nCipher
- Autoryzacja N z M przy operacjach na CA
 - Zdalna autoryzacja

Kryteria wyboru SmartCard

- ✓ Crypto Service Provider dla Windows
 - ✓ elastyczny dostawca CSP
- ✓ Logowanie do systemu Windows
 - ✓ czas logowania do domeny (od 4 do 40 s)
- ✓ Pojemność >16K (ile certyfikatów)
- ✓ Wielofunkcyjność
 - ✓ Integracja z systemem kontroli dostępu
 - ✓ Nadruk
- ✓ Wsparcie dla archiwizacji klucza prywatnego
- ✓ Wsparcie automatycznego procesu instalacji
- ✓ USB token / karta

Zabezpieczenie / Odtworzenie CA

- PKI 'umiera', jeśli wygaśnie CRL !
- Strategia backupu
 - SystemState (co kilka godzin)
 - Raz dziennie standardowy backup
- Strategia odtwarzania
 - Uszkodzenie HSM
 - Uszkodzenia serwera
 - Co zrobić z wystawionymi certyfikatami w okresie pomiędzy awarią a backup'em ?
- Regularne testy odzyskiwania CA !

Q & A



Microsoft®