Raport

Projekt metod współpracy usługi LDAP z infrastrukturą kluczy publicznych (PKI)

Wbudowanie elementów umożliwiających integrację z europejskim projektem NASTEC

Maciej Dyczkowski

Tomasz Kowal

Agnieszka Kwiecień

WCSS, PWr

Wstęp

Zgodnie z założeniami projektu LDAP użytkownik może przechowywać w bazie wiele adresów email i wiele certyfikatów. Polityka ceryfikacji Polskiego Centrum Certyfikacji EuroPKI zakłada, że publikowane mają być wszystkie certyfikaty: aktualne, poza terminem ważności, unieważnione.

Certyfikaty publikowane są zaraz po wydaniu. Ponieważ większość certyfikatów wydawanych przez Polskie Centrum Certyfikacji EuroPKI, wydawanych jest dla pracowników Politechniki Wrocławskiej, ich certyfikaty mogą być umieszczane w drzewie o=Politechnika Wrocławska,c=PL.

Scenariusze

Opisane tutaj scenariusze definiują sytuacje obsługiwane w ramach tego zadania. Pozwalają one zidentyfikować punkty styku systemów (LDAP, EuroPKI) zaangażowanych w dostarczanie wymaganych funkcjonalności oraz procedury postępowania w konkretnych przypadkach.

Procedury te są ważne szczególnie ze względu na konieczność angażowania wielu aktorów, w tym bezpośrednio użytkownika (rozumianego jako właściciela certyfikatu EuroPKI).

Scenariusz 1

Wydanie nowego certyfikatu.

1. Polskie Centrum Certyfikacji EuroPKI otrzymuje zlecenie certyfikacji od użytkownika z prośbą o Certyfikat oraz wymagane do certyfikacji dokumenty

   (zgłoszenie zawiera m.in. Imię, Nazwisko, adres email, organizację oraz jednostkę organizacyjną dla której wydawany jest certyfikat),

2. Jeżeli dane w zgłoszeniu są poprawne i dokumenty zostaną zweryfikowane poprawnie, certyfikat zostaje wydany,
3. Dodanie certyfikatu do bazy EuroPKI,
4. Dodanie certyfikatu do bazy LDAP.

   Zakłada się, że tylko adres email zawarty w certyfikacie jest elementem niepowtarzalnym, jednoznacznie identyfikującym użytkownika w bazie LDAP.

   > **Notatka:** Wynika to z faktu braku kodowania unicode we Włoskim oprogramowaniu CA Backend i CA Frontend, co powoduje różnice pomiędzy DN w certyfikacie a tym występującym w drzewie LDAP o=Politechnika Wrocławska,c=PL. Obecnie prowadzone są prace nad modifikacją oprogramowania.

   a. przeszukuj bazę LDAP w poszukiwaniu adresu email użytkownika, zawartego w Certyfikacie

      i. jeżeli znajdziesz email w bazie LDAP, dodaj certyfikat i powiadom użytkownika o wydaniu Certyfikatu i dodaniu go do jego danych w bazie LDAP,
      ii. jeżeli nie znajdziesz emaila w bazie LDAP, powiadom użytkownika o wydaniu Certyfikatu i niepowodzeniu w umieszczeniu go w bazie LDAP.

         Mogą być dwie przyczyny niepowodzenia:

         1. nie ma użytkownika w bazie LDAP,

         2.użytkownik nie chce publikować maila, dla którego przyznany jest Certyfikat i nie podał go w ankiecie LDAP.

         W obydwu przypadkach użytkownik może przejść procedurę wypełniania ankiety w celu dodania/modyfikacji wpisu do bazy LDAP i dzieje się to na jego inicjatywę (scenariusz 2).

Scenariusz 2

Użytkownik chce dodać posiadany certyfikat dla niepublikowanego w bazie LDAP adresu email.

1. Użytkownik wypełnia ankietę LDAP odpowiednio aktualizując dane (w tym adres email) i dostarcza je do osoby odpowiedzialnej za aktualizację danych w bazie LDAP
2. Certyfikat dodawany jest do bazy LDAP przy najbliższej aktualizacji certyfikatów (scenariusz 3).

Scenariusz 3

Automatyczna aktualizacja certyfikatów

Zakłada się, że ze względu na politykę bezpieczeństwa (należy odpowiednio szybko aktualizować dane o certyfikatach) automatyczna aktualizacja informacji o certyfikatach wyzwalana będzie czasem (np. `cron`) i przeprowadzana raz dziennie, niezależnie czy i ile certyfikatów w tym czasie zostało wydanych, unieważnionych czy przeterminowało się.

Dla wszystkich certyfikatów (zawartych w nich adresów email) znajdujących się w bazie EuroPKI (wydane, unieważnione, ...) przeszukiwana jest baza LDAP i jeżeli znaleziony zostanie użytkownik z adresem email takim jak zawarty w certyfikacie:

1. Sprawdzony zostanie wpis w bazie LDAP dla tego użytkownika, i w zależności od tego, czy użytkownik posiada już certyfikaty
    a. Użytkownik posiada certyfikaty
        i. Certyfikaty są pobierane z bazy LDAP
        ii. Zostaje dokonane porównanie pobranych certyfikatow z certyfikatem bieżącym
            A. Jeśli taki certyfikat jest już w bazie LDAP operacja jest przerywana
            B. Jeśli nie certyfikat bieżący jest dodawany

    b. Użytkownik nie posiada certyfikatów, certyfikat bieżący jest dodawany do wpisu użytkownika

Scenariusz 4

Poszukiwanie emaila i certyfikatu danego użytkownika.

Szukający przegląda przez interfejs www bazę LDAP i znajduje rekord użytkownika.

Użytkownik posiada kilka adresów email i kilka certyfikatów.

Szukający ma możliwość jednoznacznie wybrać adres email i odpowiadający mu certyfikat.

Szukający ma możliwość przeglądania wszystkich certyfikatów tego użytkownika oraz może rozróżnić certyfikaty ze względu na ich ważność (aktualność).

Zakres prac

Aby spełnić wymagania opisane w scenariuszach potrzebne są prace w następującym zakresie:

1. modyfikacja interfejsu www bazy LDAP w celu wyświetlania informacji o certyfikatach w sposób pełny i jednoznaczny (scenariusz 4)
2. modyfikacja narzędzi PKI aby uwzględniały wstawianie Certyfikatu do bazy LDAP po jego wydaniu (scenariusz 1 punkt 4)
3. stworzenie narzędzia do automatycznej aktualizacji certyfikatów publikowanych w bazie LDAP (scenariusz 3, 2)

Ogólne założenia projektowe:

- Do przechowywania w LDAP informacji o certyfikatach użytkownika zastosowano klasę obiektów `inetOrgPerson`. Certyfikaty składowane są tam jako wartości atrybutu `userCertificate` ze schematu `Core`:

  ```
  attributetype  ( 2.5.4.36 NAME 'userCertificate'
       DESC 'RFC2256: X.509 user certificate, use ;binary'
       SYNTAX 1.3.6.1.4.1.1466.115.121.1.8 )
  ```

- Certyfikaty użytkownika przekazywane są do LDAP w formacie binarnym `der`
- W bazie LDAP przechowywane są certyfikaty wydawane przez EuroPKI. W przypadku wstawienia do bazy certyfikatu podpisanego przez inne CA (*ang. Certificate Authority*) jego ważność będzie nieweryfikowalna.
- Stan w jakim może znajdować się certyfikat przechowywany w bazie LDAP (ze względu na ważność): ważny, poza terminem ważności (nie nabrał ważności lub stracił ważność), unieważniony przez EuroPKI, nieokreślony (nie można zweryfikować ważności certyfikatu).
- Dla potrzeb Polskiego Centrum Certyfikacji EuroPKI zastanie stworzone oddzielne drzewo o=EuroPKI,C=PL (planowana nazwa serwisu ldap.europki.pl) , w którym będą przechowywane:
  - Certyfikat Polskiego Centrum Certyfikacji EuroPKI, obecnie przechowywany w klasie `certificationAuthority`:

    ```
    objectclass ( 2.5.6.16 NAME 'certificationAuthority'
         DESC 'RFC2256: a certificate authority'
         SUP top AUXILIARY
         MUST ( authorityRevocationList $ certificateRevocationList $
               cACertificate ) MAY crossCertificatePair )
    ```

  - bieżąca lista unieważnionych CRL certyfikatów w atrybutach `authorityRevocationList`, `certificateRevocationList` klasy `certificationAuthority`
  - certyfikaty podrzednych urzędów certyfikacji wraz z bieżącą listą unieważnionych certyfikatów CRL przechowywane w klasie jak wyżej

  - docelowo certyfikaty CA będą przechowywane w nowocześniejszej klasie `pkiCA`, jak zostało to opisane w raporcie "Projekt schematu bazy (klasy obiektów, atrybuty) dla potrzeb ogólnopolskiej usługi LDAP:zdefiniowanie dodatkowych klas obiektów i atrybutów wymaganych przez projekt IST NASTEC"

- drzewo o=EuroPKI,C=PL ma zostać wykorzystane jako źródło informacji dla Online Certificate Status Protocoll (OCSP).

Rozszerzenie funkcjonalności interfejsu WWW bazy LDAP

Interfejs WWW zostanie rozszerzony o dwie dodatkowe funkcjonalności:

1. Wyświetlanie listy WAŻNYCH certyfikatów dla każego adresu email danego użytkownika
2. Wyświetlanie listy WSZYSTKICH certyfikatów danego użytkownika

Założenia ad.1:

- ważność certyfikatów użytkownika dla każdego adresu email jest weryfikowana przed wyświetleniem rekordu danych użytkownika (funkcje openssl)
- wyświetlane są tylko ważne certyfikaty dla każdego adresu email użytkownika

Założenia ad.2:

- Lista wszystkich certyfikatów uporządkowana jest według terminów wydania certyfikatów.
- Dla każdego certyfikatu podany jest adres email, dla którego wydany został certyfikat.
- Wyświetlany jest numer seryjny każdego certyfikatu (*ang. Serial Number*), pozwala on na jednoznaczną identyfikację certyfikatu użytkownika, co może być przydatne w przypadku zgłaszania ewentualnych problemów do Centrum Certyfikacji.
- wyświetlany jest termin nabrania ważności i termin utraty ważności każdego certyfikatu, aby wiadomo było w jakim okresie można certyfikatu używać oraz aby właściciel certyfikatu mógł odpowiednio wcześnie zgłosić do Centrum Certyfikacji chęć odnowienia certyfikatu.

Symbole certyfikatów:

Przewiduje się, ze certyfikaty prezentowane będą w formie graficznej, co ułatwi użytkownikowi szybką ocenę stanu ważności każdego z nich.

Powinna istnieć możliwość szybkiego pobrania certyfikatu przez przeglądarkę za pomocą kliknięcia w wybrany symbol.

Przeglądarka powinna natomiast rozpoznawać pobierane dane jako dane certyfikatu.

Tabela 1. symbole certyfikatów

		
ważny	nie można zweryfikować ważności	poza okresem ważności / unieważniony przez EuroPKI

Modyfikacja interfejsu WWW

W celu osiągnięcia zamierzonej funkcjonalności istniejący interfejs WWW (utworzony w PHP) zostanie rozszerzony o poniższe funkcje:

1. pobierającą certyfikaty z bazy LDAP i przetwarzającą je na wewnętrzny format `base64`
2. pobierającą wybrane informacje z certyfikatu (takie jak data ważności czy adres e-mail)
3. weryfikującą ważność certyfikatu
4. wyświetlającą certyfikat z możliwością pobrania go do przeglądarki

Ad. 1:

Certyfikaty w bazie LDAP przechowywane są w formacie binarnym, dlatego do ich pobrania konieczne będzie wykorzystanie odrębnych funkcji php. Dane będą też przekazywane w parametrach GET protokołu HTTP, dlatego celowa wydaje się konwersja tych danych do formatu `base64`.

Ad. 2:

Dane takie jak adres e-mail, numer seryjny lub data ważności są zakodowane w certyfikacie protokołem X509 i mogą zostać odczytane za pomocą odpowiednich funkcji openssl. Pewnych funkcji obsługi certyfikatów dostarcza php-openssl, lecz jest to jeszcze produkt niestabilny i wciąż ma duże braki. Alternatywę stanowią wywołania systemowe komend openssl z odpowiednimi parametrami.

Ad. 3:

Podobnie jak w przypadku funkcji X509, również weryfikacja certyfikatu musi odbywać się z wykorzystaniem wywołań komend systemu operacyjnego. Dodatkowo przewiduje się sprawdzenie, czy numer seryjny certyfikatu nie widnieje na liście cofniętych certyfikatów (CRL) - w takim bowiem przypadku certyfikat zostanie uznany za nieważny.

Ad. 4:

Funkcje wyświetlające certyfikat korzystać będą z opisanych w punkcie 3 metod weryfikacji w celu pobrania odpowiedniego symbolu.