BAZA ADRESOWO-INFORMACYJNA X.500 W POLSKIM ŚRODOWISKU AKADEMICKO-NAUKOWYM

Maja Górecka *Maja.Gorecka@cc.uni.torun.pl*

Tomasz Wolniewicz *twoln@hpc.uni.torun.pl*

Naukowa Akademicka Sieć Komputerowa NASK
Bartycka 18, 00-716 Warszawa

1. Wstęp

Referat jest przekrojowym opisem prowadzonych w ostatnim roku prac, związanych z projektem X.500 w Polsce.

Opracowania *[2], [3]* zawierają podstawowe informacje dotyczące standardu X.500 oraz rozwoju programu X.500 w naszym kraju.

X.500 Directory jest usługą funkcjonującą już blisko pięć lat w polskim Internecie. Prawie od samego początku działalność ta była sponsorowana przez NASK i koordynowana przez toruński zespół administratorów. Dwukrotnie, w 1994 oraz 1996 roku, Komitet Badań Naukowych przyznał Uniwersytetowi Mikołaja Kopernika dofinansowanie na aktualizację bazy X.500. Wsparcie to miało istotne znaczenie dla rozbudowy i popularyzacji X.500 w Polsce.

Do najważniejszych prac przeprowadzonych w ostatnim roku należy zaliczyć:

- aktualizację i rozbudowę zasobów X.500,
- prace nad oprogramowaniem X.500 i uruchomienie polskiego programu dostępowego do zasobów - pomostu X.500-WWW,
- przedstawienie podczas spotkań międzynarodowych propozycji modyfikacji obsługi nazw wielojęzycznych w standardzie X.500,
- zaprojektowanie metod przechowywania kluczy publicznych PGP i certyfikatów PEM w bazie X.500 oraz narzędzi obsługi nowych struktur, realizacja założeń projektu.

Opracowanie zawiera szczegółowy opis powyższych zagadnień.

2. Aktualizacja i rozbudowa zasobów bazy X.500

Zasoby X.500 to typowa baza rozproszona, zarządzana przez ustanowioną sieć serwerów, które obsługują dane lokalne i kontaktują się z pozostałymi serwerami. Serwer, zwany DSA (*Directory Service Agent*) może łączyć się nie tylko z wszystkimi DSA w kraju, ale również z tego rodzaju serwerami na świecie. Ocenia się, że światowa baza X.500 oferuje obecnie około 2 miliony haseł (*entries*), prezentujących dane dotyczące krajów, instytucji różnego poziomu i osób. W światowym projekcie X.500 uczestniczy aktualnie 39 krajów i 5146 instytucji. W Europie program X.500 nosi nazwę NameFLOW Paradise i jest kierowany przez organizację DANTE.

Polska od 1992 roku ma zarejestrowany w strukturze światowej serwer krajowy. Od tego czasu funkcjonuje polski projekt X.500, mający na celu poszerzenie zasięgu serwisu. Przedsięwzięcie obejmuje, jak na razie, wyłącznie instytucje akademickie, docelowo myślimy o współpracy z jednostkami prowadzącymi działalność nienaukową. Co roku zwiększa się ilość informacji zawartej w zasobach polskiej bazy. Prowadzenie ogólnopolskiego *HelpDesku*, pozwala stwierdzić, że znacznie wzrasta zainteresowanie X.500, zgłasza się sporo osób z zamiarem uruchomienia w swojej instytucji serwera, czy dostarczenia aktualnych danych do zasobów X.500.

Dzięki dofinansowaniu, które otrzymaliśmy w 1996 roku z Komitetu Badań Naukowych, możliwa była znaczna poprawa jakości i ilości danych reprezentowanych w X.500 Directory. Powiększyła się ilość regionów uczestniczących w projekcie. Poza Toruniem i dotychczasowymi jego partnerami, tj. Warszawą, Wrocławiem, Poznaniem, Krakowem od 1996 roku są w nim środowiska Gdańska, Łodzi i Szczecina. Rozszerzono zakres zadań przydzielonych regionom, obecnie zarządzają one danymi swojej macierzystej uczelni i opiekują się wszystkimi uczelniami tego regionu (dotychczas danymi wszystkich pozostałych uczelni administrował serwer krajowy). Takie rozwiązanie ma się przyczynić do zwiększenia sprawności uaktualniania danych. Środowiska wcześniej zaangażowane w projekt, szczególnie te, w których istnieją liczne uczelnie wyższe, starają się rozproszyć obsługę bazy, uruchamiane są kolejne DSA (np. w Poznaniu, Wrocławiu). Innym zadaniem postawionym uczestnikom przedsięwzięcia aktualizacji danych było zbudowanie programów narzędziowych służących do tzw. zmasowanego ładowania bazy danych. Chodzi tu o stworzenie mechanizmów pozwalających na automatyczne synchronizowanie zawartość bazy X.500 na podstawie okresowo pozyskiwanych źródeł danych, np. wyciągów z systemu kadrowego.

Polską bazę X.500 cechują specyficzne wymagania. Musi posiadać możliwość przechowywania informacji według prawidłowej polskiej pisowni. Baza pozbawiona tej funkcjonalności znacznie traci na atrakcyjności, a często staje się bezużyteczna. Dlatego troską projektu X.500 od zainicjowania usługi było zagwarantowanie metod wprowadzania, gromadzenia i odczytu danych w języku polskim. Wykorzystano do tego możliwość rozbudowania rodzaju informacji przechowywanej w bazie X.500, polegającą na tym, że poprzez dodanie nowych typów atrybutów rozszerzany jest opis umieszczanych w niej elementów. Takie uzupełnienia zostały zaprojektowane i obowiązują na wszystkich serwerach w Polsce. Administratorzy, w obecnej fazie projektu, wprowadzają do bazy poprawne polskie nazwy.

W 1996 roku, na zlecenie toruńskiego zespołu X.500, Andrzej Adamski z Wydziału Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu przygotował ekspertyzę dotyczącą prawnych aspektów umieszczania informacji osobowych w bazie X.500 (*[1]*). W szczególności opinia porusza problem legalności wprowadzania danych prywatnych, takich jak np. adres i telefon domowy i udostępniania tych informacji w sieci komputerowej Internet. Podstawą analizy prawnej zagadnienia stały się trzy kategorie norm prawnych:

- międzynarodowe standardy normatywne w dziedzinie ochrony danych osobowych,
- obowiązujące w Polsce przepisy prawne określające zakres zbierania danych adresowych, ich wykorzystanie i udostępnianie osobom trzecim,
- rządowy projekt ustawy o ochronie danych osobowych, przesłany do laski marszałkowskiej w dniu 3 października 1996r.

W tym świetle wielostronnie przeanalizowano legalność przedsięwzięcia i losy bazy X.500 po wejściu w życie nowej ustawy. Autor ocenił, że obecna zawartość zasobów X.500 nie jest sprzeczna z obowiązującym prawem, przyznał przy tym, że administrator powinien ograniczyć zakres danych prywatnych, jeśli ich właściciel wyrazi takie życzenie. Ponadto w ekspertyzie

stwierdzono, że prawdopodobnie projektowane normy prawne wymuszą konieczność dostosowania bazy do nowych wymogów, jednak ustawa przewiduje na tego rodzaju czynności adaptacyjne stosunkowo długi okres czasu.

Wśród elementów wskazanych jako potencjalnie możliwe do zakwestionowania są prywatne dane adresowe. Ten rodzaj informacji wprowadzony jest obecnie w niewielkiej części uczelni, większość środowisk zrezygnowała z umieszczania jej w bazie. Należy jednak podkreślić, że w usłudze X.500 określono metody ograniczania dostępu do danych poprzez umieszczanie odpowiednich uprawnień. Zastosowanie tego mechanizmu pozwoli wydzielić informacje oferowane lokalnie od ogólnodostępnych. Kontrolę dostępu definiuje szczegółowo standard X.500'93, wcześniej funkcjonalność ta była zapewniona w oparciu o konkretne implementacje (np. oprogramowanie QUIPU stosuje typ atrybutu `acl`). Nowy standard pozwala znacznie szerzej potraktować zagadnienie nadawania uprawnień do operacji na danych. Wkrótce zamierzamy przeprowadzić odpowiednie testy dotyczące bazy UMK.

Można ocenić, że kolejny rok dofinansowania projektu X.500 przyniósł nam bardzo dużo, stan serwisu i ilość prezentowanej informacji stawia nas na wysokiej pozycji w Europie.

Poniższa tabela prezentuje aktualny stan zasobów bazy X.500:

Region	**Ilość danych**
Kraków	16.596
Warszawa	8.915
Wrocław	8.062
Poznań	9.087
Łódź	6.331
Szczecin	1.917
Gdańsk	7.495
Toruń	4.337
serwer centralny	15.957
Razem	78.697

W części zasoby informacyjne usługi X.500 w Polsce podano adresy uruchamianych przez środowiska interfejsów ogólnego dostępu.

3. Oprogramowanie X.500

3.1. Oprogramowanie podstawowe

Wszystkie serwery dotychczas uczestniczące w projekcie X.500 korzystają z oprogramowania Isode, implementującego standard X.500, ostatnio kilka jednostek zgłosiło zamiar wykorzystywania oprogramowania DEC. Część środowisk pracuje na ogólnodostępnym pakiecie `Isode-8.0` (edycja z 1992 roku), pozostałe uzyskały bezpłatną licencję od Isode Consortium i stosują `ICR2.2v4`.

Wymienione wersje pakietu obsługują standard z 1984 i 1988 roku. Tymczasem dwa lata temu, z opóźnieniem, został opublikowany standard X.500'93. Stanowi on istotny przełom, wprowadza liczne modyfikacje i rozszerzenia, które podnoszą funkcjonalność i efektywność

usługi. Firma *Isode* oferuje od zeszłego roku wersję `ICR3.1` implementującą nowy standard. Jednak począwszy od tej edycji zaniechano polityki udzielania bezpłatnej licencji. Każdy zainteresowany korzystaniem z pakietu jest zobowiązany uiścić roczną subskrypcję. Uniwersytet Mikołaja Kopernika w Toruniu w 1996 wniósł odpowiednią opłatę (wykorzystując zresztą specjalną promocję) i uzyskał dostęp do pakietu `ICR3.1`. Jest to, z naszego punktu widzenia, ważny punkt zwrotny. Od lat prowadzimy prace, które wymagają modyfikacji oprogramowania podstawowego. Dotyczy to obsługi polskich znaków, czyli tabeli *Latin-2*. Isode implementowało dotychczas wyłącznie *Latin-1*. Aby zapewnić umieszczanie w bazie polskich znaków diakrytycznych i móc je następnie prawidłowo przedstawiać przy odczycie informacji konieczne było wniesienie poprawek. W trakcie prac okazało się, że niektóre funkcje obsługi wewnętrznego kodowania informacji w bazie (standardu telekomunikacyjnego T.61) zawierają błędy. Firma Isode przyjmowała informacje o usterkach, akceptowała poprawki, jednak kolejne wersje pozostawały w tej części bez zmian. Jako „konsumenci" bezpłatnej licencji nie posiadaliśmy uprawnień do formalnego zgłaszania raportów technicznych producentowi oprogramowania. Obecnie mamy taką możliwość.

Dostęp do ostatniej wersji oprogramowania (ogłoszono już, że w kwietniu br. pojawi się `ICR4.0`) oznacza także posiadanie implementacji X.500'93. W 1996 roku zgłosiliśmy do DANTE chęć brania udziału w testach nowego standardu. W styczniu 1996 roku Tomasz Wolniewicz uczestniczył, na zaproszenie organizatorów, w spotkaniu mającym na celu specyfikację rodzaju i zakresu testów. Nie mogliśmy niestety dotychczas aktywnie brać udziału w samych testach, ponieważ nie dysponowaliśmy oprogramowaniem. Teraz dołączamy do fazy drugiej, która będzie przeprowadzona w maju tego roku.

Liczymy na to, że inne ośrodki w Polsce zdecydują się na opłatę subskrypcji i będziemy mogli również w kraju prowadzić działalność testową. Należy podkreślić, że różnice pomiędzy standardami '84 i '93 są znaczne, bardzo trudne byłoby gładkie przejście na DSA'93 i niezbędne jest szczegółowe poznanie funkcjonalności nowych serwerów.

3.2. Interfejsy użytkowe

Zasoby informacyjne bazy danych muszą być udostępniane użytkownikom w prosty, wygodny sposób, należy zapewnić efektywność operacji przeszukiwania, listownia, odczytu. Polska baza X.500 musi niezbędnie w poprawny sposób prezentować dane narodowe, nie do przyjęcia jest „obcięcie" znaków diakrytycznych. Wspomniane w poprzednim punkcie modyfikacje oprogramowania podstawowego wiązały się z wprowadzeniem obsługi polskiego alfabetu, kodowania *Latin-2*. Kolejną rzeczą było dostosowanie programów dostępowych (DUA - *Directory User Agent*) do lokalnych potrzeb.

Początkowo prace dotyczyły popularnego interfejsu liniowego `de`. Popularyzacja usługi WWW sprawiła, że powstał *gateway* umożliwiający dostęp do danych z przeglądarki WWW (np. Netscape). Od ponad roku prowadzimy pracę nad polską wersją *gatewaya*, który bazuje na programie `web500gw` autorstwa F. Richtera z Uniwersytetu w Chemnitz (edycja 1.4). Polski *gateway* wykorzystuje przechowywane w bazie rozszerzone informacje (tzw. lokalne atrybuty) i dzięki temu może poprawnie prezentować dane. Poza tym przetłumaczono na język polski wszelkie napisy, komunikaty. Uzyskanie dwujęzyczności *gatewaya* nie mogło obyć się bez napotkania problemów efektywnościowych nowego systemu. Standard X.500 narzuca model strukturalny bazy, w którym identyfikacja obiektu następuje przez ciąg nazw prezentujących jego umiejscowienie w drzewie informacji tworzonym przez zasoby X.500 (DN - *Distinguished Name*). Jako DNów, zgodnie z zaleceniami ogólnoświatowego projektu, należy używać nazw pozbawionych znaków diakrytycznych. W polskiej bazie każde hasło ma nadaną unikalną

wartość atrybutu `polishRDN` (polska wyróżniona nazwa na danym poziomie). Po wyszukaniu interesujących użytkownika informacji w bazie konieczne jest odczytanie atrybutu `polishRDN` nie tylko na bieżącym poziomie, ale również na całej ścieżce drzewa prowadzącej do danego obiektu (np. *Maja Górecka, Dział Eksploatacji Komputerów, Ogólnouczelniany Ośrodek Obliczeniowy, Uniwersytet Mikołaja Kopernika w Toruniu*). Oznacza to znaczny wzrost ilości operacji odczytu. W celu zwiększenia efektywności *gateway* implementuje technikę *cachowania*, nazwy raz odczytane pozostają na pewien czas w pamięci podręcznej i są wykorzystywane przy kolejnych operacjach.

Raport *[6]* zawiera pełen opis prac wykonanych w celu zapewnienia dwujęzyczności usługi X.500.

Gateway został udostępniony uczestnikom projektu w sierpniu 1996 roku i obecnie uruchamia go większość regionów. Ciągle trwają modyfikacje i usprawnienia programu. Program został w stosunku do oryginału znacznie rozbudowany i można uznać, że jego rozwój podąża własną drogą. Zamierzamy jednak wzbogacić nasz program w niektóre, bardzo atrakcyjne cechy najnowszej wersji `web500gw-2.0`. Ponadto planujemy rozbudowę części związanej z modyfikacją danych, tak by zaoferować wygodną metodę aktualizacji danych przez ich właścicieli lub uprawnione do tej roli osoby. Program pozwala już obecnie wyszukiwać klucze publiczne osób, ten fragment, będzie również rozbudowywany.

Adres:

```
http://x500.uni.torun.pl:8888
```

wskazuje na najnowszą wersję oprogramowania polskiego gatewaya, prace nad jego modyfikacją nadal trwają.

4. Polska propozycja modyfikacji X.500 dla potrzeb wielojęzyczności

W czerwcu ubiegłego roku, na spotkaniu administratorów krajowych programu X.500, zostały zaprezentowane nasze rozwiązania służące przechowywaniu polskich nazw w bazie X.500. Przedstawiliśmy także prace nad *gatewayem*, zwracając uwagę na ograniczenia jakie stawia standard X.500 i trudności w zaprojektowaniu w oparciu o niego efektywnego wielojęzycznego systemu. Referat został przyjęty z dużym zainteresowaniem, tym bardziej, że sprawa internacjonalizacji systemów informacyjnych, w tym X.500 jest obecnie tematem projektów europejskich.

Bazy informacyjne, jak X.500 Directory powinny zawierać takie dane, aby możliwe było usatysfakcjonowanie nimi użytkowników lokalnych oraz obcojęzycznych. Dlatego polskie zasoby X.500 gromadzą również nazwy uczelni, czy opisy w języku angielskim. Sam fakt umieszczenia tych informacji w zasobach nie jest wystarczający, muszą istnieć interfejsy użytkowe umiejące wybierać informację zgodnie z życzeniem użytkowników. Te wszystkie aspekty były brane pod uwagę w projektowanym przez nas mechanizmie zapewniającym dwujęzyczność (język polski i angielski) bazy X.500.

Problem ten jest oczywiście dużo szerszy, są kraje wielojęzyczne, jak Szwajcaria czy Belgia, w tej sytuacji projekt nasz wymaga weryfikacji. W referacie, przedstawionym w czasie pobytu na konferencji poświęconej problematyce wielojęzyczności w aspekcie nowego standardu Unicode (Bled, Słowenia, listopad 1996, *CEN/T304 Providing Multilingual support in middleware: Implementing the Universal Character Set ISO 10646 in European Information Society*) *([8])* zaproponowaliśmy rozwiązanie globalne, które opierałoby się na dodaniu kolejnych typów atrybutów, dedykowanych opisom lokalnym. Przyjęto je z zainteresowaniem,

przedstawiciele Danii i Słowenii zadeklarowali chęć uczestniczenia w testach. Praca opisująca szerzej tę propozycję jest w przygotowaniu do publikacji.

Omówione wyżej prace oraz prezentacja ich wyników na spotkaniach międzynarodowych sprawia, że polski projekt X.500 jest widoczny na arenie europejskiej. Od ubiegłego roku jesteśmy również członkami grupy roboczej organizacji TERENA WG-I18N, zajmującej się problemami wielojęzyczności. Mamy nadzieję, że uda nam się uczestniczyć w szerszych projektach związanych z tą tematyką, jak np. MAITS (*Multiligual Application Interface for Telematic Services*).

Należy zaznaczyć, że ostatnio pojawiły się dokumenty prezentujące rozszerzenie standardu X.500'93 dla potrzeb internacjonalizacji (zostaną opublikowane jako X.500'97). Zawierają one uzupełnienia dotyczące redefinicji syntaksu nazw DN, tak aby mogły być wprowadzane wartości atrybutów uzależnione od kontekstu (np. nazwa polska, angielska, francuska). Takie rozwiązanie oznacza, że musi ulec istotnej zmianie oprogramowanie podstawowe i jest zdecydowanie szersze od naszej propozycji, która bazowała na założeniu, że nie jest możliwe ingerowanie w zasadnicze moduły systemu, a całość zmian miała zostać wbudowana wyłącznie w programy dostępowe, aby nie zakłócić poprawnej pracy w przypadku wykorzystywania popularnych interfejsów użytkowych. Implementacja X.500'97 z pewnością nie pojawi się szybko, jeszcze obecnie trwają prace programowe nad poprzednią wersją standardu, a zakres potrzebnych modyfikacji jest szeroki.

5. Zastosowania X.500

5.1. X.500 jako podstawowy system adresowo-informacyjny uczelni

Uniwersytet Mikołaja Kopernika w Toruniu zainicjował działalność X.500 w Polsce. Naszą ambicją jest posiadanie wzorcowo prowadzonych zasobów X.500, zawsze aktualnych, bogatych w informacje. Oprócz podstawowych danych instytucji i osób wprowadzamy dodatkowe opisy, zdjęcia, odsyłacze URL itp. Struktura bazy jest dostosowana do lokalnych potrzeb. Dobrze prowadzona baza X.500 może stać się podstawowym systemem informacyjnym uniwersytetu. Na niektórych uczelniach w Stanach Zjednoczonych funkcjonują takie systemy, w niektórych przypadkach baza X.500 spełnia równocześnie funkcję systemu autoryzującego dostęp do pomieszczeń itp.

Przedstawiony ostatnio władzom UMK projekt przewiduje m.in.:

- utworzenie wygodnych narzędzi aktualizacji zasobów X.500 przez uprawnione osoby,
- oddelegowanie zarządzania danymi do dziekanatów i sekretariatów jednostek uniwersyteckich,
- przygotowanie systemu pozwalającego na produkowanie drukowanych składów osobowych i różnorodnych wyciągów.

Planuje się przygotowanie systemu modyfikacji bazy przez upoważnione osoby oraz dokończenie trwających obecnie prac nad pomostami do innych systemów informacyjnych i bazodanowych.

5.2. Wykorzystanie zasobów X.500 do przechowywania kluczy publicznych i certyfikatów

Nasz ubiegłoroczny referat na konferencji POLMAN poświęcony był problematyce bezpieczeństwa w sieciach komputerowych oraz roli standardu X.500 w tym zagadnieniu (*[7]*). Mówił również o zastosowaniu bazy X.500 do przechowywania certyfikatów i kluczy publicznych PGP. W czerwcu 1996 powstał projekt mający na celu uruchomienie w Polsce systemu stanowiącego podstawę do bezpiecznej wymiany informacji za pomocą udostępniania poświadczonych kluczy publicznych PGP w bazie X.500, przewidziano także wprowadzanie do zasobów bazy certyfikatów PEM (zwane również X.509), które stosowane są w transakcjach operacji WWW. Projekt ten sponsorował NASK i był on realizowany w ramach naszej działalności w Zakładzie Rozproszonych Systemów Informatycznych prof. J. Brzezińskiego.

1. Założenia projektu

Zadanie obejmowało ustalenie mechanizmu certyfikacji kluczy przez wyznaczony urząd nadrzędny, przygotowanie bazy X.500 do przechowywania danych dotyczących kluczy publicznych oraz implementację programów narzędziowych do certyfikacji oraz wprowadzania informacji do X.500.

Zgodnie z zamierzeniami określonymi w naszym raporcie *[4]* ustalono, że wydawaniem poświadczeń zajmować się będzie specjalnie w tym celu powołany Centralny Urząd Certyfikacyjny (w skrócie CUC). Urząd ten poświadcza klucze publiczne otrzymywane ze wszystkich regionów Polski za pośrednictwem wyznaczonych Delegatur. W celu uproszczenia zarówno samego systemu, jak i drogi weryfikacji klucza przez użytkowników, jedynym zadaniem Delegatur jest umożliwienie użytkownikom bezpośredniego kontaktu z Urzędem Certyfikacyjnym. Kontakt taki jest niezbędny przy pierwszej weryfikacji tożsamości użytkownika. Została utworzona struktura administracyjna, rolę CUC pełni zespół toruński, jako Delegatury występują administratorzy regionalni serwerów X.500.

Kolejnym składnikiem systemu jest baza przechowująca certyfikaty. Wykorzystano tu funkcjonującą już w sieci Internet bazę X.500. Gotowe, potwierdzone przez CUC klucze przekazywane są zwrotnie odpowiednim Delegaturom, których zadaniem jest wprowadzenie ich do bazy X.500.

2. Realizacja zadań

W ramach realizacji projektu ustalono zasady wprowadzania do bazy X.500 danych związanych z bezpieczną wymianą informacji. Powstały programy służące do poświadczania dostarczonych przez użytkowników kluczy publicznych oraz narzędzia wspomagające umieszczenie tych danych w bazie X.500.

W celu udostępnienia publicznie danych umożliwiających bezpieczną komunikację do bazy X.500 wprowadzane są następujące informacje:

- klucz publiczny PGP w postaci tekstowej, poświadczony przez Centralny Urząd Certyfikacyjny,
- identyfikator klucza publicznego PGP,
- identyfikator użytkownika klucza publicznego PGP,
- certyfikat w standardzie PEM.

Standard X.500 definiuje postać wprowadzanego certyfikatu, uzupełnienia do standardu (publikowane w ramach *RFC* i *Internet-Drafts*) opisują, w jaki sposób należy gromadzić takie informacje jak np. klucze PGP.

Certyfikaty PEM i PGP korzystają z różnych sposobów identyfikacji użytkownika. W PEM jest to *Distingushed Name*, w PGP przyjęto stosowanie adresu RFC-822. W typowym przypadku użytkownik powinien występować w bazie danych X.500 w ramach instytucji, a zatem posiadać DN, dopuszcza się jednak udostępnianie usługi użytkownikom, którzy nie mogą być w naturalny sposób wprowadzeni do drzewa instytucji. W tym przypadku użytkownikowi nadany zostanie DN będący naturalną transformacją jego adresu *e-mail*.

Na przykład:

`twoln@hpc.uni.torun.pl`

podlega transformacji na:

`dc=pl@dc=torun@dc=uni@dc=hpc@uid=twoln`

Celem projektu jest również zbudowanie oddzielnego poddrzewa w bazie X.500, reprezentującego domeny internetowe. Wydaje się, że najpopularniejszą metodą wyszukiwania kluczy publicznych będzie podawanie adresów *e-mail*. Dlatego najbardziej efektywne jest wprowadzenie gałęzi ustrukturalizowanej zgodnie z domenową postacią Internetu, w której znajdują się wskaźniki do odpowiednich haseł (aliasy). Umożliwi to łatwą transformację adresu *e-mail* na odpowiedni DN w X.500. Gałąź ta będzie jednocześnie wykorzystywana do umieszczania w niej użytkowników, którzy nie mogą zostać zlokalizowani w poddrzewach instytucji.

Raport *[5]* opisuje szczegóły realizacji projektu.

3. Procedura generowania środowiska bezpiecznej wymiany informacji

W celu umieszczenia swoich danych dotyczących bezpieczeństwa w bazie X.500 niezbędne jest wykonanie następujących działań:

⇒ użytkownik generuje samodzielnie klucze PGP (prywatny i publiczny),
⇒ użytkownik przekazuje swojej Delegaturze klucz publiczny w postaci *armor*, Delegatura potwierdza tożsamość klienta,
⇒ Delegatura przekazuje (w środowisku bezpiecznej poczty) zlecenie certyfikacji do Centralnego Urzędu, dane zawierają klucz publiczny poprzedzony nazwą DN identyfikującą użytkownika w hierarchii drzewa X.500,
⇒ Centralny Urząd usuwa z odebranego klucza wszystkie podpisy i sam poświadcza go własnym podpisem, następnie generuje na jego podstawie certyfikat PEMowski i przygotowuje plik w postaci poprawek do bazy X.500,
⇒ Centralny Urząd wysyła przygotowane dane do Delegatury za pośrednictwem bezpiecznej poczty,
⇒ Delegatura wprowadza dane do bazy X.500.

Funkcjonowanie systemu bazuje na następujących programach:

- pakiet PGP - musi nim dysponować osoba generująca swój zestaw kluczy,

- program `pgp2cert`[1], z którego korzysta Urząd Certyfikacyjny,
- przygotowany zestaw skryptów w języku *Perl*, przeznaczonych do wprowadzania przez Delegatury modyfikacji do bazy X.500.

Użytkownik zainteresowany korzystaniem z opisanej usługi bezpiecznej poczty musi mieć dostęp do pakietu PGP, aby wygenerować klucze. Aktualnie pobieranie kluczy publicznych osób, z którymi chcemy korespondować za pomocą bezpiecznej poczty, odbywa się niezależnie, przez wyszukanie ich w bazie X.500, a następnie wpisanie do własnego *keyringu.* Docelowo planujemy zbudowanie interfejsu *e-mail* wykonującego te funkcje transparentnie dla użytkownika.

6. Zasoby informacyjne polskiej usługi X.500

Ogólnopolska strona WWW projektu X.500:

`http://ocelot.uni.torun.pl`

Archiwum FTP:

`ftp://ocelot.uni.torun.pl`

Adresy programów ogólnego dostępu oferowanych przez środowiska prowadzące serwis X.500 w Polsce:

URL	Region
`rlogin://dish@x500.uni.torun.pl` **`rlogin://de@x500.uni.torun.pl`** **`http://x500.uni.torun.pl:8888`**	Toruń
`rlogin://de@x500.pwr.wroc.pl` **`rlogin://sd@x500.pwr.wroc.pl`** **`http://x500.pwr.wroc.pl:8888`**	Wrocław
`http://x500.man.poznan.pl:8887`	Poznań
`http://netman.task.gda.pl:8888`	Gdańsk
`http://x500.icm.edu.pl:8888`	Warszawa
`http://lfs.cyf-kr.edu.pl:8888`	Kraków

[1] Program `pgp2cert` został napisany w oparciu o biblioteki pakietu SecuDE(Security Development Environment). Jest to oprogramowanie rozwijane przez niemiecką organizację GMD, jako zestaw narzędzi programowych wspomagających tworzenie poufnych systemów

7. Literatura

1. Andrzej Adamski *„Prawne aspekty umieszczania informacji osobowych w bazie danych X.500 na tle rządowego projektu ustawy o ochronie danych osobowych”*, grudzień 1996.
2. Maja Górecka, Tomasz Wolniewicz, Jerzy Żenkiewicz, *„X.500 Directory”*, materiały konferencyjne, Miedzeszyn’94, kwiecień 1994.
3. Maja Górecka, Tomasz Wolniewicz, *„X.500 - standard i usługi katalogowe”*, materiały konferencyjne, POLMAN’95, kwiecień 1995.
4. Maja Górecka, Tomasz Wolniewicz, *„Propozycja realizacji usługi bezpiecznej wymiany informacji w sieci Internet w Polsce”*, raport NASK, maj 1996.
5. Maja Górecka, Tomasz Wolniewicz, *„Realizacja usługi bezpiecznej wymiany informacji w sieci Internet w Polsce - stan bieżący”*, raport NASK, październik 1996.
6. Maja Górecka, Tomasz Wolniewicz, *„Dostosowanie bazy X.500 do specyfiki języka lokalnego”*, materiały konferencyjne, Miedzeszyn'96
7. Maja Górecka, Tomasz Wolniewicz, *„Bezpieczeństwo danych w sieciach komputerowych a X.500 Directory”*, materiały konferencyjne, POLMAN'96
8. Maja Górecka, Tomasz Wolniewicz, *„Use of natinal languages in X.500 Directory”*, konferencja robocza *CEN/TC304 Providing Multilingual support in middleware: Implementing the Universal Character Set ISO 10646 in European Information Society*, Bled, Słowenia, listopad 1996.