Infrastruktura kluczy publicznych w polskim środowisku akademicko-naukowym

Maja Górecka-Wolniewicz, Jerzy Żenkiewicz

Uniwersyteckie Centrum Technologii Sieciowych UMK, Toruń

Streszczenie

W artykule dokonano przeglądu technik wspomagających bezpieczeństwo sieciowych systemów komputerowych za pomocą mechanizmów kryptografii asymetrycznej. Przeanalizowano działalność w tym zakresie w środowiskach akademickich w Europie. Wskazano potrzebę stworzenia autonomicznej infrastruktury kluczy publicznych dla potrzeb polskich sieci akademicko-naukowych. Omówiono zadania projektu, którego celem byłoby ustanowienie takiej infrastruktury. Przedstawiono możliwości zastosowania tego typu technologii w różnych serwisach sieciowych.

1 Wprowadzenie

Statystyki wskazują, że bardzo szybko rośnie liczba użytkowników Internetu. Jednocześnie zwiększa się ilość i różnorodność usług sieciowych. Zaawansowane aplikacje dla zapewnienia swojej uniwersalności nie mogą ignorować zagrożeń występujących w sieciowym środowisku pracy. Podstawowe niebezpieczeństwa, które trzeba wziąć pod uwagę, to: fałszywa prezentacja jednej ze stron w celu otrzymania danych przewidzianych dla innego odbiorcy, podsłuchiwanie informacji przesyłanej przez sieć, przechwycenie danych i ich zniszczenie lub zniekształcenie przed dostarczeniem do odbiorcy, albo wyparcie się faktu nadania lub odbioru danych. Początkowo wzmocnieniu poziomu bezpieczeństwa służyła wyłącznie kryptografia symetryczna. Szerokie możliwości w zakresie ochrony sieciowych systemów komputerowych otworzyła kryptografia asymetryczna.

Infrastruktura kluczy publicznych jest niezbędną podstawą w pełni profesjonalnej, bezpiecznej komunikacji sieciowej korzystającej z kryptografii asymetrycznej. Jej ustanowienie w środowisku akademicko-naukowym nie jest jednak zadaniem prostym, wymaga koordynacji, określenia obowiązujących reguł, zagwarantowania, że używane narzędzia będą całkowicie bezpieczne. Trzeba zdefiniować wymagania stawiane urzędom certyfikacyjnym oraz użytkownikom. Konieczne jest zaprojektowanie metod generowania kluczy i przechowywania kluczy publicznych. Muszą zostać opracowane reguły rozgłaszania listy skompromitowanych certyfikatów oraz zasady przedłużania ważności kluczy. Wszystkie te zagadnienia są tematem referatu.

Istnienie infrastruktury kluczy publicznych w środowisku akademickim staje się obecnie nieuchronną potrzebą. Dzięki niej będzie można popularyzować korzystanie z metod kryptografii asymetrycznej, które są już zaimplementowane w wielu powszechnie stosowanych aplikacjach sieciowych, m.in. w usłudze WWW, poczcie elektronicznej, usłudze DNS, a w najbliższym czasie należy spodziewać się nowych zastosowań.

2 Techniki kryptograficzne stosowane w komunikacji sieciowej

2.1 Kryptografia symetryczna

Do połowy lat siedemdziesiątych jedyną znaną metodą wprowadzania poufności w procesie wymiany informacji między dwoma partnerami była kryptografia symetryczna. Technika ta polega na szyfrowaniu przekazywanych danych za pomocą klucza tajnego (*secret key*). Adresat komunikatu może rozszyfrować odebrane dane używając tego samego klucza tajnego. Dopuszcza się również, by klucz odbiorcy powstawał przez prostą transformację klucza nadawcy, nie zmienia to jednak istoty tej techniki, polegającej na tym, że obie strony dysponują identycznym lub prawie takim samym kluczem tajnym. Tego typu podejście wprowadza istotne ograniczenia. Pierwszym z nich jest trudność zainicjowania bezpiecznej komunikacji, gdyż partnerzy muszą najpierw poznać wspólny klucz. Na ogół przekazanie klucza odbywa się drogą niezależną, gwarantującą wymagany poziom bezpieczeństwa. Drugim, niemniej ważnym ograniczeniem jest zła skalowalność systemu opartego na kryptografii symetrycznej. Zasady bezpieczeństwa zalecają, by nie używać tego samego klucza do komunikacji z wieloma partnerami, gdyż zwiększa to potencjalne niebezpieczeństwo, że klucz zabezpieczający dane dostanie się w ręce niepożądanych osób. Teoretycznie do komunikacji z każdym użytkownikiem należy używać odrębnego klucza tajnego. Łatwo sobie wyobrazić wynikające z tego następstwa – duża liczba kluczy utrudnia operowanie nimi. Zaletą kryptografii symetrycznej jest stosunkowo prosta i zajmująca niewielką ilość kodu implementacja jej algorytmów oraz satysfakcjonująca wydajność. Z tego powodu, mimo swoich wad, technika ta jest stosowana w wielu sytuacjach w komunikacji sieciowej, ale w sposób, który ogranicza niebezpieczeństwo przejęcia klucza tajnego przez osoby trzecie.

2.2 Kryptografia asymetryczna

Ogromnym przełomem w dziedzinie kryptografii było zainicjowanie około 1975 roku przez Whitfielda Diffiego i Martina Hellmana nowego kierunku prac. Uczeni ci ogłosili, że jest możliwe stworzenie algorytmów, zgodnie z którymi proces szyfrowania i deszyfrowania byłby realizowany za pomocą dwóch różnych kluczy. Podejście to zostało nazwane szyfrowaniem asymetrycznym. Ta radykalna koncepcja okazała się prawdziwa, od tego czasu powstało wiele szyfrów asymetrycznych i są one tworzone nadal ([1], [16]).

Szyfry asymetryczne korzystają z dwóch różnych, ale zależnych od siebie kluczy. Jeden z tych kluczy jest nazywany publicznym, gdyż może być rozgłaszany oraz przesyłany w sieci i nie stanowi to żadnego zagrożenia dla bezpieczeństwa drugiego klucza pary, prywatnego, który musi być ściśle chroniony. Stąd bierze się nazwa techniki: kryptografia klucza publicznego (*Public Key Cryptography*, PKC). Zależność między dwoma kluczami pary ma charakter matematyczny i opiera się na informacji znanej wyłącznie twórcy klucza. Bezpieczeństwo tej technologii wynika z faktu, że nie jest możliwe, by ktoś inny poza twórcą klucza wyznaczył klucz prywatny na podstawie klucza publicznego.

Ogromną zaletą kryptografii klucza publicznego jest możliwość zastosowania obu kluczy pary zarówno do szyfrowania, jak i deszyfrowania. Drugą ważną własnością jest możliwość rozszerzenia zakresu zastosowań, zaoferowanie innych usług niż szyfrowanie. Wadą jest mała wydajność i rozbudowana implementacja.

2.3 Usługi kryptografii klucza publicznego

Używając techniki kryptografii klucza publicznego można zaszyfrować transmitowane dane kluczem publicznym odbiorcy. Adresat danych jest wówczas jedyną osobą, która może odczytać przekazane dane, gdyż tylko on dysponuje kluczem prywatnym odpowiadającym użytemu do szyfrowania kluczowi publicznemu. Drugą istotną własnością kryptografii asymetrycznej jest możliwość poświadczania własnym podpisem cyfrowym autentyczności danych. Tego typu funkcjonalności nie oferowała kryptografia symetryczna. Wysyłający dane składa swój podpis w dwóch krokach:

- poddaje komunikat do wysłania jednokierunkowej funkcji skrótu (*hash function*) i otrzymuje, niezależnie od rozmiaru komunikatu, ciąg znaków o stałym rozmiarze;
- szyfruje otrzymany w poprzednim kroku ciąg znaków swoim kluczem prywatnym.

Weryfikacji podpisu może dokonać każdy, kto zna klucz publiczny nadawcy. Odbiorca deszyfruje otrzymany podpis za pomocą klucza publicznego nadawcy, poddaje funkcji skrótu odebrany komunikat i porównuje obie wartości. Jeśli są takie same, to weryfikacja powiodła się i mamy pewność, że komunikat nie został sfałszowany, wysłała go faktycznie osoba wskazywana jako nadawca.

Z podpisem cyfrowym łączy się kolejna usługa kryptografii klucza publicznego – integralność danych. Opisany powyżej sposób służy nie tylko uwierzytelnieniu nadawcy, ale również daje gwarancję, że wysłane dane nie zostały po drodze przejęte i zmienione. Pewność taką można mieć dlatego, że jednokierunkowa funkcja skrótu nie może wyprodukować tej samej wartości na podstawie dwóch różnych ciągów znaków.

Wadą algorytmów asymetrycznych jest słaba wydajność, są one bardzo wymagające obliczeniowo. Z tego powodu często stosuje się kryptografię klucza publicznego do zainicjowania poufnej komunikacji: jeden z partnerów generuje klucz tajny, szyfruje go kluczem publicznym adresata i wysyła, odbiorca rozszyfrowuje klucz tajny swoim kluczem prywatnym, następnie klucz tajny (zwany kluczem sesji) jest stosowany do szyfrowania symetrycznego przekazywanych danych.

2.4 Wiarygodność klucza publicznego

Gdy korzystamy z klucza publicznego nadawcy (by zweryfikować podpis cyfrowy lub potwierdzić integralność danych) albo adresata komunikatu (by zaszyfrować transmitowane dane), to zawsze chcemy być pewni, że stosujemy właściwy klucz. Klucze publiczne są rozgłaszane, przesyłane przez ich właścicieli lub umieszczane w ogólnodostępnej bazie danych. Tylko zaufany klucz publiczny można traktować jako pełnowartościowy. Ufamy kluczowi publicznemu, jeśli został on poświadczony przez specjalnie ustanowiony do tego celu urząd. Urzędy takie, zwane urzędami certyfikacyjnymi spełniają ustalone wymagania i działają zgodnie ze zdefiniowaną polityką. Są sobie podporządkowane według zasad obowiązujących w danym środowisku i tworzą strukturę hierarchiczną nazywaną infrastrukturą kluczy publicznych (PKI, *Public Key Infrastructure*). Możliwe są różne modele takiej infrastruktury. W najbardziej rygorystycznym istnieje jeden nadrzędny urząd certyfikacyjny, któremu podlegają wszystkie urzędy pierwszego poziomu, te z kolei obsługują urzędy im podporządkowane itd. Tego typu podejście jest zazwyczaj mało praktyczne, na ogół zaufanie jest rozproszone między wiele urzędów certyfikacyjnych najwyższego poziomu. Przykładowo, każda większa instytucja może utrzymywać własną infrastrukturę kluczy publicznych. Często jednak zachodzi potrzeba wprowadzenia dodatkowego poziomu zaufania między urzędami działającymi uprzednio całkowicie niezależnie. W tym celu stosuje się certyfikację

pośrednią, która może mieć charakter jednostronny (urząd A ufa urzędowi B) lub dwustronny (urząd A ufa urzędowi B oraz urząd B ufa urzędowi A).
Właściwe zaprojektowanie infrastruktury kluczy publicznych, tak by uwzględniała wszystkie potencjalne potrzeby środowiska, była łatwo rozszerzalna i elastyczna, jest bardzo istotnym zagadnieniem.

3 Bezpieczne aplikacje sieciowe

Komponenty środowiska bezpiecznej komunikacji tworzą warstwę określaną w nowoczesnych systemach sieciowych jako pośrednią między siecią a właściwą aplikacją – stanowią oprogramowanie pośredniczące (*middleware*). Rolą tej warstwy jest dostarczanie usług, bez których nie mogą się obyć współczesne aplikacje internetowe, takich jak: identyfikacja, uwierzytelnianie, autoryzacja, dostęp do informacji typu katalogowego, bezpieczeństwo. Rozwijanie niezależnych technik służących wdrażaniu powyższych funkcjonalności spowodowałoby niekompatybilność i uniemożliwiałoby współpracę różnych aplikacji. Dlatego od wielu lat prowadzone są prace standaryzacyjne. Od października 1995 roku działa specjalna grupa robocza PKIX, rozwijająca standardy internetowe wspierające PKI. Powstały na ten temat liczne dokumenty serii RFC i Internet Draft ([13], [2], [3]) oraz międzynarodowe rekomendacje takich organizacji jak ISO, ITU ([11], [12]). Internet2 Middleware Initiative, I2-MI (www.midleware.internet2.edu) pracuje nad rozwojem usług pośrednich dla potrzeb edukacji. Z infrastruktury kluczy publicznych mogą korzystać zaawansowane aplikacje sieciowe, dzięki niej większość usług sieciowych dysponuje obecnie interfejsami pozwalającymi na stosowanie szyfrowanej transmisji, uwierzytelnianie komunikujących się stron i zagwarantowanie integralności przekazywanych danych. Środowisko bezpiecznej komunikacji umożliwia z jednej strony ochronę zasobów określonej aplikacji lokalnej, z drugiej gwarantuje bezpieczną interakcję z innymi aplikacjami. Podstawowym wymaganiem stawianym infrastrukturze kluczy publicznych jest łatwość integracji z dowolną aplikacją sieciową. Musi więc dostarczać prostych, naturalnych interfejsów, realizować wszystkie zadania potrzebne do zabezpieczenia zasobów oraz procesu komunikacji oraz działać w sposób transparentny, nieodczuwalny przez użytkownika.
Usługi PKI są obecnie zintegrowane z wieloma aplikacjami sieciowymi. Powstały specjalne protokoły wspomagające współpracę z infrastrukturą kluczy publicznych:

- bezpieczna poczta elektroniczna realizowana w oparciu o protokół S/MIME (*Secure/Multi-purpose Internet Mail Extensions*) w wersji 2 lub 3 ([5], [6], [14]);
- bezpieczny dostęp do serwera WWW realizowany w oparciu o protokół *Secure Sockets Layer* lub *Transport Layer Security* ([4], [9]);
- bezpieczne wirtualne sieci prywatne (*Virtual Private Network*, VPN) realizowane w oparciu o protokół IPsec ([3]);
- bezpieczna usługa DNS (*Domain Name Service*) działająca w oparciu o techniki kryptografii asymetrycznej ([7]).

Infrastruktura kluczy publicznych może również wspomagać wiele innych procedur pracy sieciowej. Przykładowo bezpieczne źródło etykiet czasowych udostępnia usługę poświadczania danych na podstawie bieżącej daty i czasu, traktowanych jako niepodważalne. Można również wydelegować specjalną jednostkę, która będzie odgrywać rolę notariusza w konkretnym środowisku. Innym przydatnym zastosowaniem PKI jest wdrożenie bezpiecznego archiwum danych.

4 Infrastruktury kluczy publicznych w sieciach europejskich

4.1 Projekty w ramach Komisji Europejskiej

Od wielu lat w Europie są realizowane projekty, których zadaniem jest wdrożenie infrastruktury klucza publicznego w konkretnym środowisku. Dużą rolę odegrał projekt o nazwie ICE-TEL (http://www.darmstadt.gmd.de/ice-tel), powołany w ramach programu aplikacji telematycznych przy Komisji Europejskiej, trwający od 1995 do 1999 roku. Uczestniczyło w nim 17 instytucji, m.in.: firma GMD z Niemiec, University College London, Uniwersytet w Salford, Politechnika w Turynie, Uniwersytet w Ljubljanie, firma ISODE. Celem projektu było stworzenie mechanizmów bezpiecznego korzystania z Internetu przez przemysł oraz środowisko akademickie. Rozwiązanie, zgodnie ze wstępnym założeniem, miało bazować na infrastrukturze kluczy publicznych, obejmującej kraje europejskie. Kontynuacją tych działań był projekt ICE-CAR (http://ice-car.darmstadt.gmd.de), który zakończył się w grudniu 2000. W efekcie powstała globalna europejska infrastruktura kluczy publicznych. Obecnie opiekę nad nią sprawuje organizacja o nazwie EuroPKI (http://www.europki.org). Nadrzędny urząd certyfikacyjny jest prowadzony przez Politechnikę w Turynie. Na pierwszym poziomie hierarchii PKI działają urzędy certyfikacyjne Włoch, Słowenii, Norwegii, Wielkiej Brytanii, Irlandii, Austrii oraz europejskiego komitetu do spraw telematyki (European Entrapreneurs Telematics Initiatives Committee). Zadaniem EuroPKI jest dostarczanie usługi certyfikacji osobom indywidualnym, instytucjom i projektom europejskim.

4.2 Projekt PKI w ramach działalności TERENY

W grudniu 2000 roku odbyło się w Amsterdamie pierwsze spotkanie projektu PKI uruchomionego przez stowarzyszenie TERENA. Celem projektu ma być koordynacja działań związanych z zarządzaniem infrastrukturą kluczy publicznych w europejskim środowisku akademickim. Podczas inaugurującego spotkania omówiono m.in. projekty realizowane przez uczestników programu National Reasearch and Educational Networks stowarzyszenia TERENA. Ze sprawozdania zamieszczonego na stronach WWW projektu (http://www.terena.nl/projects/pki/) dowiadujemy się, że od stycznia 2000 roku działa nadrzędny urząd certyfikacyjny w holenderskiej sieci akademickiej SURFnet. Jego zadaniem jest poświadczanie kluczy publicznych urzędów certyfikacyjnych instytucji (uniwersytetów oraz biur organizacji SURFnet). Jest również prowadzony serwis informacyjny na temat certyfikacji. W najbliższym czasie SURFnet zamierza zająć się dołączeniem do oferowanych aplikacji sieciowych uwierzytelniania opartego na protokole SSL, implementacją PKI za pomocą kart elektronicznych (*smartcards*) oraz integracją PKI z bazą katalogową LDAP. Na razie SURFnet nie przewiduje stosowania kwalifikowanych certyfikatów. Niemiecka sieć akademicka DFN ma własny nadrzędny urząd certyfikacyjny od 1996 roku. Ostatnio powstała samodzielna organizacja DFN CERT, która przejęła opiekę nad usługą certyfikacji. Hiszpańska sieć akademicka RedIRIS uruchomiła nadrzędny urząd certyfikacji w listopadzie 2000 roku. W ciągu miesiąca skorzystało z jej usług około 7000 użytkowników. W Wielkiej Brytanii środowisko akademickie nie ma swojej infrastruktury kluczy publicznych, ale w bieżącym roku przewiduje się jej ustanowienie. Kilka uniwersytetów utworzyło urzędy certyfikacji typu *self-signed*. Jest zapowiadana również współpraca w ramach europejskiej inicjatywy kwalifikowanych certyfikatów ([15]). W czasie spotkania podsumowano również stan prac projektu EuroPKI i przedstawiono najbliższe zadania. Planuje się m.in. implementację usługi bezpiecznych etykiet czasowych, przeznaczonych dla aplikacji, w których ele-

mentem krytycznym jest prawidłowy czas (np. transakcje finansowe). Uczestnicy zapoznali się również z raportem ze spotkania inicjatywy Internet2 (http://www.internet2.edu). Internet2 jest zrzeszeniem ponad 180 uniwersytetów w Stanach Zjednoczonych, którego celem jest rozwój i wdrażanie we współpracy z przemysłem i jednostkami rządowymi zaawansowanych aplikacji i technologii sieciowych. Funkcjonuje już specjalna grupa o nazwie HEPKI (Higher Education PKI), koordynująca działania na polu bezpieczeństwa usług sieciowych.

4.3 Stan prac w Polsce

Przegląd aktualnego stanu działań w zakresie udostępnienia przez akademickie sieci w Europie usługi certyfikacji pokazuje, że wiodące ośrodki zaczęły już intensywne prace w tym kierunku. W Polsce prace związane z PKI są stosunkowo mało zaawansowane. Jednym z pierwszych oficjalnych urzędów certyfikacji w Polsce jest Centrum Certyfikacji klucza publicznego nosi nazwę Certum, prowadzone przez firmę Unizeto ze Szczecina. Jak można dowiedzieć się ze stron www.certum.pl, Certum wydało już ponad 10 000 certyfikatów dla jednostek organizacyjnych ZUS, płatników składek, osób prywatnych, serwerów SSL oraz ruterów VPN. Krajowa Izba Rozliczeniowa, która już od ponad 5 lat świadczy usługi certyfikacji kluczy publicznych na potrzeby systemu międzybankowych rozliczeń elektronicznych ELIXIR wprowadziła ostatnio nowy system zarządzania certyfikatami, SZAFIR, zgodny ze standardem X.509v3. Od maja 2000 roku działa trzecie w Polsce centrum certyfikacji, które zostało stworzone przez firmy Telbank S.A. oraz Enigma SOI sp. z o.o. We wrześniu 2000 Narodowy Bank Polski oraz Związek Banków Polskich utworzyły firmę Centrast S.A., która ma wydawać elektroniczne certyfikaty dla potrzeb sektora bankowego. Kwestia udzielania zezwoleń na wydawanie certyfikatów dla podmiotów gospodarczych leży dotychczas w gestii Ministerstwa Gospodarki. Nadal brakuje inicjatywy odgórnej wprowadzającej potrzebne ustalenia w ramach kraju. Obecnie trwają dyskusje nad projektami „Ustawy o podpisie elektronicznym": poselskim z końca stycznia 2001 r. oraz rządowym z 12 lutego 2001 r. Projekty te różnią się między sobą skalą nadzoru i kontroli państwa. Rząd chce wprowadzić daleko idącą kontrolę nad wydawaniem certyfikatów kluczy publicznych, natomiast posłowie i kręgi informatyczne opowiadają się za podejściem wolnorynkowym i możliwością stosowania niekwalifikowanych certyfikatów, które zostały poświadczone przez nieakredytowaną firmę. Przewiduje się zatwierdzenie ostatecznej wersji ustawy regulującej stosowanie podpisów cyfrowych do lipca 2001. Ministerstwo Spraw Wewnętrznych i Administracji zamierza powołać Krajowy Urząd Certyfikacji. Na razie nie można przewidzieć, jak rozwiną się działania związane z ogólnopolską infrastrukturą kluczy publicznych. Nie wiadomo więc, czy będzie możliwe zintegrowanie działań w środowisku akademickim z krajową strukturą urzędów certyfikacyjnych i oferowanie użytkownikom tzw. kwalifikowanych certyfikatów (w pojęciu ustawy). Obecnie wiele zespołów sieci akademickich wdraża niezależnie bezpieczne technologie sieciowe dla lokalnych potrzeb. Prace te nie są w żaden sposób koordynowane. Powstają więc odseparowane struktury zastępcze o charakterze tymczasowym, stosowane do konkretnych aplikacji. Niezbędne i pilne staje się zdefiniowanie reguł tworzenia i utrzymywania infrastruktury kluczy publicznych wśród polskich uczelni i jednostek badawczo-rozwojowych. Potrzebę tego przedsięwzięcia wzmacnia fakt, że realizacji wielu zadań wymienianych w dokumencie „PIONIER: Polski Internet Optyczny – Zaawansowane Aplikacje, Usługi, Technologie dla Społeczeństwa Informacyjnego" opiera się na istnieniu infrastruktury stanowiącej postawę bezpiecznej komunikacji w Internecie.

5 Zadania projektu budowy infrastruktury kluczy publicznych w polskim środowisku akademickim

5.1 Podstawowe cele

Działania zmierzające do utworzenia w polskim środowisku akademicko-naukowym profesjonalnej, operacyjnej infrastruktury kluczy publicznych powinny polegać na:

- zainicjowaniu rozwoju technologii bezpieczeństwa pracy sieciowej;
- stworzeniu, promowaniu i utrzymywaniu infrastruktury klucza publicznego dla środowiska akademicko-naukowego, gwarantującej wiarygodność stosowanych kluczy publicznych;
- dostarczeniu w usługach sieciowych komponentów programowych niezbędnych do bezpiecznego stosowania Internetu w aplikacjach niekomercyjnych i komercyjnych;
- udoskonaleniu istniejących narzędzi pod kątem ich użyteczności, uniwersalności oraz przenośności między różnego rodzaju platformami.

5.2 Zadania szczegółowe

Priorytetowym zadaniem jest zaprojektowanie i ustanowienie infrastruktury kluczy publicznych w polskim środowisku akademicko-naukowym. Na tym etapie bardzo ważne jest skoordynowanie prac z zadaniami projektu rozwoju usługi katalogowej LDAP ([10]). Jest to konieczne nie tylko dlatego, że baza katalogowa stanowi idealne miejsce do przechowywania certyfikatów kluczy publicznych oraz list odwołanych certyfikatów. W większym stopniu wymaga tego wspólny model nazewnictwa stosowany przez obie usługi: LDAP i PKI. Certyfikat klucza publicznego powstaje, gdy uprawniona jednostka (urząd certyfikacyjny) poświadczy swoim podpisem cyfrowym dane identyfikujące właściciela klucza publicznego oraz sam klucz. Identyfikacja właścicieli kluczy oraz urzędów certyfikacyjnych opiera się na specjalnym schemacie nazewnictwa, opracowanym w ramach standardu X.500, z którego wywodzi się protokół LDAP. Dla zagwarantowania przenośności i współpracy różnych aplikacji, kwestie przypisywania nazw w celu korzystania z usługi PKI oraz budowy hierarchicznej struktury bazy katalogowej LDAP muszą byś rozwiązywanie w oparciu o dobrze zdefiniowane potrzeby wszystkich aplikacji.

Szczegółowe prace zmierzające do utworzenia środowiska PKI powinny objąć:

1. Zaprojektowanie hierarchii urzędów certyfikacyjnych w polskim środowisku akademicko-naukowym.
2. Ustalenie stosowanego nazewnictwa według standardu X.500/LDAP.
3. Sprecyzowanie polityki bezpieczeństwa obowiązującej w zaprojektowanej infrastrukurze, czyli zestawu reguł określających podstawowe obowiązki i zadania komponentów infrastruktury kluczy publicznych oraz funkcje wystawianych przez nią certyfikatów:
    a) wymagania stawiane urzędom certyfikacyjnym włączającym się w infrastrukturę;
    b) stosowany model zaufania;
    c) obowiązki urzędu certyfikacyjnego;
    d) sposób ochrony stanowisk, z których korzysta urząd certyfikacyjny;
    e) działania gwarantujące prywatność informacji zebranej w procesie certyfikacji;
    f) sposób weryfikacji instytucji oraz osób odpowiedzialnych za utrzymywanie nowego urzędu certyfikacyjnego, wstępne wymagania stawiane dołączanej instytucji;

g) sposób rejestracji użytkowników, wprowadzenie delegatur, urzędów rejestrujących i ich powiązania z urzędami certyfikacyjnymi;
h) wymagania stawiane użytkownikom;
i) rozwiązywanie konfliktów przy nadawaniu nazw;
j) wymagany poziom bezpieczeństwa certyfikatów, stosowane algorytmy kryptograficzne, rozmiar kluczy;
k) stosowany format certyfikatów;
l) typy wystawianych certyfikatów (w zależności od ich roli oraz od poziomu kontroli wiarygodności);
m) domyślny termin ważności certyfikatów;
n) sposób unieważniania certyfikatów;
o) obsługa listy odwołanych certyfikatów;
p) zasady przedłużania ważności certyfikatów;
q) reguły dotyczące archiwizacji wystawionych kluczy prywatnych;
r) reguły certyfikacji wzajemnej i łączenia dotychczas niezależnych urzędów;
s) reguły udostępniania kluczy publicznych, akceptowane formy magazynów kluczy publicznych, zastosowanie protokołu X.500 lub LDAP.

4. Ustanowienie nadrzędnego urzędu certyfikacyjnego.
5. Zdefiniowanie procedury dołączania kolejnych urzędów do infrastruktury kluczy publicznych.
6. Opracowanie reguł postępowania w przypadku awarii, utraty nośników itp.

Etap projektowania struktury urzędów certyfikacyjnych musi obejmować ustalenie, w jakiego typu oprogramowanie będą wyposażone urzędy certyfikacyjne. W tym celu należy przeprowadzić analizę pakietów programowych dostępnych na rynku, dokonać instalacji testowych, jeśli będzie to możliwe. Istotnym kryterium jest zapewnienie maksymalnej pewności i wiarygodności wszystkich komponentów programowych.
Wdrożenie infrastruktury bezpieczeństwa po jej zaprojektowaniu i ustanowieniu nadrzędnego urzędu certyfikacyjnego wymaga zbudowania narzędzi wspomagających pracę PKI. Ważnymi zagadnieniami są:

- obsługa list odwołanych certyfikatów, zastosowanie protokołu OCSP (*Online Certificate Status Protocol*);
- stworzenie mechanizmów automatycznego przedłużania ważności certyfikatów (zgodnie z ustaloną polityką), tak by użytkownik mógł nieprzerwanie korzystać ze swego certyfikatu.

Bardziej zaawansowane działania realizowane w oparciu o zaimplementowaną infrastrukturę kluczy publicznych obejmą:

- wprowadzenie usługi certyfikatów atrybutowych w celu zarządzania dystrybucją uprawnień przydzielanych właścicielom certyfikatów;
- zastosowanie technologii kart elektronicznych (*smartcards*) do przechowywania kluczy.

5.3 Integracja infrastruktury kluczy publicznych środowiska akademickiego ze strukturą ogólnopolską

Najprawdopodobniej w bieżącym roku podpis elektroniczny stanie się legalną formą poświadczania dokumentów. W projekcie ustawy o podpisie elektronicznym, zarówno w wersji rządowej, jak i poselskiej, mówi się o dwóch formach działalności certyfikacyjnej: urzędach akredytowanych oraz kwalifikowanych. Obu typom urzędów certyfikacyjnym stawia

się wysokie wymagania sprzętowe i finansowe. Najprawdopodobniej nie będzie mogła im sprostać większość instytucji akademickich, zainteresowanych wprowadzeniem bezpiecznej komunikacji w swojej sieci. Z powodu wysokich kosztu tego przedsięwzięcia jest mało prawdopodobne stworzenie oficjalnej, akredytowanej akademickiej infrastruktury kluczy publicznych. Dodatkowo, dogłębna analiza celów takich działań podważa ich zasadność wobec przewidywanych kosztów i trudności natury formalnej. Z drugiej strony warto zwrócić uwagę, że dyskutowany projekt ustawy dotyczy wyłącznie obsługi podpisu elektronicznego, nie ma w niej mowy o innych zastosowaniach metod kryptograficznych, np. o szyfrowaniu danych lub sprawdzaniu ich spójności. Projekt ustawy nie zajmuje się też zagadnieniami dostępu do kluczy publicznych, gdyż złożenie podpisu elektronicznego oznacza m.in. dołączenie klucza publicznego. Omawiany w tym artykule projekt przewiduje wszystkie prace tego typu. Wobec przewidywanych rządowych regulacji kwestii funkcjonowania urzędów certyfikacyjnych należy więc przyjąć, że dla potrzeb środowiska akademicko-naukowego Polski trzeba będzie stworzyć strukturę nieformalną, być może „nieprofesjonalną" z punktu widzenia ustawy. Ogólnopolska akademicka infrastruktura kluczy publicznych działałaby zgodnie z polityką bezpieczeństwa zdefiniowaną przez zespół znający realia sieci POL34 i NASK. Ogromną zaletą tak określonego przedsięwzięcia byłaby możliwość pewnego osłabienia rygorów bezpieczeństwa, np. w odniesieniu do ochrony stanowisk wystawiania certyfikatów i dopuszczenie korzystania z ogólnodostępnego oprogramowania.

6 Przewidywane efekty

Kryptografia klucza publicznego ma z dnia na dzień szersze zastosowanie. W coraz większej liczbie aplikacji sieciowych środowisko bezpiecznej komunikacji jest zintegrowane z podstawową usługą. Coraz więcej osób chce na co dzień korzystać z transmisji szyfrowanej i dodawać podpisy cyfrowe do przesyłanych dokumentów. Rośnie zapotrzebowanie na bezpieczny serwis WWW, chronioną pocztę elektroniczną. Zwiększają się zasoby informacyjne dostarczane w Internecie, lecz nie zawsze mają być one ogólnodostępne. Autoryzacja dostępu przez uwierzytelnienie użytkownika jest popularnym sposobem ochrony przed osobami nieuprawnionymi. Bezpieczne serwery DNS dają pewność, że otrzymywane informacje na temat domen są prawdziwe. Użytkownicy korzystają na co dzień z dużej liczby usług sieciowych, dlatego coraz bardziej uciążliwa staje się konieczność wielokrotnego „logowania", w celu uzyskania dostępu do konkretnych aplikacji. W technice „pojedynczego logowania" (*single sign-on*) każdy uwierzytelnia swoją tożsamość w systemie lokalnym (za pomocą kryptografii asymetrycznej) tylko jeden raz, a o tym czy może korzystać z konkretnej usługi sieciowej decydują wcześniej przyznane prawa dostępu, określane na podstawie danych identyfikujących użytkownika.

Wszystkie opisane funkcjonalności z jednej strony opierają się na algorytmach kryptograficznych, z drugiej bazują na dobrze zorganizowanej infrastrukturze klucza publicznego, gwarantującej maksymalny poziom zaufania. Pojawiają się wprawdzie głosy krytyczne, wskazujące, że PKI nie jest magicznym eliksirem, niwelującym wszystkie problemy bezpieczeństwa. Oczywiście, tego typu rozwiązanie ma swoje wady, o których nie można zapominać. Zostały one szczegółowo omówione w artykule [8]. Prawie wszystkie elementy wymieniane jako potencjalne ogniwo zapalne pojawiają się dlatego, że o mocy całego systemu decyduje jego najsłabszy komponent. Metody kryptograficzne można uznać za skuteczne i bezpieczne, natomiast najwięcej niepewności wnoszą systemy komputerowe i ludzie. Bezpieczeństwo sieci komputerowych to dziedzina, w której zawsze trzeba postępować ostroż-

nie, z ogromną wyobraźnią i, niestety, należy brać pod uwagę najgorsze warunki zewnętrzne, m.in. złą wolę użytkowników sieci.
Wdrożenie infrastruktury kluczy publicznych i zdefiniowanie reguł uczestnictwa w tej strukturze pozwoli na szybkie rozszerzenie usługi na terenie Polski, przede wszystkim w środowisku akademickim. Zespoły biorące udział w projekcie zdobędą doświadczenie i staną się ekspertami w dziedzinie tworzenia mechanizmów bezpiecznej pracy w sieciach komputerowych, będą gotowe do wdrażania podobnej technologii w swoich regionach. W oparciu o gotową infrastrukturę będą przygotowywane bezpieczne aplikacje sieciowe i dostarczane usługi gwarantujące całkowita poufność.

Bibliografia

1. Adams C., Lloyd S., „Understanding Public-Key Infrastructure, Concepts, Standards, and Deployment Considerations", Macmillian Technical Publishing, 1999.
2. Aresenault A., Turner S., „Internet X.509 Public Key Infrastructure, PKIX Roadmap", Internet Draft, PKIX Working Group, November 2000.
3. Chokhani S., „Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 2527, March 1999.
4. Dierks T., Allen C., „The TLS Protocol Version 1.0", RFC 2246, January 1999.
5. Dusse S., Hoffman P., Ramsdell B., Lundblade L., Repka L., „S/MIME Version 2 Message Specification", March 1998.
6. Dusse S., Hoffman P., Ramsdell B., Weinstein J., „S/MIME Version 2 Certificate Handling", RFC 2311, March 1998.
7. Eastlake D., „Domain Name System Security Extensions", RFC 2535, March 1999.
8. Ellison C., Schneier B., „Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure", Computer Security Journal Volume XVI, Number 1, 2000.
9. Frier A., Karlton P., Kocher P., „The SSL 3.0 Protocol", Netscape Communications Corp., Nov 18, 1996.
10. Górecka-Wolniewicz M., Wolniewicz T., „Zastosowanie protokołu LDAP do zarządzania zasobami sprzętowo-programowymi akademicko-naukowej sieci komputerowej w Polsce", materiały konferencyjne PIONIER2001.
11. ITU/ISO Recommendation X.500 – Information technology – Open Systems Interconnection – The directory: Overview of concepts, models, and services, November 1993.
12. ITU/ISO Recommendation X.509 – Information technology – Open Systems Interconnection – The directory: Authentication framework, June 1997.
13. Kent S., „Security Architecture for the Internet Protocol", RFC 2401, November 1998.
14. Ramsdell B., „S/MIME Version 3 Certificate Handling", RFC 2312, June 1999.
15. Santesson S., Polk W., Barzin P., Nystrom M., „Internet X.509 Public Key Infrastructure, Qualified Certificates Profile", Internet Draft, October 1999.
16. Stallings W., „Cryptography and Network Security: Principles and Practice", Prentice Hall.