Piotr Olszewski

Wydział Cybernetyki
Wojskowa Akademia Techniczna w Warszawie

Wybrane problemy zarządzania tożsamością cyfrową w instytucjach administracji państwowej

1. Wstęp

Tożsamość w ujęciu ogólnym należy do kluczowych zagadnień z dziedziny filozofii, socjologii oraz pedagogiki. Słownikowa definicja (*Słownik języka polskiego PWN*[1]) tożsamości w pierwszej kolejności określa ją jako „identyczność". Jedna z kolejnych definicji opisuje tożsamość jako zespół faktów, cech oraz danych personalnych, pozwalających zidentyfikować konkretną osobę. Okazuje się, iż taką definicję można z powodzeniem zastosować również w przypadku tożsamości cyfrowej. Jedną z prób określenia tożsamości cyfrowej jest definicja P.J. Windleya, wskazująca, że jest to zestaw danych, które w sposób unikalny opisują osobę lub rzecz oraz zawierają informację na temat jej powiązań[2].

Tożsamość w świecie realnym jest niezwykle istotna ze społecznego punktu widzenia. Biorąc pod uwagę tożsamość w sensie urzędowym, należy powiedzieć, że jest to jedyny sposób na stwierdzenie, kim jest każdy obywatel kraju. Pozwala ona nie tylko go identyfikować, ale także wiązać z innymi podmiotami, jak również po przeprowadzeniu procesu weryfikacji stwierdzać, czy ma uprawnienia do wykonywania poszczególnych czynności (np. kierowania pojazdami). Przykładem tożsamości w sensie urzędowym są dokumenty państwowe, takie jak: dowody osobiste, paszporty, prawa jazdy itd. Weryfikacji dokonuje się w kilku etapach – pierwszym i najprostszym z nich jest porównanie osoby okazującej dokument ze zdjęciem, które dokument zawiera (weryfikacja bez udziału podmiotów trzecich). Ogół procesów związanych z wnioskowaniem o dokumenty, ich wydawaniem, unieważnianiem, weryfikacją można określić jako pewien system przetwarzania i zarządzania tożsamością obywatela.

---

1 http://sjp.pwn.pl.

2 P.J. Windley, *Digital Identity*, O'Reilly Media Inc., Sebastopol 2005, s. 8–14.

Cyfrowa tożsamość jest dość podobna do realnej. Zgodnie z definicją, zawiera zestaw danych, które w sposób jednoznaczny identyfikują podmiot posługujący się tą tożsamością. Może zawierać dane i podpis wystawcy tejże tożsamości, co odgrywa rolę uwiarygodnienia informacji przez trzecią stronę. Tożsamość cyfrowa także potrzebuje metod jej wystawiania, dystrybucji oraz zestawu funkcji pozwalających na unieważnienie i weryfikację jej prawdziwości. Zadania te są jednak utrudnione, w szczególności jeżeli chodzi o weryfikację, ze względu na brak fizycznej obecności podmiotu posługującego się daną tożsamością, co eliminuje podstawową metodę oceny wiarygodności. Dodatkowe problemy pojawią się, gdy zamiast jednego scentralizowanego rejestru konieczna jest obsługa instytucji, które mogą mieć jednostki mobilne, oczekujące sposobu dostępu i przetwarzania danych związanych z tożsamością cyfrową, jednocześnie niemające możliwości utrzymania ciągłego połączenia ze scentralizowaną bazą informacji.

Poruszone zagadnienie, tj. problematyka zarządzania tożsamością cyfrową, ma istotne znaczenie dla funkcjonowania infrastruktury informacyjnej w państwie. Zarządzanie tożsamością dotyczy nie tylko relacji, w której przetwarza się dane obywateli lub innych podmiotów, ale również przetwarzania informacji na temat pracowników instytucji, systemów informatycznych (które również mogą występować jako podmioty mając cechy pozwalające na ich identyfikację i odróżnienie od siebie). Szczególna odpowiedzialność za wprowadzenie zasad oraz mechanizmów zarządzania tożsamością spoczywa na administracji rządowej[3]. Niniejszy artykuł przedstawia podstawowe kwestie związane z zarządzaniem tożsamością cyfrową w odniesieniu do systemów scentralizowanych, przy czym skupiono się w nim na tematyce systemów mobilnych. Przekazywanie informacji związanych z zaufaniem w systemach mobilnych staje się coraz bardziej istotne ze względu na gwałtowny ich rozwój w ostatnich latach. Prowadzi to do konieczności poszukiwania nowych rozwiązań oraz ulepszania obecnych przez projektowanie i wdrażanie mechanizmów przeznaczonych dla takich klas systemów. Istnienie takich rozwiązań oraz próba ich przybliżenia będą zatem osią niniejszej pracy.

2. Dystrybucja informacji o zaufaniu. Modele zaufania

Dostarczenie skutecznych metod weryfikacji tożsamości oraz – w szerszym zakresie – zarządzanie nią jest przedmiotem wielu analiz oraz badań. Niezależnie od tego, czy

[3] B. Szafrański, *Główne wyzwania związane z modernizacją funkcjonowania państwa, IT w służbie efektywnego państwa*, „Roczniki" Kolegium Analiz Ekonomicznych, z. 29, Oficyna Wydawnicza SGH, Warszawa 2013, s. 309–324.

tożsamość cyfrowa będzie odpowiadała tożsamości rzeczywistej, czy też powstanie w celu zapewnienia użytkownikowi anonimowości w sferze wirtualnej, koniecznym elementem służącym do obrotu taką tożsamością jest system informatyczny, który udostępni mechanizmy takiego obrotu. Mechanizmem kontroli oraz zarządzania tożsamością jest infrastruktura klucza publicznego (ang. *public key infrastructure* – PKI), która wprowadza narzędzia pozwalające na tworzenie, usuwanie oraz zarządzanie relacjami zaufania pomiędzy dowolną liczbą stron, wymagających weryfikacji innych podmiotów.

W tym miejscu warto krótko przybliżyć to, czym jest samo zaufanie. Zaufanie jest wartością społeczną, w szczególności w odniesieniu do relacji międzyludzkich, ale występuje również zaufanie instytucjonalne oraz systemowe, wyrażające ufność obywateli w stosunku do instytucji publicznych czy też wiarę w określony porządek prawny. Jedną z podstawowych i popularnych definicji technicznych zaufania jest ta wynikająca z normy ITU-T X.1252, która mówi o tym, iż zaufanie to przekonanie o wiarygodności i prawdziwości informacji lub zdolności danego podmiotu do zachowania w sposób właściwy w zadanym kontekście[4]. Definicja ta nie jest do końca trafna, jej analiza i dyskusja nad nią wykraczają poza ramy artykułu, w związku z czym autor proponuje przyjęcie innej, bardziej precyzyjnej definicji: „Zaufanie jest miarą tego, co oszacował obserwator A na temat zachowania podmiotu B w czasie T dla przypadku X".

Jak już wspomniano, do zarządzania tożsamością cyfrową służy infrastruktura klucza publicznego, rozumiana jako zbiór urządzeń, oprogramowania, polityk bezpieczeństwa oraz użytkowników umożliwiający tworzenie, przechowywanie, zarządzanie i dystrybucję certyfikatów klucza publicznego, stanowiących podstawę do identyfikowania tożsamości ludzi lub maszyn w Internecie i innych sieciach, które leżą w jej domenie[5].

Sama struktura PKI bywa zazwyczaj złożona i często jest dostosowana do konkretnych wymagań instytucji, która z niej korzysta. Podstawą, na której działa PKI, są jednak certyfikaty klucza publicznego i to one pozwalają na określenie i weryfikację tożsamości każdej jednostki w PKI. Zgodnie z polską normą PN-I-2000, certyfikat klucza publicznego jest taką informacją o kluczu publicznym danego podmiotu, która przez złożenie na niej podpisu cyfrowego przez zaufaną trzecią stronę staje się niemożliwa do podrobienia. Zawiera trzy zasadnicze dane: klucz publiczny tego podmiotu, opis jego tożsamości oraz podpis cyfrowy złożony przez wspomnianą uprzednio zaufaną trzecią stronę na tych strukturach[6].

---

[4] Def. 6.64, http://www.itu.int/rec/T-REC–X.1252–201004-I (data odczytu: 10.11.2014).

[5] https://depot.ceon.pl/bitstream/handle/123456789/4437/rozprawa_pjatkiewicz.pdf (data odczytu: 10.11.2014).

[6] *PN-I-02000. Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia*, Polski Komitet Normalizacyjny, 2002.

Nierzadko jednak strukturę PKI określają standardy. Jednym z najważniejszych jest standard X.509[7], pozwalający na modelowanie procesu zarządzania tożsamością cyfrową w taki sposób, aby minimalizować ryzyko związane z fałszowaniem tożsamości lub treści podlegających ochronie przez PKI. Model przyjęty przez X.509 pozwala budować strukturę PKI, którą określa się jako PKIX (*PKI for X.509*). Sam standard X.509, poza strukturą certyfikatu, definiuje również listy unieważnień certyfikatów (ang. *certificate revocation list* – CRL), certyfikaty atrybutów oraz algorytmy weryfikacji ścieżki certyfikacyjnej. Spełnia zatem rolę standardu, według którego możliwe jest zbudowanie funkcjonalnej infrastruktury klucza publicznego, która będzie w stanie kooperować z innymi, istniejącymi już strukturami. Głównymi węzłami, które tworzą szkielet takiego systemu, są urzędy certyfikacji (ang. *certification authority* – CA). Elementami często występującymi są również urzędy rejestracyjne (ang. *registration authority* – RA), których zadaniem jest weryfikacja tożsamości podmiotów wnioskujących o informację z CA. Wśród innych elementów, w dużej mierze zależnych od konkretnych implementacji PKIX, można wyróżnić m.in.: katalogi centralne, służące za miejsce składowania i indeksowania kluczy; systemy zarządzania certyfikatami, które stanowią w szczególności oprogramowanie zarządzające funkcjami CA i RA; polityki certyfikacji, które określają, jakie relacje mogą zachodzić w obrębie PKI, tworząc tzw. model zaufania.

Z cyklu życia certyfikatu wynika, iż po odgórnie określonym czasie traci on swoją ważność i musi zostać wymieniony na nowy. Zdarzają się jednak przypadki, kiedy certyfikat – pomimo swojej formalnej poprawności – musi zostać wycofany z obiegu. Dzieje się to najczęściej w momencie, gdy zostanie ujawniony klucz prywatny skojarzony z certyfikatem klucza publicznego danego podmiotu. Inne możliwe powody to np. złamanie bezpieczeństwa wystawcy certyfikatu lub zmiana danych podmiotu, wymuszająca wydanie nowego certyfikatu. Konieczne staje się wtedy poinformowanie możliwie największej liczby użytkowników o tym, że podmiot posługujący się konkretną tożsamością może być fałszywy lub nie zawiera aktualnych danych. W celu dystrybucji informacji o unieważnionych certyfikatach powstały CRL, będące listą skrótów certyfikatów, którym nie można ufać. CRL są najczęściej publikowane przez CA, jednakże mogą być tworzone i dystrybuowane również przez inne podmioty oddelegowane do pełnienia tej roli przez CA[8].

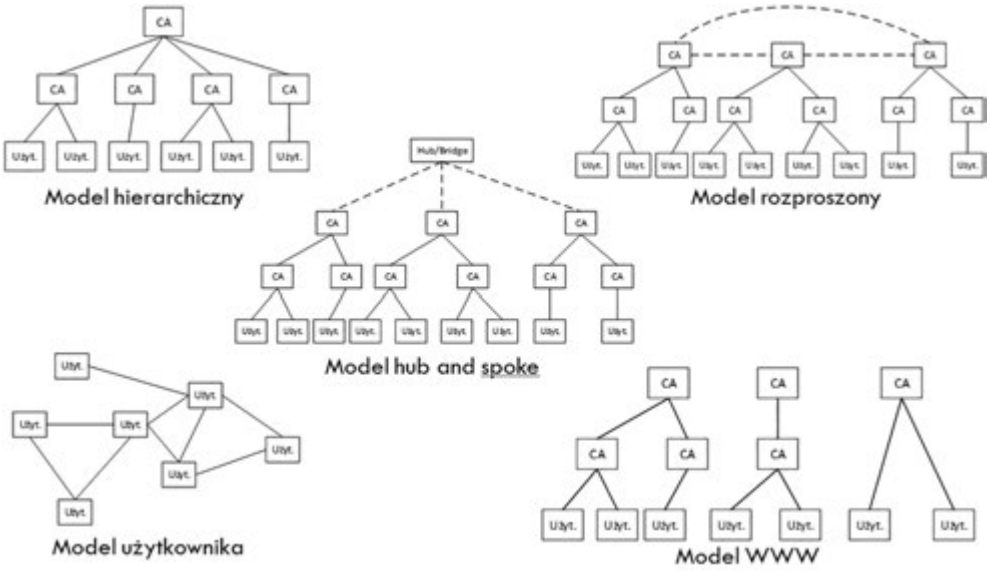
Istnieje wiele modeli zaufania, mających różne zastosowania. Jednym z popularnych modeli jest model WWW, który nazwę zawdzięcza zastosowaniu go w przeglądarkach

---

7 https://www.ietf.org/rfc/rfc5280.txt (data odczytu: 10.11.2014).

8 C. Adams, S. Lloyd, *PKI podstawy i zasady działania. Koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 134–136.

internetowych. Jego działanie opiera się na preinstalowaniu puli kluczy publicznych CA w przeglądarce dostępnej standardowo dla każdego. Pula taka ma za zadanie zdefiniować pierwotny zbiór zaufany danej przeglądarki, działając jako korzeń procesu weryfikacji innych certyfikatów[9]. Innym popularnym przykładem jest model zaufania oparty na użytkowniku i jego sieci zaufania (*web of trust*), gdy każdy z użytkowników jest odpowiedzialny za decyzję dotyczącą tego, czy certyfikat przedstawiony przez drugą stronę może uznać za zaufany, czy też należy go odrzucić. Decyzja podejmowana przez użytkownika może zależeć od wielu czynników, może być również w pełni subiektywna i zasadniczo nie określają tego żadne normy[10]. Przykładowe modele przedstawia rysunek 1.



Rysunek 1. Różne modele zaufania

Źródło: opracowanie własne.

Model hierarchiczny najlepiej odpowiada strukturze wprowadzanej przez X.509. Jest on również jednym z najpopularniejszych[11]. Jest to model o strukturze drzewa, w którym wszystkie jednostki w hierarchii obdarzają zaufaniem jeden, podstawowy CA.

[9] R. Perlman, *An Overview of PKI Trust Models*, „IEEE Network" 1999, vol. 13, November/December, s. 38–43.

[10] Ibidem, s. 160–171.

[11] http://www.itu.dk/courses/DSK/E2003/DOCS/PKI_Trust_models.pdf (data odczytu: 10.11.2014).

Taki urząd certyfikacyjny nosi nazwę kotwicy zaufania (ang. *trust anchor*)[12]. Drzewo może składać się z wielu warstw, reprezentujących pośrednie CA.

Możliwy jest także scenariusz, kiedy od razu po korzeniu (głównym CA) będą występować odbiorcy certyfikatów, czyli użytkownicy danego PKI. Jest to scenariusz dość częsty w niewielkich domenach PKI, gdy nie ma sensu utrzymywanie sztucznych warstw środkowych. Doskonałym przykładem są instytucje oraz organizacje średniej wielkości, w których możliwe jest zarządzanie tożsamościami wszystkich pracowników z jednego miejsca (centrali) bez konieczności delegowania odpowiedzialności za to do oddziałów podrzędnych. Podstawowy CA nie tylko stanowi początek całego drzewa, ale również jest bazą zaufania dla każdego węzła oraz każdego liścia w drzewie[13]. Oczywiście, istnieją różnorodne wariacje, pozwalające na budowanie podobnych schematów, które jednak nakładają mniej ograniczeń lub pozwalają na wykonywanie większej liczby operacji na węzłach. Model hierarchiczny może być składową w modelu WWW – składać się z predefiniowanej listy pojedynczych hierarchii.

3. Wybrane problemy zarządzania tożsamością cyfrową

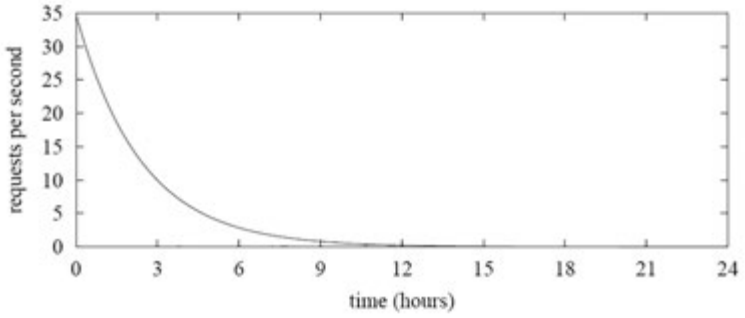
Pomimo procesu standaryzacyjnego oraz prac wielu niezależnych instytucji nad PKI (X) oraz X.509 wiele słabości oraz problemów wciąż jest nierozwiązanych. X.509 było pierwotnie projektowane ze wsparciem dla struktury X.500, obecnie natomiast jest używane na całym świecie w różnego rodzaju sieciach. Projekt związany z X.500 pozostawia jednak cały czas swój ślad, wymuszając używanie właściwych struktur tego standardu. Jednym z często przywoływanych argumentów jest konieczność użycia DN (ang. *distinguish names*) jako nazw podmiotów oraz urzędów certyfikacyjnych. DN to struktura zawierająca rekordy składające się z pól opisujących poszczególne elementy pełnej nazwy, np. nazwa użytkownika, adres, nazwa organizacji itd. Wprowadza to sztuczną strukturę, która nie pasuje do obecnego podziału organizacyjnego domen PKI (w szczególności pola *locality, administrative domain, organisational unit*)[14]. Użycie tak określonych pól często wymaga sztucznego dopasowania aktualnego schematu organizacyjnego domeny do określonego odgórnie nazewnictwa poszczególnych składowych DN.

[12] http://www.itu.int/rec/T-REC–X.509–201102-S!Cor1 (data odczytu: 10.11.2014).

[13] A. Jøsang, *PKI Trust Models*, „Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS)" 2013, May, s. 279–301.

[14] https://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf (data odczytu: 10.11.2014).

Zasadniczo niekiedy samo użycie certyfikatu już stanowi problem. X.509 wymaga, ażeby podczas wykonywania danej czynności strony ujawniły wszystkie informacje na swój temat, niezależnie od tego, czy jest to potrzebne do wykonania czynności, czy też nie. W praktyce często spotyka się sytuacje, kiedy wymagane jest ujawnienie tylko niektórych atrybutów, podczas gdy reszta mogłaby pozostać ukryta. Dobrym przykładem jest atrybut wieku – przy niektórych czynnościach wymagane jest to, aby podmiot (osoba) miała odpowiedni wiek; w normalnej sytuacji obywatel powinien ujawnić o sobie dokładnie tyle informacji, ile wymaga się do zweryfikowania wieku. Niestety, w przypadku X.509 musi odkryć swoją pełną tożsamość, wraz ze wszystkimi atrybutami, po to tylko, aby można było sprawdzić to jedno pole. Cecha taka wymusza stosowanie różnorodnych zabiegów – konieczne staje się tworzenie systemów, które filtrują i przekazują dalej tylko dane wymagane do wykonywania poszczególnych czynności, dzięki temu respektuje się prawo do prywatności danego obywatela.



Rysunek 2. Liczba żądań na sekundę w przełożeniu na czas od publikacji CRL

Źródło: http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf (data odczytu: 10.11.2014).

Problematyczne jest również zarządzanie unieważnieniami. Listy CRL są kosztowne w dystrybucji (zajmują pasmo, obciążają serwery), niewydawane bardzo często nie dają efektywnej ochrony przed atakami. Architektura opierająca się na CRL jest podatna na ataki DoS – istnieje możliwość zablokowania pobrania list unieważnień przez atak na punkty dystrybucyjne i zablokowanie do nich dostępu. Uniemożliwi to odebranie CRL przez uprawnionych użytkowników i opóźni pojawienie się informacji o skompromitowanych certyfikatach. Ponadto, sprawdzenie w CRL, czy certyfikat jest ważny, nie daje żadnej gwarancji, że w danej chwili jest on naprawdę ważny. Ze względu na opóźnienie w generowaniu CRL (dodatkowe opóźnienie wprowadza samo pobranie takiej listy i jej ewentualna propagacja dalej) może się okazać, że z powodu niewydania jeszcze aktualnego CRL certyfikat zostanie uznany za ważny, choć już taki nie jest. Podważa to zasadę niezaprzeczalności, którą powinno wspierać PKI. Kiedy

czas życia CRL wygaśnie, wszystkie strony, które muszą pobrać nowy CRL, starają się podłączyć do punktu dystrybucyjnego w celu pobrania nowej listy unieważnień[15].

Jak wynika z badań prowadzonych przez D. Coopera (NIST), maksimum żądań nowej listy CRL przypada na chwilę po wygaśnięciu poprzedniej listy (rysunek 2). Z jednej strony jest to pożądane do tego, aby węzły miały jak najnowszy CRL, z drugiej strony jest to sytuacja nie do przyjęcia w sieciach o małej przepustowości, w szczególności sieciach mobilnych lub instalacjach polowych (radiostacje wąskopasmowe). Sam standard określa, że raz pobrana CRL może być umieszczona w pamięci podręcznej w celu przyspieszenia procesu weryfikacji.

4. Problematyka jednostek mobilnych

Różnorodne organizacje, firmy czy instytucje państwowe są zazwyczaj podmiotami o stałej strukturze, mającymi stały kontakt z innymi podmiotami przez szerokopasmowe łącza. Niemniej jednak istnieje wiele instytucji, które mają jednostki mobilne, działające w terenie, przemieszczające się, które nie są w stałej łączności z jakimś punktem dostępowym. Do najważniejszych należą instytucje związane z obronnością (systemy wojskowe), utrzymaniem porządku (policja, straż graniczna), ale również ambasady, konsulaty oraz delegatury, które choć nie są obiektami ruchomymi, z różnych względów mogą nie być w stanie nawiązać łączności z centralą – możliwe jest wtedy traktowanie ich jak jednostki mobilne.

Podstawową cechą systemów mobilnych jest niezależność od dostępnej infrastruktury. Świadczy ona o przydatności danego systemu do zmiennych warunków – system taki powinien być w stanie dołączyć się do dowolnej istniejącej struktury sieciowej, w dowolnym miejscu i móc nawiązać łączność z innymi systemami. W razie braku możliwości podłączenia do jakiejkolwiek infrastruktury system powinien być na tyle autonomiczny, ażeby móc zapewnić pracę na zadanym poziomie swoim podsystemom, jak również systemom jednostek podległych. Niedopuszczalne jest przykładowo, ażeby przez zerwanie łączności z centralą wóz dowodzenia policji stracił możliwość kontaktu i przekazywania informacji podległym jednostkom. Ponadto, należy podkreślić fakt, że zazwyczaj jeżeli nawet systemy mobilne uzyskają łączność z systemem stacjonarnym, to jest to łączność z wykorzystaniem łączy wąskopasmowych (np. radiostacje), w związku z czym nie jest możliwe przesyłanie za ich pomocą dużych ilości danych (np. CRL), w dodatku z dużą częstotliwością. Konieczne staje się stosowanie innych

[15] http://people.dsv.su.se/~matei/courses/IK2002_SMOW/L8_AC6.pdf (data odczytu: 10.11.2014).

rozwiązań, uwzględniających przepustowość łącz, takich jak delta-CRL lub segmentowane unieważnienia[16].

Powyższe ujęcie systemu mobilnego przysparza od razu problemu w zakresie obsługi mechanizmów zarządzania tożsamością osób i systemów. Dotychczas stosowane techniki albo wymagały ogromnego nakładu pracy i środków, aby utrzymać spójność takiego systemu, albo opierały się na założeniu, że w scenariuszach autonomicznej pracy zadania dotychczas realizowane przez system zarządzania tożsamością zostaną obsłużone w inny sposób, np. przez zapewnienie fizycznych środków ochrony (tj. np. osobistej weryfikacji osób wymieniających informacje). Problemy z dostępem do poszczególnych zasobów miały również swoje odzwierciedlenie w sposobie projektowania oraz podejścia do tematyki zarządzania repozytoriami certyfikatów. Dotychczas powszechnym podejściem było utrzymywanie jednego, głównego centrum autoryzacyjnego, skąd dane były przenoszone na pamięciach masowych do konkretnych urządzeń na dużym terenie. Tym sposobem unikano problemów z odpytywaniem pośrednich CA o ich dane, jednakże wymuszano również pełną centralizację takiego procesu, co zawsze obarczone jest dużym ryzykiem ze względu na łatwość uszkodzenia/zniszczenia jednego, głównego miejsca zamiast wielu mniejszych. Możliwe jest również pobieranie puli certyfikatów i zapamiętywanie ich lokalne, tak aby podczas pracy w terenie nie było potrzeby sięgania do infrastruktury klucza publicznego celem ustalenia tożsamości ewentualnych drugich stron wspólnie podejmowanych akcji. Problem nabiera znaczenia w momencie, gdy jednostki odłączają się od struktur PKI na długi czas i nie mają możliwości ciągłej i stałej weryfikacji certyfikatów obcych, jak również pobierania i aktualizowania list unieważnień.

5. Podsumowanie i kierunki dalszych badań

Obecnie istnieją różne podejścia do problemu dystrybucji informacji o zaufaniu w sieciach rozległych. W przypadku niewielkich struktur dotychczasowe rozwiązania wydają się wystarczające lub wymagają tylko niewielkich modyfikacji w celu dopasowania ich do konkretnego zastosowania przez ich użytkowników. Rozwiązania te dają również wybór podczas budowania bardziej złożonych i rozległych struktur, pod warunkiem, iż struktury te są stacjonarne oraz system pracuje w trybie on-line, a zatem pozwala na stałą komunikację pomiędzy różnymi elementami modelu, aby uzyskać

[16] http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf (data odczytu: 10.11.2014).

informacje konieczne do pracy. Jedynie model WWW pozwala na ciągłą pracę off-line, ze ściśle ustaloną liczbą węzłów, co do których użytkownik ma zaufanie.

Po przeprowadzeniu analizy udało się stwierdzić, że żaden z istniejących dzisiaj modeli zaufania nie jest dostatecznie dostosowany do systemów mobilnych. Obecne modele nie przewidują długich okresów bycia off-line poszczególnych elementów (poza modelem WWW), jak również nie mają żadnych mechanizmów pozwalających przynajmniej na podjęcie próby dystrybucji informacji o zaufaniu w ramach modelu, pomimo braku obecności wszystkich jego jednostek on-line. W obecnych rozwiązaniach mobilnych problem ten omija się przez fizyczną i manualną dystrybucję informacji o zaufaniu, tj. np. przenoszenie list unieważnień ręcznie, na zewnętrznym nośniku pomiędzy obiektami albo przez konieczność zebrania wszystkich obiektów ruchomych (wozy itp.) w jednym miejscu w celu przeprogramowania urządzeń zawierających informacje o zaufaniu. Zarówno jedno, jak i drugie przykładowe rozwiązanie nie wydaje się akceptowalne w scenariuszu innym niż ćwiczeniowy.

Pozwala to sformułować tezę, iż możliwe jest opracowanie lub modyfikacja istniejącego modelu, tak aby dostosować go do warunków mobilnych, w szczególności heterogenicznych środowisk sieciowych, wykorzystywanych przez instytucje administracji publicznej oraz służby państwowe (wojsko, policja).

Istotne jest to, aby stworzyć metody swobodnego przepływu danych związanych z unieważnieniami oraz nowymi certyfikatami bez obniżania poziomu bezpieczeństwa całego modelu. W rezultacie poziom bezpieczeństwa rozwiązania powinien być wyższy niż oryginału, ze względu na zapewnienie możliwie aktualnych list unieważnień, zapobiegających próbom nawiązywania połączenia ze skompromitowanymi węzłami. Najbardziej rozsądne wydaje się utworzenie rozszerzenia obecnie istniejących modeli, tak aby możliwe było zachowanie oryginalnego sposobu działania w przypadku potrzeby komunikacji z innym podmiotem nieobsługującym danego rozszerzenia. Podstawowym założeniem rozszerzenia powinna być również kompatybilność z innymi modelami zaufania, tj. dostateczne oderwanie od szczegółów i rozwiązań konkretnych modeli, aby możliwe było dowolne ich zmienianie w ramach stosowania tych samych funkcjonalności. Dodatkowo, obiecująco dla systemów mobilnych wyglądają następujące koncepcje, które można wdrożyć w ramach rozszerzenia obecnych modeli:

- dystrybucja CRL metodą P2P[17] pomiędzy różnymi węzłami domeny PKI – oszczędność łącza oraz szybszy czas reakcji na nowe zagrożenia;
- lokalne CRL, kreowane przez jednostki podrzędne, a następnie propagowane do jednostek wyższego rzędu; taki CRL działa lokalnie natychmiastowo, oczekując

[17] http://www.comp.nus.edu.sg/~bestpeer/paper/efficient-certificate-revocation-a.pdf (data odczytu: 10.11.2014).

po przesłaniu na akceptację węzłów nadrzędnych, w celu rozesłania go po całej domenie;
- mechanizm ratingowy pozwalający na ocenę lokalnych informacji na temat zaufania (lokalnych CRLi, nowych, nieznanych węzłów);
- dystrybucja nowych certyfikatów drogą P2P – tylko dla jednostek, które wcześniej posiadały już wydany certyfikat.

Powyższe propozycje mogą wyznaczać kierunek dalszych prac badawczych zmierzających do udoskonalenia systemów zarządzania tożsamością cyfrową. Przekłada się to bezpośrednio na wzrost bezpieczeństwa tychże systemów, co powinno znajdować się w obszarze zainteresowań każdej instytucji publicznej oraz rządowej.

Bibliografia

Adams C., Lloyd S., *PKI podstawy i zasady działania. Koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Jøsang A., *PKI Trust Models*, „Theory and Practice of Cryptography Solutions for Secure Information Systems (CRYPSIS)" 2013, May, s. 279–301.

Perlman R., *An Overview of PKI Trust Models*, „IEEE Network" 1999, vol. 13, November/December, s. 38–43.

PN-I-02000. Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia, Polski Komitet Normalizacyjny, 2002.

Szafrański B., *Główne wyzwania związane z modernizacją funkcjonowania państwa, IT w służbie efektywnego państwa*, „Roczniki" Kolegium Analiz Ekonomicznych, z. 29, Oficyna Wydawnicza SGH, Warszawa 2013, s. 309–324.

Windley P.J., *Digital Identity*, O'Reilly Media Inc., Sebastopol 2005.

Źródła sieciowe

http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf (data odczytu: 10.11.2014).

https://depot.ceon.pl/bitstream/handle/123456789/4437/rozprawa_pjatkiewicz.pdf (data odczytu: 10.11.2014).

http://people.dsv.su.se/~matei/courses/IK2002_SMOW/L8_AC6.pdf (data odczytu: 10.11.2014).

http://www.comp.nus.edu.sg/~bestpeer/paper/efficient-certificate-revocation-a.pdf (data odczytu: 10.11.2014).

https://www.cs.auckland.ac.nz/~pgut001/pubs/pkitutorial.pdf (data odczytu: 10.11.2014).

https://www.ietf.org/rfc/rfc5280.txt (data odczytu: 10.11.2014).

http://www.itu.dk/courses/DSK/E2003/DOCS/PKI_Trust_models.pdf (data odczytu: 10.11.2014).
http://www.itu.int/rec/T-REC–X.1252–201004-I (data odczytu: 10.11.2014).

* * *

Chosen problems of digital identity management in public administration institutions

Summary

Trust management is one of the most important things in designing IT systems, especially in public and governmental institutions. There are many different trust models used during building PKI solutions, but none seems to be suitable for mobile environments, where there is no constant connection to central repositories. The article focuses on such systems and points out issues that can occur when building a mobile IT system.

Keywords: digital identity, trust model, X.509, mobile systems, trust distribution