ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 605 STUDIA INFORMATICA NR 25 2010

TOMASZ KLASA
Zachodniopomorski Uniwersytet Technologiczny
w Szczecinie

ELEKTRONICZNA WERYFIKACJA TOŻSAMOŚCI W MEDYCZNYCH SYSTEMACH INFORMACYJNYCH

Stale rosnąca liczba elektronicznych lub wręcz webowych systemów medycznych jest odpowiedzialna za wiele procesów, które wcześniej wymagały wizyty osobistej. Obnażyło to problem weryfikacji tożsamości. Podczas gdy tradycyjne dokumenty tożsamości są bezużyteczne, wiele innych metod nie zapewnia pewnego powiązania tożsamości elektronicznej z rzeczywistą, co stwarza ryzyko podszycia się pod czyjąś tożsamość. Bezpieczny podpis elektroniczny wymaga z kolei certyfikatów kwalifikowanych, wystawianych przez komercyjne przedsiębiorstwa.

Proponowany system weryfikacji tożsamości korzysta z bezcertyfikatowej kryptografii klucza publicznego, co eliminuje komercyjne certyfikaty i wymóg zaufania autorytetom o biznesowych korzeniach. Zaufanie wywodzi się z instytucji państwowej oraz wydanego przez nią elektronicznego dokumentu tożsamości (e-ID). Prostsza infrastruktura i w pełni porównywalny z bezpiecznym podpisem elektronicznym poziom bezpieczeństwa powodują, że proponowany system jest interesującym rozwiązaniem, szczególnie na kilka miesięcy przed wprowadzeniem e-ID w Polsce.

1. Problem weryfikacji tożsamości w systemach medycznych

Tożsamość jest wymagana, by uzyskać dostęp do wielu usług, szczególnie medycznych. Wiele z nich jest realizowanych za pomocą lub z wykorzystaniem systemów informatycznych. Można wyróżnić następujące grupy systemów medycznych:

– systemy rejestracji pacjentów;
– telemedycyna (zdalne leczenie, zdalna diagnostyka, operacje i zabiegi);
– elektroniczne kartoteki danych medycznych (EHR);
– systemy wspomagające obrót lekami (w tym e-apteki);
– systemy obrotu receptami elektronicznymi.

Użytkownikami wymienionych systemów medycznych są nie tylko pacjenci, ale także lekarze, pielęgniarki, aptekarze czy przedstawiciele instytucji ubezpieczeniowych (refundacja leczenia). Każda z tych grup ma inne oczekiwania w stosunku do systemu i powinna mieć inne uprawnienia. Jednak czy podanie użytkownika i hasła jest równoznaczne z potwierdzeniem, że wprowadził je właściciel konta w systemie? Czy jest to wystarczający dowód, że na właśnie generowanej recepcie zapisano prawidłowe leki, które nie zagrożą zdrowiu pacjenta? Niestety, ze względu na słabe powiązanie konta w systemie informatycznym z rzeczywistą tożsamością trudno jest stwierdzić, kto jest autentycznym wykonawcą operacji, co stawia pod znakiem zapytania prawidłowość dokonanych działań. Oznacza to, że powstaje problem ze zgłaszaną przez użytkowników tożsamością – jak ją zweryfikować? Bez odpowiedniej weryfikacji tożsamości możliwości rozwoju systemów staną się ograniczone albo dane medyczne będą zagrożone. Choć ryzyko jest nieodłącznym elementem każdego biznesu [7] i nie można go wyeliminować w całości pomimo osiągnięcia wysokiej efektywności postępowania z nim [3], to bezpieczeństwo danych medycznych musi być bezwzględnie chronione. Jako że najbardziej oczywistym zagrożeniem w tym obszarze, oprócz braku dostępu do usługi, jest nieautoryzowany dostęp, niezbędne jest zastosowanie mechanizmu zdolnego jednoznacznie potwierdzić rzeczywistą tożsamość użytkownika systemu.

Weryfikacja tożsamości użytkowników medycznych systemów informacyjnych wynika z rozporządzeń ministrów [4, 5]. Jest podstawą do

przydzielenia uprawnień – pacjent może zapoznać się ze swoimi wynikami, wybrani lekarze powinni móc je odczytywać i zmieniać, podczas gdy osoby postronne nie mogą mieć prawa dostępu do tych danych medycznych. To istotne ze względu na wysokie ryzyko narażenia zdrowia ludzkiego w razie nieuprawnionego działania niepowołanych osób w systemie, ale także ze względu na wiele konsekwencji grożących w razie ujawnienia danych medycznych pacjenta. Dokumentacja medyczna zawierająca historię przebiegu chorób oraz przyjmowanych leków stanowi bezcenne źródło informacji dla firm ubezpieczeniowych i pracodawców, którzy mogą wykorzystać ją na niekorzyść pacjenta. Z tego powodu przechowywanie i przetwarzanie danych medycznych wymaga zastosowania odpowiednich środków bezpieczeństwa, znacznie poważniejszych niż to jest konieczne w przypadku zwykłych danych osobowych [1].

Najpowszechniej akceptowana obecnie metoda rozwiązania problemu weryfikacji tożsamości jest oparta na kryptografii klucza publicznego i określana jako bezpieczny podpis elektroniczny, z kwalifikowanym certyfikatem. Powszechność ta wynika wprost z Ustawy o podpisie elektronicznym [8], która definiuje bezpieczny podpis elektroniczny jako jedyny prawnie wiążący sposób potwierdzenia autorstwa dokumentu elektronicznego. W tym wypadku jedynie bezpieczny podpis elektroniczny złożony pod deklaracją tożsamości i wnioskiem o udostępnienie danych jest prawnie równoznaczny z osobiście podpisanym wnioskiem. Mimo że metoda ta jest powszechnie uznawana za pewną, znacząca część bezpieczeństwa zależy od zaufanej trzeciej strony (TTP), czyli od skorzystania z usług komercyjnych centrów certyfikacyjnych, których misją nie jest służba społeczeństwu, ale trwanie w warunkach gospodarki rynkowej i zarabianie pieniędzy. Pomimo wielu ograniczeń nadal są to zwykłe przedsiębiorstwa, a nie instytucje państwowe. Niestety, nie istnieje dowód wskazujący, dlaczego dana firma jest godna zaufania. Sprawa nie dotyczy jedynie matematycznego wywodu, ale przede wszystkim ekonomii. TTP to nic innego jak w pełni komercyjne przedsiębiorstwa, jak wiele innych. Dlaczego TTP, choć ma odpowiedni certyfikat, ma wzbudzać większe zaufanie niż firma, która skorzystała z jej usług, jeśli usługobiorca nie zna żadnej z nich? Z tego powodu należy poszukać alternatywnych rozwiązań zapewniających odpowiedni poziom bezpieczeństwa.

2. Proponowany system weryfikacji tożsamości

Proponowany system korzysta z możliwości elektronicznego dowodu tożsamości oraz z bezcertyfikatowej kryptografii klucza publicznego, określanej mianem CL-PKC[1], która jest używana do generowania par kluczy, szyfrowania oraz podpisywania dokumentów elektronicznych.

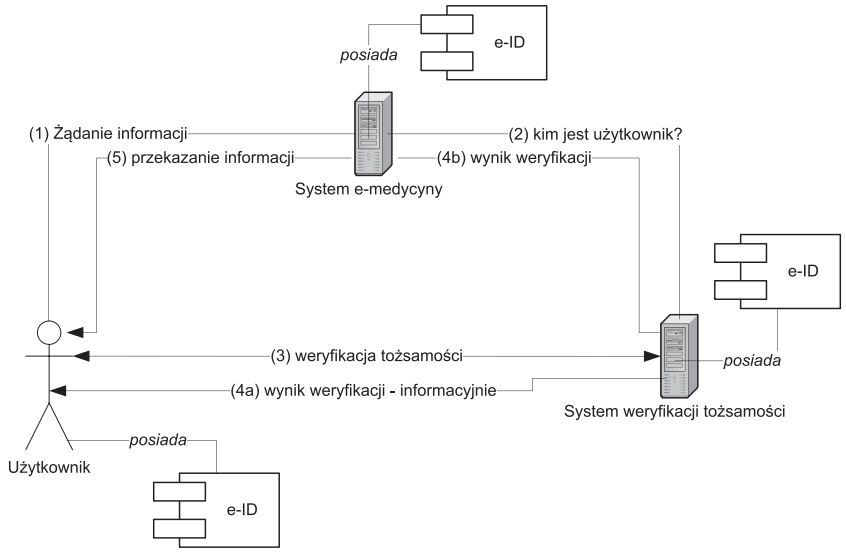
Ogólna zasada działania systemu została zaprezentowana na rysunku 1. Podstawowym założeniem, które poczyniono, jest posiadanie przez każdego uczestnika ważnego elektronicznego dokumentu tożsamości. Oznacza to, że dokument taki, co oczywiste, należałby do użytkowników (osób). Byłby jednak wystawiany także na firmy i ich systemy informatyczne, co stanowiłoby znaczną zmianę jakościową w porównaniu ze stanem obecnym. W pewnym sensie mógłby być postrzegany jako „certyfikat" firmy, ale w praktyce nie jest to nic więcej niż szereg danych podstawowych przedsiębiorstwa oraz repozytorium par kluczy, będących w jego władaniu. Na rysunku 1 dokument tożsamości odwołuje się do systemów informatycznych, ale zakłada się, że zawiera on dane podmiotu będącego właścicielem systemu. W przypadku przedsiębiorstw termin e-ID odnosi się do zawartości, natomiast zdecydowanie nie do formy. W przeciwieństwie do dokumentu osoby fizycznej może nie mieć postaci karty i istnieć jedynie jako pliki zapisane w bezpieczny sposób, np. w pamięci tokena. W każdym razie nie należy oczekiwać formy tożsamej z kartą smart z danymi podstawowymi wytłoczonymi na jej powierzchni oraz zapisanymi w jej pamięci.

Zakłada się, że wykonując krok (1) przedstawiony na rysunku 1, użytkownik jest dla systemu e-medycyny anonimowy. System nie posiada bazy danych osobowych pacjentów, a użytkownik nie jest zalogowany lub uwierzytelniony w systemie. W takiej sytuacji żądanie jakichkolwiek danych przez użytkownika musi rodzić pytanie ze strony systemu medycznego o jego tożsamość. Dlatego obsługa jest przekazywana do systemu weryfikacji tożsamości. Ten, z perspektywy użytkownika, ujawnia się jako niepomijalny pośrednik.

Przeprowadzana jest procedura weryfikacyjna, oparta na protokole weryfikacji tożsamości. Uzyskany wynik jest zwracany do systemu e-medycyny jako podstawa do podjęcia dalszych działań – np. przekazania informacji

[1] CL-PKC zostało zaproponowane przez Sattama Al-Riyami oraz Kennetha Patersona [2].

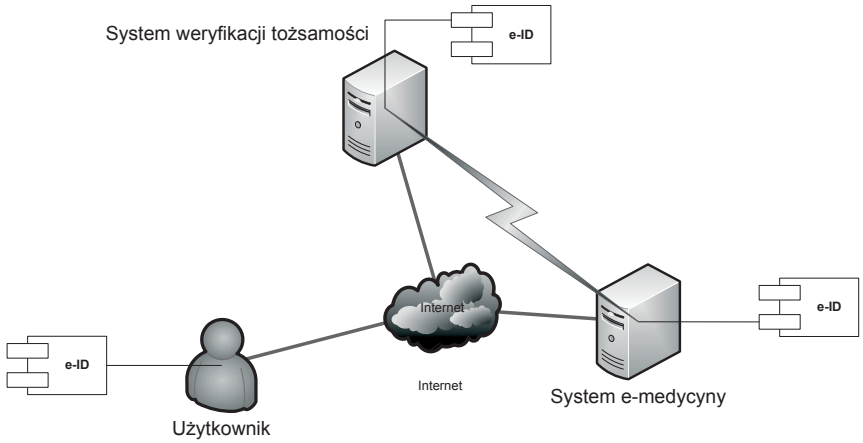
– oraz, informacyjnie, do użytkownika. Zakłada się, że pozytywna weryfikacja tożsamości nie oznacza bezwarunkowego wykonania żądanej operacji, lecz stanowi warunek konieczny do uruchomienia wewnętrznych procedur autoryzacyjnych w ramach systemu e-medycyny, które na podstawie potwierdzonej tożsamości zastosują właściwy zakres uprawnień.



Rys 1. Współpraca systemu weryfikacji tożsamości z systemem medycznym
Źródło: opracowanie własne.

Rysunek 2 przedstawia umiejscowienie systemu weryfikacji tożsamości wobec użytkownika i systemu e-medycyny. Proponowany system weryfikacji tożsamości może być połączony z systemem e-medycyny poprzez sieć lokalną, ale może też łączyć się z nim, co pokazano na rysunku 2, poprzez sieć publiczną Internet. W każdym przypadku nawiązują stałą współpracę, przy czym jeden system weryfikacji tożsamości może obsługiwać wiele systemów informacyjnych, natomiast system e-medycyny (jak i każdy inny system informacyjny), co do zasady, będzie współpracował z jednym systemem weryfikacji tożsamości. Zakłada się, że użytkownik łączy się z systemem medycznym oraz wydaje wszelkie polecenia za pośrednictwem sieci publicznej Internet. Użytkownik nie może zidentyfikować systemu weryfikacji tożsamości

jako niezależnego elementu systemu medycznego, a w szczególności nie może nawiązać z nim połączenia bezpośrednio, z pominięciem systemu e-medycyny. Oznacza to, że do chwili przekazania obsługi oraz po przejęciu obsługi przez system medyczny dla użytkownika system weryfikacji tożsamości pozostaje w pełni transparentny.



Rys. 2. Umiejscowienie systemu weryfikacji tożsamości
Źródło: opracowanie własne.

3. Protokół weryfikacji tożsamości zastosowany w proponowanym systemie

Zastosowany protokół weryfikacji tożsamości został przedstawiony na rysunku 3. Do opisu komunikatów przesyłanych pomiędzy trzema stronami użyto następujących oznaczeń:

– z1 – zawartość żądania użytkownika, zależna od systemu medycznego; zakłada się, że zawiera wartość losową
– (M) KEn – wiadomość M zaszyfrowana kluczem publicznym strony n
– H (M) – wartość skrótu[2] z M

[2] Dostępnych jest wiele funkcji skrótu, ze względu na bezpieczeństwo zakłada się użycie silnej funkcji skrótu, np. SHA-512 [6].

– IDTa – tymczasowa tożsamość użytkownika (losowy identyfikator)
– a – identyfikator sesji (liczba losowa)
– Ric – żądanie zgłoszenia tożsamości (nagłówek wiadomości)
– Sign (M) – wiadomość M podpisana elektronicznie przez stronę n ID_n – zgłaszana tożsamość strony n, tożsame z H (ID_n)
– idKGC – identyfikator KGC, które wydało dokument e-ID strony
– KSn – klucz publiczny strony n służący do weryfikacji podpisu elektronicznego
– KEn – klucz publiczny strony n służący do szyfrowania wiadomości
– b – wyzwanie (w postaci b1|b2, gdzie b1 i b2 są liczbami losowymi)
– b' – odpowiedź (wyzwanie poddane transformacji do postaci b2+5|b1)
– f – wynik weryfikacji tożsamości
– z2 – wynik weryfikacji tożsamości plus udostępnione dane albo wynik żądanej operacji.

Pierwszy krok zastosowanego protokołu to wystawienie żądania przez użytkownika. Komunikat ten jest sformatowany zgodnie z wymogami i oczekiwaniami systemu medycznego. Jedyne założenie, jakie należy poczynić, to zamieszczenie wartości losowej w ramach komunikatu. Ma to istotny wpływ na bezpieczeństwo, np. poprzez możliwość wykrycia próby ataku powtórzeniowego.

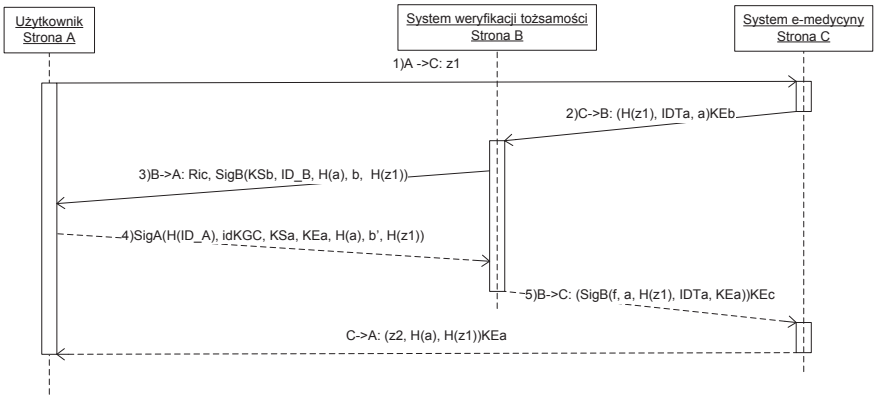
Kolejny komunikat stanowi przekazanie obsługi użytkownika do systemu weryfikacji tożsamości. Aby zapewnić poufność żądania użytkownika, przekazywany jest jedynie jego skrót – posłuży on do wykrywania powtórzonych zapytań oraz do późniejszej identyfikacji rezultatu przez system medyczny. Jednocześnie przekazywana jest tymczasowa tożsamość użytkownika. Ma ona postać losowego identyfikatora, nadawanego automatycznie przez system e-medycyny. Ponadto przekazywany jest losowy token sesyjny, który posłuży do kontroli świeżości wyniku otrzymanego od systemu weryfikacji. Wiadomość jest szyfrowana, by uniemożliwić śledzenie aktywności użytkownika na podstawie tymczasowych identyfikatorów.

Komunikat trzeci jest pierwszą wiadomością samej weryfikacji tożsamości. System weryfikacji przedstawia się użytkownikowi za pomocą podpisanego przez siebie komunikatu z własną tożsamością i identyfikatorem KGC. Do wiadomości tej dołączony jest także klucz publiczny, niezbędny

do późniejszej weryfikacji podpisu, oraz skróty tokena sesji i żądania użytkownika. Uzupełnieniem komunikatu jest losowa wartość wyzwania.

Przekazywanie tokena sesji na tym etapie pod postacią skrótu wyodrębnia dwie sesje z jednokierunkowym powiązaniem między nimi. Dzięki temu ograniczone zostaje ryzyko, że osoby postronne będą w stanie śledzić aktywność użytkownika o znanej tożsamości.

W odpowiedzi na taką wiadomość użytkownik musi się przedstawić, przesyłając skrót swojej tożsamości, identyfikator KGC, które wydało e-ID użytkownika, parę kluczy publicznych niezbędnych do szyfrowania oraz weryfikacji podpisanych wiadomości. Jako uzupełnienie przesyłany jest skrót tokena sesji, wartość odpowiedzi na wyzwanie oraz skrót żądania użytkownika.



Rys. 3. Protokół weryfikacji tożsamości zastosowany w proponowanym systemie
Źródło: opracowanie własne.

Rezultat weryfikacji tożsamości jest przekazywany szyfrogramem zwrotnie do systemu medycznego. Treść, złożona z wyniku weryfikacji, tokena sesji, skrótu żądania oraz tymczasowego identyfikatora użytkownika i jego klucza publicznego, jest podpisana elektronicznie. Szyfrowanie tej wiadomości chroni powiązanie tymczasowego identyfikatora z kluczem publicznym, co mogłoby być wykorzystane do śledzenia aktywności użytkownika przez osoby postronne.

Na zakończenie, już poza systemem weryfikacji tożsamości, system e-medycyny generuje komunikat z wynikami weryfikacji i danymi, których zażądał użytkownik. Dodatkowo zawiera on skrót tokena sesji oraz skrót żądania użytkownika, co pozwoli mu zweryfikować świeżość odpowiedzi oraz powiązać ją z odpowiednim żądaniem.

Weryfikacja podpisów elektronicznych, które już w trakcie generowania kluczy prywatnych są powiązane z tożsamością, pozwala na jednoznaczne potwierdzenie autorstwa dokumentu lub żądania operacji. Odbywa się to poprzez wykonanie sekwencji operacji matematycznych na krzywych eliptycznych, z użyciem otrzymanego wraz z tożsamością klucza publicznego. Otrzymany rezultat jest jednoznaczny i nie może być zafałszowany poprzez podmianę tożsamości lub podstawienie fałszywej pary kluczy. W obu sytuacjach próba oszustwa zostanie wykryta, a weryfikacja zakończy się niepowodzeniem.

Wnioski

Informacja jest często najistotniejszym czynnikiem wpływającym na sukces lub porażkę przedsiębiorstwa. W przypadku branży medycznej informacje te dotyczą najbardziej wrażliwego z obszarów – zdrowia pacjentów. Ich wyjawienie osobie nieupoważnionej może oznaczać zarówno problemy dla pacjenta, jak i poważne skutki dla przedsiębiorstwa medycznego, które te dane przetwarza. Dlatego tak istotne jest, by każde żądanie dostępu do danych przechowywanych i przetwarzanych przez systemy medyczne było poprzedzone skuteczną weryfikacją tożsamości użytkownika. Dopiero po potwierdzeniu tożsamości system może określić, jakie uprawnienia przysługują danej osobie, a w rezultacie – czy powinna otrzymać dostęp do żądanych informacji lub operacji systemowych. Niestety, obecnie w wielu sytuacjach trudno jest potwierdzić zgłaszaną tożsamość na poziomie systemu informatycznego.

Problem ten został częściowo rozwiązany prawnie za pomocą bezpiecznego podpisu elektronicznego opartego na certyfikacie kwalifikowanym. Niestety wiele innych problemów powstaje po zastosowaniu tej metody. Najistotniejsze z nich dotyczą zaufania i ogromnej infrastruktury wymaganej do zapewnienia bezpieczeństwa. Mimo to stosuje się ją powszechnie i aktualnie jako jedyna jest prawnie wiążącą metodą potwierdzenia dokumentu

elektronicznego. Nie oznacza to, że staje się tańsza czy mniej podatna na zawirowania ekonomiczne gospodarki, gdyż certyfikaty kwalifikowane są z reguły dostarczane przez przedsiębiorstwa komercyjne, które jak każde inne mogą stanąć w obliczu bankructwa lub zostać przejęte. Między innymi z tego powodu, że celem firm certyfikujących jest trwanie na rynku i zarabianie pieniędzy, niezbędne było rozbudowanie infrastruktury do obecnych rozmiarów.

Proponowany system opiera się na bezcertyfikatowej kryptografii klucza publicznego. Największą zaletą tego rozwiązania jest nie tyle cena, ile źródło zaufania. W proponowanym systemie nie powstaje ono w związku biznesu z państwowymi dokumentami, ale bezpośrednio w instytucji, która ten dokument wydała. Ponadto brak certyfikatów upraszcza infrastrukturę. Poziom zabezpieczeń samego dokumentu jest wyznaczany i w pewnym sensie gwarantowany przez państwo. Trudno sobie obecnie wyobrazić jakikolwiek istotny dokument państwowy bez stosownych zabezpieczeń. Proponowany system jest w rzeczywistości bardzo podobny do procedur stosowanych od stuleci w życiu codziennym. Możemy nie ufać rządowi, ale wierzymy dokumentom, które wydaje.

Proponowany system został opracowany jako proste, lecz bezpieczne rozwiązanie. Bezpieczeństwo było jednym z głównych celów podczas projektowania protokołu oraz systemu opartego na nim. Wysoki standard w tym obszarze zapewnia kryptografia bezcertyfikatowa, oparta na odwzorowaniach bilingowych na krzywych eliptycznych, oraz dodatkowe szyfrowanie wybranych komunikatów. Proponowany system jest w pełni porównywalny pod względem bezpieczeństwa z bezpiecznym podpisem elektronicznym opartym na certyfikacie kwalifikowanym. Jednocześnie jest znacznie prostszy. W całym procesie weryfikacji tożsamości uczestniczą obligatoryjnie jedynie trzy strony (użytkownik, system medyczny, system weryfikacji tożsamości), bez konieczności odwoływania się do wielu usług.

Literatura

1. Agrawal R., Johnson C., *Securing electronic health records without impending the flow of information*, „Int. J. of Medical Informatics" nr 76/2007.
2. Al.-Riyami S., Paterson K., *Certificateless public key cryptography, AsiaCrypt proceedings*, 2003.

3. Nowakowski A., Klasa T., *Evaluation of information systems' risk treatment efficiency proposal*, „Metody Informatyki Stosowanej" nr 3 (20), Polska Akademia Nauk Oddział w Gdańsku Komisja Informatyki, Szczecin 2009.
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. 2004 r. nr 100 poz. 1024 z późniejszymi zmianami.
5. Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania, Dz.U. 06.247.1819 z późniejszymi zmianami.
6. Secure Hash Standard, Federal Information Processing Standards Publication 180–2, NIST, 2002.
7. Szyjewski Z., Klasa T., *Computer-aided risk tree method in risk management*, „Polish Journal of Environmental Studies", t. 17, nr 3B, Olsztyn 2008.
8. Ustawa o podpisie elektronicznym, Dz.U. 2001 nr 130 poz. 1450 z późniejszymi zmianami.

ELECTRONIC IDENTITY VERIFICATION IN MEDICAL INFORMATION SYSYTEMS

Summary

Growing number of medical information systems is responsible for many processes that earlier required personal meeting. This revealed a problem with identity verification. While traditional ID documents are worthless, many other methods do not bind trustfully electronic identity with the real one, which causes risk of impersonification attack. And secure digital signature requires qualified certificates, issued by commercial companies.

Proposed identity verification system makes a use of certificateless public key cryptography, which eliminates commercial certificates and requirement of trust to business-based authorities. Trust origins from governmental institution and e-ID issued by it, just like in analog world. Simpler infrastructure and fully comparable security level make it an interesting alternative. Especially only months prior to introduction of e-ID documents in Poland.

Translated by Tomasz Klasa