Grzegorz Kozieł

Wydział Elektrotechniki i Informatyki
Politechnika Lubelska

Podpis elektroniczny – rozwiązania techniczne i uwarunkowania prawne

1. Wstęp

Powszechny dostęp do technologii informacyjnych oraz wypieranie form tradycyjnej komunikacji przez komunikację elektroniczną wymaga wprowadzania nowych form zabezpieczeń. Muszą one zapewniać możliwość weryfikacji tożsamości nadawcy wiadomości, zabezpieczać przed niepowołanym dostępem osób trzecich i jednocześnie potwierdzać autentyczność otrzymanych danych. W wielu przypadkach dodatkowo konieczne jest spełnienie wymogów prawa, aby przekazane dane mogły być traktowane na równi z dokumentem opatrzonym podpisem odręcznym. Formą zabezpieczenia spełniającą wszystkie powyższe wymagania jest podpis elektroniczny. Zgodnie z art. 5 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262): „Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej”[1].

2. Techniki kryptograficzne

Standardem w ochronie danych jest obecnie stosowanie rozwiązań kryptograficznych. Pozwalają one na przekształcenie danych z postaci jawnej – zrozumiałej dla człowieka – w postać niejawną, która jest inną formą zapisu

[1] http://prawo.legeo.pl/prawo/ustawa-z-dnia-18-wrzesnia-2001-r-o-podpisie-elektronicznym/rozdzial-i_przepisy-ogolne/?on=25.02.2013 (data odczytu 19.11.2013).

tych samych danych, niezrozumiałą dla odbiorcy[2]. Do przekształcania danych używamy specjalistycznych algorytmów. Ich budowa jest powszechnie znana. Jednak aby uniemożliwić odszyfrowanie danych osobie postronnej posiadającej algorytm, wprowadzono klucz kryptograficzny. Jest to dodatkowa porcja danych niezbędna w procesie szyfrowania i deszyfrowania danych. Bez użycia właściwego klucza kryptograficznego niemożliwe jest poprawne deszyfrowanie danych, a co za tym idzie – nie uda się ich odczytać. Oczywiście istnieją techniki łamania zabezpieczeń kryptograficznych, które zazwyczaj są tym skuteczniejsze, im krótszy i łatwiejszy do odgadnięcia jest klucz kryptograficzny. Od siły klucza kryptograficznego zależy więc siła stosowanego zabezpieczenia[3].

Rozróżniamy dwa rodzaje kryptografii – kryptografię symetryczną i kryptografię asymetryczną. Cechą charakterystyczną kryptografii symetrycznej jest to, że używa tego samego klucza do szyfrowania i deszyfrowania danych. Schemat symetrycznego system kryptograficznego został przedstawiony na rysunku 1.

Rysunek 1. Symetryczny system kryptograficzny

Źródło: opracowanie własne na podstawie: A. Menzenes, T.P. Oorscho, S. Vanstone, *Kryptografia stosowana*, WNT, Warszawa 2005.

Symetryczne systemy kryptograficzne doskonale nadają się do ochrony zasobów danych mających jednego właściciela. Jednak nie sprawdzają się w przypadku ochrony komunikacji pomiędzy różnymi osobami. Powodem tego jest fakt wykorzystania jednego wspólnego klucza do wszystkich operacji. Udostępnienie klucza jednej z osób daje je możliwość późniejszego odszyfrowywania danych zaszyfrowanych przy użyciu tego samego klucza, nawet jeśli są przeznaczone dla innego adresata. Aby system symetryczny zapewniał poufności komunikacji,

[2] T. Kifner, *Polityka bezpieczeństwa i ochrony informacji*, Helion, Gliwice 1999.
[3] F. Bauer, *Sekrety kryptografii*, Helion, Gliwice 2002.

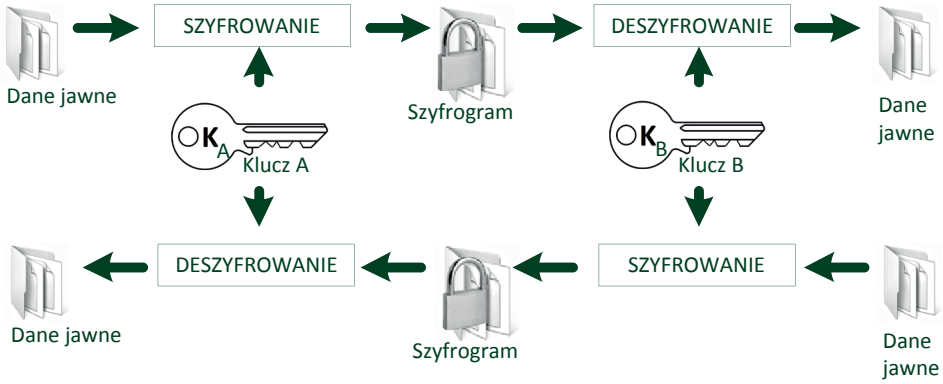
należałoby przypisać i stosować niezależny klucz w przypadku każdej osoby, z którą się komunikujemy. Wymagałoby to utworzenia olbrzymiej bazy kluczy oraz mechanizmu ich stosowania. Poza tym pozostaje jeszcze problem przekazywania kluczy drugiej stronie biorącej udział w komunikacji. Klucze muszą bowiem zostać przekazane kanałem bezpiecznym, czyli w sposób uniemożliwiający podsłuchanie. Ponadto niemożliwa do rozwiązania jest kwestia udowodnienia tożsamości nadawcy wiadomości. Istnieje bowiem możliwość „spreparowania" wiadomości przez odbiorcę, co w procesach formalnej wymiany dokumentów stanowi poważny problem.

Rozwiązanie tych problemów możliwe jest przez zastosowanie kryptografii asymetrycznej. Oferuje ona zupełnie inne podejście do szyfrowania. Korzysta bowiem z par wzajemnie się uzupełniających kluczy kryptograficznych. Jeżeli klucze należące do jednej pary oznaczymy jako K_A oraz K_B, wówczas dane zaszyfrowane za pomocą klucza K_A będą mogły zostać odszyfrowane tylko za pomocą klucza K_B. Analogicznie przedstawia się sytuacja szyfrowania kluczem K_B. Dane zaszyfrowane nim mogą zostać odszyfrowane tylko za pomocą klucza K_A. Podejście to umożliwia tworzenie systemów zabezpieczeń pozwalających na zapewnienie autentyczności i poufności wiadomości oraz na potwierdzanie tożsamości nadawcy.

Jeżeli jeden z kluczy będzie znajdował się tylko w posiadaniu osoby szyfrującej dane, a drugi zostanie udostępniony publicznie, pozwoli to na potwierdzenie tożsamości nadawcy, każdy bowiem będzie mógł pobrać klucz udostępniony publicznie i odszyfrować przy jego pomocy dane. Jeżeli proces się powiedzie, będzie to dowodem na to, że dane zostały zaszyfrowane kluczem znajdującym się w posiadaniu właściciela drugiego klucza z użytej pary kluczy[4].

Jak wiemy, możliwe jest szyfrowanie za pomocą dowolnego klucza z pary kluczy. Jeżeli zaszyfrujemy dane za pomocą klucza udostępnionego publicznie przez określoną osobę, wówczas odszyfrowanie danych będzie możliwe tylko za pomocą klucza znajdującego się w posiadaniu właściciela wzmiankowanej pary kluczy. Pozwoli to na zachowanie poufności komunikacji, gdyż klucz umożliwiający odszyfrowanie danych znajduje się w posiadaniu jednej osoby. Schemat asymetrycznego systemu kryptograficznego został przedstawiony na rysunku 2.

[4] O.O. Khalifa, M.R. Islam, S. Khan, M.S. Shebani, *Communications cryptography*, RF and Microwave Conference, 2004, RFM 2004. Proceedings, DOI: 10.1109/RFM.2004.1411111.



Rysunek 2. Asymetryczny system kryptograficzny

Źródło: opracowanie własne na podstawie: A. Menzenes, T.P. Oorscho, S. Vanstone, *Kryptografia stosowana*, WNT, Warszawa 2005.

3. Podpis cyfrowy

Rozwiązania dostarczone przez kryptografię asymetryczną zostały wykorzystane do opracowania podpisu cyfrowego. Podpis cyfrowy to nic innego jak wygenerowana para kluczy kryptograficznych przeznaczonych dla wybranego algorytmu kryptografii asymetrycznej. Zawiera on klucz prywatny (ang. *private key*) oraz klucz publiczny (ang. *public key*). Klucz prywatny znajduje się w posiadaniu właściciela podpisu cyfrowego i jest pilnie strzeżony. Klucz publiczny jest udostępniany wszystkim, najczęściej za pomocą Internetu.

Właściciel podpisu cyfrowego podpisuje dane, używając swojego klucza prywatnego. Każdy człowiek ma możliwość pobrania klucza publicznego i zweryfikowania podpisu – jeżeli operacja deszyfrowania powiedzie się, wówczas uzyskujemy pewność, że nadawcą jest właściciel podpisu cyfrowego, do którego należy użyty klucz publiczny. Dodatkowo uzyskujemy pewność, że podpisane dane są autentyczne. Wprowadzenie jakiejkolwiek modyfikacji do zaszyfrowanej wiadomości uniemożliwiłoby jej prawidłowe odszyfrowanie[5].

[5] N. Zhu, G.X. Xiao, *Application of a Scheme of Digital Signature in Electronic Government*, 2008 International Conference on Computer Science and Software Engineering, DOI: 10.1109/CSSE.2008.929.

4. Skróty kryptograficzne w podpisie cyfrowym

Przedstawione rozwiązanie nie zapewnia jednak poufności danych, każdy z użytkowników Internetu posiada bowiem dostęp do klucza publicznego nadawcy i jest w stanie odszyfrować dane. W takiej sytuacji szyfrowanie całego przesyłanego zbioru danych jest marnotrawstwem zasobów i czasu. Aby tego uniknąć, wprowadzano funkcję skrótu (ang. *hash*). Funkcją skrótu nazywamy jednokierunkowe przekształcenie matematyczne pozwalające wygenerować skrót danych. Skrót jest ciągiem bitów o określonej długości, najczęściej od 128 do 512 bitów[6]. Funkcja skrótu powinna zapewniać z prawdopodobieństwem bliskim pewności, że dla dwóch różnych zbiorów danych nie zostanie wygenerowany taki sam skrót.

Aby kryptograficzna funkcja skrótu została uznana za bezpieczną, musi spełniać następujące wymagania[7]:

- Wykazywać odporność na kolizje (ang. *collision resistance*), czyli z prawdopodobieństwem bliskim pewności uniemożliwiać wygenerowanie dwóch różnych wiadomości posiadających taki sam skrót.
- Posiadać odporność pierwszego i drugiego rzędu na kolizję dwóch wiadomości. W praktyce oznacza to, że nie może istnieć szybka metoda wyznaczania danych D na podstawie skrótu S, takich, że wartość funkcji skrótu H(D) = S. Nie może jednocześnie istnieć żadna szybka metoda pozwalająca na wyznaczenie zbioru danych D2 na podstawie zbioru danych D1, takich, że obydwa zbiory danych posiadają taki sam skrót $H(D1) \neq H(D2)$.
- Być funkcją jednokierunkową, czyli nie może istnieć możliwość wnioskowania o danych wejściowych na podstawie uzyskanego skrótu. Zmiana jednego bitu w danych wejściowych powinna powodować zmianę wartości znacznej liczby bitów skrótu w sposób uniemożliwiający przeprowadzenie kryptoanalizy różnicowej.

W praktyce nie istnieje matematyczna metoda określania stopnia bezpieczeństwa oferowanego przez określoną funkcję skrótu. Ocena opiera się więc

[6] G.W. Romney, D.W. Parry, *A Digital Signature Signing Engine to Protect the Integrity of Digital Assets*, Information Technology Based Higher Education and Training, ITHET '06. 7th International Conference, 2006, DOI: 10.1109/ITHET.2006.339702.

[7] S. Yunling, M. Xianghua, *An Overview of Incremental Hash Function Based on Pair Block Chaining, Information Technology and Applications (IFITA)*, 2010 International Forum, DOI: 10.1109/IFITA.2010.332.

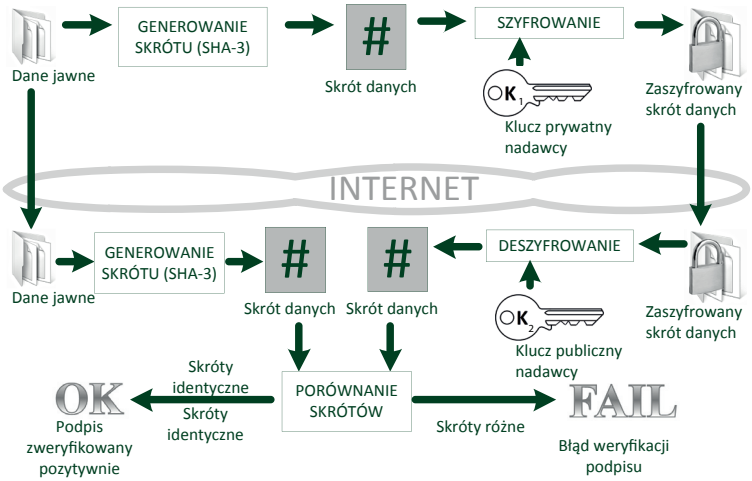
na wyniku eksperymentalnego określenia podatności funkcji na znane ataki kryptoanalityczne.

Funkcje skrótu są wykorzystywane w procesie realizacji podpisu cyfrowego. Jako że podpis cyfrowy nie zabezpiecza przed nieuprawnionym dostępem, zamiast podpisywania całego zbioru danych podpisywany jest jego skrót. Pierwszym etapem jest więc wygenerowanie skrótu podpisywanego zbioru danych. Następnie za pomocą klucza prywatnego jest podpisywany uzyskany skrót kryptograficzny. Zaszyfrowana postać skrótu stanowi podpis cyfrowy zbioru danych. Musi ona być przekazywana łącznie ze zbiorem danych, aby możliwe było zweryfikowanie ich podpisu.

Weryfikacja podpisu jest procesem trójetapowym. Na pierwszym etapie deszyfrowany jest skrót danych za pomocą klucza publicznego osoby, która podpisała dane. Drugi etap obejmuje wygenerowanie skrótu danych, które mają być zweryfikowane. Trzeci etap polega na porównaniu odszyfrowanego skrótu danych ze skrótem obliczonym na podstawie otrzymanych danych. Jeżeli skróty są identyczne uznaje się, że dane są autentyczne i pochodzą od właściciela podpisu cyfrowego użytego do odszyfrowania skrótu danych.

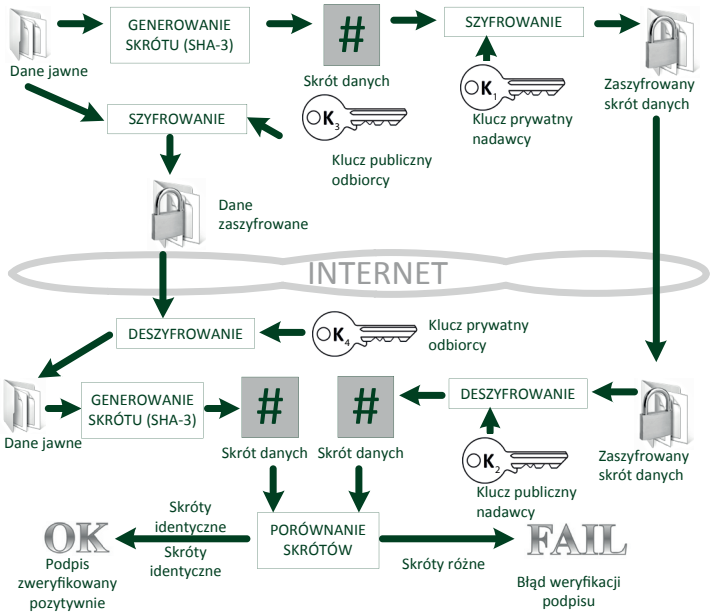
Nie istnieje inny sposób weryfikacji podpisu cyfrowego, gdyż z założenia funkcja skrótu jest jednokierunkowa i niemożliwe jest odtworzenie danych na podstawie ich skrótu. Konieczne jest więc ponowne wyliczenie skrótu danych i weryfikacja ich poprawności przez porównanie jej skrótów – aktualnie obliczonego z wygenerowanym wcześniej i podpisanym przez właściciela. Schemat systemu realizującego podpis cyfrowy został pokazany na rysunku 3.

Czynnością niezbędną w komunikacji biznesowej jest zabezpieczanie wiadomości przed niepowołanym odczytem. Samo potwierdzenie autentyczności danych oraz tożsamości nadawcy nie jest wystarczające. Możliwe jest zapewnienie poufności przy wykorzystaniu infrastruktury podpisu cyfrowego. Wykonywane jest to przed ich wysłaniem przez zaszyfrowanie danych za pomocą klucza publicznego adresata. W ten sposób uzyskujemy pewność, że jedyną osobą posiadającą możliwość odczytu danych jest adresat, będący jednocześnie posiadaczem jedynej kopii klucza prywatnego. Schemat systemu komunikacji z wykorzystaniem podpisu cyfrowego, zapewniający jednocześnie poufność przesyłanych danych, został przedstawiony na rysunku 4.



Rysunek 3. Realizacja podpisu cyfrowego z wykorzystaniem funkcji skrótu

Źródło: opracowanie własne na podstawie: A. Menzenes, T.P. Oorscho, S. Vanstone, *Kryptografia stosowana*, WNT, Warszawa 2005.



Rysunek 4. Realizacja podpisu cyfrowego z jednoczesnym szyfrowaniem danych kluczem publicznym adresata

Źródło: opracowanie własne na podstawie: A. Menzenes, T.P. Oorscho, S. Vanstone, *Kryptografia stosowana*, WNT, Warszawa 2005.

5. Certyfikacja podpisów cyfrowych

Aby podpisy cyfrowe były wiarygodne, musi istnieć sposób poświadczenia ich oryginalności. W przeciwnym przypadku możliwe byłoby wygenerowanie przez dowolną osobę fałszywego klucza i podpisywanie nim danych w cudzym imieniu.

Poświadczenie oryginalności podpisu cyfrowego, zwane również certyfikatem podpisu cyfrowego, jest wykonywane przez podpisanie klucza publicznego oraz informacji o właścicielu podpisu przez inną osobę lub instytucję. Certyfikat podpisu cyfrowego to struktura zawierająca publiczny klucz szyfrujący certyfikowanego podpisu cyfrowego, dane posiadacza podpisu oraz podpis cyfrowy tych dwóch struktur złożony przez zaufaną trzecią stronę[8]. Istnieją dwa sposoby poświadczania oryginalności podpisów cyfrowych:

- Zdecentralizowany oparty na sieci zaufania. Polega on na składaniu podpisu cyfrowego poświadczającego oryginalność przez osoby, które zweryfikowały osobiście człowieka czy też instytucję posługującą się danym podpisem elektronicznym. Wiarygodność podpisu jest wówczas równa wiarygodności certyfikujących ten podpis osób.
- Oparty na hierarchii urzędów certyfikacji. W systemie tym poświadczenie oryginalności podpisu jest wykonywane przez centrum autoryzacji, czyli zaufaną instytucję wydającą certyfikat podpisu cyfrowego, zwaną urzędem certyfikacji.

Najbardziej znanymi certyfikatami klucza publicznego są PGP, SPKI/SDSI oraz X.509. Dwa pierwsze są oparte na sieci zaufania, certyfikat X.509 bazuje na hierarchii urzędów certyfikacji[9].

6. Bezpieczny podpis elektroniczny

Omówiony powyżej podpis cyfrowy jest jedynie rozwiązaniem technicznym pozwalającym realizować funkcje poświadczania autentyczności danych, weryfikacji tożsamości osoby podpisującej dane oraz zabezpieczania danych przed niepowołanym dostępem. Nie ma on jednak skutków prawnych. Aby mógł być używany do

[8] S. Hamdy, *Towards a Better Applicability of Public-Key Certificates*, Innovations in Information Technology, 4th International Conference, 2007, DOI: 10.1109/IIT.2007.4430387.

[9] P. Wohlmacher, P. Pharow, *Applications in health care using public-key certificates and attribute certificates*, Computer Security Applications, 16th Annual Conference, 2000, DOI: 10.1109/ACSAC.2000.898866.

podpisywania danych i miał skutki prawne, musi spełniać wymogi bezpiecznego podpisu elektronicznego. Tylko bezpieczny podpis elektroniczny weryfikowany przy pomocy certyfikatu kwalifikowanego ma skutki prawne zgodnie z ustawą o podpisie elektronicznym, pod warunkiem, że został złożony w okresie ważności tego certyfikatu. Według prawa polskiego, stanowi on dowód na to, że został złożony przez osobę, która jest określona w nim jako składająca podpis elektroniczny[10].

Bezpieczny podpis elektroniczny musi – według ustawy o podpisie elektronicznym – być:

- Przyporządkowany wyłącznie do osoby, która składa ten podpis.
- Wykonany za pomocą urządzeń oraz danych podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.
- Powiązany z danymi, które zostały podpisane w taki sposób, że każda zmiana tych danych wykonana po złożeniu podpisu będzie rozpoznawalna.

Spełnienie powyższych warunków gwarantuje pewność co do tożsamości podpisującego i oryginalności podpisanych danych. Dla posiadacza podpisu oznacza to również konieczność odpowiedniego zabezpieczenia posiadanego podpisu. Utrata urządzeń i danych niezbędnych do złożenia podpisu może bowiem skutkować złożeniem podpisu przez osobę do tego nieupoważnioną, a co za tym idzie – w świetle prawa może prowadzić do podjęcia zobowiązań przez właściciela podpisu. Zgodnie z art. 6 pkt 3 ustawy o podpisie elektronicznym, nie ma możliwości unieważnienia złożonego podpisu przez powołanie się na to, że podpis elektroniczny został złożony za pomocą bezpiecznych urządzeń czy danych, które nie znajdowały się pod wyłączną kontrolą osoby składającej podpis.

Pomocne w tej sytuacji jest to, że podpis cyfrowy jest umieszczany najczęściej na karcie inteligentnej, której rozmiary pozwalają na łatwe umieszczenie jej w portfelu lub dowolnym bezpiecznym miejscu znajdującym się w wyłącznej kontroli właściciela podpisu elektronicznego. Dodatkowym zabezpieczeniem stosowanym podczas składania podpisu cyfrowego jest konieczność podania numeru PIN potwierdzającego tożsamość użytkownika. Bez podania tego numeru podpis nie zostanie złożony. Dlatego nawet w przypadku utraty karty inteligentnej ryzyko jest ograniczone. Niestety wiele osób nie posiada dostatecznej wiedzy i beztrosko łamie podstawowe zasady bezpieczeństwa, zapisując numer PIN i przechowując go razem z kartą inteligentną i urządzeniami niezbędnymi do złożenia podpisu elektronicznego.

Ustawa o podpisie elektronicznym, oprócz określenia warunków, jakie musi spełniać podpis elektroniczny, definiuje również obowiązki, które muszą wypełniać

[10] http://www.kir.com.pl/main.php?p=3990&s=69197.

podmioty świadczące usługi certyfikacyjne. Jest to konieczne w celu zapewnienia bezpieczeństwa i wiarygodności składanych podpisów elektronicznych. Kwalifikowany podmiot, który świadczy usługi certyfikacyjne, jest zobowiązany do:

- Zapewnienia technicznych i organizacyjnych środków, które pozwalają na szybkie i sprawne wydawanie certyfikatów, zawieszanie ich i unieważnianie wraz z możliwością określenia czasu wykonania tych czynności. Pozwala to na sprawne zarządzanie pulą dostępnych podpisów i bieżącą weryfikację tego, czy złożony podpis jest ważny, czy też nie.
- Sprawdzenia tożsamości osoby, dla której zostanie wydany certyfikat, przed wydaniem tego certyfikatu. W ten sposób uzyskujemy pewność, że nikt nie będzie w stanie podszyć się pod inną osobę, co mogłoby skutkować nieuprawnionym uzyskaniem podpisu przez nieuczciwego człowieka.
- Zapewnienia środków mających przeciwdziałać fałszerstwom certyfikatów oraz innych danych poświadczanych elektronicznie przez podmioty świadczące usługi certyfikacyjne. Ma się to odbywać przede wszystkim przez ochronę urządzeń i danych wykorzystywanych podczas świadczenia usług certyfikacyjnych.
- Zawarcia umowy ubezpieczenia odpowiedzialności cywilnej pokrywającej szkody wyrządzone odbiorcom usług certyfikacyjnych.
- Poinformowania osoby, której wydawany jest certyfikat, o warunkach uzyskania i używania certyfikatu, zwłaszcza o ograniczeniach nałożonych na używanie tego certyfikatu, jak również do przekazania pełnego wykazu urządzeń, za pomocą których możliwe jest złożenie bezpiecznego podpisu elektronicznego. Do wykazu muszą zostać dołączone warunki techniczne, jakie powinny spełniać te urządzenia. Dodatkowo, jeżeli podmiot certyfikujący zapewnia publiczny dostęp do certyfikatów, to musi uzyskać zgodę ubiegającego się o certyfikat na jego publikację.
- Używania systemów do tworzenia certyfikatów w taki sposób, by tworzenie oraz modyfikacje certyfikatów były możliwe do wykonania jedynie przez upoważnione do tego osoby.
- Zapewnienia poufności procesu tworzenia certyfikatów, zwłaszcza w aspekcie poufności danych służących do wygenerowania certyfikatu. Dane te nie mogą być przechowywane ani kopiowane. Po utworzeniu certyfikatu dane te mają zostać przekazane na wyłączny użytek nabywcy podpisu elektronicznego w taki sposób, by nie istniały żadne kopie tych danych. Ponadto proces tworzenia danych certyfikujących musi być zorganizowany w taki sposób, by w procesie tworzenia kolejnych podpisów cyfrowych dane stanowiące określony podpis cyfrowy wystąpiły tylko raz z prawdopodobieństwem graniczącym z pewnością.

- Publikowania danych umożliwiających weryfikację ważności i autentyczności wystawionych certyfikatów, a także innych poświadczanych danych. Dostęp do tych danych musi być bezpłatny dla odbiorców usług certyfikacyjnych.

Na podstawie przepisów prawa podmiot świadczący usługi certyfikacyjne odpowiada za wszelkie szkody spowodowane nienależytym wykonaniem obowiązków wynikających z zakresu świadczonych usług, o ile nie wynika ono z okoliczności, za które podmiot certyfikujący nie ponosi odpowiedzialności. Nie należy do zakresu odpowiedzialności podmiotu certyfikującego odpowiedzialność za szkody spowodowane niewłaściwym użyciem certyfikatu.

7. Szybkość działania

Istotnym aspektem każdego rozwiązania informatycznego jest jego szybkość. Również w wypadku podpisu cyfrowego ważne jest to, by jego użycie nie spowalniało pracy komputera oraz nie wymagało oczekiwania użytkownika na wykonanie operacji. Cykl życia podpisu cyfrowego obejmuje takie operacje, jak: generowanie kluczy, generowanie skrótów danych, podpisywanie skrótów oraz ich weryfikacja. Każda z wymienionych operacji wymaga określonego czasu. W celu określenia czasochłonności poszczególnych etapów przeprowadzono badanie. Polegało ono na zaimplementowaniu w różnych językach programowania poszczególnych operacji podpisu cyfrowego. Testy przeprowadzono dla dwóch różnych rozmiarów podpisywanych zbiorów danych – 100 KB i 10 MB. Przedstawione w tabeli 1 wyniki są wynikami średnimi uzyskanymi na komputerze z dwurdzeniowym procesorem Intel i5 M560 2,67 GHz.

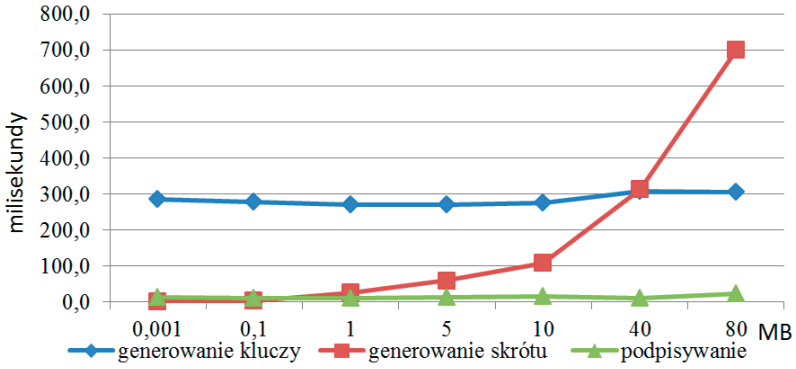
Tabela 1. Czas wykonania poszczególnych operacji podpisu cyfrowego

Operacja	Generowanie kluczy [ms]		Generowanie skrótu [ms]		Podpisywanie skrótu [ms]		Weryfikowanie podpisu [ms]	
Rozmiar danych	100 kB	10 MB	100 kB	10 MB	100 kB	10 MB	100 kB	10 MB
C#	49	30	7	234	8	24	15	176
Java	277	275	3	106	9	14	45	160
C++	1	1	1	57	7	38	10	46
php	1723	2342	94	158	108	231	145	311

Źródło: opracowanie własne.

Analiza wyników przedstawionych w tabeli 1 pozwala zauważyć, że pod względem szybkości wyróżnia się implementacja w języku C++. Najwolniejszą technologią okazało się php. Należy jednak zwrócić uwagę na fakt, że program napisany w tym języku nie działa bezpośrednio w systemie operacyjnym, lecz wymaga serwera WWW. Różnice w czasach wykonania określonych operacji w różnych technologiach nie zależą jednak w znaczącym stopniu od ich szybkości, lecz od wydajności bibliotek udostępniających przedstawione powyżej funkcjonalności. Zostały one bowiem poddane optymalizacji w różnym zakresie, a ich implementacje wykazują znaczne różnice. Należy zwrócić uwagę na fakt, że największe różnice czasu wykonania występują podczas wykonywania operacji generowania kluczy. Jest to jednak operacja jednorazowa, więc szybkość jej wykonania nie wpływa na sprawne funkcjonowanie systemu.

Do dalszych badań sprawności podpisu cyfrowego wybrano implementację w wieloplatformowym i przenośnym języku programowania Java. Przebadano czas wykonania poszczególnych operacji dla zbiorów danych o rozmiarze od 1 KB do 80 MB. Uzyskane wyniki przedstawiono na rysunku 5.

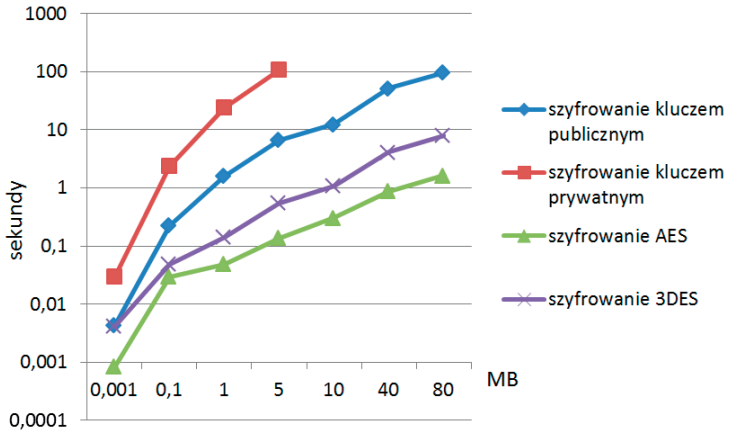


Rysunek 5. Czas wykonania poszczególnych operacji podpisu cyfrowego

Źródło: opracowanie własne.

Jak łatwo zauważyć, poszczególne operacje podpisu cyfrowego wykonywane są sprawnie. Czas oczekiwania jest nieznaczny nawet w przypadku dużych zbiorów danych – podpisywanie 80 MB danych trwa niecałe 0,7 sekundy. Problematyczne natomiast staje się zastosowanie podpisu cyfrowego do ochrony przesyłanych treści. Operacje szyfrowania i deszyfrowania kryptografii asymetrycznej są bowiem powolne. O ile potwierdzanie autentyczności danych wymagało jedynie zaszyfrowania skrótu danych, o tyle zabezpieczenie danych

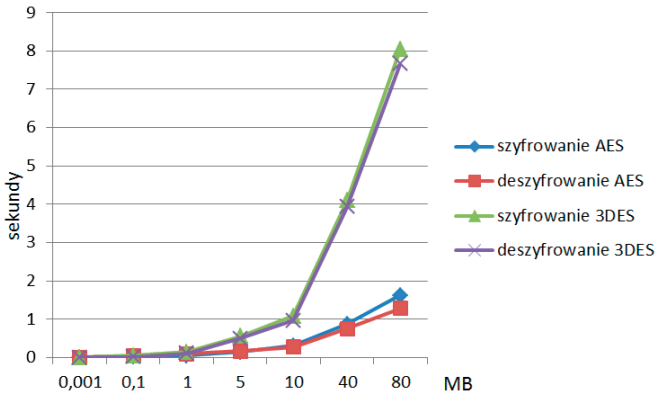
przed niepowołanym dostępem wymaga ich zaszyfrowania. O wiele wydajniejszym rozwiązaniem jest zaszyfrowanie danych za pomocą silnego algorytmu symetrycznego. Czas wykonania operacji szyfrowania za pomocą różnych algorytmów przedstawiono na rysunku 6.



Rysunek 6. Porównanie czasu szyfrowania zbiorów danych za pomocą różnych algorytmów

Źródło: opracowanie własne.

Spośród porównywanych algorytmów zdecydowanie najlepsze wyniki osiągnął AES. Szyfrowanie 80 MB danych zajęło 1,6 sekundy. Algorytm asymetryczny zupełnie się nie sprawdził. Szyfrowanie tego samego zbioru danych kluczem prywatnym zajęło ponad 28 minut. Z tego względu czasy szyfrowania tym kluczem dla zbiorów danych o rozmiarze przekraczającym 5 MB nie zostały zaprezentowane na rysunku 6. W celu doboru odpowiedniego algorytmu do zabezpieczania poufności przesyłanych danych przebadano czas szyfrowania oraz deszyfrowania uzyskane przez algorytmy 3DES oraz AES dla zbiorów danych o różnym rozmiarze. Uzyskane wyniki zaprezentowane zostały na rysunku 7. Wskazują one na wyraźną przewagę algorytmu AES w aspekcie czasu szyfrowania i deszyfrowania zbiorów danych. Uzyskane zostały one przy użyciu implementacji algorytmu w języku Java. Jednak implementacje w innych językach również wykazują dużą szybkość działania. Szyfrowanie 50 MB zbioru danych w przypadku implementacji w języku C# zajęło 3,4 sekundy, w języku Ruby 0,8 sekundy, a w Javie 1,3 sekundy. Algorytm AES oferuje również bardzo wysoki poziom bezpieczeństwa.



Rysunek 7. Porównanie czasu szyfrowania i deszyfrowania zbiorów danych za pomocą algorytmów 3DES oraz AES

Źródło: opracowanie własne.

Duża szybkość działania algorytmów symetrycznych oraz możliwości dostarczane przez podpis elektroniczny pozwalają na skuteczne chronienie dużych zbiorów danych przesyłanych kanałem publicznym bez konieczności wcześniejszego uzgadniania klucza algorytmu symetrycznego. Wystarczy, że nadawca zaszyfruje dane, używając wygenerowanego samodzielnie klucza algorytmu symetrycznego, a następnie zabezpieczy ten klucz, szyfrując go za pomocą klucza publicznego adresata. Ze względu na mały rozmiar klucza czas jego szyfrowania za pomocą algorytmu asymetrycznego będzie pomijany. Dodatkowym atutem tego rozwiązania będzie możliwość stosowania kluczy jednorazowych algorytmu symetrycznego, co znacząco zwiększy oferowany poziom bezpieczeństwa danych.

8. Podsumowanie

Zarówno unormowania prawne, jak i środki techniczne pozwalają w Polsce na stosowanie podpisów cyfrowych, które są bezpieczne i mają moc prawną tożsamą z podpisem odręcznym[11]. Pozwala to na coraz powszechniejsze stosowanie komunikacji cyfrowej w biznesie, administracji czy innych dziedzinach życia. Dzięki temu możliwe jest wprowadzanie rozwiązań w coraz większym stopniu

[11] http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Dzialalnosc+gospodarcza+i+e-przedsiebiorczosc/Podpis+elektroniczny.

dostosowanych do wymagań dzisiejszego cyfrowego społeczeństwa. Potrzeby te są widoczne zwłaszcza w administracji publicznej, w której wprowadzenie każdego udogodnienia pozwalającego na uniknięcie wizyty w urzędzie i załatwienie sprawy przez Internet jest entuzjastycznie odbierane przez społeczeństwo, jak również pozwala znacznie zredukować koszty obsługi interesantów, ze względu na brak konieczności tworzenia stanowisk pracy do bezpośredniej obsługi obywateli oraz przeniesienie na interesantów części obowiązków, takich jak choćby wprowadzenie niezbędnych danych do systemu informatycznego. Oczywiście wszystkie te operacje nie mogą być sfinalizowane bez autoryzacji użytkownika dokonywanej za pomocą podpisów elektronicznych.

Wykorzystanie podpisu elektronicznego pozwala również na realizowanie skutecznych schematów zabezpieczania dużych zbiorów danych przesyłanych przy użyciu kanału niezabezpieczonego. Konieczne jest tu jednak zastosowanie algorytmu symetrycznego do ochrony danych. Jak wykazano w artykule, najlepszym wydajnościowo rozwiązaniem będzie połączenie podpisu cyfrowego z algorytmem AES. Funkcjonalność podpisu elektronicznego pozwala natomiast na skuteczną ochronę i wymianę kluczy algorytmu symetrycznego.

Bibliografia

1. Bauer F., *Sekrety Kryptografii*, Helion, Gliwice 2002.
2. Hamdy S., *Towards a Better Applicability of Public-Key Certificates*, Innovations in Information Technology, 4th International Conference, 2007, DOI: 10.1109/IIT.2007.4430387.
3. Khalifa O.O., Islam M.R., Khan S., Shebani M.S., *Communications cryptography*, RF and Microwave Conference, 2004, DOI: 10.1109/RFM.2004.1411111.
4. Kifner T., *Polityka bezpieczeństwa i ochrony inf*ormacji, Helion, Gliwice 1999.
5. Menzenes A., Oorschot P., Vanstone S., *Kryptografia stosowana*, WNT, Warszawa 2005.
6. Romney G.W., Parry D.W., *A Digital Signature Signing Engine to Protect the Integrity of Digital Assets*, Information Technology Based Higher Education and Training, 7th International Conference, 2006, DOI: 10.1109/ITHET.2006.339702,
7. Wohlmacher P., Pharow P., *Applications in health care using public-key certificates and attribute certificates*, Computer Security Applications, 16th Annual Conference, 2000, DOI: 10.1109/ACSAC.2000.898866.

8. Yunling S., Xianghua M., *An Overview of Incremental Hash Function Based on Pair Block Chaining*, Information Technology and Applications (IFITA), International Forum, 2010, DOI: 10.1109/IFITA.2010.332.
9. Zhu N., Xiao G. X., *Application of a Scheme of Digital Signature in Electronic Government*, International Conference on Computer Science and Software Engineering, 2008, DOI: 10.1109/CSSE.2008.929.

Źródła sieciowe

1. http://www.kir.com.pl/main.php?p=3990&s=69197 (data odczytu 21.11.2013).
2. http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Dzialalnosc+gospodarcza-+i+e-przedsiebiorczosc/Podpis+elektroniczny (data odczytu 21.11.2013).
3. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (tekst jedn.: Dz. U. z 2013 r. poz. 262), http://prawo.legeo.pl/prawo/ustawa-z-dnia-18-wrzesnia-2001-r-o-podpisie-elektronicznym/rozdzial-i_przepisy-ogolne/?on=25.02.2013 (data odczytu 19.11.2013).

* * *

Digital signature in Poland

Summary

The article describes technical and legal aspects of digital signature in Poland. The crytpographical aspects of creation of a digital signature are also described. The obligations of certification firms and digital signature users are discussed.

Keywords: digital signature, security, cryptography