Wprowadzenie do zagadnienia Podpisu Cyfrowego

Sławomir Sobótka

Wstęp

Podpis jest ręcznym zapisem imienia i nazwiska osoby, przez którą został złożony. Bywa on stylizowany lub zastępowany innym sobolem lub znakiem. Podpis jest dowodem tożsamości i woli osoby składającej go – jest swego rodzaju pieczęcią.

W dobie informacji elektronicznej zachodzi potrzeba zmiany podejścia do problemu sygnowania treści. Prawo unijne (dyrektywa 1999/93/EC) wyróżnia trzy rodzaje podpisu elektronicznego:

- podpis elektroniczny - deklaracja tożsamości autora złożona pod dokumentem elektronicznym (np.: podpis pod emailem, skan podpisu odręcznego).
- zaawansowany (bezpieczny) podpis elektroniczny - jednoznacznie i w sposób trudny do sfałszowania (poprzez zastosowanie kryptografii) związany z dokumentem oraz autorem. Umożliwia on identyfikację autora oraz zabezpiecza dokument przed jakąkolwiek zmianą.
- kwalifikowany podpis elektroniczny - podpis zaawansowany, złożony przy pomocy certyfikatu kwalifikowanego oraz z użyciem bezpiecznego urządzenia do składania podpisu.

W praktyce dwie ostatnie kategorie odnoszą się do większości systemów tradycyjnie nazywanych podpisem elektronicznym dlatego niniejszy artykuł będzie próbą wprowadzenia do tematu ogólnie pojętego bezpiecznego podpisu cyfrowego (zwanego dalej po prostu podpisem cyfrowym lub podpisem elektronicznym).

Istotną cechą podpisu cyfrowego, która daje mu niebagatelną przewagę na podpisem klasycznym, jest to, że zabezpiecza on podpisany dokument przed zmianą – to znaczy, że jeżeli nastąpi jakakolwiek zmiana, wówczas będzie to widoczne podczas weryfikacji podpisu. Również podejście do problemu identyfikacji autora jest zgoła odmienne. Zastosowanie podpisu cyfrowego gwarantuje również niemożność zaprzeczenia przez nadawcę wysłania wiadomość o otrzymanej treści. Aby przedstawić wymienione zagadnienia zaczniemy od wprowadzenia do kryptografii oraz przybliżenia idei kluczy asymetrycznych (zwanych potocznie prywatnym i publicznym). Chociaż u podstaw tych zagadnień leży dosyć zaawansowana matematyka, to proszę nie obawiać – wprowadzenie będzie bezbolesne gdyż matematykę pominiemy w naszych rozważaniach.

Wprowadzenie do kryptografii

Podstawą klasycznej kryptografii jest algorytm, czyli zestaw relatywnie

skomplikowanych operacji, którym poddaje się wiadomość po to aby stworzyć jej bezpieczną postać – szyfrogram (wiadomość w postaci zaszyfrowanej). Odbiorca szyfrogramu musi znać algorytm jakim został zastosowany podczas szyfrowania po to aby móc odszyfrować wiadomość. Bezpieczeństwo takiego podejścia opiera się na założeniu, że agresor nie jest w stanie rozwikłać algorytmu. Jednak jak pokazuje historia nie jest to założenie, na którym można polegać. Po złamaniu algorytmu staje się on bezużyteczny.

Nowoczesne podejście do kryptografii jest zgoła odmienne i zakłada wręcz, że algorytm jest powszechnie znany. Bezpieczeństwo szyfrogramu jest zapewnione dzięki zastosowaniu tajnego klucza. Klucz jest to pewien ciąg znaków (w szczególności liczba), który jest używany do tego, aby przy pomocy zawiłych operacji matematycznych przekształcić wiadomość w szyfrogram. Zatem algorytm jako danych wejściowych potrzebuje oprócz samej wiadomości również klucza. Przy pomocy tegoż samego klucza możemy przekształć szyfrogram do postaci jawnej, czyli odszyfrowanej. Oczywiście pojawia się problem: co zrobić z samym kluczem? Przecież jeżeli Alicja chce wysłać szyfrogram do swego przyjaciela Bartka, wówczas musi również przesłać mu klucz, po to aby mógł on odszyfrować dokument. Jak zatem zabezpieczyć sam klucz?

Na szczęście istnieją pewne przekształcenia matematyczne, które zamieniają wiadomość w szyfrogram przy pomocy jednego klucza, natomiast rozkodowują tenże szyfrogram do postaci jawnej przy pomocy innego klucza. Mamy zatem do czynienia z parą kluczy, z których jeden nazywamy prywatnym a drugi publicznym. Klucz prywatny to taki, który jest znany jedynie jego właścicielowi i w szeroko pojętym interesie właściciela jest nieujawnianie klucza. Natomiast klucz publiczny jest publiczny w dosłownym znaczeniu tego słowa.

Oto praktyczny przykład ilustrujący zastosowanie par kluczy do szyfrowania i deszyfrowania: Załóżmy, że Alicja chce wysłać poufną wiadomość do Bartka. Bartek posiada parę swych kluczy: prywatny - znany tylko sobie oraz publiczny – powszechnie znany. Scenariusz wygląda następująco:

1. Alicja pobiera publiczny klucz Bartka
2. Alicja używa publicznego klucza Bartka do zaszyfrowania wiadomości.
3. Alicja wysyła do Bartka zaszyfrowaną wiadomość (może to zrobić bez obaw, gdyż do jej odszyfrowania potrzeba drugiego klucza z pary)
4. Bartek jako jedyny posiadacz drugiego klucza z pary (przynajmniej ma taką nadzieję) rozkodowuje szyfrogram przy pomocy swego prywatnego klucza

Wielu czytelników zastanawia się czy szyfrowanie jest aby na pewno bezpieczne. Czy do odkodowania wiadomości nie wystarczy ten sam klucz (publiczny), który został zastosowany do jej zakodowania. Na wstępie obiecałem, że będziemy unikać zaawansowanej matematyki, dlatego zainteresowanych odsyłam do zgłębienia zagadnienia faktoryzacji liczb oraz krzywych eliptycznych w ciele liczb pierwszych.

Idea podpisu cyfrowego

Mamy za sobą już wstęp do kryptografii asymetrycznej (stosującej dwa klucze) i mam nadzieję, że przynajmniej intuicyjnie czujemy czym jest klucz i do czego służy. Stąd już zaledwie jeden krok do zrozumienia idei podpisu cyfrowego, wystarczy jedynie odwrócić zastosowanie kluczy. Zacznijmy od przykładowego scenariusza tworzenia podpisu cyfrowego:

1. Alicja chce podpisać pewien dokument i posiada parę kluczy.
2. Alicja szyfruje swój dokument przy pomocy swego klucza prywatnego tworząc w ten sposób podpis.
3. Alicja dołącza do oryginalnego dokumentu podpis (dokument zaszyfrowany).

Oto jak wygląda scenariusz weryfikacji podpisu:

1. Bartek jest w posiadaniu podpisanego rzekomo przez Alicję dokumentu i chce sprawdzić czy aby na pewno ona jest jego autorem oraz czy dokument nie został zmodyfikowany po dokonaniu podpisu
2. Bartek pozyskuje klucz publiczny Alicji
3. Bartek rozkodowuje przy pomocy klucza podpis dokumentu, uzyskując w ten sposób wersję dokumentu z momentu złożenia podpisu
4. Bartek porównuje rozkodowany podpis z dokumentem, który weryfikuje

Przeanalizujmy teraz ideę podpisu śledząc kolejne kroki. Alicja generując podpis po prostu szyfruje dokument swym prywatnym kluczem. Natomiast każdy, kto chce zweryfikować podpis używa jej klucza publicznego. Dzięki temu mamy pewność co do autora, ponieważ gdyby Celina chciała podszyć się pod Alicję to podpis wygenerowany przy pomocy jakiegoś klucza Celiny nie rozkodowałby się kluczem publicznym Alicji. Mamy również pewność, że treść dokumentu nie została zmieniona, ponieważ po rozkodowaniu podpisu otrzymujemy postać dokumentu z chwili gdy podpis nastąpił i możemy ją porównać z obecną postacią dokumentu.

Uważny czytelnik zauważy oczywiście, że podpis w tej formie powodowałby zawsze znaczne zwiększenie objętości dokumentu. Z tego powodu oraz z uwagi na kwestie wydajności rzeczywiste realizacje przebiegają z drobną modyfikacją. Podczas tworzenia podpisu tworzy się tak zwany skrót treści dokumentu, czyli swego rodzaju „odcisk palca” dokumentu. Dopiero tenże skrót jest podpisywany, a podpis dołączany do dokumentu.

Potrzeba certyfikacji

Zastosowanie klucza publicznego sprawia jednak pewne problemy. Osoba otrzymująca klucz publiczny nie jest w stanie stwierdzić na podstawie samego klucza , czy jest on w ogóle kluczem publicznym ani czy klucz ten został wykorzystany zgodnie z intencją jego właściciela oraz kto tak na prawdę jest jego właścicielem. W celu rozwiązania powyższych problemów opracowano koncepcję nazw wyróżniających oraz przenoszących ich certyfikatów. Nazwy wyróżniające to po prostu pewne ustalone atrybuty niosące informacje o właścicielu klucza. Natomiast zagadnienie certyfikatów jest nieco szersze i

jemu poświęcimy dalszą część artykułu.

Mechanizm certyfikacji pozwala na poświadczenie faktu, iż pewien klucz publiczny jest powiązany z jego właścicielem. Certyfikat jest po prostu dokumentem elektronicznym, który zawiera klucz publiczny i wspomniane już atrybuty właściciela tegoż klucza (nazwy wyróżniające). Idea certyfikacji zakłada istnienie zaufanej strony trzeciej – wystawcy certyfikatu. Wystawca certyfikatów (zwany „centrum certyfikacji") tworzy listy podmiotów, które sobie ufają. Rozważmy następujący przykład: Alicja zakłada centrum certyfikacji, Alicja ufa Bartkowi, Bartek ufa Celinie. Mamy wówczas łańcuch: A -> B -> C. Alicja oraz Celina nie znają się osobiście, jednak poprzez połączenie z zaufanym przez nie Bartkiem tworzą łańcuch zaufania. Mechanizm certyfikacji polega na tym, że Alicja podpisuje swym kluczem prywatnym certyfikat Bartka a Bartek podpisuje swym kluczem prywatnym certyfikat Celiny itd. Zatem gdy ktoś chce zweryfikować klucz publiczny Celiny, wówczas musi przejść po drzewie certyfikatów aż do Alicji i kolejno weryfikować napotkane certyfikaty . Oczywiście ma to sens gdy osoba weryfikująca ufa centrum, czyli Alicji.

Jak zatem widzimy koncepcja certyfikatów jest dosyć prosta. Weryfikacja klucza i autora polega na zweryfikowaniu opisującego je certyfikatu. To z kolei polega na hierarchicznym weryfikowaniu w górę po drzewie zaufania aż do centrum certyfikacji, które to ze swej definicji jest zaufane i dba o weryfikację swych klientów.

Zakończenie

Podpis cyfrowy jest wygodnym i pewnym sposobem zapewniania bezpieczeństwa dokumentów. Wykazaliśmy, że jego stosowanie gwarantuje:

- autentyczność – pewność co do autora dokumentu,
- niezaprzeczalność – polegającą na tym, że nadawca nie może wyprzeć się wysłania wiadomości,
- integralność – pewności, że wiadomość nie została zmodyfikowana po złożeniu podpisu.

Mechanizm podpisu cyfrowego opiera się na koncepcji dwóch kluczy (ciągów znaków) pozwalających ich posiadaczowi na uzyskanie wspomnianych trzech atrybutów bezpieczeństwa. Koncepcja podpisu cyfrowego jest uzupełniona przez koncepcję certyfikacji, zapewniającą wygodny sposób weryfikacji kluczy i ich właścicieli dzięki łańcuchom zaufania.

Niniejszy artykuł miał na celu wprowadzenie do zagadnienia podpisu cyfrowego, poprzez ukazanie jego dosyć abstrakcyjnej idei. Czytelników, których zainteresował praktyczny aspekt wykorzystania podpisu cyfrowego wraz z jego technicznymi aspektami zachęcam do zapoznania się z treścią artykułu <<tytuł drugiego artykułu, strona>> traktującego o wykorzystaniu kart chipowych do podpisywania i przechowywania dokumentów medycznych.