Polskie Karty 2012 almanach
Almanach biznesu kartowego w Polsce: regionalna informacja, światowa perspektywa

Niniejszy artykuł ukaże się w Almanachu "Polskie Karty 2012", wydawnictwie firmy Medien Service, organizatora Konferencji Central European Electronic Card, w trakcie której nastąpi w dniach 30.11-01.12.br premiera tego wydawnictwa. Więcej informacji na www.cardsalmanach.eu oraz www.conkarta.pl

PKI 2.0

Lżejszy certyfikat podpisu elektronicznego

Uchwalona ponad 10 lat temu dyrektywa w sprawie podpisów elektronicznych [1]ustaliła obowiązujący w technologii podpisu elektronicznego paradygmat, że certyfikat ma identyfikować podpisującego (niezależnie czy podpisującym jest osoba fizyczna, czy prawna). Implikacją tego zapisu jest stwierdzenie, że jeżeli podpis jest weryfikowany certyfikatem to jednoznacznie wskazuje na podpisującego. W niniejszym artykule chciałbym zastanowić się, czy ograniczony technologią Infrastruktury Klucza Publicznego (ang. PKI) paradygmat certyfikatu identyfikującego podpisującego powinien w nowych zapisach dyrektywy i ustaw krajowych pozostać niezmieniony.

Infrastruktura Klucza Publicznego implementowana jest w oparciu o certyfikaty X.509, które zawierają przede wszystkim klucz publiczny skojarzony z kluczem prywatnym podpisującego. Dodatkowo obowiązkowo w treść certyfikatu wchodzą dane identyfikujące podpisującego, dane identyfikujące wydawcy certyfikatu, oraz okres ważności certyfikatu. Bardzo często certyfikaty zawierają dodatkowe informacje takie jak organizacja podpisującego, zakres upoważnień, maksymalna kwota transakcji. Celem zawarcia tych informacji w certyfikacie jest spełnienie wymagań schematu weryfikacji podpisu, w którym zawartość certyfikatu stanowi podstawę dla stwierdzenia ważności podpisu.

Powyższy mechanizm podpisu bazującego na certyfikacie statycznym miał zaletę taką, że podpisujący mógł w dowolnym momencie złożyć podpis, którego podstawą weryfikacji był statyczny i zawarty w samym podpisie certyfikat. Certyfikat ten poprzez swoją zawartość jednoznacznie daje weryfikującemu wszystkie informacje, które mogą mu pomóc w przeprowadzeniu pełnej weryfikacji ważności i wartości podpisu elektronicznego.

Zawarcie dużej liczby cech w certyfikacie ma podstawową wadę, mianowicie zmiana dowolnej z nich wymaga unieważnienia dotychczas obowiązującego certyfikatu i wydania nowego. Dla przykładu jeżeli pracownik korporacji posiada certyfikat upoważniający do wykonania dowolnej czynności prawnej to zmiana zakresu tej czynności implikuje za sobą zmianę zawartości certyfikatu – czyli wydanie nowego. Ze względu na tę wadę podpisu opartego o certyfikat już kilka lat temu wypracowano technologię certyfikatów atrybutu, których zadaniem jest potwierdzanie cech krótkoterminowych. Jednakże certyfikaty atrybutu jako mechanizm wspierający podpis elektroniczny nie zdobył zbyt dużego uznania na rynku, głównie z tego powodu, że komplikował on jeszcze bardziej korzystanie z mechanizmów podpisu elektronicznego.

Wymaganie, aby certyfikat identyfikował podpisującego uniemożliwia stosowanie podpisu elektronicznego w sposób, w który posługujemy się nim na co dzień, jako prosty mechanizm potwierdzający, który sam w sobie nie niesie cech identyfikacyjnych, a dopiero jego szczególne formy takie cechy niosą. Wobec powyższego podpis elektroniczny pozbawił nas możliwości stosowania uproszczonych mechanizmów bezpieczeństwa w transakcjach elektronicznych, które w wielu kontaktach zapewniały naszą prywatność, np. nie udostępniając drugiej stronie naszych danych osobowych jakimi jest imię i nazwisko, czy numer identyfikacyjny PESEL.

W wielu transakcjach elektronicznych, które realizujemy przez Internet przekazanie danych osobowych nie wydaje się konieczne, ważniejszymi cechami jest posiadanie odpowiednich środków na koncie, miejsce zamieszkania czy nasz wiek. Zapisanie takich informacji w certyfikacie nie zawsze jest możliwe – ze względu na ich zmienność, ale także nie zawsze podpisujący chce się tymi informacjami posługiwać i je ujawniać przy wszystkich transakcjach. Dla przykładu w Polsce część urzędników odmawia posługiwania się certyfikatem kwalifikowanym, ponieważ ten ujawnia wiek, zawarty w numerze PESEL.

Certyfikat w PKI jest podstawą weryfikacji podpisu elektronicznego, dyrektywa wyróżniła spośród zbioru certyfikatów certyfikat kwalifikowany, wskazując, że podpisy elektroniczne weryfikowane takim certyfikatem będą miały szczególne uznanie prawne w krajach Unii Europejskiej. Takie podejście determinuje wymaganie, aby na poziomie wydania certyfikatu było wiadome do czego będzie używany podpis elektroniczny, jakie będą ograniczenia jego użycia. To stało się podstawą do stanowienia wszystkich usług certyfikacyjnych, ale jednocześnie jest elementem hamującym rozwój technologii podpisu elektronicznego i jego szersze użycie. Głównym problemem jest fakt, że certyfikację klucza publicznego w technologiach PKI trzeba powiązać z rejestracją i identyfikacją podpisującego, jego jawnym zobowiązaniem do stosowania polityki bezpieczeństwa oraz zapewnieniem odpowiedniego poziomu bezpieczeństwa i gwarancji związanych z tym podpisem.

Podpis musi być znacznie bardziej elastyczny, dawać możliwość nauczenia się kooperantom podpisu, stosowania różnych technik w zależności od wymaganego poziomu bezpieczeństwa, umożliwienia oparcia wiarygodności podpisu o analizę ryzyka. Tego wszystkiego podpis elektroniczny oparty o klasyczny certyfikat nie daje, bo wymusza reguły stosowania na początku rejestracji i ustalenia wszystkich warunków korzystania z podpisu elektronicznego. Klasyczny podpis kwalifikowany oparty o kartę ma tylko dwa zabezpieczenia PIN i możliwość jego unieważnienia – wobec powyższego nie istnieje możliwość dołączania do podpisu późniejszych zabezpieczeń opartych o techniki hasła jednorazowego lub dodatkowych elementów autoryzacji transakcji.

Posiadając świadomość tego rodzaju problemów wiele firm zmieniło model działania opierając usługi związane z podpisem elektronicznym o serwisy wystawiające użytkownikowi mechanizm uwierzytelnienia i realizujące podpis elektroniczny w jego imieniu. W ten sposób działają najbardziej znane na rynku firmy DocuSign czy EchoSign, które umożliwiają łatwą rejestrację przez Internet i składanie podpisów elektronicznych tylko na tej podstawie, a po potwierdzeniu karty kredytowej zwiększenie poziomu wiarygodności podpisów elektronicznych. Nawet niektóre kraje Unii Europejskiej zgodziły się na oparcie podpisów kwalifikowanych o tego typu usługi, co budzi kontrowersje dotyczące „wyłącznej kontroli" podpisującego nad środkami służącymi do złożenia podpisu elektronicznego. Z drugiej strony warto się zastanowić, kto ma większą kontrolę nad podpisem elektronicznym ten, co posiada kartę kryptograficzną z kluczami, czy ten, który ma dostęp do rejestru złożonych przez siebie podpisów elektronicznych.

W Polsce ograniczenia podpisów elektronicznych opartych o weryfikację certyfikatem spowodowały bardzo małe ich wykorzystanie przez osoby fizyczne do załatwiania swoich spraw. Odpowiedzią na te problemy było między innymi udostępnienie mechanizmów składania deklaracji podatkowych wykorzystujących jako podpis dane będące w posiadaniu podpisującego. Drugim rozwiązaniem jest potwierdzanie prawa do podpisania dokumentu przez specjalizowane do tego usługi. Takim mechanizmem jest udostępniony w lipcu br. Profil Zaufany ePUAP.

Skoro wymienione powyżej mechanizmy są ograniczające lub nie znajdują wystarczającego uznania prawnego warto w tym miejscu opisać mechanizm, który byłby elastyczny i umożliwiłby dynamiczne dostosowanie się podpisu i potwierdzeń mu towarzyszących do potrzeb użytkownika jak i rynku, w którym ten użytkownik funkcjonuje, zachowując przy tym wyłączną kontrolę użytkownika nad środkami służącymi do składania podpisu elektronicznego.

[1] Dyrektywa Parlamenty Europejskiego i Rady 1999/93/EC z dnia 13 grudnia 1 w sprawie wspólnotowych ram w zakresie podpisów elektronicznych

Wyłączna kontrola podpisującego oznacza, zastosowanie takich środków technicznych, które uniemożliwiają powstanie podpisu elektronicznego bez świadomego działania użytkownika.

Mechanizmem takim jest zastosowanie technik opisanych w koncepcji PKI 2.0, które zapewniają taki podział środków służących do składania podpisu elektronicznego pomiędzy podpisującego a usługodawcę, aby podpis powstawał tylko wtedy gdy podpisujący użyje środków będących pod jego wyłączną kontrolą, natomiast także aby podpis nie mógł być wytworzony bez uczestnictwa mechanizmów potwierdzających po stronie świadczącego usługę nazywanego Urzędem Podpisu (ang. Signature Authority). Istnieje kilka algorytmów i technik realizujących koncepcję PKI 2.0 należy wśród nich wymienić algorytm z mediatorem, algorytm oparty o logarytm dyskretny z dzielonym kluczem, technikę opartą o zdalnie zarządzane karty kryptograficzne oraz technikę opartą o ograniczony certyfikat klucza publicznego i certyfikaty atrybutu.

Podpis elektroniczny PKI 2.0 powstaje przy udziale 2 niezależnych stron, a co za tym idzie, podpisujący kontroluje podpis nie tylko przez fakt posiadania klucza prywatnego, ale także poprzez usługi udostępniane mu przez usługodawcę – w taki sam sposób w jaki banki udostępniają konto bankowe przez Internet. Daje to podstawową zaletę polegającą na tym, że dane zawarte w treści podpisu mogą być potwierdzane przez Urząd Podpisu w momencie składania podpisu, kontrolowane dodatkowymi środkami technicznymi (np. telefonem komórkowym) a także weryfikowane przez centralne rejestrowanie złożonych podpisów. Certyfikat w PKI 2.0 może zostać ograniczony jedynie do funkcji potwierdzania, że podpis powstał w środowisku kontrolowanym przez Urząd Podpisu i za pomocą środków (klucza prywatnego) będących w posiadaniu podpisującego (bez ujawniania cech tożsamości podpisującego). Natomiast wszystkie informacje identyfikujące podpisującego, informacje o posiadanych przez niego uprawnieniach i ograniczeniach będą weryfikowane w procesie podpisywania przez Urząd Podpisu, w szczególności mogą mieć postać krótkoterminowych – ważnych tylko w momencie podpisywania certyfikatów atrybutu dołączonych do podpisu.

Zastosowanie PKI 2.0 w cyklu życia może wyglądać następująco:

1. Użytkownik rejestruje się na portalu Urzędu Podpisu, ustalając podstawowe mechanizmy zarządzania podpisami przez niego realizowanymi. Rejestracja może być potwierdzona posiadaniem adresu email, lub telefonu komórkowego.
2. Użytkownik generuje klucze w posiadanym przez siebie środowisku (TPM komputera lub telefonu, karcie kryptograficznej, pliku). Urząd Podpisu wydaje i udostępnia użytkownikowi certyfikat, który zawiera klucz publiczny, natomiast nie zawiera danych identyfikujących podpisującego.
3. Użytkownik może używać takiej formy podpisu do różnych czynności. Podpisy takie mogą potwierdzać te informacje, które zostały potwierdzone w momencie rejestracji – np. adres email lub telefon komórkowy. Potwierdzenie takich danych jest realizowane tylko na życzenie podpisującego.
4. Jeżeli dla jakiś czynności prawnych konieczne staje się posługiwanie się przez podpisującego podpisem zaawansowanym to rozpoczęcie pracy z tego rodzaju podpisem wymaga potwierdzenia jego danych identyfikujących. Urząd podpisu może to zrobić na podstawie przelewu z konta bankowego lub płatności kartą kredytową. Podpisy oznaczone w momencie podpisywania jako zaawansowane zawierają informacje identyfikujące podpisującego w zakresie przez niego określonym. W dalszym ciągu podpisujący ma możliwość korzystania z prostszych podpisów go nie identyfikujących go.
5. W przypadku gdy jakieś czynności prawne wymagają gwarancji finansowych , Urząd Podpisu może działać jako zaufana strona trzecia, potwierdzając środki finansowe, których blokada zostanie wykonana na karcie kredytowej.
6. Jeżeli dla jakiś czynności potrzebny jest podpis opatrzony atrybutem zaufania ze strony administracji publicznej, odpowiedni mechanizm w tym zakresie może zostać zrealizowany.
7. Podpisujący, którego organizacja jest zarejestrowana w Urzędzie Podpisu może mieć dynamicznie przyznawane uprawnienia do działania w imieniu swojej organizacji.
8. Podpisujący, który jest zobowiązany do podpisywania się podpisem kwalifikowanym potwierdza swoją tożsamość i akceptuje politykę certyfikacji tak jak dotychczas (np. przez kuriera), ale posługuje się cały czas tym samymi środkami do składania podpisu, ustalając tylko dodatkowe parametry autoryzacyjne dla złożenia podpisu kwalifikowanego – np. oparte o uwierzytelnienie OTP (hasłem jednorazowym).

Opisany powyżej przykład daje możliwość elastycznego korzystania z podpisu elektronicznego zależnie od potrzeb, w oparciu o usługę Urzędu Podpisu. Pozwala także na zapoznanie się podpisującego z narzędziami i korzystanie z odpowiednich mechanizmów w zależności od potrzeb. Jedynie korzystanie z podpisu kwalifikowanego może wymagać jego osobistego kontaktu z punktem rejestracji, natomiast wszystkie inne rodzaje podpisu mogą być dostępne dla podpisującego bez konieczności wychodzenia z domu.

Warunkiem takiego podejścia jest zminimalizowanie informacji znajdujących się w certyfikacie i usunięcie danych identyfikujących. Przeniesienie wszystkich dodatkowych poświadczeń do przestrzeni atrybutów (które mogą, ale nie muszą mieć postać certyfikatów atrybutu) potwierdzanych w momencie składania podpisu przez Urząd Podpisujący. Zastosowanie tych mechanizmów niezależnie od stosownego algorytmu daje możliwość zbudowania szeregu usług dodanych i znacznie szerszego spektrum stosowania podpisu.

Stojąc na progu nowelizacji dyrektywy należy podjąć działania strategiczne dotyczące tego, czy mechanizm podpisu elektronicznego opartego o certyfikat stworzony wyraźnie pod potrzeby administracji publicznej jest adekwatny dla potrzeb rozwoju biznesu i stosowania różnych mechanizmów uwierzytelniania w sieci. Zmiana podejścia z świadczenia usług certyfikacyjnych na świadczenie usług związanych z podpisem elektronicznym wymaga szerszego spojrzenia na to, czy weryfikacja podpisu oparta o certyfikat identyfikujący podpisującego jest rozwiązaniem jedynie słusznym.

Michał Tabor

Absolwent wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Posiadacz certyfikatu CISSP. Ekspert z zakresu podpisu elektronicznego, elektronicznej administracji oraz bezpieczeństwa systemów teleinformatycznych. W latach 2002-2006 kierownik Centrum Certyfikacji Signet TP Internet, był odpowiedzialny za przygotowanie centrum do świadczenia kwalifikowanych usług certyfikacyjnych i certyfikację WebTrust. Autor specjalistycznych publikacji z zakresu dokumentu elektronicznego i podpisu elektronicznego. Architekt mechanizmów uwierzytelniania użytkowników systemów administracji publicznej w ePUAP, autor technicznego rozwiązania uwierzytelniania deklaracji PIT przyjmowanych bez konieczności opatrywania ich bezpiecznym podpisem elektronicznym, pomysłodawca mechanizmów podpisu potwierdzonego profilem zaufanym. Twórca koncepcji PKI 2.0 - modelu usługowego dla podpisu elektronicznego

http://pki2.pl