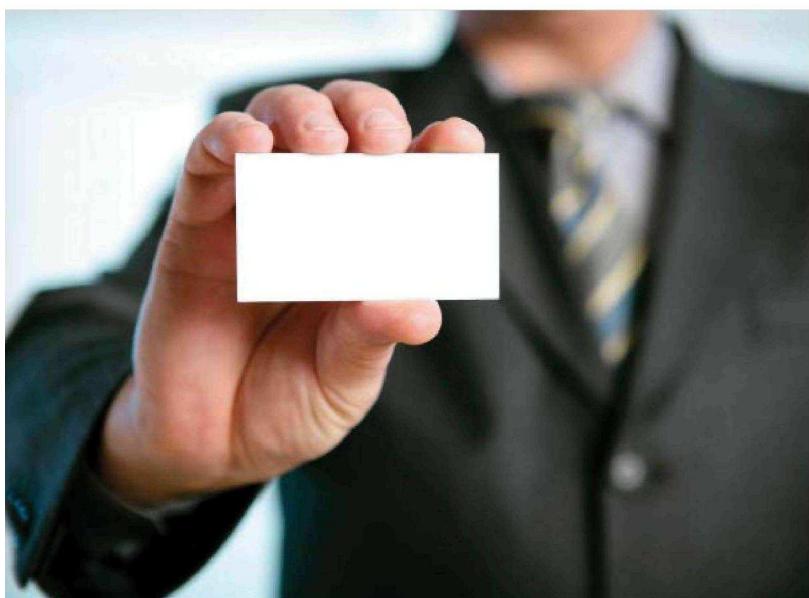


PKI i certyfikaty atrybutów



Podpis elektroniczny pozwala na zidentyfikowanie tożsamości i autentyczności dokumentu, ale nie wynika z niego, czy ktoś miał prawo złożyć go na dokumencie... **DENIS KOPYŁÓW**

Rozwiązaniem tego problemu jest odwołanie się weryfikatora e-podpisu do dodatkowych, zewnętrznych informacji lub zweryfikowanie atrybutów (nieidentyfikujących cech charakterystycznych podmiotu podpisującego) dołączonych do e-podpisu. Rozwiązanie

pierwsze wymaga tworzenia przez weryfikatora potwierdzonych zbiorów atrybutów należących do zidentyfikowanych podmiotów. Przykładowo weryfikujący może przechowywać u siebie pełnomocnictwa podmiotów podpisujących, składających podpisy w imieniu innej osoby fizycznej, która przekazała mu takie prawo.

Dla COMPUTERWORLD komentuje DR JERZY PEJAŚ z Wydziału Informatyki Politechniki Szczecińskiej

Ze względu na aktualny stan prawny w Polsce stosowanie certyfikatów atrybutów jest problematyczne. Na szczęście projekt nowelizowanej obecnie Ustawy o podpisie elektronicznym definiuje pojęcie certyfikatu atrybutów jako zaświadczenie elektroniczne powiązane z certyfikatem kwalifikowanym, określające w szczególności uprawnienia osoby wskazanej w certyfikacie. Choć wiązanie certyfikatu atrybutów tylko z certyfikatem kwalifikowanym jest znacznym ograniczeniem jego zastosowań, to należy jednak uznać, że jest to dobry punkt wyjścia do nadania certyfikatom atrybutów właściwej roli w polskim prawie.

W drugim rozwiązaniu można przyjąć, że każdy atrybut jest potwierdzany raz przez upoważniony podmiot i wiązany bezpośrednio lub pośrednio z e-podpisem przez wskazanie lokalizacji, z której poświadczony atrybut może zostać pobrany przez weryfikatora. W przypadku pełnomocnictwa oznacza to jego jednokrotne wystawienie i opublikowanie w miejscu, z którego można go pobrać zawsze wtedy, gdy jest to potrzebne.

Atrybuty i certyfikaty

Atrybuty (cechy charakterystyczne) mogą funkcjonować samodzielnie, bez wiązania ich z podpisem elektronicznym. Mogą np. być elektronicznym odpowiednikiem dyplomu papierowego, biletu miesięcznego, abonamentu, itp. Tam gdzie zastąpiono obieg papierowy obiegiem elektronicznym, atrybuty muszą mieć także postać elektroniczną. Tego typu elektroniczne atrybuty, po ich poświadczeniu przez upoważnione podmioty, nazywane są certyfikatami atrybutów.

W polskim prawie nie mam jawnego odwołania do certyfikatów atrybutów, chociaż pojęcie atrybutów jest używane głównie w kontekście kwalifikowanego podpisu elektronicznego. Przykładem jest atrybut, o którym mowa w Art.3 Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym, uprawniający do składania podpisu elektronicznego z upoważnienia innych osób. Atrybut ten nie pozwala jednak np. na określenie zakresu uprawnień. Określenie uprawnienia do składania e-podpisu w imieniu innych podmiotów można najprościej spełnić, wydając właściwej osobie certyfikat atrybutów. Tak zrobiono m.in. w niemieckiej uUstawie o podpisie elektronicznym oraz kanadyjskiej uUstawie o ustanowieniu prawnej podstawy dla stosowania technologii IT.

Obecnie istnieje już infrastruktura PKI, której podstawową usługą jest – wydawanie użytkownikom osobistych nośników cyfrowych,

zawierających dane, które go identyfikują. Istnieje również nieokreślony i potencjalnie nieograniczony krąg systemów IT w bankach, urzędach państwowych lub u operatorów sieci komórkowych, które – z różnych przyczyn – są zainteresowane obsługą użytkowników. W każdym z takich systemów istnieją odrębne wymagania i ograniczenia, dotyczące zakresu niezbędnych informacji dodatkowych.

Tradycyjnie informacje dodatkowe są zbierane niezależnie od innych systemów. Takie podejście ma szereg istotnych wad z punktu widzenia każdego z uczestników wymiany informacji: działania w celu identyfikacji użytkownika są dublowane; w większości są również dublowane działania podejmowane w celu zbierania dodatkowych informacji; z czasem pojawia się problem utrzymania aktualności i zgodności danych, dublowanych w wielu systemach informatycznych.

W polskim prawie nie ma jawnego odwołania do certyfikatów atrybutów, chociaż pojęcie atrybutów jest używane głównie w kontekście kwalifikowanego podpisu elektronicznego.

Rozwiązać te problemy można włączając informację niezbędną dla systemu dedykowanego w skład certyfikatu użytkownika. Jest to najbardziej oczywiste i ma już zastosowanie w wielu systemach korporacyjnych. Jednak takie podejście nie jest idealne, a dla publicznych systemów nie może być w ogóle zastosowane z kilku względów. W momencie wydania certyfikatu użytkownika nie jest praktycznie możliwe spełnienie wymogów, co do automatycznego udostępnienia zasobów informacyjnych ze strony nieograniczonego kręgu systemów IT, do których użytkownik może się odwoływać. Ponadto obowiązująca Ustawa o ochronie danych osobowych ogranicza tryb przetwarzania danych, które są niezbędne dla wielu systemów dedykowanych, co powoduje, że nie jest możliwe umieszczenie w rejestrze publicznym certyfikatów zawierających np. numer paszportu, a to zgodnie z Ustawą o podpisie elektronicznym jest konieczne.

Zaufana trzecia strona

Rekomendacja X.842 Międzynarodowej Unii Telekomunikacyjnej ITU (*International Telecommunication Union*) określa listę usług i serwisów, razem składających się na tzw. zaufaną trzecią stronę. W liście serwisów jest serwis atrybutów oraz przykład technicznej realizacji, przedstawiony w międzynarodowych rekomendacjach RFC 3281. Dane rekomendacje wprowadzają pojęcie certyfikatu atrybutów, kryptograficznie powiązanego z certyfikatem klucza publicznego. Certyfikatów atrybutów może być kilka, każdy z nich zawiera zgrupowaną informację, określającą rolę wcześniej identyfikowanego podmiotu.

Wykorzystanie certyfikatów atrybutów w celu przedłożenia dodatkowych danych o użytkowniku daje możliwość organizowania jednego lub kilku tematycznych rejestrów z ograniczonym dostępem, za uzupełnienie których będą odpowiadać upoważnione urzędy, a systemy użytkowe będą występować jako użytkownicy, którym udostępnia się z zaufanego źródła informacje o pełnionej roli weryfikowanego podmiotu. W tym przypadku zaufana trzecia strona faktycznie będzie „jednym okienkiem”, przez które będą realizowane oficjalne uzupełnienia, zmiany oraz uzyskanie dodatkowej informacji o użytkowniku.

Tradycyjnie informacje dodatkowe, atrybuty, zbierane są niezależnie od innych systemów. Rozwiązać te problemy można włączając informację niezbędną dla systemu dedykowanego w skład certyfikatu użytkownika.

Opisany sposób umieszczenia informacji dodatkowej nie nakłada żadnych ograniczeń na sposoby prezentacji danych wewnątrz użytkowych systemów informatycznych. Oprócz tego:

1 Znikają problemy związane z aktualnością, integralnością i wiarygodnością informacji dodatkowej.

2 Nie ma żadnego wpływu zmieniających się potrzeb systemów użytkowych na procedurę wydania osobistych certyfikatów użytkowników.

Obecnie istnieje już infrastruktura PKI, której podstawową usługą jest - wydawanie użytkownikom osobistych nośników cyfrowych, zawierających dane, które ich identyfikują.

3 Ze względu na to, że sposób publikacji jest standardowy, procedura zainstalowania dowolnego systemu użytkowego jest również standardowa i przejrzysta.

4 Dedykowane systemy wykorzystując tę technologię, pomimo standardowych instrumentów otrzymania informacji o użytkowniku od zaufanej trzeciej strony, będą w stanie bardziej efektywnie organizować współpracę pomiędzy sobą.

5 Problemy uwierzytelnienia i bezpieczeństwa informacji umieszczonej w certyfikacie atrybutów, wg wyboru urzędów upoważnionych, mogą być rozwiązane każdym zaaprobowanym sposobem (zaczynając od szyfrowania certyfikatu atrybutów i kończąc na organizowaniu bezpiecznych połączeń sieciowych).

Pomysł stworzenia serwisu certyfikatu atrybutów wywodzi się z ogólnego nurtu technologii PKI. Serwis ten jest aplikacją technologii PKI i łączy się z jej rozwojem. Obecnie są już przykłady pomyslnego wdrożenia takich serwisów, tak dla organizacji mających ograniczony dostęp do pokładów danych, jak i w celu przedłożenia danych ewidencyjnych użytkowników wewnątrz systemów dedykowanych. A w jednym z państw Unii Europejskiej jest przykład wykorzystania certyfikatu atrybutów razem z certyfikatami kwalifikowanymi. ▶

Denis Kopyłow jest dyrektorem technicznym w moskiewskiej firmie Top-Cross.