Fot. Alen Stojanac

Mariusz Skiba

Podpisz się komórką!

Podpis elektroniczny ma fundamentalne znaczenie dla rozwoju gospodarki elektronicznej i społeczeństwa informacyjnego. Stosowanie Internetu w komunikacji pomiędzy firmami, osobami i instytucjami w znaczny sposób obniża koszty prowadzania działalności, przyspiesza i automatyzuje procesy oraz przyczynia się do zwiększenia efektywności działań gospodarczych. Elektroniczna identyfikacja stron wzajemnie się komunikujących jest sprawą kluczową. Ta potrzeba dała impuls do stworzenia mechanizmów prawnych i technologicznych, które pozwoliłyby na tworzenie ważnych dowodów oświadczeń woli stron w obrocie elektronicznym. Podpis elektroniczny spełnia te wymagania poprzez jednoznaczną identyfikację stron, poufność komunikacji oraz integralność przesłanych danych.

Podpis elektroniczny oparty jest o kryptografię asymetryczną, która wykorzystuje dwie pary kluczy – prywatny i publiczny. Te klucze powiązane są ze sobą zależnością matematyczną. Klucz publiczny jest dostępny dla wszystkich, natomiast klucz prywatny znany jest tylko i wyłącznie osobie, do której został przypisany. Najczęściej klucz prywatny jest chroniony PINem i umieszczany na karcie mikroprocesorowej. Kluczem prywatnym podpisujemy dane, a klucz publiczny służy do weryfikacji poprawności podpisu. Dane osoby tj. imię, nazwisko, adres zamieszkania są przypisane do klucza publicznego tworząc certyfikat, który jest poświadczany przez instytucje do tego uprawnione zwane urzędami certyfikacji.

Usługodawcy nie inwestują w systemy wspierające podpis elektroniczny, ponieważ nie ma wielu użytkowników. Użytkownicy nie kupują certyfikatów, ponieważ nie mają potrzeby korzystania z nich. Taki stan rzeczy trwa już od roku 2001.

Fot. Davide Guglielmo

16 sierpnia 2001 roku weszła w życie Ustawa o podpisie elektronicznym zrównująca skutki prawne podpisu złożonego elektronicznie ze skutkami prawnymi podpisu własnoręcznego. Ustawa wprowadziła wymagania techniczne i prawne dla wykorzystania podpisu elektronicznego. Ważnym elementem ustawy jest określenie bezpiecznych urządzeń do ochrony klucza prywatnego. Przyjęto, iż te wymagania najlepiej spełnia karta mikroprocesorowa, która jest wkładana do czytnika kart mikroprocesorowych, podłączonego do komputera. Klucz prywatny jest chroniony PINem i tylko właściciel karty ma do niego dostęp.

Jednakże, pomimo istnienia możliwości prawnych i technologicznych, rozwój rynku podpisu elektronicznego do tej pory nie jest satysfakcjonujący. Jest klika przyczyn tego stanu rzeczy. Po pierwsze, certyfikaty wystawiane przez urzędy certyfikacji są drogie (obecna cena kształtuje się na poziomie ok. 500 zł). Znaczną część tej kwoty stanowi wartość czytnika i karty mikroprocesorowej. Urzędy certyfikacji nie obniżają cen, ponieważ popyt na certyfikaty nie jest wystarczająco duży. Po drugie, nie ma zbyt wielu możliwości wykorzystania podpisu elektronicznego. Główni usługodawcy, którzy mogliby akceptować podpisane dokumenty: bankowość i administracja państwowa, nie kwapią się do przygotowania swoich systemów do obsługi podpisu elektronicznego. Po trzecie, uzyskanie certyfikatu nie jest łatwe. W Polsce jest tylko kilka miejsc, w którym użytkownik może zdobyć certyfikat i narzędzia do jego obsługi. Póki co nie jest to produkt masowy.

Problemy rozwoju rynku podpisu elektronicznego to klincz, w jakim znajdują się usługodawcy i potencjalni klienci. Usługodawcy nie inwestują w systemy wspierające podpis elektroniczny, ponieważ nie ma wielu użytkowników. Użytkownicy nie kupują certyfikatów, ponieważ nie mają potrzeby korzystania z nich. Taki stan rzeczy trwa już od roku 2001. Ważnym impulsem dla rozwoju rynku podpisu elektronicznego byłaby większa determinacja administracji państwowej przy tworzeniu systemów akceptujących podpis elektroniczny. Już widać pierwsze oznaki poprawy w tym zakresie. Wprowadzana jest ustawa o informatyzacji, w której usługi podpisu elektronicznego będą silniej wspierane przez instytucje państwowe. Niebagatelną rolę odgrywa też Unia Europejska, która wspiera inicjatywy wprowadzające podpis elektroniczny w relacjach obywatel – administracja. Tak naprawdę obecnie jedynym dużym systemem, w którym wykorzystuje się podpis elektroniczny jest składanie deklaracji ZUS w systemie Płatnik. Do tej pory wydano około 500 000 certyfikatów dla użytkowników składających elektroniczne zeznania ZUS.

Problemy, które są przyczyną słabego rozwoju rynku podpisu elektronicznego mogą być rozwiązane poprzez zastosowanie nowej technologii – mobilnego podpisu elektronicznego. Rozwiązanie opiera się na wykorzystaniu specjalnej karty SIM (z algorytmem RSA), jako elementu przechowującego klucz prywatny użytkownika i dokonujących operacji kryptograficznych na dostarczanych danych. Karta SIM może być uważana za rodzaj karty mikroprocesorowej o tym samym stopniu zabezpieczeń. Dzięki temu telefon komórkowy może być uważany za bezpieczne urządzenie do składania podpisu elektronicznego i spełniające wymagania ustawy o podpisie elektronicznym. To otwiera zupełnie nowe możliwości. Telefon komórkowy może być używany do podpisu różnego typu oświadczeń woli: składnia deklaracji podatkowych, podpisywania umów ubezpieczeniowych, głosowania w wyborach etc., oraz być uniwersalnym tokenem uwierzytelniającym w bankowości elektronicznej, w dostępie do informatycznych rejestrów państwowych (KRS, księgi wieczyste itp.), serwisów aukcyjnych. Wszystkie te sprawy można załatwić używając jednego narzędzia, jakim jest telefon komórkowy, znanego przez użytkownika i łatwego w obsłudze.

Mobilny podpis elektroniczny to tak naprawdę rozproszony system informatyczny, w którego skład wchodzi

platforma transakcyjna, karta SIM, interfejsy do usługodawców, urzędów certyfikacji oraz operatorów GSM. Całość tworzy bezpieczny system, który łączy wszystkich uczestników. Platforma transakcyjna jest centralną częścią systemu i jej zadaniem jest składanie podpisu, weryfikacja certyfikatów, zapewnienie poufności transmisji i rozliczanie opłat za usługi pomiędzy uczestnikami. Jej działanie jest niewidoczne dla podpisującego.

Możemy wyróżnić dwa sposoby podpisywania dokumentów. Pierwszy to podpisywanie treści czytanej na ekranie telefonu komórkowego, a drugi to podpisywanie treści czytanej na ekranie komputera. Ten pierwszy przypadek może być wykorzystany do realizacji usług m-commerce, gdzie telefon pełni funkcje terminala do akceptacji transakcji. W tym drugim przypadku telefon staje się bezprzewodowym czytnikiem kart mikroprocesorowych i proces podpisu dokumentów przebiega następująco:

1. Użytkownik czyta treść dokumentu na ekranie komputera, po akceptacji treści naciska przycisk „Podpisz”.

Fot. John Lee

2. Skrót dokumentu jest wysyłany w bezpieczny sposób do telefonu, dokładnie mówiąc do karty SIM. Telefon podłączony jest z komputerem poprzez: port podczerwieni, łącze bluetooth, kabel lub SMS.
3. Użytkownik proszony jest o wprowadzenie PIN.
4. Skrót jest podpisywany przez kartę SIM i odsyłany do komputera.
5. Podpisany dokument odsyłany jest do odbiorcy, który na podstawie certyfikatu jest w stanie ocenić poprawność złożonego podpisu.

Zastosowanie telefonu komórkowego jako narzędzia do składania podpisu elektronicznego likwiduje wady poprzednich rozwiązań opartych o tradycyjne karty mikroprocesorowe i otwiera zupełnie nowe możliwości.

Dzieje się tak z kilku powodów. Po pierwsze jest to bardzo tanie rozwiązanie dla użytkowników. Karta SIM jest kartą mikroprocesorową, a telefon czytnikiem tej karty. Nie ma potrzeby zakupu dodatkowych urządzeń. Po drugie, punkty sprzedaży telefonów GSM mogą pełnić funkcję punktów rejestracji i wydawać certyfikaty. Podczas zakupu telefonu sprawdzana jest tożsamość klienta (przy niedużych zmianach proceduralnych można wystawiać certyfikaty). Operatorzy GSM posiadają bardzo dobrze zorganizowaną i nowoczesną sieć sprzedaży – punktów obsługi klienta. To może być bardzo łatwy sposób nabywania certyfikatów. Niejako przy okazji zakupu telefonu użytkownik będzie mógł posiadać elektroniczną tożsamość.

Po trzecie telefonia komórkowa jest bardzo popularna (w Polsce jest około 25 milionów abonentów GSM). Dzięki temu istnieje bardzo duża liczba potencjalnych posiadaczy certyfikatów. Ten potencjał może skłonić usługodawców do oferowania usług w Sieci.

Biorąc pod uwagę te czynniki należy oczekiwać, iż wprowadzanie technologii mobilnego podpisu elektronicznego skłoniłoby instytucje i firmy do oferowania usług podpisu elektronicznego z pożytkiem dla nich samych i użytkowników. Podpis elektroniczny w komórce to tak naprawdę nadanie użytkownikowi elektronicznej tożsamości, dzięki której będzie on rozpoznawalny przez innych użytkowników w sposób szybki, bezpieczny i tani. To może odmienić w znaczący sposób handel elektroniczny, usługi e-government czy też usługi finansowe.