Mirosław Kutyłowski

Elektroniczna pieczątka

Fot. Davide Guglielmo

Technologia podpisu cyfrowego na dobre zadomowiła się w systemach informatycznych. Stosowana jest w kluczowych komponentach systemów, jej brak uniemożliwiłby w istocie działanie bezpiecznych protokołów komunikacyjnych. To z kolei unieruchomiłoby szereg kluczowych obszarów obrotu danymi – w tym części informatycznych systemów bankowych.

Podczas gdy podpis cyfrowy zaszyty w protokołach jest powszechnie używany, stosowanie go na najwyższych poziomach protokołów komunikacyjnych w sposób widoczny dla użytkownika nie jest rozpowszechniony i napotyka na szereg fundamentalnych trudności. Wynikają one nie z braku możliwości technologicznych, lecz z niezrozumienia ich natury, z błędnych założeń ekonomicznych, wreszcie z braku sprzyjającego otoczenia prawnego.

Na etapie fali inicjatyw ustawodawczych, w tym również w Polsce, skoncentrowano się na regulowaniu obszaru związanego z polem działania osób fizycznych. Zastosowania w zakresie działania podmiotów gospodarczych, podmiotów publicznych miały być załatwione przy pomocy czynności dokonywanych przez osoby fizyczne. Doświadczenia ostatnich lat wskazują, że podejście to okazało się błędem – nie nastąpiło upowszechnienie stosowania podpisu elektronicznego inicjowane przez osoby prywatne.

Na etapie fali inicjatyw ustawodawczych, w tym również w Polsce, skoncentrowano się na regulowaniu obszaru związanego z polem działania osób fizycznych. Zastosowania w zakresie działania podmiotów gospodarczych, podmiotów publicznych miały być załatwione przy pomocy czynności dokonywanych przez osoby fizyczne.

Lobbying na rzecz podpisu elektronicznego

Analizując powstające akty prawne można zauważyć silną tendencję do wprowadzania obowiązku stosowania bezpiecznego podpisu elektronicznego opartego o kwalifikowany certyfikat. Szczególnie interesująca okazuje się nowelizacja przepisów dotyczących ZUS. Obecnie funkcjonujący system uwierzytelniania komunikacji pomiędzy płatnikiem a ZUS, opiera się o technologię podpisu cyfrowego. Wykorzystano tu zarówno klasyczny podpis cyfrowy (RSA), jak

i standardowy sposób kodowania. System zabezpieczenia klucza prywatnego zaprojektowano zgodnie z oceną zagrożeń – klucz chroniony jest w sposób adekwatny do poziomu ochrony danych przekazywanych przez płatnika – bez korzystania ze specjalnych urządzeń hardware'owych. Uwierzytelnianie kluczy publicznych oparto o standardową technologię X.509 – de facto jedyną w momencie powstawania systemu.

Ustawa o informatyzacji wprowadza jednak głębokie modyfikacje w systemie. Uwierzytelnianie komunikacji ma odbywać się za pomocą bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu. Co prawda, postanowienie to wchodzi w życie dopiero po 27 miesiącach od daty ogłoszenia ustawy, nie dotyka więc przedsiębiorców już dzisiaj.

Pod względem samego podpisu cyfrowego zmiana ta nie zmienia właściwie nic. Przypuszczalnie większość użytkowników nadal stosować będzie podpis RSA. Jednak dla użytkowników preferujących inne schematy podpisu będą musiały być stworzone odpowiednie moduły działające po stronie ZUS. Po stronie płatnika konieczne będzie zaopatrzenie się w kwalifikowane certyfikaty i bezpieczne urządzenia do składania podpisu elektronicznego. Co więcej, ponieważ informacje przekazywane do ZUS będą podpisywane przez osoby fizyczne, konieczne będzie zaopatrzenie w kwalifikowane certyfikaty więcej niż jednego pracownika – ze względu na urlopy pracownicze, choroby itp. Dodajmy, że dziś ten problem nie istnieje – prywatny klucz kryptograficzny jest przypisany nie do osoby fizycznej ale do podmiotu składającego raporty w ZUS.

Podobnie kontrowersyjne ustalenia zawarte są na przykład w nowelizacji Kodeksu Postępowania Administracyjnego wprowadzonej przez ustawę o informatyzacji. Zgodnie z tą regulacją wszelkie podania (żądania, zażalenia, zapytania, odwołania) kierowane do podmiotów publicznych powinny być opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu.

Podpisywanie dokumentów masowych

Najbardziej naturalnym obszarem zastosowania podpisu cyfrowego jest uwierzytelnianie danych cyfrowych generowanych w sposób automatyczny. Podczas gdy generowanie takich dokumentów przez systemy informatyczne stało się bardzo łatwe, ich uwierzytelnianie pozostało problematyczne. Nie dotyczy to jednak warstwy technologicznej – tu istnieje szereg rozwiązań, od tych najtańszych po drogie, ale bezpieczne, oparte o urządzenia HSM. Przeszkodą okazały się koncepcje prawne związane z okresem „przedelektronicznym", w którym stosowano zarówno podpis własnoręczny jak i pieczątkę jako formy uwierzytelniania dokumentów.

Wraz z powstawaniem elektronicznych rejestrów i możliwością wydawania wydruków z rejestru pojawiło się zagadnienie ich uwierzytelniania. Pragmatycznym rozwiązaniem zastosowanym między innymi w Niemczech była rezygnacja z podpisu i pieczęci na takich dokumentach. Zasadą tą nie objęto jednak dokumentów prywatnych.

Kolejnym etapem jest generowanie za pomocą rejestrów elektronicznych dokumentów elektronicznych. Tu sytuacja jest nieco bardziej skomplikowana (w przypadku drukowania na papierze istnieje na przykład możliwość zapisywania ukrytych treści pozwalających zweryfikować pochodzenie wydruku). Niezbędnym okazało się zastosowanie podpisu cyfrowego. Podpis taki może być elektroniczną wersją podpisu własnoręcznego albo pieczątki. Pierwsza możliwość została zrealizowana (gorzej czy lepiej) przez ustawę o podpisie elektronicznym, druga nie. Okazuje się, że podpis elektroniczny osoby fizycznej nie do końca stanowić może zamiennik dla pieczątki elektronicznej. Najpoważniejszą przeszkodą jest reguła zawarta w dyrektywie unijnej o podpisie elektronicznym i przeniesiona do ustaw krajowych, iż osoba składająca podpis musi podjąć odpowiednią decyzję o jego złożeniu po otrzymaniu dokumentu. Decyzja ta nie może być domniemana na podstawie włączenia odpowiedniego urządzenia. Tym samym wykluczone jest opatrywanie podpisem w trybie real time bez udziału człowieka. A to właśnie wydaje się bardzo atrakcyjnym zastosowaniem choćby w przypadku faktur elektronicznych.

Czeska pieczątka elektroniczna

Koncepcja wprowadzenia odpowiednika pieczęci do świata elektronicznego nie jest niczym nowym. Możliwość taką wprowadziła explicite ustawa irlandzka powstała w mniej więcej w tym samym czasie co polska ustawa o podpisie elektronicznym. Umożliwia ona składanie podpisu przez osobę prawną i przez podmioty publiczne – w tym również jednostki nie posiadające osobowości prawnej. Jednak czeska koncepcja z nowelizacji ustawy z 2004 roku wprowadza możliwości szczególnie interesujące z naszego punktu widzenia ze względu na pokrewieństwo polskiego i czeskiego systemu prawnego.

Oprócz drastycznego potanienia certyfikatów po włączeniu się w rynek podpisów przez czeską pocztę, najważniejszym

impulsem rozwoju ma być tak zwana *elektronicka značka*. Wymagania stawiane wobec takiej pieczątki elektronicznej są właściwie takie same jak wobec podpisu elektronicznego osoby fizycznej: pieczątka elektroniczna ma uniemożliwiać modyfikację opieczętowanego dokumentu, ma umożliwiać identyfikację podmiotu składającego pieczęć, wreszcie ma być dokonana za pomocą środków, które „właściciel pieczęci" może utrzymywać pod swoją wyłączną kontrolą. Z jednej strony są to własności jakich byśmy oczekiwali od pieczęci elektronicznej, a z drugiej strony są to własności jakie można zaimplementować choćby za pomocą algorytmu podpisu RSA i zastosowania bezpiecznego modułu dla przechowywania klucza prywatnego.

Różnice pojawiają się w warstwie prawnej. Czeska ustawa stanowi, iż złożenie pieczęci elektronicznej umożliwia uwierzytelnienie, że pieczęć elektroniczna została złożona przez właściciela pieczęci. Ponadto - i jest to kluczowe - uważa się, że osoba (fizyczna lub prawna) składająca pieczęć uczyniła to automatycznie bez bezpośredniego uwierzytelnienia zawartości dokumentu elektronicznego i wyraziła tym swoją wolę.

Zastosowania

Nie jest zaskoczeniem, że zastosowania pieczątki elektronicznej mają być wielorakie. Pierwszy przykład można podać ... z Polski. Elektroniczny system do komunikacji płatnika z ZUSem oparty jest o uwierzytelnianie za pomocą algorytmu RSA. Nie jest to podpis elektroniczny zarówno w przypadku płatników jak i Zakładu Ubezpieczeń Społecznych. Istotnie, z wyjątkiem płatników będących osobami fizycznymi, podpis cyfrowy przyporządkowany jest do osób prawnych. W przypadku ZUS jest to podpis generowany za pomocą automatycznego systemu bez ingerencji człowieka reagującego na napływające raporty. Okazuje się więc, że możliwe jest, choć zostało to wprowadzone odrębnymi przepisami, stosowanie pieczęci elektronicznych. System ten okazał się sprawny, co więcej, zastąpił on początkowo wdrażany system „papierowy", który mógł doprowadzić system ZUS do stanu trwałej niewydolności.

Drugim, analogicznym systemem stosowania elektronicznej pieczątki ma być w Czechach system podatkowy. Tak jak i w Polsce, duże koszty związane są z ręcznym obiegiem informacji podatkowych. Paradoksalnie, informacje podatkowe generowane w systemie elektronicznym są przenoszone na papier, podpisywane, następnie dostarczane drogą tradycyjną a następnie żmudnie (i zapewne z błędami) z powrotem elektronizowane. Długa i zawodna droga obiegu informacji nie pozwala na efektywną kontrolę zachodzących procesów, generuje wysokie koszty zarówno po stronie podatników jak i administracji państwowej. System dławi się wskutek liczby krążących dokumentów papierowych. Nie negując potrzeby upraszczania zasad podatkowych, w tej sytuacji elektroniczna pieczątka jest i pozostanie niezbędna.

Kolejny obszar zastosowań to elektroniczne biuro podawcze – nawet w przypadku, gdy obywatel dysponuje podpisem elektronicznym, to podmiot publiczny przyjmujący podanie i wprowadzający je do swego systemu informatycznego powinien wystawić potwierdzenie odbioru. Takie potwierdzenie powinno być uwierzytelnione. Właśnie pieczatką elektroniczną podmiotu, a nie osoby pracującej w urzędzie. Na takiej samej zasadzie powinny działać podpisy pod elektronicznymi dokumentami bankowymi. Szczęśliwie, rozporządzenie Rady Ministrów wydane w tej sprawie nie traktuje podpisu pod elektronicznym dokumentem bankowym równoznacznie z podpisem elektronicznym według ustawy o podpisie. Lepiej by jednak było, aby unikać takich uergulowań specjalnych i tworzyć jednolity system, w którym jedno pojęcie o jasnym znaczeniu stosowane jest niezależnie od obszaru aktywności.

Wreszcie niesłychanie ważnym obszarem zastosowań pieczątki elektronicznej mógłoby być sądownictwo. Szereg procedur w sprawach o stosunkowo niewielkiej wadze mogłoby być skutecznie realizowane w ramach procedur elektronicznych - odciążyłoby to aparat sprawiedliwości i pozwoliło na skoncentrowanie uwagi na tych etapach procedur, które naprawdę wymagają rozstrzygnięcia „ręcznego". Powszechne stosowanie pieczątek elektronicznych znakomicie ułatwiłoby i uprościło takie procedury.

Nie sposób na koniec pominąć problemu faktur elektronicznych. Właśnie tutaj marzą się systemy pozwalające nie tylko na wygenerowanie zamówienia, przyjęcia go, kierowanie logistyką realizacji, lecz także pozwalające na wystawianie faktur *on-line*. Dziś taka możliwość istnieje w ramach systemów EDI, jednak ogranicza to zakres zastosowań do partnerów, między którymi istnieją stałe powiązania gospodarcze.

Regulacje czeskie wprowadzające pieczątkę elektroniczną po kilku latach nieudanych prób z podpisem elektronicznym osoby fizycznej są oznaką nieuchronności pewnego procesu. Mimo wszystkich zjawisk hamujących postęp w tej dziedzinie będziemy musieli zaakceptować i w Polsce konieczność wprowadzenia tego rozwiązania. Otwartym pytaniem pozostaje tylko kiedy to nastąpi.

Prof. dr hab. Mirosław Kutyłowski jest profesorem zwyczajnym Politechniki Wrocławskiej