Zagadka elektronicznej skrzynki podawczej

Zadaniem skrzynki podawczej jest tylko przyjęcie dokumentu i wprowadzenie go do systemu teleinformatycznego urzędu. Skrzynka nie ocenia wartości merytorycznej dokumentu ani jego zasadności. Skrzynka powinna zatem przeprowadzić weryfikację autentyczności i integralności podpisanego dokumentu, wprowadzić go do systemu i niezwłocznie wydać UPO.

Rozporządzenie w sprawie warunków organizacyjno–technicznych doręczania dokumentów elektronicznych podmiotom publicznym (Dz.U.2005.200.1651) określa sposób, w jaki ma być wydawane Urzędowe Poświadczenie Odbioru (UPO), czyli elektroniczny kwit potwierdzający fakt złożenia dokumentu do urzędu w określonym terminie. Z rozporządzeniem tym wiążą się co najmniej trzy wątpliwości natury techniczno prawnej.

Rozporządzenie definiuje UPO w sposób następujący:

§ 2. Użyte w rozporządzeniu określenia oznaczają: (...)

4) urzędowe poświadczenie odbioru – dane elektroniczne dołączone do dokumentu elektronicznego doręczonego podmiotowi publicznemu lub połączone z tym dokumentem w taki sposób, że jakakolwiek późniejsza zmiana dokonana w tym dokumencie jest rozpoznawalna, określające:

a) pełną nazwę podmiotu publicznego, któremu doręczono dokument elektroniczny,

b) datę i czas doręczenia dokumentu elektronicznego rozumiane jako data i czas wprowadzenia albo przeniesienia dokumentu elektronicznego do systemu teleinformatycznego podmiotu publicznego,

c) datę i czas wytworzenia urzędowego poświadczenia odbioru.

Warto zwrócić uwagę, że początek tej definicji („*dane elektroniczne...*") bardzo przypominają definicję podpisu elektronicznego w ustawie o podpisie elektronicznym. W istocie jest to właśnie definicja podpisu elektronicznego pozostawiająca sporą swobodę, jeśli chodzi o sposób jej implementacji (certyfikat, format, standard).

Jakim certyfikatem podpisywać UPO?

Jak wynika z tekstu rozporządzenia, UPO może być podpisane praktycznie dowolną formą podpisu elektronicznego (PGP?), pod warunkiem, że będzie ona spełniać wymagania w punktach a–c. Skąd taki liberalizm w polskim prawie, w którym zwykle, gdzie to tylko możliwe, używa się sformułowania „i musi być podpisane bezpiecznym podpisem elektronicznym zgodnym z ustawą..."?

Zgodnie z polską definicją podpisu kwalifikowanego, musi być on przypisany do osoby fizycznej, zaś sposób jego składania powinien umożliwiać m.in. prezentację podpisywanej treści oraz zawierać ostrzeżenie o skutkach prawnych złożenia podpisu. Kto miałby być osobą fizyczną w przypadku automatycznego podpisywania przez HSM? Jak miałby być realizowany proces prezentacji? Wymagania te nijak nie pasują do profilu zastosowań ESP.

Konsekwentnie należy więc uznać, że do podpisywania UPO, które są wystawiane *ad hoc* przez automat (HSM), nie można stosować certyfikatu kwalifikowanego.

Być może są to wnioski oczywiste, ale nie były one oczywiste dla szeregowych pracowników administracji publicznej, którym polecono przygotować wdrożenie takiego systemu. Interpretacje zahaczały o absurd – np. rozważano, czy w razie wsadzenia do HSM certyfikatu osobowego nie będzie problemów z inspekcją pracy, skoro podpis jest równoważny podpisowi odręcznemu, a HSM podpisuje 24h na dobę, z czego wynika ciągła obecność administratora w pracy.

Problemy te są połowicznie winą nowości technologicznych oraz niespójności i oderwania od rzeczywistości tworzonego *ad hoc* prawa. Dlaczego np. rozporządzenie nie odwołuje się do definicji podpisu z ustawy, tylko tworzy własną?

Nasuwa się pytanie – jeśli nie certyfikat kwalifikowany, to jaki? Pracownicy administracji publicznej interpretowali to jako możliwość stosowania dowolnego certyfikatu niekwalifikowanego, co nie stoi w sprzeczności z literą rozporządzenia. Z drugiej strony stwarza to ryzyko powstania chaosu, jeśli każda jednostka zacznie tworzyć własne drzewo certyfikacji. Wiele instytucji publicznych takimi drzewami już dysponuje – funkcjonują one w oparciu o lokalne, prywatne centra certyfikacji i spełniają swoje zadanie w zakresie np. uwierzytelnienia pracowników tam, gdzie zakup certyfikatów w komercyjnych CA byłby nieopłacalny.

Drugie ryzyko to chłonność pojęcia „podpis niekwalifikowany", co oznacza w Polsce wszystko, co nie jest podpisem kwalifikowanym – czyli, poczynając od PGP, a skończywszy na prywatnych drzewach X.509. Jaka będzie po kilku latach wartość dowodowa UPO podpisanego takim certyfikatem?

Na każdym kroku widoczna jest tutaj przepaść pomiędzy precyzyjnie zdefiniowanym, ale nieużywanym w tym zastosowaniu, podpisem kwalifikowanym i resztą, czyli każdym innym. Prowadzi to do powstawania takich właśnie lokalnych definicji podpisu elektronicznego, wprowadzanych w sytuacjach, kiedy nie da się już po prostu nic zrobić, żeby po raz kolejny zatwierdzić w rozporządzeniu podpis kwalifikowany.

UPO w praktyce

Jak to wygląda w praktyce? Jedyną ESP, jaką udało mi się przetestować w praktyce była Elektroniczna Skrzynka Podawcza ZUS postawiona w technologii opracowanej przez Certum.

W rozwiązaniu Certum UPO podpisywane jest zaświadczeniem certyfikacyjnym z drzewa Centrast, wystawionym na „Certum QDA". Jest to rozsądny sposób na ułatwienie weryfikacji podpisu pod UPO, ale budzi wątpliwości z jednego powodu – zaświadczenia certyfikacyjne są przez ustawę o podpisie zastrzeżone dla centrów certyfikacji.

Innymi słowy, tylko podmiot świadczący usługi certyfikacyjne może otrzymać od Centrastu zaświadczenie certyfikacyjne w drzewie kwalifikowanym, nadający się do załadowania do HSM. Równocześnie, certyfikatów w drzewie kwalifikowanym, które może uzyskać każdy, nie można wsadzić do HSM (osoba fizyczna). Kto ma więc wyłączność na podpisywanie naszych UPO w drzewie Centrastu...? Inne informacje praktyczne o ESP ZUS, które mogą kogoś zainteresować:

- UPO jest zapisywane w formacie S/MIME, co jest zręcznym połączeniem interoperacyjności (plikowi wystarczy dodać rozszerzenie .eml żeby zweryfikować go w Thunderbirdze lub Outlooku) ze zgodnością z rozporządzeniem o minimalnych wymaganiach wobec systemów teleinformatycznych, wskazanym przez §3 omawianego tutaj „rozporządzenia w sprawie warunków...";
- UPO zostało zaimplementowane za pomocą zgrabnych formularzy XML/XSL, które sprawiają wrażenie że powinny działać w każdej przeglądarce. Moduł podpisu elektronicznego – ze zrozumiałych względów (dostęp do karty) – jest zaimplementowany w Javie i w Firefoxie.

Kiedy można wystawić UPO?

Podczas implementacji ESP nieuchronnie pojawia się problem czasu wystawienia UPO w stosunku do momentu przysłania dokumentu. Problem bierze się stąd, że w momencie, gdy dokument jest przesyłany, podpisany z pomocą certyfi-

katu kwalifikowanego do ESP, skrzynka powinna zweryfikować mój podpis pod tym dokumentem. Jednak zgodnie z prawem nie może tego zrobić – pełna weryfikacja podpisu kwalifikowanego nie jest możliwa, dopóki nie zostanie wydany kolejny CRL, co oznacza zwłokę od 1 do 12 godzin.

Nie jest to problem trywialny. Pełna weryfikacja podpisu kwalifikowanego musi dokładnie zająć tyle czasu, chyba że zostanie wykorzystane OCSP, które jednak ze strony centrów nie jest obowiązkowe. Z punktu widzenia osoby składającej dokument pożądane jest jak najszybsze otrzymanie UPO.

Praktyczne rozwiązanie tego problemu jest stosunkowo proste, jeśli przeanalizuje się cel tak długiego oczekiwania na weryfikację podpisu – ma to zabezpieczyć przed sytuacją, kiedy podpis zostanie złożony skradzioną kartą i kodem PIN już po jej odwołaniu, ale przed wydaniem kolejnego CRL. Pytanie tylko, czy taka sytuacja stanowi jakieś zagrożenie dla urzędu?

Otóż zadaniem skrzynki podawczej jest tylko przyjęcie dokumentu i wprowadzenie go do systemu teleinformatycznego urzędu. Skrzynka nie ocenia wartości merytorycznej dokumentu ani jego zasadności. Skrzynka powinna zatem przeprowadzić weryfikację autentyczności i integralności („weryfikacja matematyczna") podpisanego dokumentu, wprowadzić go do systemu i niezwłocznie wydać UPO. Pełna weryfikacja następuje po zakończeniu „okienka niepewności" i dopiero po jej pomyślnym przeprowadzeniu dokument może być skierowany do dalszego przetwarzania.

Byłby to więc pewien etap pośredni pomiędzy przyjęciem dokumentu przez skrzynkę, a wprowadzeniem jej w proces biznesowy w urzędzie. W tym okresie dokument pozostawałby w stanie zawieszenia. Po kompletnym zweryfikowaniu podpisu nabierałby wszystkich cech z tego wynikających, czyli głównie dotyczących autorstwa oraz daty pewnej. W razie negatywnej weryfikacji dokument byłby odrzucany, zaś UPO potwierdzałoby tylko złożenie nieważnego dokumentu.

Jeśli wyślemy do Urzędu Skarbowego listem poleconym pustą kartkę, to potwierdzenie nadania nie dowodzi wcale złożenia wymaganego dokumentu.

Jakie normy musi spełniać HSM?

Rozporządzenie w sprawie warunków techniczno–organizacyjnych wymienia również precyzyjnie wymagania, jakie ma spełniać HSM stosowany w ESP: System teleinformatyczny (...) do wytworzenia urzędowego poświadczenia odbioru zawiera sprzętowy moduł bezpieczeństwa (Hardware Security Module), spełniający wymagania normy FIPS 140–2 (...) poziom trzeci lub wyższy, wydanej przez National Institute of Standards and Technology (NIST). Zapis ten budzi dwojakie kontrowersje.

Po pierwsze, narzucająca się z lektury rozporządzenia interpretacja jest taka, że oto każdy urząd musi zaopatrzyć się w ESP wyposażoną w HSM. Koszt samego HSM to 15–30 tysięcy złotych. Argumentacja– przemawiająca za stosowaniem HSM – wydajność, bezpieczeństwo, niezaprzeczalność – jest słuszna (Michał Tabor, „Uczciwość i problem techniczny", Computerworld), ale w zderzeniu z sytuacją finansową wielu instytucji publicznych w Polsce oraz przewidywaną liczbą dokumentów elektronicznych, oscylującą na początku w okolicach zera, forsowanie modelu „HSM w każdym urzędzie" jest całkowicie nieracjonalne.

Jest to interpretacja narzucająca się podczas lektury rozporządzenia i była tak odbierana przez wielu pracowników administracji. W chwili obecnej powszechna jest opinia, że duże urzędy macierzyste stawiają ESP i obsługują w ten sposób wiele małych urzędów potomnych . Nadal jednak jest to specyficzna interpretacja, niewynikająca za bardzo z litery rozporządzenia.

Po drugie, dziwi wskazanie w rozporządzeniu tylko jednej normy dotyczącej bezpieczeństwa, jaką jest FIPS 140–2 certyfikowanej przez amerykański instytut NIST.

Realia rynku są takie, iż wiele tych urządzeń istotnie posiada certyfikaty FIPS 140–2, która jest normą ukierunkowaną stricte na rozwiązania kryptograficzne. Ale rozporządzenie do ustawy o podpisie elektronicznym, mówiąc o kartach kryptograficznych, wymienia trzy standardy oceny bezpieczeństwa – FIPS, ITSEC oraz Common Criteria. Ustawa o informacji niejawnej powołuje się z kolei na normę ITSEC. Ocenę – według Common Criteria oraz ITSEC – prowadzi wiele laboratoriów europejskich, w tym także polski Departament Bezpieczeństwa Teleinformatycznego ABW, który wystawia na podstawie tej oceny certyfikat ochrony kryptograficznej. Dlaczego zatem HSM może mieć tylko certyfikat wydany przez amerykański NIST?

Chaos pogłębia kolejne rozporządzenie, tym razem o doręczaniu pism elektronicznych interesantom (Dz.U.2006.227.1664). Rozporządzenia te są często mylone, regulują bowiem bardzo podobne kwestie – w rzeczywistości pierwsze z nich (Dz.U.2005.200.1651) promuje doręczanie pism do urzędu, a drugie – wspomniane wyżej – od urzędu do interesanta. Jest to o tyle uzasadnione, że ze skutecznego doręczenia pisma wynika szereg istotnych konsekwencji, np. możliwość odwołania od decyzji. Rozporządzenie określa sposób doręczania pism interesantom w sposób zapewniający stosunkowo wysoką niezaprzeczalność – a co za tym idzie skuteczność – doręczenia.

Problem polega na tym, że rozporządzenie reguluje również kwestię HSM, używanego przez system, ale posługując się inną normą. Mówi ono, iż moduł HSM, stosowany w systemie, powinien spełniać wymagania normy FIPS 140–2 poziom 3 lub – i to jest nowość – standardu CEN–CWA 14167–2.

Biorąc pod uwagę, że rzadko kiedy będzie miało sens stosowanie dwóch niezależnych HSM – jednego do przyjmowania, drugiego do doręczania pism. To drugie rozporządzenie sprawia wrażenie, jakby jego autorzy zapomnieli o istnieniu pierwszego, które dopuszcza tylko normę FIPS. ■

Paweł Krawczyk
Specjalista z zakresu bezpieczeństwa sieci komputerowych i kryptografii. Od 1992 r. związany z pierwszą w Polsce siecią komputerową FidoNet, a od 1994 r. z Politechniką Krakowską. Od 1996 r. projektuje oprogramowanie kryptograficzne, prowadzi analizy bezpieczeństwa systemów teleinformatycznych. Jednocześnie zrealizował kilkadziesiąt niezależnych audytów, analiz bezpieczeństwa, prac doradczych i innych zleceń w ramach swojej firmy Bolanda Networks. Od 2005 r. członek grupy ekspertów ENISA (European Network and Information SecurityAgency). Od 2006 r. członek zarządu Internet Society Polska.