

Artykuł opublikowany w Computerworld 23 stycznia 2007 (NR 4/751)

Michał Tabor

## Uczciwość i problem techniczny

Od ponad roku obowiązuje rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym (Dz.U.05.200.1651). W tym samym czasie trwa dyskusja czy wpisany w rozporządzeniu wymóg zastosowania HSM spełniającego wymagania normy FIPS 140-2 Level 3 nie ogranicza informatyzacji urzędów.

W dyskusji prowadzonej pomiędzy twórcami rozporządzenia, podmiotami świadczącymi usługi certyfikacyjne, dostawcami sprzętu i urzędnikami podstawowym pojawiającym się argumentem jest koszt urządzenia HSM, brakuje natomiast merytorycznej analizy czym jest elektroniczna skrzynka podawcza, jaką pełni rolę w procedurze administracyjnej i jaki jest wymagany poziom bezpieczeństwa.

Przekazanie dokumentu lub wniesienie podania do urzędu ma zasadnicze znaczenie w procedurze administracyjnej, a termin jego dokonania wpływa na skuteczność prawną i sposób działania urzędu. Od daty, a czasem także godziny biegą terminy związane z załatwieniem sprawy, które mogą także mieć wpływ na ważność wykonanych czynności prawnych. Wprowadzenie odpowiednich mechanizmów umożliwiających pewne i automatyczne przekazanie dokumentów do podmiotu publicznego oraz niezaprzeczalne potwierdzenie ich wniesienia jest jednym z najważniejszych zadań elektronizacji podmiotów publicznych.

**Niezaprzeczalność** (ang. non-repudiation) - brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jedną z uczestniczących w tej wymianie stron. W szczególności niezaprzeczalność podpisu elektronicznego jest zagwarantowana w artykule 6 ustęp 3 ustawy o podpisie elektronicznym:

Art. 6.

1. Bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu stanowi dowód tego, że został on złożony przez osobę określoną w tym certyfikacie jako składającą podpis elektroniczny.
2. Przepis ust. 1 nie odnosi się do certyfikatu po upływie terminu jego ważności lub od dnia jego unieważnienia oraz w okresie jego zawieszenia, chyba że zostanie udowodnione, że podpis został złożony przed upływem terminu ważności certyfikatu lub przed jego unieważnieniem albo zawieszeniem.
3. Nie można powoływać się, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.

Usługa niezaprzeczalności – Zgodnie z Polską Normą PN-ISO/IEC 13888-1 – usługa, której celem jest wystawienie, gromadzenie, obsługiwanie, udostępnianie oraz sprawdzanie poświadczenia, związanego z deklarowanym zdarzeniem lub działaniem tak, aby możliwe było rozstrzygnięcie wszelkich sporów dotyczących wystąpienia lub nie wystąpienia deklarowanego zdarzenia lub działania. Definiuje się następujące usługi niezaprzeczalności: niezaprzeczalność pochodzenia, niezaprzeczalność dostarczenia, niezaprzeczalność przedłożenia oraz niezaprzeczalność przestania.

Niezaprzeczalność wynikająca ze złożenia podpisu elektronicznego pod dokumentem powoduje, że żadna ze stron nie będzie mogła podważyć wiarygodności i ważności podpisu opierając się jedynie na fakcie, że posiada on formę elektroniczną. Niezaprzeczalność jest podstawowym atrybutem bezpieczeństwa podpisu elektronicznego wykorzystywanym w komunikacji dwustronnej, podpisywaniu umów oraz potwierdzaniu zdarzeń.

Systemy teleinformatyczne wdrażane w administracji państwowej i samorządowej mają za zadanie nie tylko usprawnić działanie urzędów, ale także wyeliminować zjawiska niepożądane takie jak korupcja urzędników. Typowym zjawiskiem korupcyjnym występującym w Polskiej administracji jest antydatowanie terminu otrzymania dokumentów niż rzeczywisty oraz możliwość podmiany wcześniej przekazanych dokumentów i zastąpienie ich nowymi. W świecie papierowym urzędnik posiadający pieczęć „WPŁYNEŁO DNIA” może taką operację wykonać w dowolnym momencie, w komunikacji przez Poczta Polską taka możliwość została ograniczona ze względu na wprowadzenie numerowanych oznaczeń listu poleconego, a zastosowanie banderoli z numerem wcześniejszym może zostać łatwo wykryte.

Oczekiwania społeczne związane z elektronicznym dostępem do urzędu oraz konieczność wprowadzenia adekwatnych uregulowań zmniejszających możliwość działania nieuczciwych urzędników wymagają wprowadzenia nowoczesnych rozwiązań. W szczególności dotyczy to całodobowego udostępnienia e-urzędów przez Internet, w sposób nie nakładających dodatkowych obciążeń na samego obywatela.

Warunki, które powinien spełniać elektroniczny urząd przyjmujący dokumenty:

- działać 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku;
- zabezpieczać integralność przekazywanych dokumentów;
- zapewniać niezaprzeczalność oznaczenia czasu przyjęcia dokumentu;
- zapewniać wydanie niezaprzeczalnego potwierdzenia przyjęcia dokumentu niezwłocznie po jego przekazaniu do systemu teleinformatycznego urzędu;
- zapewniać możliwość udowodnienia, że dokument został dostarczony (a więc także podpisany) w okresie ważności certyfikatu;
- uniemożliwiać wydanie nieautoryzowanego potwierdzenia odbioru.

Ważnym aspektem elektronicznej skrzynki podawczej jest jej ciągłość działania, bezobsługowość i automatyczne realizowanie procesu przyjęcia dokumentu. Ponieważ przyjęcie pisma do urzędu musi zostać potwierdzone praktycznie w momencie wnoszenia, nie jest możliwe wykorzystanie do realizacji tego zadania urzędnika posługującego się bezpiecznym podpisem, który jest weryfikowany kwalifikowanym certyfikatem. Należy także zwrócić uwagę, że aktualnie obowiązująca ustawa o podpisie elektronicznym (Dz.U.01.130.1450 z późn.zm.) przypisuje podpis elektroniczny do osoby fizycznej co uniemożliwia zastosowanie tego rodzaju podpisu do automatycznego sygnowania potwierdzenia odbioru. W praktyce oznacza to, że ustawa o podpisie elektronicznym nie może mieć zastosowania dla elektronicznej skrzynki podawczej, a wydane przez skrzynkę podpisy nie będą miały poziomu bezpieczeństwa gwarantowanego artykułem 6 ustęp 3 ustawy. Powyższe argumenty wskazują na konieczność niezwłocznej nowelizacji ustawy o podpisie elektronicznym oraz do czasu wprowadzenia zmian, utrzymanie przepisów

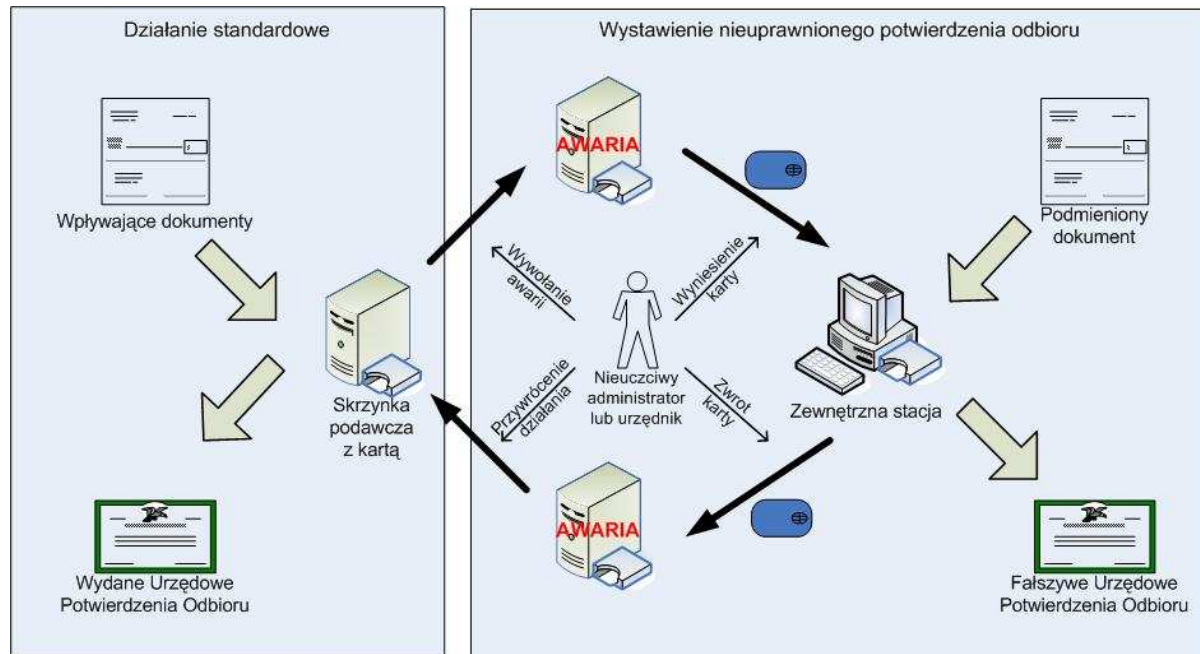
wykonawczych umożliwiających realizację potwierdzeń w sposób automatyczny z pominięciem przepisów ustawy.

Wymienione w punktach powyżej warunki dotyczą zapewnienia odpowiedniego poziomu bezpieczeństwa rozumianego jako dostępność skrzynki, integralność przekazywanych i wytwarzanych przez nie dokumentów oraz poufność kluczy podpisujących. W praktyce, zapewnienie odpowiedniego modelu bezpieczeństwa realizuje się z wykorzystaniem zaufanej trzeciej strony – systemu zewnętrznego spełniającego zaawansowane warunki bezpieczeństwa zarówno w zakresie technologicznym jak i organizacyjnym. Takie podejście daje zarówno podmiotom publicznym jak i podmiotom prywatnym możliwość zaufania, że wydawane przez trzecią stronę potwierdzenia gwarantują odpowiedni model bezpieczeństwa.

Pojawiające się w dyskusji interpretacje prawne oraz niechęć urzędów do korzystania z usług outsourcingowych wymagają zbudowania skrzynek podawczych wewnątrz poszczególnych urzędów administracji publicznej. Aby spełniać swoją rolę skrzynki powstające w urzędach powinny zapewnić odpowiedni poziom bezpieczeństwa, a także powinny być zbudowane w taki sposób, aby w postępowaniach dowodowych nie można było podważyć generowanych przez nie poświadczeń. Dlatego zbudowanie i zarządzanie skrzynką podawczą powinno podlegać ścisłym restrykcjom, aby uniemożliwić nadużycia. Najważniejsze dla zapewnienia bezpieczeństwa jest:

- zastosowanie urządzenia, zabezpieczającego klucze do podpisu w sposób uniemożliwiający ich wykorzystanie poza urządzeniem;
- zastosowanie rozwiązania technicznego uniemożliwiającego użycie kluczy poza bezpiecznym środowiskiem – dla przykładu wykorzystanie urządzenia poza środowiskiem skrzynki podawczej;
- zapewnienie wiarygodnego źródła czasu dla oznaczenia czasu w potwierdzeniach;
- wprowadzenie regulacji organizacyjnych i wymuszenie komisyjnej kontroli procesów uruchamiania i modyfikacji środowiska skrzynki podawczej;
- zapewnienie audytu i rozliczalności wszystkich zdarzeń w systemie;
- zabezpieczenie sieciowe i fizyczne urządzeń.

W tym miejscu konieczne jest przedstawienie podstawowych zagrożeń wynikających z zastosowania rozwiązań o niewystarczającym poziomie bezpieczeństwa. Takim zagrożeniem jest możliwość pozyskania danych służących do składania podpisu elektronicznego i wykorzystania ich do wystawienia poświadczeń niezgodnie z prawem. Warto tu zwrócić uwagę, że samo zastosowanie komponentu technicznego do przechowywania kluczy uniemożliwia zwielokrotnienie kopii kluczy, ale nie chroni kluczy przed ich „wypożyczeniem”. Przykładowy sposób ataku, na system wykorzystujący do generacji poświadczeń kartę kryptograficzną prezentuje rysunek 1.



Rysunek 1. Urzędnik posiadający dostęp do systemu Elektronicznej Skrzynki Podawczej wywołuje sztuczną awarię systemu – np. wyłączenie zasilania, lub odłączenie przewodów czytnika kart kryptograficznych. Komponent techniczny (karta kryptograficzna) zostaje tymczasowo umieszczona w stacji, która dokonuje podpisania dokumentów. Po zwrocie karty system jest przywracany do działania.

Atak przeprowadzony w powyższy sposób jest niewykrywalny – ze względu na to, że wykonuje go osoba mająca dostęp do systemu i posiadająca możliwość jego uruchomienia. Zastosowana w takim środowisku karta kryptograficzna mimo posiadanej certyfikacji bezpieczeństwa kluczy sama jest chroniona jedynie pinem, którego zapamiętanie nie stanowi większego problemu.

Karta kryptograficzna jest urządzeniem personalnym – przewidzianym do użytkowania przez indywidualną osobę, która jest jedynym posiadaczem indywidualnego numeru identyfikującego PIN (ang. Personal Identification Number). Zastosowanie modułu kryptograficznego, którego bezpieczeństwo jest oparte o role administratorów, czyli podział obowiązków i sekretów, uniemożliwi wykorzystanie modułu poza bezpiecznym środowiskiem. Dla przykładu celowe jest takie rozdysponowanie sekretów (hasła i kluczy dostępowych) pomiędzy obsługą systemu, aby uruchomienie modułu było możliwie tylko przy udziale przynajmniej trzech z ośmiu osób posiadających uprawnienia do tej operacji. Bezpieczeństwo modułów kryptograficznych spełniających wymagania bezpieczeństwa sekretów i podziału na role ocenia się zgodnie ze standardami FIPS 140-2 poziom 3 i CEN-CWA 14167-2.

W świetle opisanych w niniejszym artykule wymagań bezpieczeństwa, wprowadzone w rozporządzeniu wymagania dotyczące zastosowania modułu HSM o odpowiednim poziomie bezpieczeństwa i umieszczenia systemu w pomieszczeniu chronionym wydaje się niezbędnym minimum. Przytoczony przykład wykorzystania karty poza bezpiecznym środowiskiem jednoznacznie wskazuje na nieadekwatność zastosowania karty kryptograficznej do realizacji zadania skrzynki podawczej.

Poniższa tabela przedstawia podstawowe różnice pomiędzy zastosowaniem karty i HSM w tym środowisku:

Wymaganie	Karta kryptograficzna FIPS 140-2	Moduł HSM FIPS 140-2 Level 3
Realizacja podpisu zgodnie ze standardem PKCS#11	TAK	TAK
Spełnia wymagania FIPS 140-2 Level 3	TAK w odpowiednim środowisku z zastosowaniem autoryzowanej aplikacji	TAK
Rozliczalność	NIE	TAK
Role użytkowników	NIE	TAK
Możliwość wprowadzenia komisijnego zarządzania	NIE	TAK
Trudność wyniesienia poza bezpieczne środowisko	ŁATWO	TRUDNIEJ
Szybkość	Kilkadziesiąt operacji na minutę	Kilka tysięcy operacji na sekundę

Istnieje niebezpieczeństwo, że w procesie dowodowym podważeniu nie będzie podlegał sam podpis złożony pod potwierdzeniem odbioru, ale możliwość jego złożenia poza środowiskiem, tym bardziej, że brak uregulowań organizacyjnych i technicznych w podmiocie publicznym może umożliwić podpisanie poza bezpiecznym środowiskiem. Dodatkowym ważnym aspektem jest niewystarczające określenie przepisów karnych dla nieuprawnionego wykorzystania kluczy prywatnych elektronicznej skrzynki podawczej, ponieważ całość rozwiązania i składane podpisy nie podlegają ustawie o podpisie elektronicznym.

Istotnym zabezpieczeniem dla procesu przyjmowania dokumentów przez Elektroniczną Skrzynkę Podawczą jest dołączenie do potwierdzenia odbioru oznaczenia czasem realizowanego przez zaufaną trzecią stronę. Nie wydaje się dla tego procesu konieczne znakowanie czasem realizowane przez kwalifikowany podmiot świadczący usługi certyfikacyjne, jednak oznaczenie czasem pochodzące od niezależnego podmiotu uniemożliwia sfalszowanie czasu wydania poświadczenia oraz zabezpiecza także informacje umożliwiające weryfikację ważności podpisu elektronicznego pod przyjmowanym dokumentem elektronicznym. Alternatywnym rozwiązaniem mogłoby być rozszerzenie funkcji HSM tak, by używany przy konstruowaniu poświadczenia odbioru czas pochodził z wewnętrznego zegara, którego nie może modyfikować administrator systemu i który jest ustawiany lub kalibrowany przez zewnętrzne źródło czasu urzędowego.

Przyjmowanie dokumentów przez podmioty publiczne powinno być realizowane w sposób bezpieczny dla osoby składającej dokument oraz uniemożliwiający nieuprawnione działanie ze strony urzędnika. W interesie zarówno podmiotów rządowych jak i samorządowych jest wykorzystywanie środków zapewniających odpowiedni poziom bezpieczeństwa komunikacji, ponieważ ewentualne nadużycia mogą skutkować obciążeniem skarbu państwa. Ważnym krokiem naprzód jest budowa przez Ministerstwo Spraw Wewnętrznych i Administracji systemu Elektronicznej Platformy Usług Administracji Publicznej (ePUAP), który będzie systemem pośredniczącym w komunikacji pomiędzy firmą i obywatelem a administracją. W ramach tego systemu będą świadczone usługi Elektronicznej Skrzynki Podawczej zarówno w procedurze wnoszenia pism jak i doręczeń.

---

Autorem niniejszego artykułu jest Michał Tabor - *Absolwent wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego. Ekspert w zakresie systemów PKI, elektronicznej administracji oraz bezpieczeństwa systemów teleinformatycznych. Dyrektor operacyjny Trusted Information Consulting, firmy świadczącej usługi z zakresu zarządzania bezpieczeństwem informacji, podpisu elektronicznego oraz Infrastruktury Klucza Publicznego (PKI).*

**Kontakt:**

Trusted Information Consulting Sp. z o.o.

ul. Domaniewska 41, Budynek Galaxy

02-672 Warszawa

[www.ticons.pl](http://www.ticons.pl)

[ticons@ticons.pl](mailto:ticons@ticons.pl)