Warszawa, 27 czerwca 2005

Opinia Polskiej Izby Informatyki i Telekomunikacji
w sprawie projektu Rozporządzenia Ministerstwa Finansów dotyczącego elektronicznej faktury ze szczególnym uwzględnieniem problemu masowego podpisywania za pomocą bezpiecznego podpisu elektronicznego

Stanowisko zostało opracowane na podstawie opinii ekspertów:

- **Dr inż. Elżbiety Andrukiewicz** - Wiceprzewodnicząca KT nr 182 ds. Ochrony Informacji w Sieciach Teleinformatycznych przy Polskim Komitecie Normalizacyjnym, Ekspert normalizacyjny ISO,
- **Prof. Mirosława Kutyłowskiego**, Inst. Matematyki i Informatyki, Politechnika Wrocławska

Zgodnie z art. 3 pkt 1 projektu rozporządzenia z 12.04.2005 e-faktury maja być podpisywane bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. W istocie, w cytowanym przepisie Projektu jest mowa o 'bezpiecznym podpisie elektronicznym, weryfikowanym przy pomocy kwalifikowanego certyfikatu".

Ta szczególna forma podpisu elektronicznego odnosi się do równoważności formy pisemnej i formy elektronicznej pod względem skutków prawnych. Zgodnie z art. 5.2 Ustawy o podpisie elektronicznym:

2. Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi [...]

Od faktury nie wymaga się zachowania formy pisemnej (zob. art. 8.1 Rozporządzenia MF z 25.05.2005 Dz.U.95 poz. 798), na jakiej podstawie zatem faktura w postaci elektronicznej ma ją zachowywać?

1. Dyrektywa Rady 115/2001 wprowadzająca fakturę realizowaną za pośrednictwem środków elektronicznych w art. 2(c) wymaga, aby "była zagwarantowana autentyczność źródła pochodzenia i integralność treści [faktury]) przez zastosowanie: "zaawansowanego podpisu elektronicznego w rozumieniu art. 2 ust. 2 dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram dla podpisów elektronicznych; jednakże Państwa Członkowskie mogą zażądać, by zaawansowany podpis elektroniczny był oparty na certyfikacie kwalifikowanym i złożony przy użyciu bezpiecznego urządzenia do składania podpisów w rozumieniu art. 2 ust. 6 i 10 wymienionej dyrektywy". Państwa członkowskie w olbrzymiej większości nie żądają zachowania formy pisemnej dla faktury elektronicznej, pozostając przy funkcjonalnej definicji "zaawansowanego podpisu elektronicznego" (zob. załącznik A).
2. Zwraca szczególną uwagę błąd oficjalnego tłumaczenia Dyrektywy Rady 115/2001 dotyczący pojęcia "zaawansowany podpis elektroniczny (*advanced electronic signature*)" (w rozumieniu Dyrektywy 93/99/WE art. 2 pkt 2) i zastąpienie go terminem "bezpieczny podpis elektroniczny" w rozumieniu Ustawy o podpisie elektronicznym art. 3 pkt. 2. To nie są równoważne pojęcia , co skutkuje błędnym wdrożeniem Dyrektywy 93/99/WE w projektowanym rozporządzeniu. W ten sposób problem uznawania faktur, które byłyby wystawiane przez polskich przedsiębiorców

partnerom z UE. Rozważania na temat błędnego utożsamiania instytucji zaawansowanego podpisu z dyrektywy o podpisie elektronicznym z bezpiecznym podpisem w polskiej ustawie zawarte są w ekspertyzie dr E. Andrukiewicz stanowiącym załącznik A do niniejszej opinii.

3. Upowszechniany w ostatnim czasie tekst "Techniczna realizacja masowego bezpiecznego podpisu elektronicznego" m.in. na łamach Gazety Prawnej, którego autorzy próbują przekonywać, że bezpieczny podpis elektroniczny może być wykorzystywany do masowego podpisywania dokumentów elektronicznych jest pełen błędów prawnych, normalizacyjnych i technicznych. PIIT uważa ,że jest to niemożliwe ze względów prawnych jak i może być bardzo trudne technologicznie. Szczegółowe odniesienie do stosownych zapisów tego dokumentu zostały przedstawione w załączonej ekspertyzie prof. Mirosława Kutyłowskiego (załącznik B). Jest to naszym zdaniem przykład naginania przepisów ustawy o podpisie elektronicznym po to tylko, aby uzasadnić zastosowanie konstrukcji stanowiącej błędne wdrożenie Dyrektywy (W ministerstwie Gospodarki Pracy u Spraw Socjalnych zostały zainicjowane prace nad nowelizacja Ustawy) służy tylko interesom kilku firm, ze szkodą dla interesu całej polskiej gospodarki .
4. W przyjętej , przez Sejm RP w ostatnim czasie, ustawie o zmianie ordynacji podatkowej, autor – Ministerstwo finansów, dopuszcza stosowanie niektórych rodzajów zwykłego podpisu elektronicznego do składania e-deklaracji. Zupełnie niezrozumiałym jest dlaczego te podpisy nie mogą być używane do wystawiania e-faktur ? Tym bardziej ,że zarówno dyrektywa o podpisie elektronicznym z 1999 r. jak i polska ustawa wyraźnie stanowią, iż podpisowi takiemu nie można odmówić mocy dowodowej (skutków prawnych).
5. PIIT , zgodnie ze stanowiskiem wyrażonym w Opinii PIIT z dnia 27.04.2005 r. ponownie opowiada się za stosowaniem do wystawiania e-faktur nowoczesnych technologii opartych o PKI które gwarantują integralność i autentyczność ich pochodzenia. Postulujemy zatem aby katalog tych rozwiązań, poza bezpiecznym podpisem elektronicznym, który powinien być jednym z dopuszczonych rozwiązań ale nie jedynym, został wzbogacony w rozporządzeniu Ministra Finansów o niektóre rodzaje zwykłego podpisu elektronicznego a zwłaszcza o instytucje które mogą mieć zastosowanie do masowego wystawiania e-faktur takie jak stemplowanie czasem.

Załącznik A

Dr Elżbieta Andrukiewicz

Zaawansowany podpis elektroniczny a bezpieczny podpis elektroniczny

W celu podniesienia bezpieczeństwa podpisu elektronicznego w Dyrektywie opisano dodatkowe jego właściwości, definiując nową kategorię podpisu. Zgodnie z art. 2 pkt 2) „zaawansowany podpis elektroniczny" oznacza podpis elektroniczny spełniający następujące wymogi:

a) przyporządkowany jest wyłącznie podpisującemu;
b) umożliwia ustalenie tożsamości podpisującego;
c) stworzony jest za pomocą środków, które podpisujący **może** mieć pod swoją wyłączną kontrolą; i
d) jest tak powiązany z danymi, do których się odnosi, że każda późniejsza zmiana danych jest wykrywalna;

Z punktu widzenia praktycznych zastosowań zaawansowany podpis elektroniczny jest bardzo użyteczną konstrukcją pozwalającą na swobodny rozwój nowych usług elektronicznych opartych na tożsamości komunikujących się stron (podpisujących), w tym także (ale nie tylko!) osób fizycznych i szeroko stosowaną w unijnych rozwiązaniach prawnych. Zaawansowany podpis elektroniczny umożliwia wykorzystanie **funkcjonalności** podpisu dla zapewnienia bezpieczeństwa komunikacji, bez dodatkowych rygorów związania tego podpisu z formą pisemną.

Koncepcja bezpiecznego podpisu elektronicznego w polskiej Ustawie

W Ustawie wprowadzono nowe pojęcie – tzw. bezpiecznego podpisu elektronicznego - podpisu elektronicznego, który:

a) jest przyporządkowany wyłącznie do osoby składającej ten podpis,
b) jest sporządzany za pomocą podlegających wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego,
c) jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna,

W koncepcji bezpiecznego podpisu elektronicznego istnieje kilka poważnych problemów o charakterze merytorycznym.

a. Ustawa **rozszerza w zupełnie nieuzasadniony sposób definicję zaawansowanego podpisu elektronicznego**, uzupełniając definicję funkcjonalną o warunek zrealizowania funkcji podpisu za pomocą bezpiecznego urządzenia. Sęk w tym, że po złożeniu podpisu jest to warunek nieweryfikowalny (żadne urządzenie weryfikujące nie może tego sprawdzić, ponieważ w sensie funkcjonalnym może rozpoznać jedynie zaawansowany podpis elektroniczny). Zatem nie ma równoważności między terminami 'zaawansowany' i 'bezpieczny', Ustawodawca poradził sobie z tym problem w sposób kuriozalny. Z definicji założył (art. 6 ust. 3 Ustawy), że jeśli podpis jest weryfikowany za pomocą ważnego certyfikatu kwalifikowanego, to

domniemywa się, że do jego złożenia wykorzystano bezpieczne urządzenie, co po pierwsze, jest przejawem myślenia życzeniowego a po drugie, jest złamaniem fundamentalnych zasad przyjętych w prawie cywilnym, pozbawiając ochrony prawnej osobę podpisującą (w przypadku, gdyby z jakichś przyczyn chciała jednak podpisany dokument elektroniczny zakwestionować).

b. Pominięto istotną cechę definicji 'zaawansowanego podpisu elektronicznego' – punkt b) definicji Dyrektywy, oznaczający, że w mechanizmie podpisu są już zawarte funkcje, które potrafią doprowadzić do identyfikacji podpisującego (np. za pomocą certyfikatu). Tego warunku nie ma w definicji 'bezpiecznego podpisu elektronicznego'.

c. Na odmienność koncepcji tzw. bezpiecznego podpisu elektronicznego i zaawansowanego podpisu elektronicznego zwrócili także uwagę eksperci unijni[1] Pierwsi z nich uznali ja wręcz za błędne wdrożenie, drudzy – za wprowadzenie wymagań ponad poziom zaawansowanego podpisu elektronicznego określonego w Dyrektywie.

Niepoprawna z normalizacyjnego punktu widzenia (opisuje nie tylko funkcjonalność, ale wskazuje też sposób wdrożenia) i zbyt restrykcyjna definicja 'bezpiecznego podpisu' praktycznie uniemożliwia zastosowanie wystarczająco bezpiecznej formy 'zaawansowanego podpisu elektronicznego' tam, gdzie zachowanie formy pisemnej w odniesieniu do dokumentu elektronicznego nie jest konieczne (np. e-faktura). Niezgodność pojęć stosowanych w Ustawie i Dyrektywie może spowodować problem interpretacyjny w przypadku zastosowania zaawansowanego podpisu rozpoznawanego przez systemy prawne części Krajów Członkowskich, ponieważ to pojęcie w polskim prawie nie występuje. Warto zaznaczyć, że od strony technicznej realizacja bezpiecznego podpisu jest znacznie trudniejsza niż zestaw 'zaawansowany podpis' + 'bezpieczne urządzenie' (w definicji unijnej, która też jest odmienna niż w polskiej Ustawie), a to oznacza trudniejsze warunki dla polskich dostawców produktów związanych z podpisem elektronicznym.

[1] *The Implementation of Directive 1999/93/EC on Electronic Signatures Preliminary check of Polish implementation, July 2003* by Prof. Dr. Brigitta Lurger, LL.M., University of Salzburg and Dr. Hans Peter Lehofer, Austrian Communications Authority (raport sporządzony na zlecenie UOKiK) str 2 oraz *Legal and market aspects of the application of Directive 99/93/EC and practical applications of electronic signatures in Member States, the EEA, the Candidate and Accession countries* – Study for the European Commission (October 2003) str. 73

Załącznik B

Komentarz dotyczący dokumentu pt. "Techniczna realizacja masowego bezpiecznego podpisu elektronicznego"

Uwagi do stanowiska UNIZETO na temat *wielokrotnego składania podpisu elektronicznego w trakcie jednej sesji*

Autor: prof. Mirosław Kutyłowski, Inst. Matematyki i Informatyki, Politechnika Wrocławska
Data: 26.06.2005
Przeznaczenie dokumentu: materiał dla ekspertów PIIT i PTI, oraz MG
Omawiany materiał: plik autorstwa (wg cech dokumentu) dr J. Pejasia (UNIZETO) i R. Podpłońskiego (KIR)

1.1 ad 2. prawna dopuszczalność wielokrotnego składania bezpiecznego podpisu elektronicznego w czasie jednej sesji

Autorzy stawiają tezę, że *Ustawa o podpisie elektronicznym, towarzyszące jej rozporządzenia, a także normy i standardy nie tylko nie ograniczają, lecz wręcz sprzyjają wykorzystaniu bezpiecznego podpisu elektronicznego do uwierzytelniania dokumentów w sposób masowy.* Przytaczanych jest kilka argumentów:

- Podpisywany dokument może być przedstawiony podpisującemu, ale nie musi. Zgoda – ale wyklucza to automatyczne wystawianie faktury np. po przesłaniu zamówienia towaru on-line i przesłaniu płatności elektronicznie. Po stronie wystawiającej fakturę musi siedzieć osoba, która ewentualnie może zrezygnować z obejrzenia wystawianej faktury.
- *Innym istotnym wymogiem bezpieczeństwa składania podpisu elektronicznego – zgodnie z art. 18 ust. 1 pkt 2 ustawy – jest zachowanie zasady „co jest prezentowane jest podpisywane ... ”* - cały ten długi akapit jest nie na temat.
- Autor odnosi się do Rozporządzenia RM 1094 i cytuje: *„ułatwienia ograniczające liczbę czynności, jakie musi wykonać podpisujący lub poświadczający przy składaniu pojedynczego bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego, muszą być ograniczone czasem ich trwania lub liczbą składanych bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych.”*. Postanowienia tego typu mają być jedynie uszczegółowieniem ustawy i nie mogą jej naruszać. O ile istotnie można jednorazowo uwierzytelnić się wobec karty (PIN itp.) dla złożenia wielu podpisów, **to decydujące w aspekcie praktycznym znaczenie ma tutaj brzmienie art. 18, ust. 1 Ustawy o podpisie elektronicznym:**

  Art. 18.
  1. Bezpieczne urządzenie służące do składania podpisu elektronicznego powinno co najmniej:
  1)...,
  2)...,

3) gwarantować, że złożenie podpisu będzie poprzedzone wyraźnym ostrzeżeniem, że kontynuacja operacji będzie równoznaczna ***ze złożeniem podpisu elektronicznego****,*

Ustawodawca użył tu sformułowania „***ze złożeniem podpisu elektronicznego***" a nie ***„ze złożeniem podpisów elektronicznych".*** Sformułowanie to świadczy jednoznacznie, że ze względów bezpieczeństwa każdorazowe złożenie podpisu elektronicznego wymaga ukazania się odpowiedniego komunikatu i reakcji podpisującego realizującej prawną funkcję finalizacyjną. Podejście to mieści się doskonale w regułach dotyczących składania oświadczeń woli.

Wspomniane wyżej brzmienie art. 18.1 wyklucza pod względem prawnym złożenie pojedynczego podpisu ostrzeżenia i bez akceptacji podpisującego. W praktyce oznacza to, że podpisujący będzie musiał dokonać pewnej czynności akceptującej dla każdego podpisu z osobna.

1.2 Ad 3: Techniczna realizowalność wielokrotnego składania bezpiecznego podpisu elektronicznego w czasie jednej sesji

Autorzy omawiają szeroko wymagania dotyczące bezpiecznego urządzenia do składania podpisu elektronicznego (większość tekstu jest nie na temat). Autorzy przyznają, że „*Definicja ta jest szersza niż w Dyrektywie Europejskiej*" oraz że „*W polskim dokumencie jest postawiony ostrzejszy warunek, ale dotyczy to szczególnie wrażliwego elementu systemu*". Oznacza to między innymi, że urządzenia uznane w innych krajach UE za „secure signature device" nie mogą być automatycznie uznane za bezpieczne urządzenia do składania podpisu elektronicznego.

Proponowane są dwie realizacje techniczne:

1. Karta kryptograficzna
2. HSM

Ad 1. karta kryptograficzna

Nie ma oczywiście problemu z budową odpowiedniego oprogramowania, które pozwoli na ładowanie do karty wielu wartości w celu podpisania. Mogą się jednak pojawić problemy natury technicznej:

- Automat stanowy karty kryptograficznej może nie dopuszczać składania wielu podpisów. Co więcej ingerencja w system operacyjny karty może być nawet technicznie niemożliwa, gdyż automat stanowy może być zapisany w pamięci ROM. Ze względów bezpieczeństwa automat ten nawet powinien być tam zapisany.
- Karta nie posiada własnego zegara. Zatem nie jest technicznie możliwe ograniczenie czasu składania podpisów, tak jak to sobie autorzy wyobrażają.
- Zarówno system operacyjny jak i inne składniki karty mogą być tajemnicą producenta. Z tego względu jakiekolwiek modyfikacje mogą być również niemożliwe ze względów na konieczność łamania prawa.

Znacznie poważniejsze problemy kryją się jednak w warstwie hardware'owej:

- Karty są urządzeniami o stosunkowo niskiej trwałości. Nasze praktyczne doświadczenia z kartami wiodących producentów (GEMPLUS, Schlumberger) wskazują na niską żywotność kart w warunkach silnego użytkowania (przez studentów w trakcie prac programistycznych). Znaczący procent kart nie przeżywa jednego semestru zajęć, mimo że intensywność użytkowania znacznie odbiega od tej, o jakiej mówią autorzy (jakkolwiek jest też dużo wyższa od tej zakładanej w normalnym użytkowaniu przez osobę fizyczną - kilka, kilkadziesiąt operacji dziennie).
- O ile system operacyjny w trakcie operacji składania podpisu wykorzystuje pamięć typu EEPROM, to narażamy się na niebezpieczeństwo szybkiego zużycia karty. Pamięć tego typu ma bowiem ograniczoną liczbę zapisów i proces zużywania się pamięci ma charakter nieuchronny.

Konkluzja: przydatność karty kryptograficznej w wersji dostępnej na rynku do operacji masowych stoi pod znakiem zapytania. Przed „skazaniem się" na rozwiązanie tego typu poprzez regulacje prawne należałoby przeprowadzić niezależne badania laboratoryjne dostępnych na rynku kart celem wyjaśnienia, czy karty te gwarantują odpowiednią trwałość. Wstępne doświadczenia mówią, że nie.

Ad 2: HSM

Cena

Żaden z podmiotów, w tym UNIZETO i KIR nie wymieniają zresztą HSM jako bezpiecznego urządzenia do składania podpisu elektronicznego (na mocy prawa mają obowiązek informowania o pełnej liście takich urządzeń).