Uznawanie podpisów elektronicznych w krajach Unii Europejskiej

inż. ŁUKASZ STROIŃSKI, Instytut Maszyn Matematycznych, Warszawa
mgr inż. BARTOSZ NAKIELSKI, Narodowy Bank Polski, Warszawa
mgr MARCIN FIJAŁKOWSKI, Ministerstwo Gospodarki, Warszawa

Stopniowe rozpowszechnianie podpisu elektronicznego na terenie Unii Europejskiej powoduje, że kwestia wzajemnego akceptowania podpisów złożonych w różnych krajach nabiera istotnego znaczenia. Dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 roku w sprawie wspólnotowych ram w zakresie podpisu elektronicznego posługuje się co do zasady pojęciem certyfikatów kwalifikowanych bez względu na kraj ich wystawienia. Wyjątek stanowią przepisy dotyczące uznawania certyfikatów z tzw. krajów trzecich, czyli spoza Unii Europejskiej lub Europejskiego Obszaru Gospodarczego. W związku z tym art. 5.1 dyrektywy regulujący zrównanie w skutkach z podpisem własnoręcznym obliguje państwa członkowskie również do akceptowania podpisów z certyfikatem kwalifikowanym z innych państw członkowskich UE oraz EOG.

Zapisy artykułów 3 i 4 dyrektywy zobowiązują państwa członkowskie Unii Europejskiej do zapewnienia transgranicznych mechanizmów, umożliwiających akceptowanie certyfikatów elektronicznych wystawionych przez różne centra certyfikacji pomiędzy administracjami państw członkowskich, jak i również pomiędzy administracjami i obywatelami oraz podmiotami gospodarczymi. Państwa członkowskie mogą poddać zastosowanie podpisu elektronicznego w sektorze publicznym ewentualnym wymaganiom dodatkowym. Wymagania muszą być obiektywne, transparentne oraz proporcjonalne i niedyskryminujące, a także mogą odnosić się jedynie do specyficznych cech danych zastosowań. Dyrektywa stwierdza jednak wyraźnie, że wymagania te nie mogą stanowić przeszkód w ponadgranicznych usługach dla obywatela.

O ile dyrektywa nakazuje państwom członkowskim publikację informacji o działających urzędach wydających certyfikaty kwalifikowane, to nie precyzuje w jaki sposób ma to być robione. Większość krajów publikuje te informacje na stronach internetowych – jednak często są to strony jedynie w oficjalnym języku danego kraju. Nie istnieje europejski root centralny, albo rejestr kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie podpisu elektronicznego. Niepełne i nie zawsze aktualne informacje o urzędach nadzoru, systemach akredytacji i podmiotach kwalifikowanych publikowane są na stronach Unii Europejskiej [1]. Różnice językowe na poziomie aplikacji, stron internetowych i polityk certyfikacji sprawiają, że weryfikacja podpisu elektronicznego pochodzącego z innego kraju jest procesem trudnym i czasochłonnym (a czasem praktycznie niemożliwym, gdy podmiot nie publikuje w łatwy sposób klucza publicznego służącego do weryfikacji ścieżki certyfikacji). Sprawę jeszcze bardziej utrudnia fakt, iż w Europie funkcjonuje około 100 urzędów certyfikacji wydających certyfikaty kwalifikowane (w Polsce jest ich obecnie 5).

Lista TSL

Ważnym narzędziem wychodzącym na przeciw problemowi akceptacji zagranicznych podpisów z certyfikatem kwalifikowanym jest, wprowadzona Decyzją 2009/767/EC, lista TSL (*ang. Trusted Services Status List*), zwana listą usług zaufanych. Lista ta pozwala m.in. odpowiedzieć na pytanie, które podmioty są kwalifikowane lub akredytowane w danym kraju oraz jakie usługi otoczenia podpisu elektronicznego podlegają nadzorowi. Europejski Instytut Standardów Telekomunikacyjnych ETSI opracował specyfikację umożliwiającą tworzenie i zarządzanie listami usług zaufanych. Szczegółowe informacje techniczne odnośnie list TSL można znaleźć w normie ETSI TS 102 231. Listy w tym standardzie mogą być tworzone zarówno w ramach europejskiego systemu list TSL, jak i poza tym systemem. Nie ma przeszkód, aby standard ETSI był wykorzystany przez przedsiębiorstwa lub instytucje do tworzenia własnych list zaufania obejmujących centra certyfikacji inne niż kwalifikowane oraz odmienne rodzaje zaufanych usług.

Potrzeba wdrożenia list TSL w naszym kraju bierze się z faktu, iż istnieją systemy administracji publicznej oraz podmiotów gospodarczych, które służą walidacji serwerowej oraz przygotowane jeszcze przed powstaniem europejskiego systemu list TSL aplikacje weryfikujące. W praktyce akceptacji certyfikatów z zagranicy można napotkać na wiele trudności, zwłaszcza jeśli chodzi o określenie poziomu zaufania lub dostępności list CRL (*Certyficate Revocation List*). Lista TSL obejmuje zagadnienia związane nie tylko z usługami certyfikacyjnymi, ale i szeroko rozumianymi usługami zaufania stanowiącymi otoczenie podpisu elektronicznego w danym państwie członkowskim. Pojęcie usług zaufania rozumiane jest szerzej niż usługi certyfikacyjne, ale jest ściśle związane z usługami otoczenia podpisu elektronicznego.

Lista TSL stanowi wiarygodne i aktualne źródło informacji na temat statusu nadzoru lub akredytacji usług certyfikacyjnych (np. wydawania certyfikatów kwalifikowanych), które są nadzorowane lub akredytowane przez państwa członkowskie Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego zgodnie z przepisami dyrektywy 1999/93/WE. Jest ona dostępna w języku angielskim i ma identyczną strukturę dla wszystkich krajów obowiązanych do stosowania dyrektywy oraz zawiera certyfikaty potrzebne do weryfikacji ścieżki (w przypadku weryfikacji certyfikatu znacznie ważniejszy od nazwy urzędu jest jego klucz publiczny). Dzięki temu, lista TSL pozwala ustalić czy dany certyfikat jest rzeczywiście wydany przez wymieniony podmiot świadczący usługi certyfikacyjne, czy wystawca tego certyfikatu może wydawać certyfikaty kwalifikowane oraz, czy weryfikowany tym certyfikatem

podpis został złożony przy użyciu bezpiecznego urządzenia do składania podpisu elektronicznego. W teorii dane zawarte w certyfikacie powinny umożliwiać sprawdzenie, czy certyfikat jest rzeczywiście certyfikatem kwalifikowanym i czy został on złożony za pomocą bezpiecznego urządzenia. Jednak ze względu na występowanie krajowych modalności związanych z wydawaniem certyfikatów oraz semantyką certyfikatów kwalifikowanych w poszczególnych krajach członkowskich, informacje zawarte w samym certyfikacie sygnatariusza nie zawsze okazują się wystarczające do przeprowadzenia takiej operacji. Listy TSL stanowią ważne subsydiarne źródło informacji, chociaż nie można wykluczyć wystąpienia sytuacji atypowych, których obsłużenie może nie być możliwe przez mechanizmy automatycznej walidacji.

Listy TSL dostarczają danych na temat zaufanej usługi i umożliwiają zainteresowanym stronom określenie czasu, w którym zaufana usługa podlegała nadzorowi lub akredytacji w danym kraju członkowskim. Listy TSL zawierają także informacje historyczne takie, jak czas zatwierdzenia, zawieszenia, anulowania lub odwołania zaufanej usługi. Pod pojęciem utrzymywania listy rozumiany jest proces aktualizacji listy tak, aby odzwierciedlała ona aktualny stan nadzoru lub akredytacji usług certyfikacyjnych.

Zaufana lista publikowana przez państwo członkowskie musi zawierać co najmniej informacje o nadzorowanych lub akredytowanych podmiotach świadczących usługi certyfikacyjne, które wydają certyfikaty kwalifikowane zgodnie z zapisami dyrektywy 1999/93/WE. Umieszczenie na krajowej zaufanej liście dodatkowych informacji o innych nadzorowanych lub akredytowanych podmiotach świadczących usługi certyfikacyjne i niewydające certyfikatów kwalifikowanych, ale świadczących usługi związane z podpisem elektronicznym (znakowanie czasem, podmioty wydające certyfikaty niekwalifikowane) jest dobrowolne i zależy od państwa członkowskiego.

Zgodnie z Decyzją 2009/767/EC każdy kraj ma obowiązek publikować listę w formacie czytelnym dla człowieka (w postaci pliku PDF). Od dnia 1 grudnia 2010 roku obowiązkowa będzie publikacja listy w formie czytelnej maszynowo (XML). Dodatkowo, w celu zwiększenia bezpieczeństwa, każdy kraj będzie musiał podpisywać publikowaną listę (obecnie nie jest to wymagane). W Polsce za publikacje list TSL odpowiedzialny jest Narodowy Bank Polski.

Ponieważ każdy kraj publikuje własną listę TSL, Komisja Europejska prowadzi centralną listę (zwaną „listą list") zawierającą linki do list krajowych. Dodatkowo każda lista krajowa zawiera link do „listy list" – dzięki temu posiadając np. polską listę TSL bardzo szybko można uzyskać dostęp do każdej innej listy. Od 1 grudnia 2010 r. na europejskiej liście list znajdą się certyfikaty służące do weryfikacji podpisów złożonych pod krajowymi listami TSL.

Zasady publikacji list TSL

Operatorzy odpowiedzialni za publikację list TSL w większości przypadków udostępniają listy TSL na serwerze WWW lub katalogu sieciowym. Mechanizmy wbudowane w protokoły takie, jak: LDAP (*Lightweight Directory Access Protocol*), http oraz ftp oferują metody certyfikacji i dystrybucji list TSL. Dostawca repozytoriów musi zapewnić dostęp do listy TSL przynajmniej za pomocą protokołu http, dodatkowo może umożliwiać dostęp za pomocą protokołu ftp, bądź LDAP.

Aby zminimalizować możliwości ataku, wskazane jest użycie bezpiecznego kanału opartego na mechanizmach TLS (ang. *Transport Layer Security*), gdyż wówczas nie są wymagane żadne dodatkowe funkcjonalności zapewniające bezpieczeństwo. Aplikacje przetwarzające listy TSL, muszą wspierać mechanizmy bezpiecznego kanału TLS poprzez protokół http.

Listy TSL mają na celu:

- Dostarczenie wiarygodnych informacji na temat statusu nadzoru lub akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne, które są nadzorowane lub akredytowane w danym kraju zgodnie z dyrektywą 1999/93/WE oraz krajowymi przepisami w tym zakresie.
- Usprawnienie walidacji podpisów elektronicznych, które wykorzystują wymienione nadzorowane lub akredytowane usługi certyfikacyjne świadczone przez podmioty wymienione na liście podmiotów świadczących usługi certyfikacyjne.

Lista TSL składa się z czterech głównych komponentów, które:

- zawierają informację o operatorze systemu (ang. *scheme operator*),
- wskazują dostawców usług zaufanych funkcjonujących w danym kraju,
- wskazują usługi świadczone przez tych dostawców usług zaufanych i ich aktualny status,
- dla każdej usługi zawierają jej historię.

Jeżeli zachodzi potrzeba, wszystkie części listy z wyjątkiem pierwszej mogą być replikowane.

Zawartość listy TSL:

1. **Informacje o infrastrukturze krajowej**
- Organy nadzoru (akredytacji),
- Przepisy (ewentualnie odnośniki do odpowiednich stron internetowych).

2. **Informacje o urzędach kwalifikowanych**
- Dane adresowe,
- Lista usług.

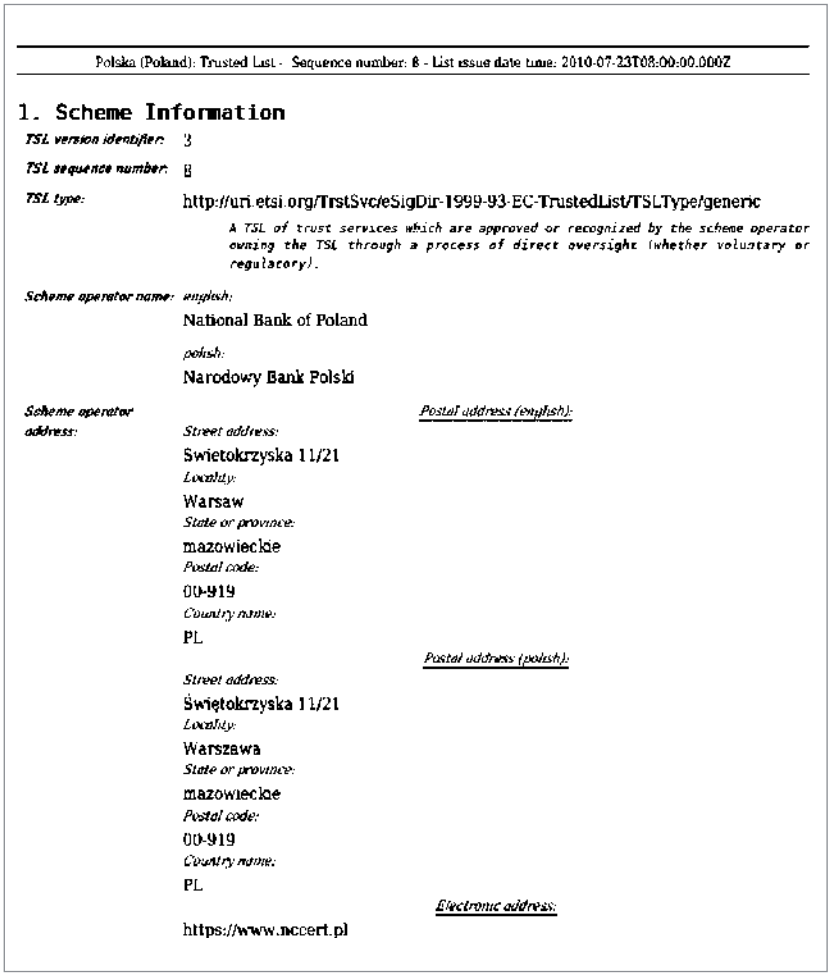
3. **Informacje o usługach**
- Nazwa usługi, jej aktualny status oraz ewentualnie historia,
- Cyfrowy identyfikator usługi (SDI) – certyfikat jednoznacznie identyfikujący daną usługę,
- Informacje dodatkowe.

Uwierzytelnienie listy TSL odbywa się za pomocą weryfikacji klucza, którym ta lista została podpisana oraz sprawdzeniu ważności listy (według stanu na wrzesień 2010 większość list nie jest jeszcze podpisywana; obowiązek podpisywania krajowych list TSL wchodzi w życie od dnia 1 grudnia 2010). Dodatkowym mechanizmem uwierzytelnienia może być uwierzytelnienie po stronie serwera za pomocą mechanizmów TLS. Operator może również opublikować skrót klucza publicznego odpowiadającego kluczowi prywatnemu służącemu do podpisywania list np. w oficjalnym biuletynie.

1. Użytkownik z kraju A podpisuje dokument i przesyła go do aplikacji e-administracji w kraju B.
2. Aplikacja w kraju B łączy się z listą list w celu pobrania listy TSL wystawionej przez kraj A.
3. Aplikacja weryfikuje listę (podpis i ważność), a następnie sprawdza czy urząd, który wystawił certyfikat użytkownikowi podpisującemu, znajduje się na liście TSL (i czy jego status jest „pod nadzorem").

4. W przypadku poprawnej weryfikacji w punkcie 3 następuje weryfikacja podpisu elektronicznego (porównanie skrótu dokumentu z podpisem, weryfikacja CRL).

W przypadku braku obsługi list TSL aplikacja e-administracji w kraju B będzie mogła co najwyżej sprawdzić poprawność podpisu – bez możliwości sprawdzenia autentyczności certyfikatu.



Polska (Poland): Trusted List - Sequence number: 8 - List issue date time: 2010-07-23T08:00:00.000Z

1. Scheme Information

TSL version identifier: 3

TSL sequence number: 8

TSL type: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

A TSL of trust services which are approved or recognized by the scheme operator owning the TSL through a process of direct oversight (whether voluntary or regulatory).

Scheme operator name: english:
National Bank of Poland
polish:
Narodowy Bank Polski

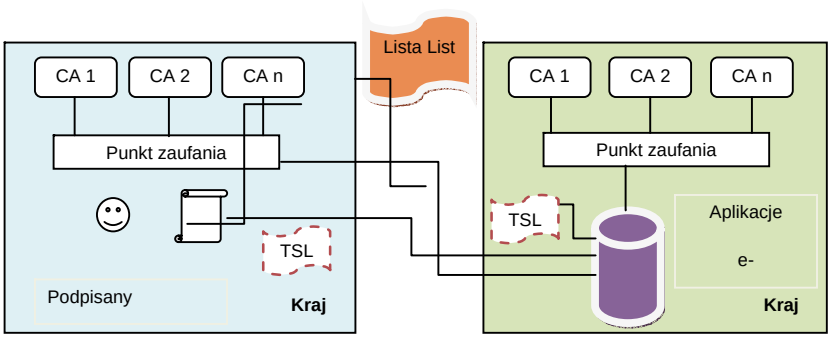
Scheme operator address:

Postal address (english):
Street address:
Swietokrzyska 11/21
Locality:
Warsaw
State or province:
mazowieckie
Postal code:
00-919
Country name:
PL

Postal address (polish):
Street address:
Świętokrzyska 11/21
Locality:
Warszawa
State or province:
mazowieckie
Postal code:
00-919
Country name:
PL

Electronic address:
https://www.nccert.pl

Rys. 1. Fragment polskiej listy TSL w formie czytelnej dla człowieka
Fig. 1. Polish TSL fragment in human readable form



Rys. 2. Weryfikacja podpisu przy użyciu listy TSL
Fig. 2. Signature verification with TSL

Walidacja zagranicznych podpisów w Polsce

Zaczynają się już pojawiać polskie usługi walidacji zagranicznych podpisów. Unizeto Technologies wdraża obsługę list TSL według najnowszych standardów DVCS (ang. *Data Validation And Certification Service*) pod nazwą WebNotarius. Usługa jest bezpłatna dla celów niekomercyjnych, czyli np. dla obywateli dostających pisma z urzędów. Chcąc korzystać z WebNotariusa w celach komercyjnych, w tym dla potrzeb serwerowej walidacji podpisu elektronicznego, trzeba wykupić licencję zależną od liczby przetwarzanych dokumentów. Obecnie usługę obsługują weryfikacje certyfikatów z 88 centrów certyfikacji (wraz z serwerami znakowania czasem). Wspierane formaty podpisu to: PKCS7 – basic, CMS, XML signature, PDF signature, XADES, CADES, SDOC, Sign Pro Sigillum CA, ZEP (słowacki), Multi Signature.

Do weryfikacji podpisów z krajów Unii Europejskiej jest przygotowana Elektroniczna Platforma Usług Administracji Publicznej (ePUAP). Funkcjonalność ta jest zaimplementowana, przetestowana i zgodna ze wytycznymi Komisji Europejskiej, lecz na razie ukryta przed użytkownikami. Teoretycznie ePUAP weryfikuje wszystkie urzędy wydające kwalifikowane certyfikaty, które znajdują się na „liście list" TSL, jednak z powodu braku testów na podpisanych dokumentach z innych państw, nie można tego z całą pewnością stwierdzić. Weryfikacja transgranicznego podpisu dla końcowego odbiorcy będzie bezpłatna. Wspierane są formaty bezpiecznego podpisu elektronicznego w formacie XML: XMLDSIG, XAdES, XadES-BES oraz formaty bezpiecznego podopisu w dokumentach PDF (PAdES).

Literatura

[1] http://ec.europa.eu/information_society/policy/esignature/eu_legislation/notification/index_en.htm
[2] ETSI 102 231 – Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information
[3] https://www.nccert.pl/tsl/PL_TSL.pdf
[4] https://www.nccert.pl/tsl/PL_TSL.xml
[5] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:299:0018:0054:EN:PDF
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:13:24:31999L0093:PL:PDF
[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:0035:EN:PDF
[8] http://ec.europa.eu/information_society/policy/esignature/docs/crobies_deliverables/crobiesd2.1.pdf