Rozporządzenie eIDAS – na pograniczu technologii i prawa

mgr inż. DANIEL WACHNIK, Instytut Maszyn Matematycznych, Warszawa

W wyniku prac regulujących obszar podpisu elektronicznego została wydana Dyrektywa 1999/93/WE dotycząca wspólnotowych ram podpisu elektronicznego [1]. W trakcie 10-ciu lat obowiązywania Dyrektywy nie odnotowano oczekiwanego nasycenia rynku podpisów elektronicznych. W roku 2008 Komisja Europejska zaadoptowała plan działań w zakresie e-podpisu i e-identyfikacji, który zaowocował między innymi wytworzeniem raportów CROBIES [2]. Raporty CROBIES stanowiły istotny wkład przy określeniu zakresu mandatu standaryzacyjnego M/460, wydanego w 2009 roku przez Komisję Europejską. Mandat ten miał na celu uporządkowanie standardów związanych z szeroko pojętymi usługami zaufania.

Rys. 1. Przebieg prac nad Regulacja eIDAS
Fig. 1. eIDAS workflow

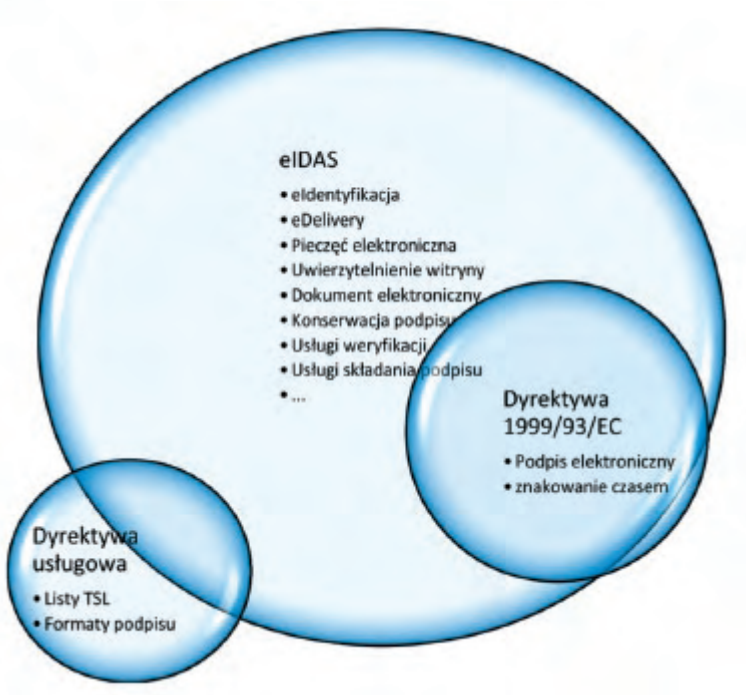
Początkowo, rozważano zastosowano możliwość nowelizacji Dyrektywy 1999/93/EC, jednak w na podstawie analiz postanowiono, że najkorzystniejszym aktem prawnym, z punktu widzenia harmonizacji usług jest Rozporządzenie unijne. Draft rozporządzenia został opublikowany przez Komisję Europejską w dniu 04.06.2012 roku [3], a sam fakt publikacji został po raz pierwszy ogłoszony publicznie w Polsce, w trakcie konferencji EFPE.

Warto nadmienić, że Rozporządzenie Unii Europejskiej jest aktem prawnym zasadniczo różniącym się od Dyrektywy. O ile Dyrektywa jest implementowana przez kraje członkowskie w prawie krajowym, o tyle Rozporządzenie nie pozostawia tego rodzaju swobody. Rozporządzenie jest stosowane bezpośrednio. Zastosowanie tego rodzaju aktu oznacza z jednej strony brak rozbieżności na poziomie krajów członkowskich, ale oznacza także, że państwa członkowskie nie mają możliwości korygowania tych przepisów, które z ich punk-tu widzenia są uciążliwe. Przykładowo, jeśli zapisy rozporządzenia będą wykluczać możliwość zastosowania w kontaktach z administracją publiczną określonego rodzaju mechanizmu, nie będzie można stosować tego mechanizmu, bez względu na fakt jakie koszty z tego powodu będzie musiało ponieść państwo członkowskie.

W trakcie dotychczasowych prac legislacyjnych, państwa członkowskie zgłaszały uwagi do poszczególnych sekcji projektu Rozporządzenia. Obowiązkiem państwa przewodniczącego Unii Europejskiej (Prezydencji) jest nanoszenie komentarzy i proponowanie wspólnie z Komisją Europejską kolejnych wersji Rozporządzenia. Równolegle prowadzone są prace w Parlamencie Europejskim nad tekstem Rozporządzenia.

Zakres merytoryczny rozporządzenia i jego ewolucja

Zakres merytoryczny rozporządzenia został poszerzony w stosunku do Dyrektywy 1999/93/EC (*rys. 2*). O ile reguluje ona wyłącznie materię podpisów elektronicznych, o tyle Regulacja eIDAS wprowadza szereg usług zaufanych, oraz elektroniczną identyfikację. Rozporządzenie oprócz dobrze zdefiniowanych rodzajów usług zaufania takich jak podpis elektroniczny, znakowanie czasem i usługi związane z wydawaniem certyfikatów, definiuje także szereg nowych usług:



Rys. 2. Porównanie zakresu merytorycznego eIDAS i aktów prawnych z zakresu podpisu elektronicznego
Fig. 2. Comparison between eIDAS and electronic signature law

Usługa	Opis	Uwagi
Pieczęć elektroniczna	Odpowiednik podpisu elektronicznego osoby prawnej (Ang. „legal person". Jednym z zagadnień podnoszonych między innymi przez stronę polską jest fakt istnienia jednostek nieposiadających osobowości prawnej, które są pomijane przez sformułowanie „legal person".)	Wykorzystuje narzędzia analogiczne do podpisu elektronicznego. Część wymagań dla podpisu elektronicznego jest stosowana „mutatis mutandis" (Łac. „po dokonaniu niezbędnych zmian; z uwzględnieniem istniejących różnic") dla pieczęci elektronicznych.
e-Delivery	Usługi związane z doręczaniem dokumentów w formie elektronicznej, zapewniające informację dowodową dotyczącą doręczenia czy odbioru.	Tego typu usługi w Polsce realizowane są za pomocą elektronicznych skrzynek podawczych i urzędowych potwierdzeń UPO, UPD.
Website Authentication	Certyfikat SSL witryny internetowej.	
Publikacja listy TSL	Listy TSL zostały wprowadzone w ramach Dyrektywy Usługowej na potrzeby zestawiania ścieżki zaufania dla aplikacji weryfikujących certyfikaty kwalifikowane.	

Co ciekawe – projekt regulacji przewiduje wprowadzenie całego spektrum usług „kwalifikowanych". Jest to istotna różnica w stosunku do Dyrektywy 1999/93/EC, która przewiduje wyłącznie kwalifikowany certyfikat do podpisu elektronicznego. Rozporządzenie eIDAS, przewiduje dodatkowo kwalifikowane znakowanie czasem (realizowane obecnie w polskim systemie prawnym), kwalifikowaną usługę e-doręczenia, kwalifikowaną pieczęć elektroniczną, oraz kwalifikowane usługi walidacji i uwierzytelnienia witryny internetowej.

Modele e-identyfikacji na podstawie eIDAS

Obok przedstawionych usług projekt Rozporządzenia reguluje także obszar elektronicznej identyfikacji. Identyfikacja została zdefiniowana jako: *„[…] proces używania danych identyfikujących osobę w formie elektronicznej, w sposób jednoznaczny reprezentujący osobę fizyczną lub prawną;"*

Obszar ten budzi największe emocje, ze względu na fakt, iż każdy z krajów członkowskich stosuje już określone rozwiązania w zakresie e-identyfikacji. W przypadku elektronicznej identyfikacji duży wpływ na Rozporządzenie może mieć wypracowany w ramach projektu STORK (*Secure Identity Across Borders Linked* – https://www.eid-stork.eu/) model interoperacyjności. Inną możliwością implementacji usług transgranicznego uwierzytelnienia jest zastosowanie certyfikatów do uwierzytelnienia.

Model uwierzytelnienia STORK

Celem projektu STORK było wypracowanie metod transgranicznego uwierzytelnienia i identyfikacji obywatela. Na dyskusje przeprowadzane w trakcie posiedzeń Zespołu Gospodarki Elektronicznej pozwalają stwierdzić, że postępy prac nad rozporządzeniem zmierzają w kierunku wykorzystania dorobku projektu STORK, do ustanowienia obowiązującej na terenie UE metody identyfikacji elektronicznej.

W ramach projektu wypracowano sfederowany model uwierzytelnienia i identyfikacji umożliwiający federację systemów dostawców tożsamości – model PEPS (ang. *Pan-European Proxy Services* – Paneuropejskie usługi pośredniczące), jak również systemy wykorzystujące karty kryptograficzne, jako źródło informacji na temat tożsamości obywatela (model Middleware).

W modelu uwierzytelnienia STORK przeglądarka użytkownika jest przekierowywana do krajowych usług uwierzytelniających. Za pomocą uwierzytelnienia potwierdzana jest tożsamość użytkownika, a następnie uwierzytelnione dane identyfikacyjne mogą być przekazane do usługodawcy. W przypadku, gdyby Polska dołączyła ePUAP do projektu STORK, komunikacja mogłaby wyglądać w sposób przedstawiony na *rysunku 3.*

Model Middleware (MW) różni się od wskazanego tym, że uwierzytelnienie i odczyt danych identyfikacyjnych jest realizowany na karcie kryptograficznej i odbywa się za pośrednictwem oprogramowania *middleware* zainstalowanego na stacji użytkownika. Komunikacja z usługami PEPS, w modelu MW odbywa się poprzez wirtualnego dostawcę tożsamości (V-IDP). W obu przypadkach uwierzytelnione dane są przekazywane do usługodawcy, jako asercje zgodne ze standardem SAML.

Model uwierzytelnienia w oparciu o certyfikaty

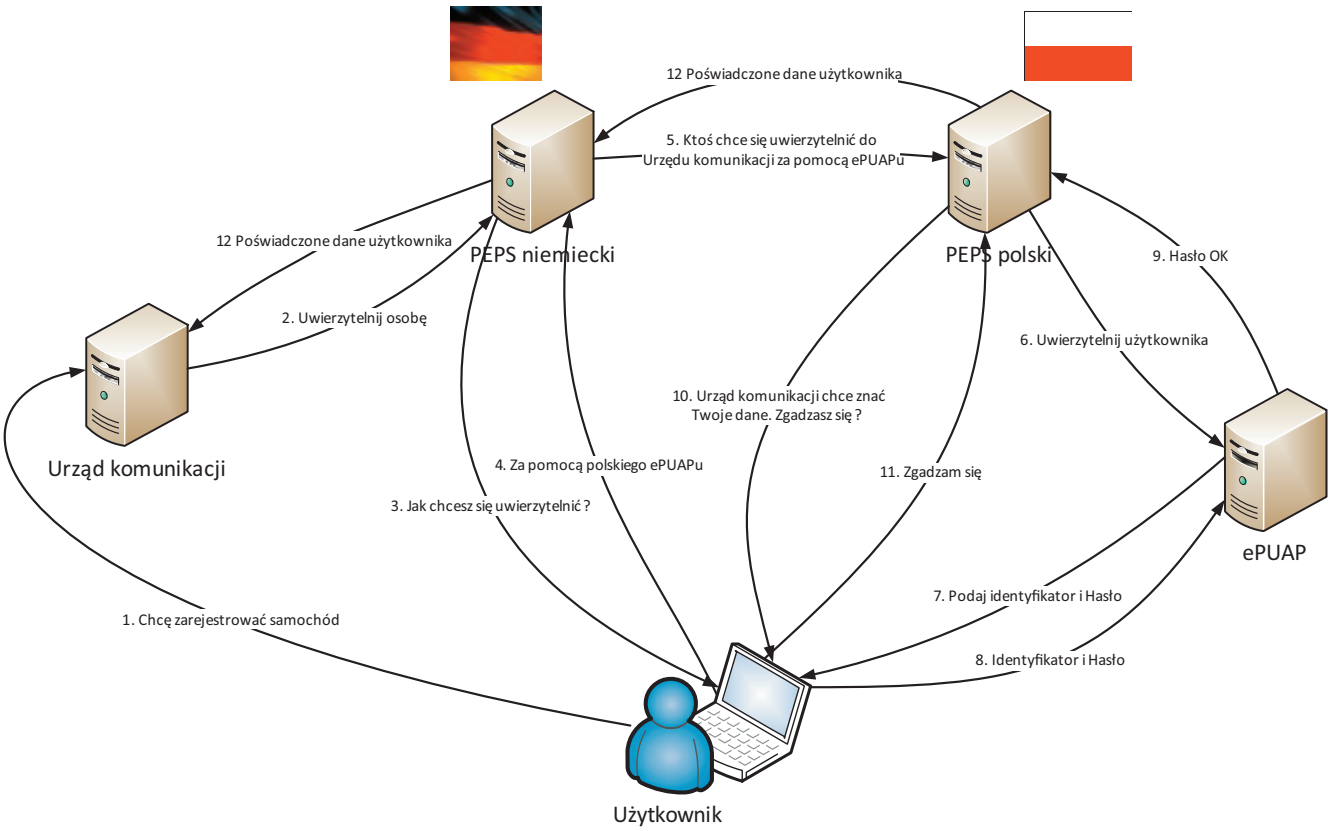
Uwierzytelnienie w oparciu o certyfikaty wykorzystuje infrastrukturę klucza publicznego (PKI). W tym przypadku do uwierzytelnienia stosowana jest wyłącznie jedna technologia – certyfikat, który może zawierać zestaw danych identyfikujących użytkownika. Jest on stosowany w zastępstwie innych metod uwierzytelnienia, takich jak np. login i hasło. Certyfikat obywatela, który mógłby posłużyć do uwierzytelnienia, na chwilę obecną nie został przewidziany w ramach Rozporządzenia eIDAS.

Rozpoznawanie certyfikatów wydawanych przez inne państwa członkowskie mogłoby być realizowane poprzez bezpośrednie wskazywanie certyfikatów wydawców w ramach systemu usługodawcy. Trzeba jednak zauważyć, że ze względu na potencjalną ilość wydawców (na dzień 2013-07-02 europejskie listy TSL zawierały 565 wpisów dla wydawców certyfikatów kwalifikowanych służących do podpisu. Źródło: http://eutsl.3xasecurity.com/tools/) pożądane jest zastosowanie mechanizmów automatycznego zarządzania zaufaniem do usługodawców. Rozwiązaniem tego problemu mogłoby być utworzenie europejskiej hierarchii usług certyfikacyjnych, bądź zastosowanie mechanizmów list TSL.

Podsumowanie

Porównując oba modele (*tab. 1*) można zauważyć, że model STORK jest znacznie bardziej elastyczny od modelu certyfikatu. Uwierzytelnienie przy pomocy certyfikatu jest natomiast stosunkowo łatwe do realizacji przy pomocy istniejącego oprogramowania. Z drugiej strony, przeprowadzenie identyfikacji na podstawie certyfikatu, nie jest już sprawą trywialną.

Polska na chwilę obecną posiada jedną metodę uwierzytelnienia, która mogłaby być uznana za ogólnokrajową. Jest nią profil zaufany ePUAP. W trakcie przygotowań i w fazie budowy są inne systemy, które mogą pretendować do tego miana (mowa o platformie uwierzytelnienia budowanej przez CSIOZ na potrzeby usług medycznych, oraz o karcie zdrowia, której wydanie planuje NFZ).



Rys. 3. Model komunikacji PEPS-PEPS na przykładzie rejestracji samochodu w urzędzie niemieckim.
Fig. 3. Communication PEPS-PEPS in example of car registration in German office

Tab. 1. Porównanie modeli e-identyfikacji. Tabl. 1. Comparison of e-identifiction models

	STORK	Certyfikat do uwierzytelnienia
Zakres danych identyfikacyjnych	Możliwe dostosowywania zakresu danych osobowych w zależności od potrzeb usługi	Sztywny, zdefiniowany przy rejestracji zakres danych
Metody uwierzytelnienia	Wiele.	Wyłącznie certyfikat
Łatwość implementacji	Konieczne zaimplementowanie SAML po stronie usługodawcy.	Praktycznie każdy serwer WWW pozwala na konfigurację uwierzytelnienia za pomocą SSL. **Żaden z dostępnych serwerów nie obsługuje TSL**
Łatwość wykorzystania danych	Dane identyfikacyjne są mapowane przez PEPS, konieczność implementacji SAML po stronie usługodawcy	Konieczność dokładnej standaryzacji danych identyfikacyjnych. Konieczność implementacji mechanizmów parsowania certyfikatu i mapowania pól na dane identyfikacyjne

Zróżnicowanie modeli uwierzytelnienia, oraz fakt, że część z nich wspiera standard SAML (ePUAP, system administracji w P2) wskazuje, że w interesie Polski byłoby zastosowanie modelu identyfikacji w oparciu o STORK. Trzeba jednak zauważyć, że na chwilę obecną nie są prowadzone żadne prace związane z integracją wymienionych mechanizmów uwierzytelnienia z platformą STORK. Wybór modelu STORK w powiązaniu z brakiem działania w kierunku integracji systemów z platformą może spowodować, że dzień wejścia w życie Rozporządzenia zastanie Polskę nieprzygotowaną na wdrożenie modeli e-identyfikacji.

Literatura

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic Signatures.

[2] http://ec.europa.eu/information_society/policy/esignature/ias_crobies_studies/index_en.htm

[3] Opublikowana wersja dokumentu jest dostępna pod adresem http://ec.europa.eu/digital-agenda/en/news/draft-regulation-electronic-identification-and-trusted-services-electronic-transactions-0