Europejska Agenda Cyfrowa

Działanie nr 3 - Zaproponowanie w 2011 r. przeglądu dyrektywy w sprawie podpisów elektronicznych w celu stworzenia ram prawnych dla transgranicznego uznawania i interoperacyjności bezpiecznych systemów e-uwierzytelniania

1. Definicja tematu

Podpis elektroniczny jest narzędziem służącym zagwarantowaniu tożsamości, autentyczności i integralności przy wymianie informacji drogą elektroniczną. Istota podpisu elektronicznego polega na zapewnieniu unikalności oznaczania dokumentu w taki sposób, że na podstawie tego oznaczenia można zagwarantować identyfikację osoby, która dokonała czynności podpisania oraz niezaprzeczalność podpisania przez nią dokumentu. Zapewnienie funkcji identyfikacji i niezaprzeczalności pozwala zrównać pod określonymi warunkami podpis elektroniczny z podpisem własnoręcznym. W konsekwencji dane w postaci elektronicznej opatrzone podpisem elektronicznym mogą stanowić samodzielny dowód, który możliwy jest do weryfikacji przy pomocy przeznaczonych do tego celu aplikacji. Autentyczność wszelkich innych dokumentów, które nie zostały opatrzone podpisem elektronicznym może być stwierdzona tylko w powiązaniu z systemami informatycznymi w których istnieją i w których zostały wytworzone, oraz w związku z okolicznościami w których powstawały. Ważną funkcją zaawansowanego podpisu elektronicznego jest funkcja zapewnienia integralności dokumentu, która umożliwia wykrycie zmian, które zostały wprowadzone po podpisaniu dokumentu. Poprzez wykorzystanie w podpisie funkcji obliczenia skrótu dokumentu podpis staje się powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna. Podpis elektroniczny wnosi zatem ważną wartość dodaną w elektroniczny obrót gospodarczy oraz prawny.

Technologie podpisu cyfrowego upowszechniły się w połowie lat 90-tych XX wieku i doprowadziły do uchwalenia pierwszych aktów prawnych, które uznawały, że zaawansowany podpis cyfrowy (*advanced digital signature*) może być stosowany zamiennie z podpisem własnoręcznym w obrocie prawnym. Za przykładem pierwszych krajów należących do Unii Europejskiej podążyły instytucje wspólnotowe przyjmując akty prawne regulujące ramy funkcjonowania podpisu w warunkach wspólnego rynku. Obecnie kwestie usług certyfikacyjnych w zakresie podpisu elektronicznego są regulowane w przepisach krajowych wszystkich państw członkowskich Unii Europejskiej. Konieczność istnienia ustawy regulującej świadczenie usług certyfikacyjnych w zakresie podpisu elektronicznego wynika m.in. z obowiązku implementacji dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. *w sprawie wspólnotowych ram dla podpisów elektronicznych*. W Polsce aktem podstawowym dla regulacji podpisu elektronicznego jest ustawa z dnia 18 września 2001 r. *o podpisie elektronicznym* (wraz z systemem aktów wykonawczych oraz przepisami w innych ustawach, takich jak np. Kodeks Cywilny).

W Dyrektywie 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych mowa jest o trzech rodzajach podpisu elektronicznego[1].Pierwszym z nich jest, posiadający duże znaczenie, zwykły „podpis elektroniczny”**.** Podpis ten służy do weryfikacji tożsamości i uwierzytelnienia danych. Może przy tym chodzić o tak prostą czynność jak podpisanie wiadomości elektronicznej nazwiskiem nadawcy lub przy użyciu kodu PIN. Aby stanowić podpis, uwierzytelnienie musi dotyczyć danych, a nie służyć tylko jako metoda lub technika uwierzytelniania dla podmiotu. Drugim zdefiniowanym w dyrektywie rodzajem podpisu elektronicznego jest „zaawansowany podpis elektroniczny”**.** Podpis ten musi spełniać wymagania określone w art. 2 ust. 2 Dyrektywy. Dyrektywa nie preferuje żadnej technologii, ale w praktyce definicja ta dotyczy głównie podpisów elektronicznych opartych na infrastrukturze klucza publicznego (PKI). W rozwiązaniu tym dane podpisywane są z wykorzystaniem technik szyfrowania, które wymagają użycia klucza prywatnego. W art. 5 ust. 1 Dyrektywy mowa jest o trzecim rodzaju podpisu elektronicznego, który w dyrektywie nie otrzymał własnej nazwy, a w dokumentach wspólnotowych nazywany jest „kwalifikowanym podpisem elektronicznym”**.** Chodzi o zaawansowany podpis elektroniczny oparty na kwalifikowanym certyfikacie i złożony za pomocą bezpiecznego urządzenia służącego do składania podpisu. Podpis taki musi spełniać wymagania określone w załącznikach I, II i III[2] do wymienionej dyrektywy.

2. Opis sytuacji i problemu

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 z poza 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 wzajemne 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 wymogom dodatkowym. Wymagania te muszą być zgodnie z art. 3.7 dyrektywy obiektywne, transparentne, proporcjonalne i nie dyskryminujące i mogą odnosić się jedynie do specyficznych cech danych zastosowań. Wymagania te nie mogą stanowić przeszkód w transgranicznych usługach dla obywatela.

Ważnym rozwiązaniem pomocnym w akceptacji wspólnotowych podpisów z certyfikatem kwalifikowanym jest tzw. lista TSL. Listy te służą m.in. odpowiedzi na pytanie, które podmioty są kwalifikowane lub akredytowane w danym państwie oraz jakie usługi otoczenia podpisu elektronicznego podlegają nadzorowi w danym państwie. Europejski Instytut

[1] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady z wykonania dyrektywy 1999/93/WE *w sprawie wspólnotowych ram w zakresie podpisów elektronicznych*, COM(2006) 120 wersja ostateczna, Bruksela, 17 marca 2006.

[2] ZAŁĄCZNIK I „Wymogi dotyczące certyfikatów kwalifikowanych”, ZAŁĄCZNIK II „Wymogi wobec podmiotów świadczących usługi certyfikacyjne, wystawiających certyfikaty kwalifikowane”, ZAŁĄCZNIK III „Wymogi dotyczące bezpiecznych urządzeń służących do składania podpisu elektronicznego”.

Standardów Telekomunikacyjnych ETSI opracował specyfikację umożliwiającą tworzenie i zarządzanie listami usług zaufanych (TSL – Trusted-service Status List). Szczegółowe informacje techniczne odnośnie list TSL można znaleźć w normie ETSI TS 102 231. Dokument ten opisuje format list TSL wykorzystywany m.in. w procesie walidacji certyfikatów z zagranicy. Potrzeba wprowadzenia list TSL bierze się z faktu, że wiele systemów administracji publicznej oraz podmiotów gospodarczych stosuje systemy walidacji serwerowej lub aplikacje weryfikujące przygotowane przed powstaniem list TSL. W praktyce akceptacji certyfikatów z zagranicy można napotkać na wiele trudności, zwłaszcza jeśli chodzi o aspekt określenia poziomu zaufania lub dostępności list CRL.. Lista TSL obejmuje zagadnienia związane nie tylko z usługami certyfikacyjnymi ale i szeroko rozumianymi usługami zaufania stanowiącymi otoczenie podpisu elektronicznego w danym państwie członkowskim.

W świetle obecnych prac wspólnotowych nad wykorzystaniem podpisu elektronicznego, które prowadzone są w ramach implementacji Dyrektywy o usługach na rynku wewnętrznym, możliwość osiągnięcia transgranicznej interoperacyjności procedur elektronicznych wiązana jest wyłącznie z certyfikatem kwalifikowanym. Wprowadzenie podpisu zaawansowanego, który nie wymaga stosowania tzw. bezpiecznego urządzenia powinno być zatem wdrażane z ostrożnością oraz bez szkody dla rozwiązań dotychczas istniejących. Chociaż stosowanie certyfikatu kwalifikowanego nie jest w przypadku podpisu zaawansowanego techniczną koniecznością, wskazane będzie jego wykorzystanie, jeśli niezbędna jest akceptacja podpisu za granicą. Podpis zaawansowany odmiennie, od podpisu opartego o kwalifikowany certyfikat, nie posiadał dotychczas wystandaryzowanego formatu i profilu w skali Unii Europejskiej. Usługi certyfikacyjne dla podpisów zaawansowanych realizowane są w ponad dwudziestu różnych modelach implementacji, a państwa członkowskie mają swobodę wyboru technologii zaawansowanych podpisów elektronicznych dla potrzeb krajowych zastosowań. W chwili obecnej prowadzone są prace zmierzające do wybrania formatów referencyjnych dla podpisu zaawansowanego, który powinny być uznawane przez wszystkie państwa członkowskie w procedurach transgranicznych. W ramach prowadzonych obecnie prac wspólnotowych w zakresie podpisu elektronicznego wskazano wstępnie na formaty XAdES, CAdES oraz PAdES w rozszerzeniach EPES/BES jako standardy referencyjne spełniające minimalne wymogi niezbędne do wzajemnego uznawania podpisu elektronicznego. Prowadzone w tym zakresie prace wskazują na konieczność przygotowania dodatkowej specyfikacji, które będą prowadzone przez ETSI. Podkreślić należy, że podpisy zaawansowane w usługach transgranicznych będą wymagały certyfikatu kwalifikowanego.

Zaawansowany podpis elektroniczny może występować w szczególności bez certyfikatów kwalifikowanych. Opracowany przez Komisję Europejską *„Plan działania na rzecz e-podpisu i e-identyfikacji w celu ułatwienia świadczenia transgranicznych usług publicznych na jednolitym rynku”*[3] stwierdza m.in., że w przeciwieństwie do podpisów kwalifikowanych, zaawansowane e-podpisy nie otrzymały w dyrektywie w sprawie podpisów elektronicznych takiego samego, jasnego statusu prawnego, zakładającego ich równoważność z podpisem odręcznym. Państwa członkowskie mają jedynie obowiązek zapewnić, żeby zaawansowanemu e-podpisowi nie odmawiano skuteczności prawnej jedynie dlatego, że jest w formie elektronicznej. Oznacza to, że państwa członkowskie mają większą swobodę decyzji

[3] Komunikat Komisji do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Plan działania na rzecz e-podpisu i e-identyfikacji w celu ułatwienia świadczenia transgranicznych usług publicznych na jednolitym rynku*, KOM(2008) 798 wersja ostateczna, Bruksela, 28.11.2008.

w sprawie akceptowania lub nieakceptowania określonych rodzajów zaawansowanego e-podpisu i przy podejmowaniu tej decyzji mogą się kierować własnymi wymogami dotyczącymi danego zastosowania podpisu. Dodatkowa trudność wiąże się z faktem, że wprawdzie zaawansowany e-podpis może być w teorii akceptowany w innym państwie członkowskim, ale w praktyce akceptacja taka nastręcza trudności ze względu na różnorodne rozwiązania techniczne, które są stosowane. W związku z tym walidacja zaawansowanego e-podpisu przez odbiorcę oraz ocena skuteczności prawnej czy poziomu bezpieczeństwa tego podpisu, w kontekście danego zastosowania, stanowią obecnie bardzo trudne zadania, które wymagają często szczegółowego badania każdego otrzymanego podpisu. Ponieważ definicja zaawansowanego podpisu elektronicznego zawarta w art. 2 ust. 2 Dyrektywy 1999/93/WE ma charakter ogólny, państwa członkowskie stosują bardzo różnorodne rozwiązania techniczne, które cechują różne poziomy bezpieczeństwa. W przypadku niektórych zastosowań tych podpisów państwa członkowskie mogą również wymagać obowiązkowego stosowania określonych rozwiązań krajowych, co tworzy dodatkowe bariery dla transgranicznego stosowania podpisów zaawansowanych.

3. Odniesienie do dokumentów programowych

Najważniejszym dokumentem w tym zakresie jest opracowany przez Komisję Europejską *„Plan działania na rzecz e-podpisu i e-identyfikacji w celu ułatwienia świadczenia transgranicznych usług publicznych na jednolitym rynku”* (COM(2008)798). W stanowisku Rządu RP do przedmiotowego dokumentu stwierdza się m.in., że Rząd Rzeczpospolitej Polskiej popiera inicjatywę mającą na celu zapewnienie interoperacyjności podpisu elektronicznego oraz elektronicznej identyfikacji tożsamości (eIDM). Obowiązująca dyrektywa 1999/93/WE jako dyrektywa dot. wymagań minimalnych doprowadziła do pluralizmu rozwiązań w zakresie aplikacji, infrastruktury oraz nadzoru w zakresie podpisu elektronicznego oraz licznych różnic co do rodzajów podpisu elektronicznego wykorzystanych przez administrację poszczególnych państw członkowskich. Wspólnotowe działania na rzecz zapewnienia faktycznych możliwości uznawania podpisów pomiędzy państwami UE oraz EOG podjęte w roku ubiegłym po blisko ośmiu latach obowiązywania dyrektywy uznać należy za w najwyższym stopniu pilne i niezbędne. Rząd Rzeczpospolitej Polskiej popiera działania wynikające z przedmiotowego komunikatu Komisji Europejskiej, przyjmując za zgodne z dyrektywą 1999/93/WE dążenie do zapewnienia uznawania nie tylko kwalifikowanych podpisów elektronicznych, ale również podpisów zaawansowanych weryfikowanych przy pomocy certyfikatów kwalifikowanych. Projektowane działania wspólnotowe sprzyjają budowaniu wspólnej europejskiej przestrzeni zaufania do podpisów elektronicznych weryfikowanych przy pomocy kwalifikowanych certyfikatów z innych państw członkowskich UE oraz EOG.

4. Działania podejmowane w Polsce

W latach 2008-2010 podjęto serię działań systemowych, które mają prowadzić do upowszechnienia usług publicznych opartych o elektroniczną identyfikację obywatela lub przedsiębiorcy. Prowadzone są prace związane z przygotowaniem nowej ustawy o podpisach elektronicznych, która obecnie zakończyła notyfikację wspólnotową i w miesiącu wrześniu br skierowana zostanie pod obrady Sejmu RP. Podkreślić należy, że dla upowszechnienia stosowania podpisanych elektronicznie dokumentów nie wystarczy zmiana ustawy o podpisach elektronicznych, ale niezbędne jest przeprowadzenie szeregu innych zmian prawnych oraz infrastrukturalnych.

W MSWiA realizowany jest projekt „pl.ID – polska ID karta", którego głównym celem jest wdrożenie wielofunkcyjnego elektronicznego dowodu tożsamości z funkcją uwierzytelniania w systemach IT jednostek sektora publicznego, zgodnego z unijnymi koncepcjami, narodowego dokumentu identyfikacyjnego (eID). W ramach tego projektu zawierają się również działania związane z przebudową, modernizacja i integracją istniejących rejestrów państwowych. Elektroniczny dowód tożsamości zawierać będzie podpis elektroniczny ułatwiający każdemu obywatelowi uwierzytelnianie w kontaktach z administracją. Dzięki kompleksowej realizacji projektu zostaną zniwelowane bariery administracyjne oraz stworzone warunki dla dalszego rozwoju zintegrowanych usług publicznych. Ponadto przeprowadzono nowelizację ustawy o informatyzacji połączoną z nowelizacją kodeksu postępowania administracyjnego i ustawy – Ordynacja podatkowa, umożliwiająca zastosowanie w komunikacji z podmiotami publicznymi innych form identyfikacji takich jak profil zaufany ePUAP (działanie Ministerstwa Spraw Wewnętrznych i Administracji).

W odniesieniu do działań ściśle związanych z transgraniczną interoperacyjnością podpisu elektronicznego przeprowadzone zostały prace związane z zapewnieniem udziału Polski w europejskim systemie list TSL. Od dnia 28 grudnia 2009 zgodnie z decyzją Komisji Europejskiej z dnia 16 października 2009 r. ustanawiającą środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez pojedyncze punkty kontaktowe w kontekście Dyrektywy 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (C(2009) 7806) na stronie Narodowego Centrum Certyfikacji publikowana jest krajowa lista TSL. Lista stanowi subsydiarne narzędzie informacji o podmiotach kwalifikowanych lub akredytowanych świadczących usługi certyfikacyjne, które jest dostępne za pośrednictwem europejskiej listy list w każdym z państw członkowskich UE oraz EOG. Począwszy od dnia 1 grudnia 2010 listy TSL będą dodatkowo sygnowane podpisem elektronicznym krajowego operatora systemu TSL. Oprócz publikacji krajowej listy TSL niezbędne jest podjęcie działań związanych z zapewnieniem akceptacji podpisów weryfikowanych kwalifikowanym certyfikatem z zagranicy. Wskazane jest, aby implementacja usług walidacyjnych uwzględniała europejską listę list oraz krajowe listy TSL.

5. Ustosunkowanie się do planów Komisji Europejskiej

Strona polska wyraża swoje poparcie dla przedstawionej w dokumencie Europejska Agenda Cyfrowa inicjatywy Komisji Europejskiej w zakresie zaproponowania przeglądu dyrektywy w sprawie podpisów elektronicznych w celu stworzenia ram prawnych dla transgranicznego uznawania i interoperacyjności bezpiecznych systemów e-uwierzytelniania. Potrzeba taka wynika z konieczności dostosowania obowiązującej od ponad dekady dyrektywy do potrzeb obrotu prawnego w Unii Europejskiej, w tym rozwoju usług transgranicznych. Jest to zarazem część przewidzianych na najbliższe lata działań wspólnotowych, które obejmą również racjonalizację standardów podpisu elektronicznego, zgodnie z udzielonym przez Komisję mandatem dla CEN, CENELEC oraz ETSI[4]. Należy monitorować rozwijające się usługi walidacji podpisu elektronicznego oraz uwierzytelnienia przy użyciu eID. W przypadku zaistnienia potrzeby dostosowania do zmienionych przepisów wspólnotowych lub nowych standardów w tym zakresie należy podejmować działania

[4] Standarisation Mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the Field of Information And Communication Technologies Applied to Electronic Signatures, M/460 EN, Bruksela, 22.12.2009.

zmierzające do dostosowania obowiązujących przepisów, w taki sposób aby uwzględniały one rozwój acquis communautaire.

W odniesieniu do merytoryki zmian, które powinny zostać rozważone w związku z możliwą nowelizacją dyrektywy w sprawie wspólnotowych ram prawnych dla podpisu elektronicznego wskazane będzie precyzyjne uregulowanie instytucji gwarancji za certyfikat z krajów trzecich. Z uwagi na fakt, że dyrektywa 1999/93/WE nie była dotychczas nigdy nowelizowana wskazane jest również, aby rozważone zostało nie tylko wprowadzenie zmian związanych z transgranicznym uznawaniem i interoperacyjnością bezpiecznych systemów e-uwierzytelniania ale również usunięcie dostrzeżonych błędów lub rozwiązań ograniczających rynek usług certyfikacyjnych. Przykładowo wg dyrektywy podpisujący to osoba, która posiada *urządzenie* do składania podpisu elektronicznego a podpis zaawansowany, to podpis stworzony m.in. za pomocą środków, który podpisujący może mieć pod swoją *wyłączną kontrolą*. Wskazana jest analiza czy przepisy dyrektywy nie są w tym zakresie nadmiarowe z punktu widzenia podpisów składanych wyłącznie przy użyciu oprogramowania lub podpisów składanych w oparciu o serwer podmiotu zewnętrznego.

6. Działania planowane w Polsce

Wśród prowadzonych obecnie lub planowanych działań wymienić należy m.in.:

1) przygotowanie nowej ustawy o podpisach elektronicznych umożliwiającej szersze wykorzystanie podpisów innych niż bezpieczny podpis elektroniczny opatrzony ważnym kwalifikowanym certyfikatem wraz systemem aktów wykonawczych (działanie Ministerstwa Gospodarki),

2) udostępnienie mechanizmów weryfikacji podpisu elektronicznego z certyfikatem kwalifikowanym z krajów Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego na Elektronicznej Platformie Usług Administracji Publicznej (projekt ePUAP prowadzi Centrum Projektów Informatycznych MSWiA),

3) realizacja projektu pl.ID w związku z uchwaloną ustawą o dowodach osobistych, co umożliwi wydawanie od 2011 r. dowodu osobistego z mikroprocesorem, przy pomocy którego obywatel będzie mógł złożyć podpis osobisty lub opcjonalnie kwalifikowany podpis elektroniczny (projekt pl.ID prowadzi Centrum Projektów Informatycznych MSWIA),

4) ograniczenie barier administracyjnych poprzez usunięcie wymogu stosowania na wyłączność bezpiecznego podpisu elektronicznego w tych procedurach administracyjnych, w których tak wysoki poziom bezpieczeństwa nie znajduje uzasadnienia. Ze względu na konieczność analizy ryzyka poszczególnych procedur prace w tym zakresie powinien przeprowadzić każdy resort.

7. Główne akty prawne

W UNII EUROPEJSKIEJ:

1. Dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z 13 grudnia 1999 r. w sprawie wspólnotowych ram dla podpisów elektronicznych

2. Decyzja Komisji z 6 listopada 2000 r. w sprawie minimalnych kryteriów jakie powinny zostać wzięte pod uwagę przez Państwa Członkowskie przy wyznaczaniu organów zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady w sprawie wspólnotowych ram w zakresie podpisu elektronicznego (2000/709/WE)

3. Decyzja Komisji Europejskiej z 14 lipca 2003 w sprawie publikacji ogólnie uznanych standardów dla produktów podpisu elektronicznego zgodnie z dyrektywą1999/93/WE Parlamentu Europejskiego i Rady w sprawie wspólnotowych ram w zakresie podpisu elektronicznego (2003/511/EC)

4. Decyzja Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiająca środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez „pojedyncze punkty kontaktowe" zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz.U. L 274 z 20.10.2009)

5. Decyzja Komisji z dnia 28 lipca 2010 r. zmieniająca decyzję 2009/767/WE w odniesieniu do tworzenia, prowadzenia i publikowania zaufanych list podmiotów świadczących usługi certyfikacyjne nadzorowanych/akredytowanych przez państwa członkowskie (notyfikowana jako dokument nr C(2010) 5063)

W POLSCE:

Ustawa z 18 września 2001 o podpisie elektronicznym ogłoszona w Dzienniku Ustaw z 2001 r. nr 130, poz. 1450 ze zm. Ustawa wraz z pakietem podstawowych aktów wykonawczych weszła w życie w 16 sierpnia 2002.

Akty wykonawcze do ustawy o podpisie elektronicznym:

Poniższe akty prawne regulują obowiązki usługodawców i warunki niezbędne do świadczenia usług certyfikacyjnych w zakresie podpisu elektronicznego

1. Rozporządzenie Rady Ministrów z 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego - określa wymagania technologiczne i organizacyjne, jakie musi spełniać kwalifikowany podmiot świadczący usługi certyfikacyjne, warunki dla urządzeń, jakie powinien rekomendować swoim klientom jako bezpieczne, a także ogólne zasady polityk certyfikacji stanowiących o szczegółowych regułach świadczenia usług w stosunkach z klientem i odbiorca usług certyfikacyjnych. Podaje obowiązujący profil certyfikatu i listy CRL, nakłada no kwalifikowany podmiot świadczący usługi certyfikacyjne szereg obowiązków i jest podstawą merytoryczną do kontroli wstępnych i późniejszego nadzoru nad kwalifikowanymi podmiotami świadczącymi usługi certyfikacyjne. (Dz.U. nr 229 z 31 grudnia 2003 r.)

2. Rozporządzenie Ministra Finansów z 8 sierpnia 2002 r. w sprawie sposobu i szczegółowych warunków spełnienia obowiązku ubezpieczenia odpowiedzialności cywilnej przez kwalifikowany podmiot – określa w jaki sposób i w jakich granicach kwalifikowany podmiot świadczący usługi certyfikacyjne ma obowiązek ubezpieczyć się, zanim otrzyma zaświadczeni certyfikacyjne od ministra. (Dz.U. nr 229 z 31 grudnia 2003 r.)

3. Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 r. w sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym – określa dokładnie zawartość i wzór wniosku, jaki podmiot musi złożyć ubiegając się o wpis do rejestru. (Dz.U. nr 229 z 31 grudnia 2003 r.)

4. Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 r. w sprawie wysokości opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym – określa wysokość opłaty za rozpatrzenie wniosku na kwotę równowartości 10 tys. €. (Dz.U. nr 229 z 31 grudnia 2003 r.)

5. Rozporządzenie Ministra Gospodarki z 6 sierpnia 2002 r. w sprawie sposobu prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzoru tego rejestru oraz szczegółowego trybu postępowania w sprawach o wpis do rejestru – określa wzór rejestru, zawartość jego pól, sposób prowadzenia, miejsce przechowywania i zasady udostępniania rejestru, zarówno w wersji papierowej jak i online. (Dz.U. nr 229 z 31 grudnia 2003 r.)

6. Rozporządzenie Ministra Gospodarki z 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym – określa zasady wytwarzania i wydawania zaświadczeń certyfikacyjnych, rodzaje zaświadczeń, podmioty do zobowiązane do ich wydawania oraz zasady wydawania list unieważnionych zaświadczeń. Zaświadczenia wydaje minister lub w jego imieniu podmiot upoważniony oraz kwalifikowane podmioty świadczące usługi certyfikacyjne. System zaświadczeń umożliwia uwierzytelnianie przy dowolnie przez klienta wybranym punkcie zaufania, od którego rozpocznie on weryfikację kolejnych zaświadczeń i certyfikatów. (Dz. U. nr 229 z 31 grudnia 2003 r.)

7. Rozporządzenie Ministra Gospodarki, Pracy i Polityki Społecznej z 23 grudnia 2003 r. w sprawie opłat za przechowywanie dokumentów i danych związanych z usługami certyfikacyjnymi - określa odpłatność za przechowywanie danych po podmiotach kwalifikowanych, które zaprzestają prowadzenia działalności (Dz.U. nr 6 z 15 stycznia 2004 r.)

8. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 24 lipca 2007 r. w sprawie warunków udostępniania formularzy i wzorów dokumentów w postaci elektronicznej – określa wymogi związane z wykonaniem obowiązku umożliwienia przez organy władzy publicznej odbiorcom usług certyfikacyjnych wnoszenia podań i wniosków oraz innych czynności w postaci elektronicznej, w przypadkach gdy przepisy prawa wymagają składania ich w określonej formie lub według określonego wzoru (Dz.U. nr 151 z dnia 22 sierpnia 2007 r.).

Źródło: MSWiA