ROZPORZĄDZENIE

RADY MINISTRÓW

z dnia ..... 2014 r.

zmieniające rozporządzenie 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[1)]

Na podstawie art. 10 ust. 4, art. 17 ust. 2 i art. 18 ust. 3 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz 262) zarządza się, co następuje:

§ 1. W rozporządzeniu Rady Ministrów z dnia 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 (Dz. U. Nr 128, poz. 1094) wprowadza się następujące zmiany:

1) § 10-12 otrzymują brzmienie:

„§ 10. Bezpieczne urządzenia do składania lub weryfikacji podpisu elektronicznego jednoznacznie rozpoznają wartości pól zawierających dane, o których mowa w art. 20 ust. 1 pkt 1-7 oraz art. 22 ust. 3 ustawy oraz występujące pola rozszerzeń oznaczone jako krytyczne.

§ 11. Bezpieczne urządzenia do składania podpisu elektronicznego zapewniają, że dane służące do składania bezpiecznego podpisu elektronicznego będą wykorzystywane w sposób zgodny z użyciem klucza „(keyUsage)" wskazanym w certyfikacie kwalifikowanym.

§ 12. 1. Maksymalny okres ważności kwalifikowanego certyfikatu przewidziany przez politykę certyfikacji wynosi nie więcej niż 2 lata.

[1)] Niniejsze rozporządzenie zostało notyfikowane Komisji Europejskiej w dniu ... 2014 r., pod numerem ..., zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239 , poz. 2039 oraz z 2004 r. Nr 65 , poz. 597), które wdraża postanowienia dyrektywy 98/34/WE z dnia 22 czerwca 1998 r. ustanawiającej procedurę udzielania informacji w zakresie norm i przepisów technicznych (Dz. Urz. WE L 204 z 21.07.1998, z poźn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 20, str. 337).

2. W przypadku kwalifikowanego certyfikatu, spełniającego minimalne wymagania dla funkcji skrótu i algorytmów szyfrowych na dzień 1 czerwca 2015 r., okres ważności przewidziany przez politykę certyfikacji, wynosi nie więcej niż 5 lat.";

2) w § 15 uchyla się ust. 8 i 9;

3) w § 21 ust. 4 otrzymuje brzmienie:

„4. W przypadku, o którym mowa w ust. 2, podmiot świadczący usługi certyfikacyjne:

1) sprawdza prawdziwość danych podanych przez osobę ubiegającą się o kwalifikowany certyfikat przez porównanie ich z danymi znajdującymi się w certyfikacie kwalifikowanym użytym do podpisania umowy;
2) zapewnia, aby zakres danych identyfikujących właściciela certyfikatu nie był szerszy od zakresu danych znajdujących się w certyfikacie kwalifikowanym użytym do podpisania umowy chyba, że dostarczy on dowody potwierdzające ich prawdziwość;
3) aktualizuje wartość wymienioną w pkt 1.6 załącznika nr 2 do rozporządzenia;
4) zapewnia, aby wartość zapisana zgodnie z pkt 1.6 załącznika nr 2 do rozporządzenia nie była mniejsza niż 10.";

4) w § 25 pkt 2 otrzymuje brzmienie:

„2) dane służące do weryfikacji bezpiecznego podpisu lub poświadczenia elektronicznego i publiczne klucze infrastruktury były wysyłane do użytkowników w sposób zapewniający ich integralność i autentyczność, przy czym samo zastosowanie zaświadczeń certyfikacyjnych, w których pola: wydawca „(issuer)" i właściciel „(subject)", są identyczne, nie zapewnia wystarczającego poziomu pewności co do autentyczności danych lub klucza.";

5) w § 30 po ust. 2 dodaje się ust. 2a i 2b w brzmieniu:

„2a. Podmiot kwalifikowany wskazuje na wykazie, o którym mowa w art. 10 ust. 1 pkt 8 ustawy, bezpieczne urządzenia do składania podpisów elektronicznych, które spełniają warunki techniczne umożliwiające złożenie podpisu zgodnego z co najmniej jedną ze specyfikacji opisanej w załączniku dyrektywy 2011/130/WE Parlamentu Europejskiego i Rady dotyczącej usług na rynku wewnętrznym.

2b. Podmiot kwalifikowany wskazuje na wykazie, o którym mowa w art. 10 ust. 1 pkt 8 ustawy, bezpieczne urządzenia do weryfikacji podpisów elektronicznych, które spełniają warunki techniczne umożliwiające weryfikację podpisów zgodnych ze wszystkimi

specyfikacjami opisanymi w załączniku dyrektywy 2011/130/WE Parlamentu Europejskiego i Rady dotyczącej usług na rynku wewnętrznym.";

6) w § 49 w ust. 2 po pkt 4 dodaje się pkt 4a i 4b w brzmieniu:

„4a) specyfikacja techniczna ETSI TS 102 778 - PDF Advanced Electronic Signature Profiles, wydana przez European Telecommunications Standards Institute;

4b) specyfikacja techniczna ETSI TS 102 918 – Associated Signature Containers (ASiC), wydana przez European Telecommunications Standards Institute;";

7) po § 49 dodaje się § 49a – 49b w brzmieniu:

„§ 49a. Minister właściwy do spraw gospodarki zamieszcza w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego tego ministra listę kodów, o których mowa w załączniku nr 2 pkt 1.4.5.

§ 49b. 1. Stosowanie funkcji skrótu SHA-1 oraz RIPEMD-160 dopuszcza się:

1) do dnia 31 maja 2015 r. – w celu składania poświadczeń elektronicznych wykorzystujących te funkcje lub składania poświadczeń elektronicznych weryfikowanych w ścieżce certyfikacji wykorzystującej te funkcje;
2) do dnia 31 grudnia 2016 r. – w celu składania bezpiecznego podpisu elektronicznego;
3) do dnia wygaśnięcia zaświadczenia certyfikacyjnego urzędu certyfikacji zawierającego wymienione funkcje – w celu składania poświadczeń elektronicznych pod listami certyfikatów unieważnionych wydawanych przez ten urząd certyfikacji;
4) bezterminowo – w celu weryfikacji złożonych poświadczeń elektronicznych lub bezpiecznych podpisów elektronicznych.

2. Stosowanie funkcji skrótu wymienionych w załączniku nr 1 do rozporządzenia, z wyłączeniem funkcji skrótu, o których mowa w ust. 1, dopuszcza się od dnia 1 stycznia 2015 r.

3. Dopuszcza się wykorzystanie certyfikatów kwalifikowanych nie spełniających wymagań załącznika 2 do rozporządzenia, pod warunkiem, że zostały wydane przed dniem 1 czerwca 2015 r.

4. Dopuszcza się wykorzystanie zaświadczeń certyfikacyjnych nie spełniających wymagań załącznika nr 2 do rozporządzenia pod warunkiem, że zostały wydane przed dniem 1 czerwca 2015 r.";

8) tytuł Rozdziału 5 otrzymuje brzmienie:

„Przepisy przejściowe i końcowe";

9) załączniki nr 1 – 3 do rozporządzenia otrzymują brzmienie określone w załącznikach do niniejszego rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem 1 grudnia 2014 r.

PREZES RADY MINISTRÓW

ZA ZGODNOŚĆ POD WZGLĘDEM
PRAWNYM I REDAKCYJNYM
DYREKTOR
Departamentu Prawnego
20.05.2014 r.
Monika Studzińska
radca prawny

Załączniki do rozporządzenia
Rady Ministrów z dnia .....2014 r.
(Dz.U. 2014 r. poz. .....)

Załącznik nr 1

WYKAZ ALGORYTMÓW SZYFROWYCH i FUNKCJI SKRÓTU WYKORZYSTYWANYCH DO TWORZENIA BEZPIECZNYCH PODPISÓW ELEKTRONICZNYCH, ZAŚWIADCZEŃ i POŚWIADCZEŃ ELEKTRONICZNYCH

1. Funkcje skrótu „(hash functions)", których identyfikatory obiektu zostały wymienione w specyfikacji technicznej ETSI TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, wydanej przez European Telecommunications Standards Institute.

2. Algorytmy „(signature algorithms)", których identyfikatory obiektu zostały wymienione w specyfikacji technicznej ETSI TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, wydanej przez European Telecommunications Standards Institute.

3. Identyfikatory obiektów, o których mowa w ust. 1 i 2 zapisane są przy użyciu notacji ASN.1, opisanej w normie ISO/IEC 8824 - Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1), wydanej przez International Organization for Standardization.

Załącznik nr 2

SZCZEGÓŁOWE WYMAGANIA DOTYCZĄCE KWALIFIKOWANEGO CERTYFIKATU i ZAŚWIADCZENIA CERTYFIKACYJNEGO ORAZ LISTY UNIEWAŻNIONYCH i ZAWIESZONYCH CERTYFIKATÓW

1. Wymagania dotyczące kwalifikowanego certyfikatu:

1.1 certyfikat kwalifikowany zawiera co najmniej zestaw danych wymieniony w art. 20 ust. 1 ustawy;

1.2 certyfikat kwalifikowany może być wydawany różnym kategoriom osób fizycznych:

1.2.1 kategoria I zawiera w nazwie podmiotu „(subject)" przynajmniej następujące atrybuty: nazwa kraju „(countryName)", nazwisko „(surname)", imię (imiona) „(givenName)", numer seryjny „(serialNumber)",

1.2.2 kategoria II zawiera w nazwie podmiotu „(subject)" przynajmniej następujące atrybuty: nazwa kraju „(countryName)", nazwa powszechna „(commonName)", numer seryjny „(serialNumber)",

1.2.3 kategoria III zawiera w nazwie podmiotu „(subject)" przynajmniej następujące atrybuty; nazwa kraju „(countryName)", pseudonim „(pseudonym)";

1.3 profil certyfikatu kwalifikowanego jest zgodny z dokumentem ETSI EN 319 412-5 – Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile wydanym przez European Telecommunications Standards Institute;

1.4 w przypadku użycia w nazwie podmiotu „(subject)" atrybutu „serialNumber" odnoszącego się do osoby fizycznej, dla atrybutu serialNumber zgodnego ze składnią oznaczoną identyfikatorem „id-etsi-qcs-SemanticsId-Natural", w ramach wymienionej składni stosuje się odpowiednio:

1.4.1 „IDC" – dla oznaczenia numeru dowodu tożsamości,

1.4.2 „PNO" – dla oznaczenia numeru PESEL,

1.4.3 „PAS" – dla oznaczenia numeru paszportu,

1.4.4 „TAX" – dla oznaczenia numeru identyfikacji podatkowej,

1.4.5 dwuliterowy kod opublikowany przez ministra właściwego do spraw gospodarki, zgodny ze składnią identyfikatora id-etsi-qcs-SemanticsId-Natural dla oznaczenia numeru seryjnego innego niż wymienione,

1.4.6 w przypadku, gdy norma zaleca zastąpienie identyfikatora

zdefiniowanego w ramach składni id-etsi-qcs-SemanticsID-Natural innym, dopuszcza się odpowiednio stosowanie nowego identyfikatora,

1.5 certyfikat kwalifikowany zawiera identyfikator „id-etsi-qcs-QcSSCD", wskazany przez dokument ETSI EN 319 412-5 – Profiles for Trust Service Providers issuing certificates;Part 5: Extension for Qualified Certificate profile, wydany przez European Telecommunications Standards Institute;

1.6 certyfikat kwalifikowany zawiera rozszerzenie id-etsi-qcs-QcRetentionPeriod opisane w dokumencie ETSI EN 319 412-5, zawierające informację o okresie przechowywania dokumentacji dotyczącej weryfikacji tożsamości właściciela certyfikatu, zawierającej odręczny podpis wnioskodawcy, wyrażonej jako liczba lat przechowywania począwszy od daty wygaśnięcia certyfikatu;

1.7 poświadczenie elektroniczne złożone pod certyfikatem kwalifikowanym oraz dane służące do weryfikacji podpisu elektronicznego spełniają wymagania określone w załączniku 1 i załączniku 3 niniejszego rozporządzenia, lub w przypadku braku takich wymagań odpowiednio stosuje się zalecenia specyfikacji technicznej TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms wydanego przez European Telecommunications Standards Institute.

2. Wymagania dotyczące zaświadczenia certyfikacyjnego:

2.1 zaświadczenie certyfikacyjne zawiera rozszerzenie wskazujące na usługę udostępniania list certyfikatów unieważnionych (CRL Distribution Points);

2.2 zaświadczenie certyfikacyjne jest zgodne z dokumentem RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile wydanym przez Internet Engineering Task Force (IETF);

2.3 poświadczenie elektroniczne złożone pod zaświadczeniem oraz dane służące do weryfikacji poświadczenia elektronicznego spełniają wymagania określone w załączniku 1 i załączniku 3 niniejszego rozporządzenia, lub w przypadku braku takich wymagań odpowiednio stosuje się, zalecenia specyfikacji technicznej TS 102 176-1 – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms wydanego przez European Telecommunications Standards Institute;

2.4 zaświadczenie certyfikacyjne zawiera rozszerzenie wskazujące na lokalizację zaświadczenia wydawcy (Authority Information Access z numerem OID accessMethod ustawionym na id-ad-caIssuers i wartością accessLocation wskazującą na zaświadczenie wydawcy);

2.5 zaświadczenie certyfikacyjne zawiera identyfikator klucza podmiotu (Subject Key Identifier);

2.6 zaświadczenie certyfikacyjne zawiera identyfikator klucza wydawcy (Authority Key Identifier);

2.7 wymagania wymienione w punktach 2.1 i 2.4 nie dotyczą zaświadczenia zawierającego dane do weryfikacji poświadczenia złożonego pod tymże zaświadczeniem.

3. Wymagania dotyczące listy CRL:

3.1 listy CRL zawierają co najmniej elementy wymienione w art. 22 ust. 3 ustawy;

3.2 listy CRL są zgodne z dokumentem RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile wydanym przez Internet Engineering Task Force (IETF);

3.3 poświadczenie elektroniczne złożone pod listą CRL wykorzystuje algorytmy i funkcje skrótu o sile co najmniej równej algorytmom i funkcjom skrótu użytym w zaświadczeniu certyfikacyjnym urzędu certyfikacji, który wydaje listę CRL.

Załącznik nr 3

WYMAGANIA DLA ALGORYTMÓW SZYFROWYCH

1. Dla algorytmu RSA do dnia 31 maja 2015 r.:
- minimalna długość klucza, rozumianego jako moduł p*q, wynosi 1020 bitów,
- długości liczb pierwszych p i q, składających się na moduł, nie mogą się różnić więcej niż o 30 bitów.

2. Dla algorytmu RSA po dniu 31 maja 2015 r.:
- minimalna długość klucza, rozumianego jako moduł p*q, wynosi 2048 bitów,
- długości liczb pierwszych p i q, składających się na moduł, nie mogą się różnić więcej niż o 30 bitów.

3. Dla algorytmu DSA do dnia 31 maja 2015 r.:
- minimalna długość klucza, rozumianego jako moduł p, wynosi 1024 bity,
- minimalna długość parametru q, będącego dzielnikiem liczby (p-1), wynosi 160 bitów.

4. Dla algorytmu DSA po dniu 31 maja 2015 r.:
- minimalna długość klucza, rozumianego jako moduł p, wynosi 2048 bitów,
- minimalna długość parametru q, będącego dzielnikiem liczby (p-1), wynosi 256 bitów.

5. Dla algorytmu ECDSA i ECGDSA do dnia 31 maja 2015 r.:
- minimalna długość parametru q wynosi 160 bitów,
- minimalny współczynnik r0 wynosi 10^4,
- minimalna wartość parametru MinClass wynosi 200.

6. Dla algorytmu ECDSA i ECGDSA po dniu 31 maja 2015 r.:
- minimalna długość parametru q wynosi 224 bity,
- minimalny współczynnik r0 wynosi 10^4,
- minimalna wartość parametru MinClass wynosi 200.",
- iloraz n/q, gdzie n jest rzędem krzywej, a q jest rzędem generatora, jest równy nie więcej niż 4.

7. Nazewnictwo parametrów, o których mowa w punktach 1-6 jest zgodne ze specyfikacją techniczną TS 102 176-1 Electronic – Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms, wydaną przez European Telecommunications Standards Institute.

8. Wymagania wymienione w pkt 1-7 nie dotyczą procesu weryfikacji ważności poświadczenia i podpisu elektronicznego.

Uzasadnienie

Zmiany wprowadzone w niniejszym rozporządzeniu można podzielić na następujące grupy:

1) aktualizacja listy i parametrów algorytmów kryptograficznych;
2) aktualizacja profili certyfikatów i list CRL;
3) dopuszczenie nowych formatów podpisu elektronicznego.

Aktualizacja listy i parametrów algorytmów kryptograficznych

W obszarze podpisu elektronicznego algorytmy kryptograficzne wykorzystywane są do generowania funkcji skrótu i wartości podpisu elektronicznego. w obowiązującym stanie prawnym do użytku dopuszczone zostały algorytmy funkcji skrótu SHA-1 oraz RIPEMD-160. w obszarze algorytmów bezpiecznego podpisu elektronicznego dotychczasowe brzmienie rozporządzenia dopuszczało stosowanie algorytmów RSA o minimalnej długości klucza 1020 bitów, DSA o minimalnej długości klucza 1024 bitów, ECDSA i ECGDSA o minimalnej długości klucza 160 bitów. Algorytmy te w świetle dzisiejszej wiedzy nie są zalecane do stosowane jako algorytmy podpisu elektronicznego. Niniejsza nowelizacja wprowadza w tym zakresie istotną modyfikację polegającą na stopniowym wycofywaniu algorytmów niezalecanych i zastąpieniu ich przez nowsze algorytmy, które są uznawane za bezpieczne w świetle obecnego stanu wiedzy. Zwiększeniu ulega minimalna długość kluczy.

Postęp wiedzy kryptograficznej powoduje konieczność stałego podnoszenia poziomu bezpieczeństwa algorytmów stosowanych w zakresie podpisu elektronicznego. Prace nad bezpieczeństwem algorytmów prowadzone są przez organizacje standaryzacyjne, takie jak Europejski Instytut Standardów Telekomunikacyjnych (ETSI), które zalecają stosowanie lub odejście od stosowania danych algorytmów w określonym horyzoncie czasowym. ETSI publikuje dokument "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms (ETSI TS 102 176-1)", określany skrótowo mianem ALGO. Dokument ten nie posiada waloru normatywnego i nie obliguje państw członkowskich UE do jego stosowania, ale stanowi istotną rekomendację odnośnie bezpieczeństwa poszczególnych algorytmów dla potrzeb bezpiecznego podpisu elektronicznego. Każdy kraj we własnym zakresie podejmuje decyzję o terminie i sposobie odejścia od poszczególnych algorytmów. Jednocześnie należy zaznaczyć, że stosowanie algorytmów zgodnych z wymienioną specyfikacją techniczną jest narzucone Decyzją Komisji nr 511 z dnia 14 lipca 2003 roku[2].

Niezależnie od ww. dokumentu ETSI, każde państwo członkowskie określa, które algorytmy są adekwatne dla poszczególnych zastosowań (takich jak m.in. kwalifikowany podpis elektroniczny, znakowanie czasem). w części krajów odpowiednie agencje rządowe publikują listy algorytmów oraz okres ich ważności dla poszczególnych zastosowań (w Niemczech - BSI, w Stanach Zjednoczonych - NIST). Dokument ALGO w wersji 2.0 wskazuje na potrzebę odejścia od algorytmów SHA-1, w zakresie funkcji skrótu oraz RSA-1024, w zakresie funkcji podpisu elektronicznego. Jeśli chodzi o dopuszczalne długości kluczy algorytmu RSA do składania "nowych" podpisów (weryfikacja "starych" podpisów pozostanie w postaci niezmienionej), wg ALGO od 2010

2) „COMMISSION DECISION of 14 July 2003 on the publication of reference numbers of generally recognized standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council" (2003/511/EC)

r. powinno stosować się klucz o długości minimum 1536 i SHA-2 (można się też doszukać informacji, że od 2012 r. RSA klucz o długości minimum 2048 i oczywiście SHA-2). Dla porównania wg NIST (norm amerykańskich) 1024-bitowy klucz można stosować tylko do końca 2010 r. (łącznie z SHA-1), po tym czasie należy przejść na klucz min. 2048-bitowy oraz funkcję skrótu SHA-2.

Z przeprowadzonych przez Ministerstwo Gospodarki prac eksperckich wynika, że algorytm SHA-1 powinien zostać zastąpiony rodziną algorytmów SHA-2 (SHA-256, SHA-348, SHA-512), a algorytm RSA-1024 odpowiednio algorytmami RSA-2048 lub o długości klucza, w zależności od tego, czy chodzi o podpis składany przez użytkownika końcowego, czy też podpisy centrów certyfikacji lub tzw. root'a centralnego. Nastąpi również odejście od algorytmu RIPEMD-160, który nigdy nie zyskał popularności w obszarze podpisu elektronicznego i również nie jest rekomendowany przez ETSI. Z uwagi na konieczność ewolucyjnego zastępowania dotychczasowych kart, wydanych certyfikatów oraz aplikacji niezbędny będzie okres przejściowy, który powinien około dwóch lat, czyli w przybliżeniu do końca 2016 roku.

Rosnąca moc obliczeniowa komputerów może skutkować tym, że w najbliższych latach prawdopodobne stanie się przeprowadzanie skutecznego ataku na podpisy elektroniczne bazujące na słabych kluczach kryptograficznych. Rekomendacje ETSI zalecają stosowanie kluczy kryptograficznych RSA o długości 1024 bitów do końca 2009 r. Nowelizacja rozporządzenia aktualizuje minimalne wymagania dla algorytmów kryptograficznych, tak, aby wskazywały na parametry rekomendowane. Wprowadzenie zmian w zestawie minimalnych wymagań powoduje, że od momentu wejścia w życie rozporządzenia konieczne będzie wydawanie certyfikatów, zgodnych z nowymi wymaganiami minimalnymi. Zmiana rozmiaru klucza kryptograficznego na większy, nie powinna powodować problemów związanych z użytkowaniem aplikacji przez urzędy certyfikacji. Wprowadzenie wymagań co do długości klucza będzie mieć wpływ na rynek bezpiecznych urządzeń do składania podpisu. Wiele modeli urządzeń nie wspiera rozmiaru klucza większego niż 1024 bity. Zmiana minimalnych wymagań spowoduje konieczność stosowania takich bezpiecznych urządzeń, które wspierają wykorzystanie kluczy o długości 2048 bitów, w przypadku wydawania nowych certyfikatów. Nałożenie wymagań wyłącznie na proces wydawania certyfikatów powoduje, że po wejściu rozporządzenia w życie wymiana wydanych już urządzeń nie będzie konieczna.

W przypadku zaświadczeń certyfikacyjnych ewentualna zmiana długości klucza może nastąpić w momencie wymiany zaświadczeń związanych z wycofaniem funkcji skrótu SHA-1.

Aktualizacja profili certyfikatów i list CRL

Profil certyfikatu określa jego zawartość i strukturę. w profilu określony jest sposób umieszczania w certyfikacie danych użytkownika, oraz danych wspierających proces weryfikacji certyfikatu.

W odniesieniu do obowiązującego stanu prawnego wprowadzane są zmiany w zakresie profilu certyfikatu kwalifikowanego. w dotychczasowym stanie prawnym przy ustalaniu zawartości pola SerialNumber stosowano notację <Identyfikator>: <wartość>. w pracach na poziomie Unii Europejskiej wypracowano nową notację różniącą się od stosowanej w Polsce. w ramach profilu certyfikatu kwalifikowanego nie było obowiązkowe wprowadzanie pola identyfikującego certyfikat, jako wygenerowany w bezpiecznym urządzeniu do składania podpisu id-etsi-qcs-QcSSCD. Nie było

także regulacji umożliwiających umieszczenie w certyfikacie kwalifikowanym informacji na temat czasu przechowywania dowodów dotyczących uwierzytelnienia użytkownika na potrzeby wydania certyfikatu kwalifikowanego. w obecnym kształcie rozporządzenie zawiera w załączniku 2 zestaw specyfikacji technicznych opisujących format certyfikatu i listy CRL, którego treść jest nadmiarowa, gdyż zagadnienia te uregulowane zostały w normatywnej części rozporządzenia.

W zmienionym niniejszym rozporządzeniem stanie prawnym opisano precyzyjnie format danych, które mogą być umieszczone w polu serialNumber. Dodano także obowiązek stosowania identyfikatora id-etsi-qcs-QcSSCD w certyfikacie kwalifikowanym. Kolejną zmianą jest wykorzystanie identyfikatora id-etsi-qcs-QcRetentionPeriod chroniącego przed sytuacją utraty materiału dowodowego dotyczącego uwierzytelnienia użytkownika w przypadku wielokrotnego odnawiania certyfikatu. Specyfikacje techniczne znajdujące się w załączniku 2 zostały zastąpione odwołaniem do specyfikacji technicznej (RFC 5280). Wprost wymienione zostały wyłącznie elementy wymagające doprecyzowania.

Specyfikacja profilu certyfikatu kwalifikowanego została dostosowana do zmian wprowadzonych przez ETSI w ramach prac standaryzacyjnych wykonywanych na zlecenie Komisji Europejskiej w ramach mandatu m460. Jako źródło informacji na temat profilu certyfikatu kwalifikowanego została wskazana norma EN 319 412-5, zawierająca rozszerzenia dla profilu certyfikatu kwalifikowanego, a odwołująca się do specyfikacji technicznej TS 119 412-2opisującej profil certyfikatu dla osoby fizycznej. Zastosowanie tych specyfikacji, wprowadza dodatkowe zmiany ułatwiające przeprowadzenie procesu weryfikacji certyfikatu.

W ramach specyfikacji TS 119 412-2, do której odwołuje się specyfikacja techniczna opisująca profil certyfikatu kwalifikowanego, obowiązkowe staje się umieszczenie w certyfikacie odwołania do usługi OCSP, oraz odwołania do zaświadczenia urzędu CA wydającego certyfikat. Dzięki tym zmianom łatwiejsze staje się weryfikowanie certyfikatów oraz budowanie ścieżki certyfikacji.

Wymagania dla certyfikatu kwalifikowanego zostały doprecyzowane w celu zwiększenia interoperacyjności, oraz wprowadzenia dodatkowych identyfikatorów, innych niż PESEL, który po wycofaniu obowiązku stosowania identyfikatora NIP stał się jedynym dopuszczonym do umieszczenia w certyfikacie kwalifikowanym. Sytuacja taka jest kwestionowana przez GIODO.

W przypadku pola serialNumber znajdującego się w określeniu posiadacza certyfikatu został rozszerzony dopuszczalny zakres wartości. Dopuszczono umieszczanie w wymienionym polu numeru seryjnego paszportu lub dokumentu tożsamości. Rozszerzenie to umożliwi wydawanie certyfikatów kwalifikowanych cudzoziemcom posiadającym paszport. Dzięki tej zmianie podmioty świadczące usługi certyfikacyjne w zakresie wydawania certyfikatów w jednolity sposób będą wprowadzać dane dotyczące unikalnego numeru przypisanego użytkownikowi. Dla pola serialNumber odpowiednia składnia została zaproponowana w dokumencie TS 119 412-2, natomiast przepisy prawa doprecyzowały, które z identyfikatorów należy stosować w odniesieniu do polskich systemów numeracji. Doprecyzowano również sposób, w jaki będą wprowadzane oznaczenia numerów identyfikacyjnych charakterystycznych dla Polski. Publikacja listy numerów identyfikacyjnych została uregulowana w § 2 niniejszego rozporządzenia.

Wprowadzenie obowiązku wpisywania identyfikatora id-etsi-qcs-QcSSCD ma na celu osiągnięcie maksymalnego poziomu interoperacyjności. Dzięki zastosowaniu obu mechanizmów wskazywania,

że certyfikat kwalifikowany jest wydany dla kluczy przechowywanych na bezpiecznym urządzeniu do składania podpisu, certyfikaty wydawane przez polskich dostawców usług certyfikacyjnych będą rozpoznawane dla aplikacji stosujących dowolną z wymienionych metod.

Obowiązek umieszczania w certyfikacie rozszerzenia id-etsi-qcs-QcRetentionPeriod zawierającego informacje o okresie przechowywania informacji o weryfikacji tożsamości właściciela certyfikatu pozwala na określenie czasu odnawiania certyfikatu bez utraty możliwości weryfikacji danych dostarczonych w ramach tego procesu.

W załączniku 2 obowiązującego rozporządzenia nie zostały wydzielone wymagania dla zaświadczeń certyfikacyjnych. Merytorycznie wymagania nie uległy istotnej zmianie, wskazano natomiast dokument techniczny, zamiast określania szczegółowych zapisów. Wprowadzono wymóg, aby zaświadczenie certyfikacyjne zawierało rozszerzenie wskazujące na usługę udostępniania list certyfikatów unieważnionych (tzw. CRL Distribution Points) oraz wskazanie na zaświadczenie urzędu CA wydającego certyfikat.

Wprowadzono także do zaświadczeń obowiązek stosowania identyfikatorów klucza podmiotu i wydawcy zaświadczenia. Odpowiednie struktury były do tej pory włączane do certyfikatu na zasadzie dobrych praktyk.

Zmiany w przepisach związane z wymaganiami dla list CRL są podyktowane troską o przejrzystość przepisów. Merytorycznie wymagania nie uległy zmianie, wskazano natomiast dokument techniczny, zamiast przenoszenia części tego standardu do treści załącznika 2 rozporządzenia.

Dostosowanie wszystkich aplikacji dostępnych na rynku, do decyzji z dnia 25 lutego 2011 w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym, jest działaniem nieracjonalnym ze względu na fakt, że niektóre z aplikacji mogą obsługiwać tylko jeden format podpisu elektronicznego, bez utraty funkcjonalności i utrudnień dla użytkowników. w celu upowszechnienia specyfikacji referencyjnego formatu podpisu, nałożono na podmioty świadczące kwalifikowane usługi certyfikacyjne obowiązek oznaczania na publikowanym wykazie bezpiecznych urządzeń do składania i weryfikacji podpisu tych, które potrafią obsługiwać referencyjne formaty podpisu. Rozwiązanie takie umożliwi osobie nabywającej zestaw z certyfikatem kwalifikowanym świadomy wybór, uwzględniający potrzebę kontaktów z administracją publiczną.

Dopuszczenie nowych formatów podpisu elektronicznego

Obecne przepisy nie uwzględniają nowego standardu podpisu elektronicznego (PAdES). Prace ETSI nad jego specyfikacją techniczną zostały zakończone w lipcu 2009 r., a więc po wejściu w życie przedmiotowego rozporządzenia. Nowelizacja rozporządzenia dopuszcza stosowanie w obszarze kwalifikowanego podpisu elektronicznego formatu określonego przez specyfikację techniczną ETSI TS 102 778 (PAdES). Standard ten dotyczy opatrywania podpisem elektronicznym plików Portable Document Format (PDF). Umożliwia m.in. długookresową walidację podpisu elektronicznego oraz jest rekomendowany przez Komisję Europejską, jako jeden z formatów podpisu możliwych do wykorzystania w usługach transgranicznych. Innym formatem, który jest rekomendowany przez

Komisję Europejską jako format podpisu zaawansowanego, jest format ASiC. Wprowadzenie specyfikacji ETSI TS 102 918 – Associated Signature Containers (ASiC) umożliwi tworzenie podpisów dokumentów w formacie kontenerowym takim jak np. Zip. Inne rekomendowane formaty to XAdES i CAdES, które zostały dopuszczone uprzednio przepisami przedmiotowego rozporządzenia.

Przepisy zawarte w projekcie nowelizacji rozporządzenia nie stanowią bezpośredniej transpozycji przepisów objętych przedmiotem regulacji prawa wspólnotowego, stanowią jednak przesłankę do zafunkcjonowania w krajowym porządku prawnym decyzji wykonawczej Komisji z dnia 17 marca 2014 r. *zmieniającej decyzję Komisji 2011/130/UE w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym.*

W § 2 niniejszego projektu wskazano, że rozporządzenie wchodzi w życie z dniem 1 grudnia 2014 r., co odbiega od terminów wskazanych w § 1 ust. 1 Uchwały Rady Ministrów Nr 20 z dnia 18 lutego 2014 r. *w sprawie zaleceń ujednolicenia terminów wejścia w życie niektórych aktów normatywnych* (M.P. poz. 205). Powyższe odstąpienie od ww. terminów nastąpiło jednak zgodnie z § 1 ust. 2 przedmiotowej Uchwały, poprzez wzgląd na interes publiczny polegający na zapewnieniu funkcjonowania wymienionej decyzji wykonawczej Komisji z dnia 17 marca 2014 r.

Projekt podlega notyfikacji w trybie przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w *sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych* (Dz. U. Nr 239, poz. 2039, z późn. zm.).

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 o działalności lobbingowej w procesie stanowienia prawa (Dz. U. Nr 169, poz. 1414 oraz z 2009 r. Nr 42, poz. 337) projekt rozporządzenia zostanie umieszczony w BIP Ministerstwa Gospodarki oraz zgodnie z §52 Regulaminu pracy Rady Ministrów (M.P. z 2013 r. poz. 979) w serwisie RPL na stronie Rządowego Centrum Legislacji.

Ocena Skutków Regulacji

Nazwa projektu Projekt rozporządzenia Rady Ministrów zmieniającego rozporządzenie 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 **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Gospodarki **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Podsekretarz Stanu Dariusz Bogdan **Kontakt do opiekuna merytorycznego projektu** Marcin Fijałkowski, Radca Ministra DGE MG, marcin.fijalkowski@mg.gov.pl, tel: +48 22 693 52 82	**Data sporządzenia** 24 kwietnia 2014 r. **Źródło:** art. 10 ust. 4, art. 17 ust. 2 i art. 18 ust. 3 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz 262) **Nr w wykazie prac legislacyjnych Rady Ministrów** RD25

1. Jaki problem jest rozwiązywany?

Rozporządzenie dostosowuje obowiązujące regulacje w zakresie podpisu elektronicznego do rekomendacji Europejskiego Instytutu Standardów Telekomunikacyjnych (ETSI) wskazujących bezpieczne i zalecane do wykorzystania na potrzeby podpisów elektronicznych funkcje skrótu oraz algorytmy szyfrowe. Istniejącym aktualnie problemem jest dopuszczanie przez Polskę możliwości stosowania na potrzeby generowania podpisów elektronicznych takich algorytmów szyfrowych (RSA o minimalnej długości klucza 1020 bitów, DSA o minimalnej długości klucza 1024 bitów, ECDSA i ECGDSA o minimalnej długości klucza 160 bitów) i funkcji skrótu (SHA-1, RIPEMD-160), które w świetle obecnej wiedzy nie są uznawane za zapewniające wystarczające bezpieczeństwo. Ze względu na potencjalną możliwość przeprowadzenia zakończonego sukcesem ataku na usługi wykorzystujące wskazane standardy, ETSI zalecił stosowanie od początku roku 2012 wyłącznie algorytmów szyfrowych o kluczach długości co najmniej 2048 bitów i funkcji skrótu nie słabszych niż SHA-2.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Z uwagi na fakt, że funkcja SHA-1 była w praktyce jedyną funkcją skrótu stosowaną w certyfikatach kwalifikowanych, konieczne jest zaktualizowanie produktów wykorzystujących tę funkcję. Rozporządzenie realizuje podejście ewolucyjne dopuszczając przejściowe wydawanie certyfikatów weryfikujących się w ścieżce wykorzystującej dotychczasowe algorytmy. Wykorzystanie funkcji SHA-1 (i ewentualnie RIPEMD160) do składania podpisów zostało dopuszczone do dnia wygaśnięcia certyfikatów wykorzystujących te funkcje. Zastosowanie okresu przejściowego pozwoli zminimalizować uciążliwość zmiany dla osób, które zakupiły zestawy do składania bezpiecznego podpisu elektronicznego. Przyjęcie takiej opcji regulacyjnej pozwoli uniknąć użytkownikom podpisu elektronicznego kosztu zakupu nowych certyfikatów i kart kryptograficznych przed upływem ważności kart dotychczasowych. W miarę upływu ważności dotychczasowych certyfikatów osoby odnawiające certyfikat kwalifikowany kupować będą certyfikaty oraz karty obsługujące nowe algorytmy.

Alternatywną opcją regulacyjną jest zmiana polegająca na unieważnieniu aktualnych certyfikatów kwalifikowanych, co nieuchronnie związane byłoby z koniecznością przyspieszenia zakupu przez użytkownika końcowego nowego certyfikatu kwalifikowanego oraz karty wspierającej nowe algorytmy. Wybór tego wariantu może być argumentowany faktem, że z uwagi na rosnące ryzyko związane z wykorzystaniem słabości funkcji skrótu SHA-1, konieczne jest zaprzestanie jej wykorzystania w obszarze bezpiecznego podpisu elektronicznego. Rekomendacje ETSI[3] zalecały stosowanie SHA-1 do końca 2009 r.

3) ETSI TS 102 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

Przekroczenie tego okresu nie oznacza jednak, że po tym okresie możliwe jest fałszowanie podpisów opartych na wymienionej funkcji skrótu. Na chwilę obecną nie został udokumentowany atak polegający na semantycznie sensownej podmianie certyfikatu lub podpisanego elektronicznie dokumentu z wykorzystaniem kolizji funkcji skrótu SHA-1. Z tego względu wybrano opcję z zastosowaniem okresu przejściowego oraz wydłużeniem okresu stosowania dotychczasowych algorytmów. Zaproponowany sposób wycofywania funkcji skrótu powoduje, że bezpieczne urządzenia do składania podpisu wykorzystujące wyłącznie funkcję SHA-1 będą wycofywane z rynku stopniowo, w miarę wygasania certyfikatów wykorzystujących tę funkcję skrótu.

Opcja regulacyjna polegająca na powstrzymaniu się od wprowadzenia regulacji nie może znaleźć zastosowania. W naszym kraju algorytmy podpisu oraz funkcji skrótu publikowane są w rozporządzeniu Rady Ministrów z dnia 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* (Dz. U. z 2002 r., nr 128, poz. 1094). Zmiana algorytmów w zakresie krajowej infrastruktury klucza publicznego wymagać będzie zmiany rozporządzenia. Nowelizacja rozporządzenia stanowi przesłankę do działań organizacyjnych, które służyć będą implementacji zmiany algorytmów w krajowej infrastrukturze klucza publicznego, jak również infrastrukturze informatycznej administracji i gospodarki. Mogłoby się wydawać, że w przypadku dostawców usług, rynek powinien sam wymusić odpowiednie dostosowania, jednakże rozwiązania przez nich proponowane muszą być dostosowane do rozwiązań podmiotów akceptujących podpisy elektroniczne, w tym głównie do usług oferowanych przez jednostki administracji publicznej. Mechanizmy rynkowe nie są więc w tym przypadku wystarczające.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Główna zmiana wprowadzana przedmiotowym rozporządzeniem, polegająca na wycofaniu przestarzałych funkcji skrótu i algorytmów szyfrowych, oparta jest na okresowo aktualizowanych standardach i rekomendacjach organizacji standaryzacyjnych, takich jak Europejski Instytutu Standardów Telekomunikacyjnych (ETSI). Czas oraz sposób ich wdrożenia pozostają jednak w gestii poszczególnych państw. Niemniej, państwa w których funkcjonują podpisy elektroniczne powinny dostosować swoje prawo, o ile chcą zapewnić użytkownikom tych podpisów odpowiedni poziom bezpieczeństwa i zaufania wobec usług obecnych na rynku.

Przykładem państwa, które rozwiązało ten problem w taki sam sposób jest Słowacja.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty krajowej infrastruktury klucza publicznego	Narodowe Centrum Certyfikacji oraz kwalifikowane podmioty świadczące usługi certyfikacyjne w zakresie podpisu elektronicznego. W sumie 5 podmiotów.	http://www.nccert.pl/podmioty3.htm	Obok certyfikatów kwalifikowanych, funkcja skrótu SHA-1 była wykorzystywana również przy wydawaniu zaświadczeń certyfikacyjnych. Wycofanie jej spowoduje, że konieczna będzie wymiana zaświadczeń certyfikacyjnych znajdujących się w ścieżce certyfikacji certyfikatu kwalifikowanego. Wydanie nowych zaświadczeń certyfikacyjnych musi nastąpić przed dniem wskazanym jako wycofanie funkcji skrótu SHA-1. Wprowadzenie nowych algorytmów spowoduje konieczność zakupu sprzętowych modułów bezpieczeństwa. Nowe moduły HSM zakupiły dotychczas Narodowe Centrum Certyfikacji oraz jeden z pięciu podmiotów kwalifikowanych. Infrastruktura pozostałych podmiotów kwalifikowanych będzie wymagać dodatkowych inwestycji w tym

			zakresie.
Urzędy centralne	Ok. 250 urzędów centralnych i organów administracji podległych Prezesowi Rady Ministrów, Radzie Ministrów lub jej członkom (w sumie 16 organom nadrzędnym)	http://pl.wikipedia.org/wiki/Spis_urzędów_centralnych_w_Polsce	Ze względu na dotychczasowe uregulowania prawne, systemy wykorzystujące podpis elektroniczny mogą nie być dostosowane do weryfikacji podpisów elektronicznych, oraz ścieżki certyfikacji wykorzystującej nowe funkcje skrótu. Problem ten może być szczególnie dotkliwy w przypadku instytucji takich jak ZUS, wykorzystujących bezpieczny podpis elektroniczny na dużą skalę. Inne systemy w których stosowany jest bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem to m.in. ePUAP, KRS oraz GIIF. Obsługę bezpiecznego podpisu elektronicznego zawiera również większość Elektronicznych Skrzynek Podawczych. Konieczne jest dostosowanie obsługi systemów do weryfikacji podpisów wykorzystujących nowe funkcje skrótu. Zmiana formatu pola certyfikatu dotyczącego danych PESEL może spowodować konieczność dostosowania systemów wykorzystujących certyfikaty kwalifikowane do pozyskiwania danych o tożsamości obywatela, takich jak ePUAP. Implementacja zmian może wymagać czasu na przeprowadzenie procedur przetargowych, opracowanie aktualizacji oprogramowania oraz przeprowadzenie niezbędnych testów. z tego względu najdłuższy okres przygotowawczy należy przewidzieć dla modernizacji systemów informatycznych firm i instytucji.
Producenci aplikacji mających funkcjonalność składania lub weryfikowania podpisu elektronicznego		Raport z testów interoperacyjności podpisu elektronicznego *CommonSign Warsaw 2012*	
Użytkownicy podpisu elektronicznego	288 544 aktywnych certyfikatów kwalifikowanych (dane zbiorcze skumulowane w dn. 14.04.2014 r.)	Comiesięczne badanie rynku prowadzone przez Departament Gospodarki Elektronicznej MG wśród podmiotów kwalifikowanych Wyniki zestawienia aktualizowane pod adresem: http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Dzi	Przyjęty w rozporządzeniu wariant wymiany algorytmów kryptograficznych pozwoli na zminimalizowanie wpływu na użytkownika końcowego podpisu elektronicznego. Subskrybent, który w związku z upływem ważności poprzedniego certyfikatu kwalifikowanego zdecyduje się na odnowienie certyfikatu otrzyma

		alalnosc+gospodarcza+i+e-przedsiebiorczosc/Podpis+elektroniczny	certyfikat kwalifikowany oraz kartę wspierającą nowe algorytmy. Z punktu widzenia użytkownika końcowego zmiany wymagać będzie aplikacja do składania i weryfikacji podpisu elektronicznego. Aplikacje do składania i weryfikacji bezpiecznego podpisu elektronicznego wykorzystujące nowe biblioteki kryptograficzne zapewnią kwalifikowane podmioty świadczące usługi certyfikacyjne.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Z uwagi na pilność prowadzonych prac konsultacje będą trwały przez minimalny przewidziany prawem okres 21 dni. W tym czasie zebrane zostaną uwagi branży usług certyfikacyjnych (Enigma SOI, EuroCert, KIR, PWPW, Unizeto Technologies), jednostek badawczych (IMM, ILIM, Narodowe Centrum Kryptologii) oraz izb gospodarczych (PIIT, KIGEIT, eCommerce Polska - Izba Gospodarki Elektronicznej). Niezbędne jest również uwzględnienie niezależnych deweloperów aplikacji do składania i weryfikacji podpisu elektronicznego, takich jak np. PEMI (Protektor), COMARCH (SOPEL) lub ZETO (CEIDG).

Z punktu widzenia prowadzonych konsultacji publicznych istotne jest, aby przedsiębiorcy mogli dokonać oceny merytorycznej prawidłowości i realności zaproponowanych terminów wprowadzenia zmian. Poprzez proces konsultacji publicznych rozpropagowana zostanie również wiedza o tym, że konieczne będzie z wyprzedzeniem dostosowanie aplikacji e-podpisowych do zmian wprowadzanych przepisami. Z punktu widzenia urzędu przygotowującego przedmiotową regulację wskazane będzie wykorzystanie konsultacji do zebrania także dodatkowych informacji o kosztach wprowadzanej zmiany. W konsultacjach zostaną uwzględnione reprezentatywne organizacje pracodawców i organizacje samorządu terytorialnego (Związek Miast Polskich, Związek Gmin Wiejskich RP).

W podsumowaniu wyników konsultacji stwierdzić należy, że konieczność wprowadzenia zmian w zakresie algorytmów oraz profili certyfikatów została przesądzana zmianami w standardach europejskich. Analogiczne zmiany w zakresie wzmocnienia siły algorytmów kryptograficznych wprowadzane są również poza Unią Europejską (np. przez NIST w standardach FIPS). Istotne jest zatem nie to czy należy wprowadzać zmianę, ale jak zmiana powinna być wprowadzana.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**-7**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**-7**
budżet państwa	7	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**-7**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**-7**
budżet państwa	-7	0	0	0	0	0	0	0	0	0	0	-7

JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Koszty niezbędnych dostosowań systemów informatycznych, wymiany odpowiednich komponentów, czy urządzeń umożliwiających korzystanie z silniejszych niż dotychczas funkcji skrótu i algorytmów szyfrowych będą ponoszone przez jednostki dostosowujące. Uchwalenie przedmiotowego rozporządzenia zapewni niezbędną podstawę prawną do zapotrzebowania środków niezbędnych na przeprowadzenie prac informatycznych przez ministerstwa i urzędy. Wydatki te posiadają charakter konieczny z uwagi na powszechne odejście od dotychczasowych algorytmów w zakresie podpisu elektronicznego oraz wzrastające ryzyko związane z wykorzystaniem kwalifikowanych podpisów opartych na przestarzałych algorytmach.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Rozporządzenie będzie wywierać wpływ na budżet państwa. Z uwagi na brak przekrojowej informacji na temat wszystkich systemów wykorzystujących w administracji publicznej mechanizmy podpisywania i weryfikacji podpisu elektronicznego informacje dotyczące ewentualnych skutków dla budżetu zostały przedstawione wyłącznie w takim zakresie, w jakim urzędy odpowiedziały na pytania w tej sprawie skierowane przez Ministra Gospodarki. Podkreślić należy, że koszt implementacji nowych algorytmów będzie różny w zakresie poszczególnych rozwiązań z uwagi na ich różnorodność. Zmiana algorytmów w zakresie Elektronicznej Skrzynki Podawczej może nie być związana z dodatkowymi kosztami, jeśli zakup oprogramowania uprawnia do korzystania z aktualizacji producenta. Zmiana aplikacji do składania i weryfikacji podpisu elektronicznego dostarczanych wraz z zestawem do składania bezpiecznego podpisu elektronicznego będzie również mogła następować nieodpłatnie. W przypadku mechanizmów walidacji serwerowej lub dedykowanych aplikacji do składania podpisu elektronicznego sytuacja będzie zróżnicowana w zależności od tego, czy wykorzystane prace informatyczne prowadzone będą we własnym zakresie, czy też niezbędne będzie zlecenie zewnętrznych prac informatycznych. Wiele podmiotów administracji publicznej korzysta wyłącznie z usług zewnętrznych usługodawców w zakresie podpisu elektronicznego, co tym samym przenosi zadanie adaptowania nowych rozwiązań na podmioty zewnętrzne. w takiej sytuacji są m.in. Ministerstwo Sportu i Turystyki, a także Ministerstwo Skarbu Państwa, Ministerstwo Edukacji Narodowej, Polska Agencja Rozwoju Przedsiębiorczości, Główny Urząd Nadzoru Budowlanego, Główny Urząd Miar, Urząd Komunikacji Elektronicznej. Centrum Projektów Informatycznych MAiC, sprawujące pieczę nad systemem ePUAP szacuje koszt dostosowania tej platformy do algorytmów RSA2048 i SHA-2 na ok. 1 000 000 zł. Ministerstwo Sprawiedliwości szacuje koszt dostosowania aplikacji w Krajowym Rejestrze Sądowym oraz Rejestrze Zastawów, połączony z wymianą ok. 200 podpisów elektronicznych na ok. 500 000 zł. W przypadku zmian w rozwijanej przez Urząd Patentowy platformie Internetowego Portalu Usług koszty dostosowania tego systemu do obsługi SHA-2 i RSA2048 wykonawca zewnętrzny szacuje na 120 000 zł, zaś czas modernizacji ma wynieść 3 miesiące. Zmiany w Elektronicznej Skrzynce Podawczej Kancelarii Prezesa Rady Ministrów kosztować będą ok. 20 000 zł. Rządowe Centrum Legislacji ocenia koszty wdrożenia nowych algorytmów na 3606 zł. przy okresie prac nie przekraczającym 5 dni. Ministerstwo Rolnictwa i Rozwoju Wsi szacuje koszt wdrożenia nowych algorytmów w podpisach elektronicznych na ok. 32 000 zł, z zastrzeżeniem dwuletniego okresu wdrożenia – w takim przypadku nie byłoby dodatkowych kosztów dla dwóch jednostek podległych Ministerstwu. Ministerstwo Kultury i Dziedzictwa Narodowego szacuje koszt dostosowania na ok. 20 000 zł. Zainstalowane w systemie informatycznym Narodowego Centrum Certyfikacji oprogramowanie oraz sprzętowe moduły bezpieczeństwa obsługują nowe algorytmy kryptograficzne wskazane w projekcie rozporządzenia. Powoduje to, iż zmiany w zakresie zaświadczeń certyfikacyjnych nie spowodują kosztów po stronie NBP.

	Wpływ rozporządzenia na budżety jednostek samorządu terytorialnego nie będzie znaczący. Większość rozwiązań wykorzystywanych w jednostkach samorządu terytorialnego to aplikacje, które bezkosztowo aktualizowane są przez ich dostawców. Samorządy nie dysponują bardzo złożonymi dedykowanymi systemami obsługującymi podpisy elektroniczne. Zakładamy więc, że zmiana obowiązujących regulacji nie wpłynie znacząco na bieżące koszty ponoszone przez te jednostki.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z ..... r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	W związku z koniecznością dostosowania systemów wykorzystywanych do generowania lub weryfikacji podpisów elektronicznych do nowych wymagań, ilość zamówień na usługi i produkty w ramach tego obszaru może zanotować jednorazowy wzrost.						
	sektor mikro-, małych i średnich przedsiębiorstw	W związku z koniecznością dostosowania systemów wykorzystywanych do generowania lub weryfikacji podpisów elektronicznych do nowych wymagań, ilość zamówień na usługi i produkty w ramach tego obszaru może zanotować jednorazowy wzrost.						
	rodzina, obywatele oraz gospodarstwa domowe	Rozporządzenie zawiera odpowiednie okresy przejściowe.						

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Zmiana nie wpływa znacząco na konkurencyjność gospodarki. Należy jednak zaznaczyć, że bezczynność w kwestii objętej regulacją może pociągnąć za sobą negatywne skutki dla sektora elektronicznych usług zaufania. Mimo, iż do tej pory nie został przeprowadzony żaden udany atak na podmiot posługujący się podpisem elektronicznym wykorzystującym wycofywane funkcje skrótu SHA-1 i RIPEMD-160 oraz algorytmy szyfrowe o kluczu długości 1020 lub 1024 bitów, to atak taki uważa się za potencjalnie możliwy. Zagrożenie rośnie wraz ze wzrostem mocy obliczeniowej komputerów i rozwojem wiedzy kryptograficznej. Związany ze wzrostem zagrożenia spadek pewności co do autentyczności i integralności podpisywanych danych może mieć wpływ na spowolnienie rozwoju elektronicznych usług zaufania w Polsce.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Zmiana dopuszczalnych funkcji skrótu i algorytmów szyfrowych ma na celu poprawę bezpieczeństwa stosowanych obecnie podpisów elektronicznych. Nie są wprowadzane żadne dodatkowe obciążenia regulacyjne w stosunku do stanu obecnego.

9. Wpływ na rynek pracy

Wpływ regulacji na rynek pracy poprzez dodatkowe zamówienia na usługi informatyczne będzie nieznaczny. W większości przypadków zmiana nie spowoduje utworzenia nowych miejsc pracy.

10. Wpływ na pozostałe obszary

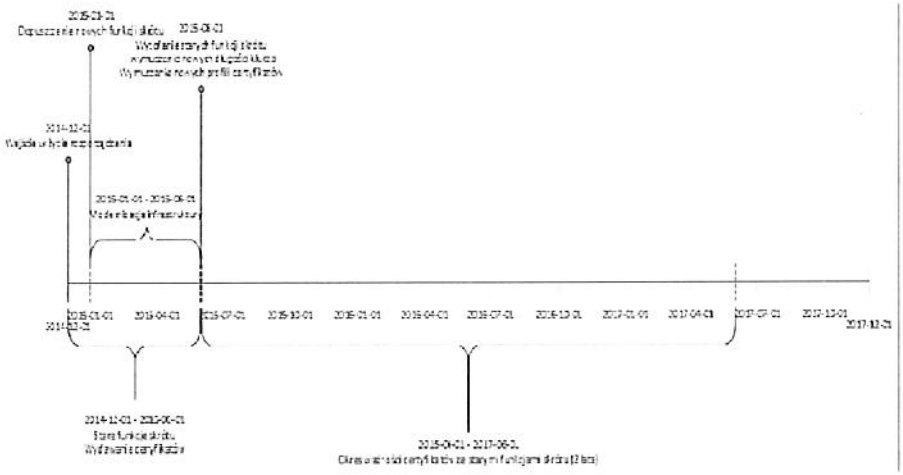
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Nie dotyczy.

11. Planowane wykonanie przepisów aktu prawnego

Nowe regulacje wejdą w życie 1 grudnia 2014 r. Zgodnie z decyzją wykonawczą Komisji z dnia 17 marca 2014 r. *zmieniającą decyzję Komisji 2011/130/UE w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym* od dnia 1 grudnia 2014 r. funkcje skrótu i algorytmy, które utraciły rekomendację ETSI nie będą mogły być dłużej stosowane. W celu składania poświadczeń elektronicznych w ścieżce certyfikacji wycofywane funkcje skrótu i algorytmy będą mogły być wykorzystywane do 31 maja 2015 r. Od planowanego momentu uchwalenia rozporządzenia pozostaje więc rok na wprowadzenie wymaganych zmian przez odpowiednie podmioty. Rozporządzenie zawiera jednak szereg okresów przejściowych, zmniejszających obciążenia dla akceptantów podpisów elektronicznych i ich użytkowników. Wycofywanych funkcji skrótu będzie można nadal używać:

- dla składania bezpiecznego podpisu elektronicznego – do 31 grudnia 2016 r.;
- dla składania poświadczeń elektronicznych pod listami certyfikatów unieważnionych wydawanych przez urząd certyfikacji – do dnia wygaśnięcia zaświadczenia certyfikacyjnego tego urzędu;
- dla weryfikacji złożonych poświadczeń elektronicznych lub bezpiecznych podpisów elektronicznych – bezterminowo.



12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Istotą proponowanej regulacji jest dostosowanie polskiego prawa do europejskich i międzynarodowych norm i standardów dla funkcji skrótu i algorytmów szyfrowych wykorzystywanych do generowania podpisów elektronicznych. Ewaluacja ex-post nie jest zasadna, gdyż rozporządzenie bezwzględnie wymusza porzucenie rozwiązań, które utraciły rekomendację, przez dostawców usług podpisu elektronicznego oraz ich akceptantów.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Algorytmy i parametry dla bezpiecznych podpisów elektronicznych
http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/02.01.01_60/ts_10217601v020101p.pdf v 2.1.1.

Profile dla dostawców usług zaufania wydających certyfikaty; Część 5 profil certyfikatu dla certyfikatów wydawanych dla osób fizycznych. TS 119 412-2 v 1.2.1
http://www.etsi.org/deliver/etsi_ts/119400_119499/11941202/01.02.01_60/ts_11941202v010201p.pdf

Profile dla dostawców usług zaufania wydających certyfikaty; Część 5 Rozszerzenia dla profilu certyfikatu kwalifikowanego EN 319 412-5 v 1.1.1
http://www.etsi.org/deliver/etsi_en/319400_319499/31941205/01.01.01_60/en_31941205v010101p.pdf

Polityki i wymagania bezpieczeństwa dla dostawców usług zaufania wydających certyfikaty; Część 2 wymagania polityk dla wydawców certyfikatów wydających certyfikaty kwalifikowane. EN 319 411-2 v 1.1.1.
http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/01.01.01_60/en_31941102v010101p.pdf

Podstawowy profil XAdES ETSI TS 103 171 v.2.1.1
http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf

Podstawowy profil CAdES ETSI TS 103 173 v.2.2.1
http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf

Podstawowy profil PAdES ETSI TS 103 172 v.2.2.2
http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Podstawowy profil podpisu w formacie ASiC ETSI TS 103 174 v.2.2.1
http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf