

**ROZPORZĄDZENIE**  
**MINISTRA SPRAW WEWNĘTRZNYCH I ADMINISTRACJI<sup>1)</sup>**

z dnia 27 listopada 2006 r.

**w sprawie sporządzania i doręczania pism w formie dokumentów elektronicznych**

Na podstawie art. 39<sup>1</sup> § 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071, z późn. zm.<sup>2)</sup>) zarządza się, co następuje:

**§ 1.**

Rozporządzenie określa:

- 1) strukturę i sposób sporządzania pism w formie dokumentów elektronicznych;
- 2) warunki organizacyjno-techniczne doręczania pism w formie dokumentów elektronicznych, w tym formę urzędowego poświadczenia odbioru tych pism przez ich adresata;
- 3) sposób udostępniania kopii dokumentów elektronicznych.

**§ 2.**

Określenia użyte w rozporządzeniu oznaczają:

- 1) struktura logiczna dokumentu elektronicznego - sposób ułożenia informacji w dokumencie elektronicznym zdefiniowany poprzez określenie elementów informacyjnych tego dokumentu oraz powiązań między nimi;

---

<sup>1)</sup> Minister Spraw Wewnętrznych i Administracji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 lipca 2006 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych i Administracji (Dz. U. Nr 131, poz. 919).

<sup>2)</sup> Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2001 r. Nr 49, poz. 509, z 2002 r. Nr 113, poz. 984, Nr 153, poz. 1271 i Nr 169, poz. 1387, z 2003 r. Nr 130, poz. 1188 i Nr 170, poz. 1660, z 2004 r. Nr 162, poz. 1692 oraz z 2005 r. Nr 64, poz. 565 i Nr 78, poz. 682.

- 2) struktura fizyczna dokumentu elektronicznego – wynik przetworzenia, w tym kodowania i szyfrowania, informacji zawartych w dokumencie elektronicznym na dane w układzie bitowym (format danych);
- 3) wyróżnik – element struktury logicznej dokumentu elektronicznego służący do automatyzacji obsługi pism w formie elektronicznej, a w szczególności pozwalający na automatyczne ich przekazywanie według kompetencji właściwym organom;
- 4) zakres użytkowy dokumentu elektronicznego – zawartość dokumentu elektronicznego zdefiniowana przez określenie struktury logicznej dokumentu elektronicznego zgodnie z wymaganiami wynikającymi z przepisów prawa oraz rodzaju spraw załatwianych przez podmiot publiczny;
- 5) urzędowe poświadczenie odbioru - dane elektroniczne dołączone do doręczanego pisma w formie dokumentu elektronicznego lub połączone z tym dokumentem w taki sposób, że jakakolwiek późniejsza zmiana dokonana w tym dokumencie jest rozpoznawalna.

### § 3.

1. Pisma w formie dokumentów elektronicznych oraz urzędowe poświadczenie odbioru sporządza się w strukturach fizycznych dokumentów elektronicznych w formie zgodnej z formatami danych, określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 i z 2006 r. Nr 12, poz. 65 oraz Nr 73, poz. 501) „zwana dalej ustawą o informatyzacji” i podpisuje bezpiecznym podpisem elektronicznym.
2. Sporządzone przez organy administracji publicznej pisma w formie dokumentów elektronicznych powinny zostać opatrzone danymi pozwalającymi na ustalenie ważności certyfikatów kwalifikowanych w momencie złożenia bezpiecznego podpisu elektronicznego oraz czasu dokonania jego weryfikacji zgodnie ze specyfikacją techniczną ETSI TS 101 903 1.3.2 lub nowszą.
3. Przy sporządzaniu pism w formie dokumentu elektronicznego wykorzystuje się wzory dokumentów elektronicznych, które zawierają wyróżnik określający szczegółowo zakres użytkowy dokumentu elektronicznego.
4. Minister właściwy do spraw informatyzacji tworzy i udostępnia organom administracji publicznej centralne repozytorium wzorów pism w formie dokumentów elektronicznych. W centralnym repozytorium umieszcza się, przechowuje i udostępnia wzory pism, które:

- 1) spełniają wymagania określone w przepisach wydanych na podstawie art. 16 ust. 3 ustawy o informatyzacji;
  - 2) spełniają wymagania określone w przepisach wydanych na podstawie art. 18 pkt 1 ustawy o informatyzacji;
  - 3) uwzględniają niezbędne elementy struktury dokumentów elektronicznych określone w przepisach wydanych na podstawie art. 5 ust. 2a ustawy o narodowym zasobie archiwalnym i archiwach.
5. Organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory pism w formie dokumentów elektronicznych. Przy sporządzaniu wzorów pism stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej z uwzględnieniem konieczności podpisywania ich bezpiecznym podpisem elektronicznym. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej zasady tworzenia wyróżników, o których mowa w ust. 3.
6. Niezależnie od obowiązku wynikającego z ust. 5 organy administracji publicznej mogą prowadzić własne lub wspólnie z innymi organami administracji publicznej repozytoria wzorów pism w formie dokumentów elektronicznych.
7. Jeżeli wzór podania określają odrębne przepisy, to umieszczenie wzoru dokumentu elektronicznego przez organy administracji publicznej w centralnym repozytorium jest równoznaczne z określeniem wzoru wnoszenia podań – pism w postaci dokumentu elektronicznego, o którym mowa w art. 63 § 3a ust. 2 k.p.a.

#### **§ 4.**

1. W celu doręczenia pisma w formie dokumentu elektronicznego organ administracji publicznej przesyła na adres elektroniczny adresata informację zawierającą:
  - 1) wskazanie, że adresat może odebrać pismo w formie dokumentu elektronicznego;
  - 2) wskazanie adresu elektronicznego (skrytki), z którego adresat może pobrać pismo i pod którym powinien dokonać potwierdzenia doręczenia pisma;
  - 3) pouczenie dotyczące sposobu odbioru pisma, a w szczególności sposobu autoryzacji pod wskazanym adresem elektronicznym oraz informacji o wymogu podpisania urzędowego poświadczenia odbioru bezpiecznym podpisem elektronicznym.
2. Autoryzacja pod wskazanym adresem elektronicznym następuje poprzez podanie kodu dostępu, którym może być w szczególności indywidualny identyfikator, hasło lub

certyfiakat cyfrowy, autoryzowane przez organ administracji publicznej, lub za pomocą bezpiecznego podpisu elektronicznego i związanego z nim certyfikatu kwalifikowanego adresata pisma.

3. Po prawidłowo zakończonym procesie autoryzacji adresat pisma potwierdza odebranie pisma poprzez opatrzenie urzędowego poświadczenia odbioru bezpiecznym podpisem elektronicznym.
4. **Urzędowe poświadczenie odbioru określa:**
  - 1) **pełną nazwę podmiotu wystawiającego poświadczenie;**
  - 2) **pełną nazwę podmiotu, któremu doręcza się dokument elektroniczny (adresata);**
  - 3) **datę i czas podpisania bezpiecznym podpisem elektronicznym urzędowego poświadczenia odbioru oraz datą odbioru wpisaną przez adresata;**
  - 4) **oznaczenie sprawy;**
  - 5) **oznaczenie pisma, którego dotyczy.**
5. Po opatrzeniu bezpiecznym podpisem elektronicznym system teleinformatyczny służący do obsługi doręczeń pism udostępnia do pobrania pismo wraz z urzędowym poświadczeniem odbioru, nie później niż w ciągu 10 sekund od zakończenia procesu weryfikacji bezpiecznego podpisu elektronicznego adresata.
6. System teleinformatyczny służący do obsługi doręczeń pism zapisuje dane niezbędne do określenia czasu wystawienia urzędowego poświadczenia odbioru oraz odbioru pism.
7. Do przesyłania kodów dostępu, pism oraz potwierdzania doręczeń organy administracji publicznej wykorzystują bezpieczny kanał komunikacji oparty na jednym z protokołów określonych przepisami wydanymi na podstawie art. 18 pkt 1 ustawy o informatyzacji albo na protokole https oraz zapisują dane niezbędne do określenia czasu wysłania oraz dotarcia pisma do komputera adresata.
8. System teleinformatyczny służący do obsługi doręczeń pism, zapewnia oznaczanie pism w postaci dokumentów elektronicznych danymi stwierdzającymi ważność kwalifikowanych certyfikatów i czas ich weryfikacji. Przy dokonywaniu oznaczeń za pomocą systemu teleinformatycznego należy:
  - 1) spełniać, co najmniej, wymagania zgodnie z normą Europejskiego Instytutu Standaryzacyjnego CEN-CWA 14167-1 (marzec 2003) lub nowszą;
  - 2) wykorzystywać bezpieczne moduły kryptograficzne (HSM), spełniające wymagania normy FIPS 140-2 poziom 3 lub CEN-CWA 14167-2 lub nowszą, w szczególności poprzez:

- a) zapewnienie generowania i przechowywania materiału kryptograficznego służącego do oznaczania danymi stwierdzającymi ważność certyfikatów kwalifikowanych,
  - b) ochronę przed nieuprawnionym dostępem, w bezpiecznej obudowie odpornej na nieuprawnioną ingerencję z zewnątrz,
  - c) zabezpieczenie przed nieuprawnioną ingerencją przez zniszczenie materiału kryptograficznego w przypadku jej wykrycia,
- 3) wykorzystywać urządzenia udostępniające urzędowy koordynowany czas UTC(PL) zgodnie z rozporządzeniem Ministra Gospodarki z dnia 19 marca 2004 w sprawie sposobów rozpowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL);
- 4) wykorzystywać algorytmy szyfrowe z długością klucza co najmniej 2040 bitów.

## § 5.

1. Organ administracji publicznej wykorzystuje do doręczania pism w formie dokumentu elektronicznego system teleinformatyczny, spełniający wymagania techniczne i organizacyjne określone w przepisach wydanych na podstawie art. 18 pkt 1 ustawy o informatyzacji. System ten w szczególności uzależnia zapoznanie się przez odbiorcę z treścią pisma od złożenia bezpiecznego podpisu elektronicznego na urzędowym poświadczeniu odbioru.
2. System teleinformatyczny umożliwia automatyczne generowanie informacji wskazujących pisma doręczane za pomocą środków komunikacji elektronicznej, co do których nie wpłynęło potwierdzone urzędowe poświadczenie odbioru w terminie określonym w art. 46 § 3 k.p.a.
3. System teleinformatyczny umożliwia udostępnianie pism i urzędowych poświadczeń odbioru oraz ewidencjonowanie dokumentów elektronicznych doręczonych poszczególnym adresatom oraz urzędowych poświadczeń odbioru, a także czasu podpisania urzędowego poświadczenia odbioru oraz dotarcia wysłanego pisma do komputera adresata.
4. Organ administracji publicznej przechowuje otrzymane i potwierdzone urzędowe poświadczenia odbioru przez co najmniej taki okres, przez jaki obowiązany jest przechowywać pismo, którego dotyczy to poświadczenie.

5. Za datę doręczenia pisma w formie dokumentu elektronicznego wysyłanego przez organ administracji publicznej uważa się dzień podpisania urzędowego poświadczenia odbioru.
6. Organ administracji publicznej nieodpłatnie udostępnia oprogramowanie, które umożliwia:
  - 1) prezentację umożliwiającą odczytanie przesyłanego pisma wraz z weryfikacją bezpiecznego podpisu osoby, która podpisała pismo;
  - 2) weryfikację autentyczności urzędowego poświadczenia odbioru i prezentację czasu podpisania potwierdzenia;
  - 3) weryfikację bezpiecznego podpisu elektronicznego osoby odbierającej pismo, która podpisała urzędowe poświadczenie odbioru.
7. Minister właściwy do spraw informatyzacji może utworzyć elektroniczną skrzynkę podawczą umożliwiającą obsługę systemu **teleinformatycznego** do doręczeń dla organów administracji rządowej. Inne organy administracji publicznej mogą upoważnić, w drodze porozumienia, ministra właściwego do spraw informatyzacji do obsługi doręczeń dotyczących tych organów.
8. Doręczenia dokonywane przy pomocy upoważnionej elektronicznej skrzynki podawczej uważa się za dokonywane przez organ administracji publicznej, który wystawił upoważnienie.
9. Elektroniczna skrzynka podawcza, nie później niż w czasie 2 godzin od doręczenia dokumentu, przekazuje właściwym organom administracji publicznej urzędowe poświadczenie odbioru.

## § 6.

Jeżeli adresatem pisma w formie dokumentu elektronicznego jest organ administracji publicznej, doręczenie następuje na warunkach i w formie określonej w przepisach wydanych na podstawie art. 16 ust. 3 ustawy o informatyzacji.

## § 7.

1. Kopie pism w formie dokumentów elektronicznych sporządza się i udostępnia w postaci dokumentu elektronicznego, podpisanego bezpiecznym podpisem elektronicznym osoby sporządzającej kopię, a składającego się z treści udostępnianego dokumentu elektronicznego i elementów informacyjnych określających co najmniej informację kto sporządził kopię, datę jej sporządzenia oraz nazwę urzędu i jego adres. Elementy

informacyjne dokumentu muszą być zgodne z danymi zawartymi w kwalifikowanym certyfikacie osoby sporządzającej kopie.

2. Pisma w formie dokumentów elektronicznych mogą być także udostępniane w postaci elektronicznej kopii dokumentu oryginalnego, o ile zostały podpisane bezpiecznym podpisem elektronicznym, a okres ważności kwalifikowanego certyfikatu pozwoli na jego weryfikację przez odbiorcę.
3. Kopia pisma w formie dokumentu elektronicznego może być sporządzona w postaci uwierzytelnionego wydruku komputerowego.
4. Do sporządzania kopii pism w formie dokumentów elektronicznych stosuje się odpowiednio przepisy k.p.a. dotyczące uwierzytelnionych odpisów z akt sprawy.
5. Kopie pism w formie dokumentów elektronicznych, o których mowa w ust. 1 i 2, mogą być udostępnione za pośrednictwem środków komunikacji elektronicznej albo na informatycznych nośnikach danych.

#### **§ 8.**

Rozporządzenie wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia.

**MINISTER  
SPRAW WEWNĘTRZNYCH I ADMINISTRACJI**

## UZASADNIENIE

Projekt rozporządzenia stanowi wykonanie upoważnienia określonego art. 39<sup>1</sup> § 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Przedmiotem regulacji niniejszego rozporządzenia jest sposób dokonywania doręczeń pism za pomocą środków komunikacji elektronicznej. W szczególności projekt rozporządzenia określa: strukturę i sposób sporządzania pism w formie dokumentów elektronicznych, warunki organizacyjno-techniczne doręczania pism w formie dokumentów elektronicznych, w tym formę urzędowego poświadczania ich odbioru przez adresata oraz sposób udostępniania kopii dokumentów elektronicznych.

Projekt rozporządzenia, określając formę dokumentów elektronicznych – wykorzystuje w tym celu format danych, o których mowa w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. Nr 64, poz. 565, z późn. zm.).

Utworzenie przez Ministra właściwego do spraw informatyzacji centralnego repozytorium wzorów pism w formie dokumentów elektronicznych zostanie zapisane w Planie Informatyzacji Państwa.

Zgodnie z projektem rozporządzenia organy administracji publicznej będą obowiązane do przekazywania do centralnego repozytorium wzorów pism w formie dokumentów elektronicznych, które zamierzają udostępniać i wykorzystywać.

Wzór pisma przekazany do centralnego repozytorium równoznaczny jest z określeniem wzoru wnoszenia podań o którym mowa w art. 63 § 3a ust. 2 k.p.a. Podania wnoszone w formie elektronicznej, niezgodne z takim wzorem, nie spełniają wymagań, o których mowa w wymienionym wyżej artykule.

Ponadto na organy administracji publicznej nałożony został obowiązek udostępniania wzorów pism w formie dokumentów elektronicznych w Biuletynie Informacji Publicznej.

Projekt rozporządzenia precyzuje także procedurę doręczania pism elektronicznych. W przypadku, gdy adresatem pisma jest organ administracji publicznej - projekt odsyła do rozporządzenia Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym (Dz. U. z 2005 r. Nr 200, poz. 1651).

Projekt rozporządzenia reguluje również kwestię doręczeń w przypadku, gdy adresatem jest osoba niebędąca organem administracji publicznej.

Projekt określa wymagania, jakie musi spełniać wysyłana do adresata informacja o oczekującym na odbiór piśmie, sposobie identyfikacji adresata, procedurze pobrania pisma

oraz poświadczenia odbioru ze skrytki (adresu elektronicznego), jak również sposób potwierdzenia odbioru pisma.

Uregulowane też zostały warunki techniczne, jakie musi spełniać używany przez wysyłający pismo organ administracji publicznej system informatyczny obsługujący doręczenie. Warunki te nawiązują do rozwiązań zawartych w powołanym powyżej rozporządzeniu Prezesa Rady Ministrów w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym.

Na organ administracji publicznej nałożony zostaje również obowiązek nieodpłatnego udostępnienia oprogramowania umożliwiającego prezentację przesyłanego pisma, weryfikację autentyczności zastosowanych podpisów elektronicznych oraz określenie czasu doręczenia. Pozwala to na obsługę wszystkich bezpiecznych podpisów elektronicznych oferowanych obecnie przez cztery kwalifikowane podmioty świadczące usługi certyfikacyjne wpisane do rejestru Ministra Gospodarki, bez preferowania jakiegokolwiek z nich.

Ponadto organ administracji publicznej zgodnie z projektem rozporządzenia wydaje zainteresowanym podmiotom kody dostępu, w szczególności identyfikator lub hasło albo używają oni swoich bezpiecznych podpisów elektronicznych (kwalifikowanych certyfikatów) lub certyfikatów uznawanych przez organy administracji publicznej, służące do autoryzacji i identyfikacji adresata. Stosowanie identyfikatorów i haseł wydawanych przez organy administracji publicznej pozwoli na dalsze wykorzystanie rozwiązań już funkcjonujących w licznych urzędach.

Projekt rozporządzenia przewiduje, że minister właściwy do spraw informatyzacji będzie mógł utworzyć elektroniczną skrynkę podawczą do obsługi elektronicznego systemu teleinformatycznego do doręczeń dla organów administracji rządowej. Także inne organy administracji publicznej będą mogły wykorzystać elektroniczną skrynkę podawczą do obsługi doręczeń w drodze porozumienia. Elektroniczna skrynka podawczą będzie mogła zatem przejąć część obowiązków organów administracji publicznej związanych z obsługą doręczeń, a zarazem doręczenie dokonane przy pomocy elektronicznej skrytki podawczej będzie równoznaczne z doręczeniem dokonany przez sam organ.

Projekt rozporządzenia określa również sposób sporządzania oraz udostępniania kopii dokumentów elektronicznych zarówno w postaci elektronicznej kopii dokumentu elektronicznego, jak też uwierzytelnionego wydruku komputerowego – w tym zakresie odsyła do przepisów ustawy Kodeks postępowania administracyjnego.

Dla powyższego aktu prawnego przewidziano 6-cio miesięczne *vacatio legis*.

**Przy projektowaniu rozporządzenia przyjęto następujące warunki i założenia techniczne związane z normami i standardami międzynarodowymi:**

*Założenia warunków technicznych*

1. Dokumenty elektroniczne sporządzane przez podmiot publiczny powinny być:
  - a) zgodne z formatami danych wymienionymi w załączniku 2 do rozporządzenia Prezesa Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766),
  - b) w szczególności w postaci dokumentów XML, stworzonych na podstawie ustalonych i opublikowanych przez podmiot publiczny wzorców (XML-Schema),
  - c) podpisane bezpiecznym podpisem elektronicznym weryfikowanym kwalifikowanym certyfikatem uprawnionego urzędnika sporządzającego pismo.
2. Wszystkie podpisy pod dokumentami elektronicznymi tworzonymi przez podmioty publiczne
  - a) przygotowywane są zgodnie ze specyfikacją techniczną ETSI TS 101 903 v 1.3.2 XML Advanced Electronic Signatures (XAdES),
  - b) oznaczane są informacjami stwierdzającymi ważność certyfikatów kwalifikowanych i ich czas weryfikacji, zgodnie ze specyfikacją techniczną ETSI TS 101 903 w formatach XAdES-XL lub XAdES-A.
3. Urzędowe poświadczenie odbioru
  - a) sporządzane jest w strukturach fizycznych dokumentu XML podpisane bezpiecznym podpisem zgodnie ze specyfikacją techniczną ETSI TS 101 903,
  - b) może być oznakowane czasem zgodnie ze standardem XAdES-T,
  - c) tworzone jest na podstawie udostępnionego przez podmiot publiczny wzorca (XML-Schema).
4. System teleinformatyczny wykorzystywany przez podmiot publiczny do oznaczania dokumentu danymi stwierdzającymi ważność certyfikatów i czas weryfikacji:
  - a) powinien co najmniej spełniać wymagania systemu zgodnie z normą Europejskiego Instytutu Standaryzacyjnego CEN-CWA 14167-1,
  - b) powinien wykorzystywać bezpieczne moduły kryptograficzne (HSM):
    - i. spełniające wymagania normy FIPS 140-2 poziom 3 lub CEN-CWA 14167-2,
    - ii. generujące i przechowujące materiał kryptograficzny służący do oznaczania danymi stwierdzającymi ważność certyfikatów kwalifikowanych,
    - iii. zapewniające ochronę przed nieuprawnionym dostępem, w bezpiecznej obudowie odpornej na nieuprawnioną ingerencję z zewnątrz,
    - iv. zabezpieczone przed nieuprawnioną ingerencją przez zniszczenie materiału kryptograficznego w przypadku jej wykrycia.
  - c) powinien wykorzystywać urządzenia udostępniające w sposób zaufany, urzędowy koordynowany czas UTC(PL) zgodnie z rozporządzeniem Ministra Gospodarki z dnia 19 marca 2004 r. w sprawie sposobów upowszechniania sygnałów czasu urzędowego i uniwersalnego czasu koordynowanego UTC(PL) – Dz. U. Nr 56, poz. 548,

- d) powinien wykorzystywać algorytmy szyfrowe z długością klucza co najmniej 2040 bitów.
5. Do oznaczania dokumentów danymi stwierdzającymi ważność certyfikatów mogą być wykorzystywane usługi certyfikacyjne innych podmiotów spełniających powyższe wymagania, jak i centrów wydających certyfikaty kwalifikowane.

*Założenia dodatkowe :*

1. Pisma urzędowe w postaci dokumentów elektronicznych, a w szczególności typu: wezwania i decyzje powinny spełniać warunki interoperacyjności, tj.:
  - a) być rozpoznawalne przez inne systemy komputerowe,
  - b) posiadać jednoznacznie zidentyfikowane pola informacyjne,
  - c) mieć jednoznacznie zdefiniowany format podpisu.
2. Czas ważności dokumentu nie powinien być ograniczony ważnością podpisu złożonego pod nim. Dlatego proponowane jest zastosowanie techniki, opisanej standardami europejskimi ETSI, poprzez zintegrowanie w jednym dokumencie – podpisu, oznakowania czasem, odpowiedzi OCSP lub list CRL.
3. Przyjęto, że znakowanie czasem – nie musi być usługą kwalifikowaną w rozumieniu ustawy o podpisie elektronicznym, której podstawową wadą jest czas ważności zaświadczenia urzędu do znakowania czasem ograniczony do 5 lat.
4. Ze względu na brak delegacji prawnych dla usługi OCSP, nie wymieniono jej literalnie, choć podstawą prawną może być dyrektywa oraz normy ETSI
5. Warunki techniczne nie nakładają obowiązku, aby system działał w ramach podmiotu publicznego – w szczególności może to być centrum certyfikacji spełniające wymagania CWA 14167-1
6. Przy usługach oznaczania czasem i tworzeniu systemu XAdES-A wykorzystuje się silniejsze algorytmy i dłuższe klucze kryptograficzne niż przy tworzeniu podpisu elektronicznego, dlatego zaproponowano użycie klucza o długości co najmniej 2040 bitów

*Następujące wymagania wynikają wprost z normy CWA 14167-1:*

Klucze służące do podpisywania certyfikatów kwalifikowanych i certyfikatów niekwalifikowanych powinny być generowane i przechowywane w bezpiecznym module kryptograficznym.

Bezpieczny moduł kryptograficzny, powinien być oceniony i certyfikowany zgodnie z następującymi wymaganiami:

- 1) urządzenie powinno zapewnić poufność i integralność kluczy podczas ich całego czasu życia;
- 2) urządzenie powinno zapewnić identyfikację i uwierzytelnienie użytkowników;
- 3) urządzenie powinno ograniczać dostęp do swoich usług, w zależności od użytkownika i jego przywilejów przypisanych do tych usług;
- 4) urządzenie powinno wykonywać serię testów sprawdzających poprawność jego pracy, a w przypadku wykrycia błędów - przełączyć się w stan bezpieczny;

- 5) urządzenie powinno wykrywać próby sabotażu i w przypadku wykrycia takiej próby przełączyć się w stan bezpieczny;
- 6) urządzenie powinno tworzyć zapisy zdarzeń dla każdej zmiany związanej z bezpieczeństwem;
- 7) dopuszcza się, aby urządzenie umożliwiło wykonie kopii zapasowej klucza oraz jego odtworzenie, ale powinno zapewnić poufność i integralność kopii bezpieczeństwa i wymagać co najmniej dwuosobowego tworzenia kopii zapasowej i odtwarzania. Ocena powinna być przeprowadzona zgodnie z normą CWA 14167-2 lub innym standardem, zawierającym porównywalny poziom wymagań.

W czasie generowanie kluczy służących do podpisywania certyfikatów kwalifikowanych i certyfikatów niekwalifikowanych przy pomocy bezpiecznego urządzenia kryptograficznego, powinno ono być obsługiwane przez dwie osoby jednocześnie.

Dopuszcza się aby funkcjonalność "podwójnej kontroli" była zapewniona albo przez bezpieczny moduł kryptograficzny, albo wdrożona w zaufanym systemie.

Klucze infrastruktury i klucze kontrolne powinny być generowane i utrzymywane w sprzętowym urządzeniu kryptograficznym.

Moduł kryptograficzny, powinien być oceniony i certyfikowany na poziomie co najmniej [FIPS140-2] Level 3 lub zgodnie z innym odpowiednim standardem.

Generowanie kluczy, wszędzie tam gdzie ma to zastosowanie, powinno być zgodne z wymaganiami kryptograficznymi określonymi w ETSI SR 002 176

### **Opinia wstępna o zgodności rozporządzenia z prawem Unii Europejskiej**

Rozporządzenie zawiera rozwiązania stanowiące domenę prawa krajowego.

*Problematyka regulowana w rozporządzeniu nie jest objęta zakresem prawa Unii Europejskiej.*

### **Ocena skutków regulacji**

#### **1. Podmioty, na które oddziałuje akt normatywny:**

Przepisy zawarte w projekcie rozporządzenia stosuje się organów administracji w rozumieniu art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Projekt rozporządzenia określa również sytuację podmiotów, którym doręczane są pisma w formie elektronicznej.

#### **2. Wpływ regulacji na sektor finansów publicznych.**

Wejście w życie projektowanej regulacji nie spowoduje dodatkowych skutków finansowych dla budżetu państwa pod warunkiem, że organy rządowe i samorządowe przystąpią do porozumienia mającego na celu wspólne wykorzystywanie elektronicznej skrzynki podawczej w ramach projektu ePUAP. W przeciwnym wypadku będą musiały samodzielnie ponosić koszty budowy elektronicznej skrzynki podawczej.

Koszty związane z obsługą systemu, o którym mowa w § 5 ust.1 projektowanego rozporządzenia, zostały przewidziane we współfinansowanym z funduszy strukturalnych projekcie ePUAP.

### **3. Konsultacje społeczne.**

Projekt rozporządzenia został przekazany do zaopiniowania Polskiej Izbie Informatyki i Telekomunikacji (PIIT), Polskiemu Towarzystwu Informatycznemu (PTI), Radzie Informatyzacji, Stowarzyszeniu do spraw audytu i kontroli systemów informatycznych. Projekt został także umieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Spraw Wewnętrznych i Administracji. PIIT i PTI zgłosiło wspólną opinię która w olbrzymiej większości została uwzględniona. Rada Informatyzacji zaopiniowała projekt pozytywnie na posiedzeniu w dniu 20 stycznia 2006 r. Zgłoszone uwagi zostały w zdecydowanej większości uwzględnione.

### **4. Wpływ na konkurencyjność gospodarki i przedsiębiorczość**

Rozporządzenie zwiększy konkurencyjność wewnętrzną i zewnętrzną gospodarki, poprzez zmniejszenie barier „komunikacyjnych” oraz tworzy realne możliwości i gwarancje prawne do załatwiania spraw administracyjnych przez przedsiębiorstwa w formach elektronicznych. Usprawni ponadto obsługę tychże firm przez organy administracji.

### **5. Wpływ na sytuację i rozwój regionów**

Rozporządzenie poprawi sytuację i rozwój regionów, poprzez zmniejszenie barier „komunikacyjnych”.

### **6. Wpływ na rynek pracy**

Rozporządzenie nie będzie miało bezpośredniego wpływu na rynek pracy.