

# Uwagi do projektu nowelizacji ustawy o informatyzacji

## PROJEKT

*Internet Society Poland (ISOC-PL)*

25 lipca 2009

### Zgłaszający

ISOC Polska

ul. Pasteura 7

02-093 Warszawa

tel/fax: +48 22 621 30 17

email: [zarzad@isoc.org.pl](mailto:zarzad@isoc.org.pl)

### Dokument źródłowy

Uwagi zostały oparte o następujący dokument:

Druk sejmowy nr 2110

2009-06-17

*Rządowy projekt ustawy o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawy - Kodeks postępowania administracyjnego, ustawy - Ordynacja podatkowa oraz niektórych innych ustaw.*

<http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/2110>

### Uwagi do poszczególnych punktów

Art. 3 pkt 9 - "minimalne wymagania dla systemów teleinformatycznych (...) umożliwia wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych (...) zapewnia dostęp do zasobów informacji udostępnianych za pomocą tych systemów także osobom niepełnosprawnym"

- Zgodnie z tą definicją odczytaną dosłownie minimalne wymagania służą wyłącznie zapewnieniu wymiany danych z **innymi systemami** i z **osobami niepełnosprawnymi**. A co z osobami **pełnosprawnymi**? Proponujemy po „wymianę danych z innymi systemami” napisać „zapewnia dostęp do zasobów osobom, z uwzględnieniem potrzeb osób niepełnosprawnych” lub pozostawić tylko „osoby”. Konkretnie odwołania do standardów Web Accessibility powinny się znajdować dopiero w rozporządzeniu o minimalnych wymaganiach lub Krajowych Ramach Interoperacyjności.
- Dotychczasowe rozporządzenie o minimalnych wymaganiach nie spełnia swojego celu ze

względu na złe zdefiniowanie problemu. Dla użytkowników nie jest problemem publikacja dokumentu przez urząd w – przykładowo – starszym formacie PDF 1.3 (niezgodny z "minimalnymi wymaganiami") zamiast nowszego PDF 1.4 (zgodny), ponieważ starszy format jest wstecznie kompatybilny z nowszym.

- Problemem jest użycie **zbyt nowych** formatów oraz niestandardowych profili lub **prywatnych rozszerzeń** do formatów ustandaryzowanych.<sup>1</sup>
- Problemem jest niekompatybilność formatów **publikowanych i przyjmowanych** przez **różne** urzędy, zwłaszcza w sytuacji gdy na rynku pojawiło się kilkanaście niestandardowych formatów związanych z bezpiecznym podpisem elektronicznym<sup>2</sup>.
- Nowe rozporządzenie powinno zakreślać **dolną i górną granicę wersji standardów**, które są przyjmowane przez administrację publiczną jak i stosowane przez nią przy publikacji.
- Proponujemy określenie **listy standardów tolerowanych (C), zalecanych (B) oraz obligatoryjnych (A)**. Grupa A będzie stanowić zamknięty, wspólny mianownik gwarantujący interoperacyjną komunikację z administracją publiczną. Grupa C będzie zapewniać wsteczną kompatybilność, zaś grupa B – stymulować przejście w kierunku przyszłych standardów obligatoryjnych.
- Większe ograniczenia powinny obowiązywać przy **udostępnianiu** dokumentów (tylko formaty A), mniejsze przy **przyjmowaniu (B, C)**. Pozwoli to uniknąć obecnych problemów z obiegiem dokumentów pomiędzy obywatelem a urzędami. Niedopuszczalna jest sytuacja – obecnie powszechna - w której jeden urząd wydaje obywatelowi decyzję w formie elektronicznej, której drugi urząd nie przyjmie bo akurat ma inną skrzynkę podawczą.

---

Art. 3 pkt 14 - "profil zaufany ePUAP – zestaw informacji identyfikujących i opisujących podmiot lub osobę, będącą dysponentem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego"

- Proponujemy wykorzystanie jednego z dostępnych produkcyjnie i ustandaryzowanych **protokołów federacji tożsamości i pojedynczego logowania** (*single sign-on*), takich jak OpenID<sup>3</sup>, Identity Metasystem Interoperability (Infocard)<sup>4</sup> czy SAML<sup>5</sup>.
- Zwracamy uwagę na konieczność **dostosowania poziomu bezpieczeństwa** zapewnianego przez konkretny mechanizm używany do uwierzytelnienia użytkownika **do wymagań poszczególnych procedur** administracyjnych. Jeśli dla **wszystkich** procedur zastosowany będzie **wyłącznie jeden** mechanizm, to siłą rzeczy będzie to musiał być mechanizm odpowiedni dla procedur o **najwyższych** wymaganiach, nawet jeśli popyt na nie jest niewielki. Dotychczasowe doświadczenia z bezpiecznym podpisem elektronicznym pokazują, że takie podejście **drastycznie ogranicza dostęp obywateli do usług nie wymagających najwyższego poziomu bezpieczeństwa**<sup>6</sup>. Dlatego postulujemy wprowadzenie takiej liczby **różnych**

1 Przykłady: niekompatybilność różnych wersji formatów MS Word. Niekompatybilność rozszerzeń formatu PDF wykraczających poza ISO 32000, typowych dla Adobe Acrobat 9 i nowszych. Publikacja tekstu w postaci obrazu (*bitmapy*) osadzonej w pliku DOC lub PDF, co uniemożliwia przeszukiwanie, indeksowanie i kopiowanie tekstu.

2 Przykład: oprogramowanie jednego z polskich centrów certyfikacji generuje plik podpisany w formacie XAdES z rozszerzeniem SIG, którego nie potrafi odczytać oprogramowanie innego centrum, które w plikach SIG oczekuje formatu CMS.

3 OpenID Authentication 2.0 <http://openid.net/developers/specs/>

4 OASIS Identity Metasystem Interoperability Version 1.0 <http://docs.oasis-open.org/imi/identity/v1.0/identity.html>

5 OASIS Security Assertion Markup Language (SAML) v2.0 <http://saml.xml.org/saml-specifications>

6 Przykładem jest 5% upowszechnienie polskiej faktury elektronicznej opartej o bezpieczny podpis w porównaniu z 60% upowszechnieniem e-faktur w Danii, która nie wymaga bezpiecznego podpisu. Drugim przykładem jest elektroniczny PIT-37, który – po zniesieniu obowiązku stosowania bezpiecznego podpisu – złożyło blisko 50 tys. podatników, bez

mechanizmów uwierzytelnienia jaka jest potrzebna do zaspokojenia wymagań bezpieczeństwa dla różnych procedur. Doboru tych mechanizmów należy dokonać na podstawie racjonalnej analizy ryzyka.

- Niepokoi nas zaawansowanie prac nad ustawą o informatyzacji z całkowitym pominięciem prac prowadzonych przez MG nad ustawą o podpisach oraz brak jakichkolwiek szczegółów na temat architektury innych rozwiązań, na które często powołuje się MSWiA. Apelujemy o możliwie jak najszybszą zsynchronizowanie prac pomiędzy resortami, rozpoczęcie debaty publicznej oraz udostępnienie choćby ogólnych założeń następujących mechanizmów:
  - koncepcja elektronicznego uwierzytelnienia i autoryzacji obywateli do różnych procedur administracyjnych;
  - koncepcja podpisu osobistego i pl.ID;
  - koncepcja profilu zaufanego ePUAP;
  - koncepcja weryfikacji podpisu elektronicznego w administracji publicznej;

---

Art. 3 pkt 15) „elektroniczna skrzynka podawcza – dostępny publicznie środek komunikacji elektronicznej służący do przekazywania dokumentu elektronicznego do podmiotu publicznego przy wykorzystaniu powszechnie dostępnego systemu teleinformatycznego; „

- Dla zachowania spójności języka proponujemy konsekwentne używanie pojęcia „publicznie dostępny” albo „powszechnie dostępny”, ale nie obu jako synonimów.

---

Art. 3 pkt. 16-17, czyli definicje interoperacyjności i neutralności technologicznej.

- Ustawa powinna gwarantować, że system teleinformatyczny zbudowany na zamówienie podmiotów publicznych **nie będzie podlegał uzależnieniu technologicznemu** - to znaczy, że w razie potrzeby **możliwe będzie przejście utrzymania, serwisowania lub dalszego rozwoju systemu** przez zamawiającego lub podmioty trzecie wyłonione zgodnie z prawem zamówień publicznych<sup>7</sup>.
- Jako jeden ze środków zapobiegania uzależnieniu technologicznemu ustandaryzowane powinny zostać **minimalne wymagania wobec stanu prawnego oraz dokumentacji systemów teleinformatycznych** kupowanych lub zamawianych przez podmioty publiczne. W szczególności podmioty publiczne powinny mieć obowiązek:
  - Dla **jednostkowego systemu wyspecjalizowanego**, tworzonych wyłącznie na zamówienie określonego podmiotu - obowiązek żądania kodu źródłowego oraz dokumentacji niezbędnej do utrzymania lub zmian systemu oraz przeniesienia praw autorskich, także jeśli w danym momencie umowa przewiduje wsparcie i serwis dla danego systemu. Rozwiąże to problem kupowania przez podmioty publiczne systemów pisanych na ich wyłączne potrzeby ale posiadających wady prawne, prowadzące do

---

szkody dla bezpieczeństwa.

<sup>7</sup> Wrażenie takie można odnieść w przypadku Kompleksowego Rozproszonego Systemu Bezpieczeństwa (KRSB) ZUS, gdzie dostarczono komputery z zaimplementowaną niskopoziomową, niestandardową kontrolą dostępu, specyficzną tylko dla jednego dostawcy. Firma ta od lat jest jedynym oferentem startującym w przetargach na aktualizacje tych komputerów ponieważ jest jedynym dysponentem tej technologii i jako jedyna może ją serwisować.

- ponoszenia nadmiernych kosztów ze względu na uzależnienie od producenta.
- Dla **systemu wyspecjalizowanego**, tworzonego na zamówienie podmiotu ale **odpowiadającego na potrzeby wielu podobnych podmiotów publicznych** - obowiązek żądania ponadto prawa do samodzielnej modyfikacji i przekazywania systemu innym podmiotom publicznym. Pozwoli to na uniknięcie wielokrotnego zamawiania tego samego systemu przez wiele podmiotów publicznych prowadzących identyczną działalność i podlegających identycznym wymaganiom prawnym. Wymóg ten, wprowadzony powszechnie w USA i krajach Europy Zachodniej (licencje typu Government Purpose Rights), doprowadził do znacznej racjonalizacji wydatków publicznych i ograniczenia korupcji, bez szkody dla dostawców systemów, którzy nadal mogą oferować podmiotom usługi wsparcia tych systemów.
  - Dla **systemów niewyspecjalizowanych** i kupowanych na wolnym rynku - obowiązek żądania by zapewniały one interoperacyjność, w tym co najmniej eksport danych do otwartych formatów oraz komunikację za pomocą otwartych protokołów komunikacji.
  - Zwracamy uwagę, że przyjęta w obecnej wersji projektu koncepcja „jawności standardu” nie stanowi wystarczającej ochrony przed innymi formami ograniczania jego dostępności, jak na przykład patenty.
    - Przez otwartość standardu rozumiemy jawność jego specyfikacji, jej dostępność bezpłatnie lub po kosztach sporządzenia kopii, brak ograniczeń w stosowaniu wynikający z praw własności intelektualnej (IP) oraz deklarację podmiotu odpowiedzialnego o braku ukrytych zobowiązań lub oświadczenie o udzieleniu nieograniczonej licencji, jeśli podmiot jest właścicielem tych praw.
      - Zwracamy uwagę, że nie zostały rozstrzygnięte spory o europejskie regulacje dotyczące patentowania rozwiązań informatycznych oraz o inne regulacje praw własności intelektualnej związane z informatyką. Europejski Urząd Patentowy (EPO) i inne urzędy patentowe udzieliły tysiące patentów na rozwiązania informatyczne, w tym takie które są wykorzystywane w licznych międzynarodowych standardach. Niektóre z tych patentów obowiązują także w Polsce.
      - W interesie państwa polskiego jest dążenie do stanu, w którym administracja publiczna nie jest uzależniona od algorytmów i formatów, których wykorzystanie może się wiązać z koniecznością uiszczania opłat licencyjnych. Stan ten można stosunkowo łatwo osiągnąć przyjmując proponowane przez nas rozumienie otwartości standardu i preferowanie tak rozumianych otwartych standardów przy ustalaniu list standardów zalecanych, tolerowanych i obligatoryjnych.
    - Wyjątki od stosowania otwartych standardów powinny być dopuszczalne z odpowiednim uzasadnieniem, dlaczego wykorzystanie otwartego standardu jest niemożliwe. W szczególności dotyczy to przypadków kiedy na rynku nie ma rozwiązań stosujących formaty w pełni otwarte (np. GSM, HDCP) lub korzystanie z otwartych standardów byłoby w dłuższej perspektywie nieopłacalne.
  - Uregulowane powinny zostać **prawa do utworów finansowanych ze środków publicznych**. W szczególności wymagane jest określenie, **czy prawa do powielania, dystrybucji i modyfikacji tych utworów mogą być ograniczane**, a jeśli tak to w jakim zakresie, w jakich przypadkach i na jakich warunkach. Internet Society Poland stoi na stanowisku, że utwory tworzone za pieniądze publiczne powinny być jak najszerszej dostępne dla obywateli, którzy sfinansowali ich powstanie, oraz innych organów administracji publicznej. W szczególności należy tutaj wymienić:

- Programy radiowe i telewizyjne tworzone przez media publiczne na przestrzeni lat, w szczególności utwory do których wygasły prawa autorskie i które powinny stanowić własność publiczną. Pozwoli to ograniczyć nadużycia związane z przypadkami, gdy podmioty powołane do ich udostępniania pobierają opłaty niewspółmierne do kosztów udostępnienia.
- Ekspertyzy, analizy i inne opracowania zamawiane przez podmioty publiczne, które jako finansowane ze środków publicznych powinny stanowić informację publiczną oraz powinny być szeroko wykorzystywane przez inne podmioty publiczne. W obecnej sytuacji poszczególne urzędy wielokrotnie zamawiają analizy prawne tego samego przepisu lub opracowania na identyczny temat (np. analiza procesów), nieracjonalnie wydając środki publiczne. W wielu przypadkach wadliwy sposób zamówienia powoduje, że prawa zamawiającego do dysponowania danym dziełem są na różne sposoby ograniczane, nawet jeśli stoi to w sprzeczności z innymi przepisami prawa (np. ustawa o dostępie do informacji publicznej czy art. 4 pkt 2 prawa autorskiego).

---

---

Art. 12 pkt 3b *"Do wniosku, o którym mowa w ust. 1, dołącza się (...) analizę ekonomiczno-finansową celowości ustanowienia przedsięwzięcia"*

- Do wniosku poza analizą kosztów i zysków powinna być dołączana także podstawowa analiza ryzyka biznesowego.
- Dla zagwarantowania transparentności życia publicznego oraz przeciwdziałania korupcji napływające wnioski powinny być publikowane przez podmiot je rozpatrujący wraz opiniami Rady oraz ewentualnymi opiniami ekspertów zewnętrznych.

---

---

Art. 13 pkt 1a *"Postanowienia ust.1 nie stosuje się do systemów teleinformatycznych używanych do celów naukowych i dydaktycznych"*

- Dopisać: "oraz testowych"

---

---

Art. 16 ust. 3 - *"uwzględniając (...) potrzebę zapewnienia integralności dokumentów elektronicznych"*

- Dopisać: "integralności oraz autentyczności"

---

---

Art. 17 pkt 9 - *"Rekomendowany do Rady kandydat posiada wykształcenie wyższe"*

- Dyskryminacja nieuzasadniona względami merytorycznymi.

---

---

Zmiany do Kodeksu postępowania administracyjnego, art. 46 *"Doręczenie dokumentu w formie dokumentu elektronicznego do podmiotu publicznego w rozumieniu przepisów ustawy, o której mowa w § 4 pkt 3, następuje przez elektroniczną skrzynkę podawczą tego podmiotu, w sposób określony w tej ustawie"*

- Celem strategicznym powinno być zagwarantowanie, że realizowana będzie **faktyczna**

interoperacyjność pomiędzy urzędami polegająca na tym, że obywatel **może otrzymać dokument elektroniczny od jednego urzędu a następnie złożyć go w tej samej formie w drugim urzędzie ze skutkiem prawnym**. W chwili obecnej jest to w praktyce niemożliwe ze względu na brak interoperacyjności w zakresie formatów dokumentów wytwarzanych i akceptowanych przez poszczególne urzędy. Interoperacyjność na tym poziomie zaburza także wyłączenie z wymagań ustawy znacznych grup urzędów, które w rezultacie nie muszą udostępniać ani akceptować dokumentów w formatach akceptowanych przez pozostałe urzędy.

---

Zmiany do Kodeksu postępowania administracyjnego, Art. 107 § 1, art. 124 § 1, w art. 238 § 1 - *"Decyzja powinna zawierać (...) jeżeli decyzja wydana została w formie dokumentu elektronicznego, powinna być opatrzona bezpiecznym podpisem elektronicznym weryfikowanym za pomocą **ważnego kwalifikowanego certyfikatu**"*

- Z powyższego zapisu należy usunąć słowo "ważnego" - jest to zmiana zgodna z wprowadzoną w projekcie ustawy o podpisach. Wymóg ten **w obecnej formie ogranicza ważność decyzji do czasu ważności certyfikatu osoby, która podpisała decyzję**, jeśli decyzja zostanie wystawiona bez dodatkowego mechanizmu potwierdzającego datę złożenia podpisu (a o takim wymogu się tutaj nie wspomina). W rezultacie obywatel chcący przy pomocy takiej decyzji wykonywać czynności prawne zostanie tej możliwości pozbawiony po wygaśnięciu certyfikatu wystawcy (czyli do ok. dwóch lat)
- Problem ten, wynikający z zapisu ustawy o podpisie elektronicznym, jest obecnie widoczny w sposób szczególnie dotkliwy w przypadku faktur elektronicznych, które – opatrzone jedynie bezpiecznym podpisem – przestają być poprawnie weryfikowane po wygaśnięciu certyfikatu osoby podpisującej (maksymalnie 2 lata). Równocześnie okres ich ważności wymagany przez urzędy skarbowe to pięć lat.
- Jest to część szerszego problemu jakim jest **racjonalna polityka weryfikacji dokumentów podpisanych podpisem elektronicznym**. Zachęcamy MSWiA do ustosunkowania się do tego problemu przez publikację spójnych zasad weryfikacji różnego rodzaju dokumentów, z uwzględnieniem różnych scenariuszy (elektroniczna dokumentacja medyczna, faktury elektroniczne, decyzje urzędowe, akty prawne itd.) i różnych poziomów pewności wymaganych w różnych zastosowaniach.
- Konieczne jest także umieszczenie w treści dokumentu **jednoznacznych wskazówek na temat okresu ważności dokumentu** w tej formie oraz możliwości jej podtrzymania tak, by zagwarantować obywatelowi ciągłość obowiązywania decyzji urzędowej na wiele lat po jej wydaniu w formie elektronicznej.

Zmiany do Kodeksu postępowania administracyjnego, art. 220 § 1 - *"Organ administracji publicznej nie może żądać zaświadczenia na potwierdzenie faktów lub stanu prawnego, jeżeli: 1) znane są one organowi z urzędu; 2) możliwe są do ustalenia przez organ na podstawie..."*

- Zdecydowanie wspieramy ten zapis i uważamy za niezwykle istotne ograniczenie ilości informacji, których domagają się urzędy przy uruchamianiu procedur urzędowych, a które są i tak w ich posiadaniu lub łatwo dostępne na podstawie indywidualnych numerów identyfikacyjnych. W obecnej sytuacji każda procedura wymaga podania ogromnych ilości zduplikowanych informacji, które trzeba wielokrotnie i za każdym razem wpisywać w urzędowych formularzach.

---

Zmiany do Prawa o ruchu drogowym w art. 80c, 100c - *"Każdy może uzyskać, nieodpłatnie, potwierdzenie lub zaprzeczenie zgodności danych (...)"*

- Proponujemy tak sformułować ten zapis, by dane te można było uzyskać za pomocą **interfejsu automatycznego** (np. SOAP, XML-RPC), a nie tylko za pomocą interaktywnego formularza wymagającego obecności osoby fizycznej.

---

Zmiany do Prawa o ruchu drogowym w art. 80c, 100c - "3b. Potwierdzenie lub zaprzeczenie, o którym mowa w ust. 3a, może otrzymać osoba, której tożsamość została ustalona"

- Prosimy o uzasadnienie, dlaczego do ustalenie zgodności danych z dowodu rejestracyjnego samochodu lub prawa jazdy wymaga się uwierzytelnienia. Użytkownik usługi i tak posiada dane, które ma zamiar zweryfikować, zaś udzielana jest wyłącznie odpowiedź o zgodności bądź jej braku.