

Paweł Krawczyk
ul. Miechowity 15/19
31-475 Kraków
tel +48 602 776959
email pawel.krawczyk@hush.com

Kraków, 28 maja 2010

Ministerstwo Spraw Wewnętrznych i Administracji
ul. Stefana Batorego 5
02-591 Warszawa

Uwagi do projektów rozporządzeń związanych z platformą ePUAP

Uwagi do projektu Ministra Spraw Wewnętrznych i Administracji w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników

W §3 opisane są cechy "systemu certyfikacyjnego". Wcześniej jest on zdefiniowany jako "system teleinformatyczny" (§2 pkt 2) więc niezręczne wydaje się sformułowanie, że "system stwierdza tożsamość" (§3 pkt 3) czy "stosuje zabezpieczenia" (§3 pkt 4). System teleinformatyczny jest narzędziem i w sytuacji osobistego potwierdzenia tożsamości to operator systemu będzie ją stwierdzać, zaś system jedynie taki fakt zarejestruje.

W §3 ust. 1 pkt 2 wymaga się "precyzyjnego określenia czasu" bez podania o jaki wzorzec czasu chodzi, w związku z czym wymóg "precyzji" traci punkt odniesienia.

Wymagania wymienione w ust. 1 uznaje się za spełnione jeśli "podmiot odpowiedzialny za system certyfikacyjny" zapewnia warunki zgodne z wymaganiami CWA 14167. Samo w sobie odniesienie się do tego standardu jest korzystne, ale nieokreślony jest zakres w jakim te wymagania mają być spełniane (czy np. system certyfikacyjny ma spełniać wymagania CWA 14167 dotyczące znakowania czasem?) oraz poziom bezpieczeństwa (CWA 14167 określa dwa, właściwy w tym przypadku wydaje się poziom NQC).

Zasadne wydaje się zatem rozdzielenie funkcji biznesowych od wymagań dotyczących określonego poziomu bezpieczeństwa, które w §3 ust. 1 są wymienione jednym ciągiem. Wartościową publikacją opisującą funkcje biznesowe systemu uwierzytelnienia z podziałem na jednorazową rejestrację użytkownika oraz cykliczne korzystanie z danych uwierzytelniających jest dokument IDABC Authentication Policy.

Właściwe byłoby precyzyjne określenie funkcji biznesowych (np. przyjęcie wniosku, potwierdzenie tożsamości, wydanie certyfikatu, przyjęcie informacji o konieczności anulowania certyfikatu, anulowanie certyfikatu, publikacja certyfikatów, publikacja anulowanych certyfikatów), których oczekuje się od podmiotu odpowiedzialnego za zarządzanie certyfikatami. Lista funkcji biznesowych określi właściwy kontekst do interpretacji poszczególnych wymagań CWA 14167.

Równocześnie oddzielić należy wymagania organizacyjne wobec podmiotu od wymagań technicznych wobec systemu. Wymagania te są zdefiniowane niekonsekwentnie – wobec systemu zarządzania tożsamością wymaga się stosowania i oceny na zgodność ISO 27001, a wobec systemu certyfikacyjnego – zapewnienia warunków zgodnych z CWA 14167.

Normy z serii ISO 27000 są normami organizacyjnymi i powinny być stosowane wobec podmiotu będącego operatorem każdego z tych systemów, a nie wobec systemów jako takich. Nie ma również

powodu by stosować je wobec jednego z nich, a nie stosować wobec drugiego. Jeśli ustawodawca wymaga "oceny zgodności" wg ISO 27001 to należy określić zakres organizacyjny takiej oceny – cały podmiot, wydzielony dział zarządzający systemem itd.

Nieprecyzyjny jest wymóg by (§2 ust 2 pkt 3) stosowania "systemów i produktów zgodnych z wymaganiami standardu CWA 14167-2,3". Standardy te definiują profil ochrony (protection profile), który może być używany jako podstawa do oceny zgodności i uzyskania certyfikatu według Common Criteria.

Nie jest jasne w jaki sposób ta zgodność ma być potwierdzona (deklaracja zgodności, certyfikat CC) a zbyt szeroki zakres ("systemów i produktów") powoduje, że spełnienie tego wymagania jest w praktyce niemożliwe – nie ma np. dysków twardych czy systemów operacyjnych "zgodnych z wymaganiami" CWA 14167-2,3 bo norma ta dotyczy wąskiej klasy urządzeń kryptograficznych.

Ostatnim opisywanym systemem jest system uwierzytelnienia (§5), który jak się wydaje ma być systemem lub systemami wyeksponowanymi do publicznego Internetu, które będą realizować właściwą funkcjonalność uwierzytelnienia zaufanego profilu i innych mechanizmów.

Systemy te będą w największym stopniu narażone na codzienne ataki ze strony sieci publicznej, w związku z czym w szczególności one powinny podlegać rozsądnemu zbiorowi wymagań technicznych jakie zawarto w §3 ust 1 – na przykład wymóg stosowania aktualnego stanu wiedzy czy regularnej oceny skuteczności zabezpieczeń (np. testy penetracyjne).

Jako, że będzie to prawdopodobnie system oparty o technologie web services, warto odwołać się do zaleceń branżowych w zakresie budowy (OWASP Development Guide) oraz testowania takich systemów (OWASP ASVS).

Podsumowując:

- W rozporządzeniu należy najpierw określić funkcje biznesowe, następnie podmioty, które będą je realizować, a potem systemy teleinformatyczne i elementy składowe systemów, które wymagają regulacji.
- Dla tak wydzielonych elementów należy stosować adekwatne standardy – np. ISO 27002 jako zalecenia organizacyjne, CWA 14167 jako standard organizacyjno-techniczny czy ISO 27001 jako standard audytowy.
- Należy precyzyjnie określić poziomy wymagań – zalecenie, deklaracja zgodności, audyt pierwszej strony, audyt zewnętrzny trzeciej strony, certyfikacja przez podmiot akredytowany.
- W przypadku cyklicznych ocen bezpieczeństwa należy określić ich minimalną częstotliwość.

Uwagi do projektu rozporządzenia w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej ("regulamin ePUAP")

§3. ust 2 "siłę kryptograficzną hasła kontroluje ePUAP" – właściwsze byłoby sformułowanie, że system określa minimalny poziom złożoności hasła. Równocześnie jednak poza minimalnym poziomem złożoności celowe wydaje się określenie dodatkowych wymagań jak np. ewentualny czas wymuszonej zmiany hasła oraz sposób odtwarzania hasła w razie jego utraty.

Niniejsze rozporządzenie nie wydaje się być właściwym miejscem do tak niskopoziomowych szczegółów i należy je przenieść albo do rozporządzenia o wymaganiach technicznych albo w ogóle do zewnętrznego dokumentu technicznego tak, by była możliwa jego zmiana bez potrzeby nowelizacji rozporządzeń. W ten sposób możliwe będzie również rozszerzanie katalogu "innych metod uwierzytelnienia (pkt 3) w miarę potrzeb (np. uwierzytelnienia SMS czy tokenem).

§6. Minister powinien być również zobowiązany do przyjmowania zgłoszeń o nieprawidłowościach w działaniu platformy i reagowaniu na nie.

Uwagi do projektu rozporządzenia w sprawie zasad potwierdzania, przedłużania ważności, wykorzystania i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej

§6 ust 1 "osoba wnioskująca, która posiada ważny bezpieczny podpis elektroniczny weryfikowany za pomocą kwalifikowanego certyfikatu" – sformułowanie jest niezręczne, bo podpis elektroniczny generalnie się składa a nie "posiada" (posiada podpis czego?). Zamiast tego należy napisać, że możliwe jest potwierdzenie profilu zaufanego za pomocą podpisu kwalifikowanego jeśli certyfikat zawiera wymienione dane.

§7 oraz §9 brakuje zakończenia ważności profilu jeśli wygaśnie podpis kwalifikowany użyty do jego potwierdzenia.

§10 "Złożenie podpisu (...) wymaga autoryzacji ePUAP" – nie jest jasne czy chodzi o autoryzację "przez ePUAP" (ktoś w ePUAP autoryzuje złożenie podpisu przez użytkownika profilu) czy autoryzację "w ePUAP" (przed złożeniem podpisu użytkownik musi się zalogować w ePUAP czy też będąc zalogowanym w ePUAP potwierdzić ten konkretny podpis).

Nigdzie nie jest także wprost zdefiniowane pojęcie "podpisu potwierzonego profilem zaufanym ePUAP".

Uwagi do uzasadnienia, rozdział "Ocena Skutków Regulacji 4. Wpływ regulacji na rynek pracy; wpływ regulacji na konkurencyjność gospodarki i przedsiębiorczość".

Wbrew zawartej w tym rozdziale deklaracji, że rozporządzenie nie będzie miało wpływu na konkurencyjność wpływ ten będzie jak najbardziej istniał – w danym przypadku głównie pozytywny. Fakt, że "przedmiotu regulacji nie stanowią kwestie związane z konkurencyjnością" nie powoduje, że dana regulacja nie ma wpływu na gospodarkę.

Regulamin Pracy Rady Ministrów, który do procesu legislacyjnego wprowadza instytucję OSR mówi wprost o "przedstawieniu wyników analizy wpływu aktu normatywnego na konkurencyjność wewnętrzną i zewnętrzną gospodarki" (§10 ust 6 RPRM). Analiza taka musi obejmować szacunek rzeczywistych skutków danej regulacji, a nie to czy konkurencyjność stanowi jej przedmiot czy nie. Dokument "Wytyczne do Oceny Skutków Regulacji" opublikowany przez Ministerstwo Gospodarki opisuje precyzyjnie w jaki sposób analizę taką należy tworzyć.

W tym konkretnym przypadku można przewidywać, że wpływ dopuszczenia zaufanego profilu na gospodarkę i konkurencyjność będzie pozytywny, ze względu na zmniejszenie kosztów operacyjnych kontaktów z administracją publiczną obywateli i przedsiębiorców.

Samo tylko zastosowanie zaufanego profilu do deklaracji przesyłanych do ZUS ograniczy koszty przedsiębiorców o ok. 30 mln zł rocznie, które obecnie muszą oni wydawać na odnawianie certyfikatów kwalifikowanych zakupionych w większości firm wyłącznie w wyniku nowelizacji ustawy o informatyzacji w 2005 roku i wyłącznie do kontaktów z ZUS.

Na oszczędności przełoży się również ograniczenie kosztów związanych z przesyłaniem dokumentów papierowych do i od administracji publicznej, a także możliwość wykorzystania tych samych mechanizmów w komunikacji między firmami. Jest to zarówno oszczędność wynikająca z kosztów bezpośrednich (wydruk pisma, pakowanie, obsługa pocztowa, czas pracownika) ale także wynikająca z przyspieszenia obiegu dokumentów elektronicznych.

Biorąc pod uwagę wieloletnie trudności ze zmianą status quo utrwalonego przez ustawę o podpisie elektronicznym z 2001 roku warto by Ministerstwo rozważyło przygotowanie i rozpropagowanie szerszej analizy korzyści ekonomicznych wynikających ze stosowania zaufanego profilu.

Z poważaniem,

Paweł Krawczyk

