

Doghouse: Uroki deklaracji zgodności na przykładzie skrzynki GIODO

<http://ipsec.pl/podpis-elektroniczny/2009/doghouse-uroki-deklaracji-zgodnosci-na-przykladzie-skrzynki-giodo.1>

Przy niedawnej próbie złożenia formularza do {GIODO natrafiłem na problemy, które spowodowały że cała procedura zajęła prawie tydzień. Dodatkowo zaczynam mieć wątpliwości czy i na jakiej podstawie wystawiane są deklaracje zgodności dla różnych produktów podpisu elektronicznego.

{Pierwszy problem pojawił się w momencie wejścia do formularza ESP na stronie {GIODO. Aplikacja wymaga {Internet Explorera działającego pod Windows z prawami administratora oraz doinstalowania (z prawami administratora) specjalnej aplikacji, która zmienia uprawnienia .NET w systemie. O ile instalacje można uznać za rzecz dopuszczalną, o tyle żądanie by przeglądarka działała z prawami administratora jest zwyczajnym błędem projektowym (patrz punkt A.11.2.2 normy PN-ISO/IEC 27001:2007). Z punktu widzenia bezpieczeństwa systemu Windows jest to dość śmieszne w kontekście "wysokiego poziomu bezpieczeństwa" jaki ma zapewniać podpis elektroniczny.

{Drugi problem pojawił się w momencie złożenia dokumentu z załącznikiem, którym był plik JPG zawierający potwierdzenie przelewu opłaty skarbowej. Po elektronicznym podpisaniu i wysłaniu formularza dostałem email, w którym skrzynka poinformowała mnie o ograniczonej liczbie rozszerzeń plików jakie akceptuje. Nie było wśród nich rozszerzenia JPG - było za to "jpg". Wniosek? Projektant aplikacji najwyraźniej nie wiedział, że w systemie Windows wielkość liter nie ma znaczenia w nazwach plików.

{Trzeci problem - najpoważniejszy ujawnił się po kolejnej próbie wysłania formularza z rozszerzeniem pliku zmienionym na "jpg". Otrzymałem mailem Urzędowe Poświadczenie Odbioru i spoczałem na laurach. Po paru dniach otrzymałem kolejny email, tym razem od pracownika, który zwracał uwagę, że mój wniosek jest pozbawiony podpisu elektronicznego. Dalsze śledztwo i eksperymenty szybko doprowadziły do wniosku, że problem leżał po mojej stronie - nie miałem w świeżym systemie zainstalowanych certyfikatów NCC i QCA należących do ścieżki mojego certyfikatu kwalifikowanego. Z punktu widzenia Windows certyfikat był więc nieważny (niemożliwy do zweryfikowania), co widać było od razu po jego podejrzeniu. Nasuwa się jednak pytanie, w jakis sposób aplikacja podpisująca skrzynki podawczej (applet ActiveX) mogła złożyć bezpieczny podpis elektroniczny nie weryfikując ważności certyfikatu?

{Komentarz na temat deklaracji zgodności

Deklaracja zgodności ma charakter dobrowolny i jak mi się wydaje w niektórych przypadkach fikcyjny. Nie jest to absolutnie nawoływanie do zastąpienia jej certyfikacją - to byłby dopiero gwóźdź do trumny podpisu. Być może sytuacje poprawiłaby spójna, pisana z pozycji technicznej, checklista wymagań wobec aplikacji, udostępniona np. przez stowarzyszenie branżowe lub ministerstwo.

Próba uzyskania deklaracji zgodności dla Programu Płatnika zarówno w ZUS jak i Prokombie, która podjąłem kilka miesięcy temu skończyła się w obu instytucjach łańcuszkiem spychotechniki ("to nie my, to oni"). Deklaracji nigdy nie otrzymałem. Czy widział ktoś deklaracje zgodności dla skrzynki podawczej ZETO Białystok albo systemu e-Deklaracje?

Znam przypadek aplikacji do weryfikacji faktur elektronicznych udostępnianej za darmo przez jedno z kwalifikowanych centrów, która radośnie weryfikowała "bezpieczny podpis" złożony przy pomocy samopodpisanego certyfikatu EFS (Encrypted Filesystem) z Windows czy dowolnego.

Najwyraźniej nikt tego nie sprawdza ani nie kwestionuje. Taka strategia wydaje się być uzasadniona o tyle, że jeden taki precedens może spowodować łańcuszek publikacji kompromitujących dla części rodzimych producentów, którzy wyposażyli urzędy w nikomu niepotrzebne rozwiązania w ramach "przetargowej paniki" w latach 2006-2008.

Dla administracji publicznej oznaczałoby to konieczność wymyślania kabalistycznych interpretacji obecnego rozporządzenia tak, by dowieść że to co utrzymują (i z rzadka używają) jest jednak zgodne z prawem. Prawem, które całościowo rozumie zapewne kilkaset osób w Polsce.

<http://ipsec.pl/podpis-elektroniczny/2008/ekscytujaco-prosta-w-uzyciu-skrzynka-podawcza.html>

Gdzie to "bezpieczeństwo" zapewniane przed "bezpieczny podpis", którym tak szermują zwolennicy stosowania podpisu kwalifikowanego wszędzie gdzie się da? I dlaczego do skorzystania ze skrzynki podawczej trzeba mieć doktorat z informatyki ze specjalizacją w PKI oraz platformach do budowy aplikacji webowych?