

Bezpieczeństwo a używalność

<http://ipsec.pl/x509/2007/bezpieczenstwo-uzywalnosc.html>

Kryterium używalności jest często traktowane przez speców od bezpieczeństwa po macoszemu. Niesłusznie, bo jeśli jakieś zabezpieczenie jest mało używalne to użytkownicy go... nie używają. Wynikowe bezpieczeństwo jest więc mniejsze, a koszt - rośnie. Niestety, przykładem takiego wysoce bezpiecznego i wysoce nieużywalnego mechanizmu staje się powoli podpis elektroniczny.

Początkowy entuzjazm podczas tworzenia podwalin współczesnego podpisu opartego o X.509 wspierały hasła takie jak: redukcja kosztów, uproszczenie komunikacji, wysokie bezpieczeństwo okraszone słowami-kluczami takimi jak "walka z cyfrowym wykluczeniem", "e-biznes", "e-government". Co z nich zostało? Głównie sterty zakurzonych papierów.

Zamiast "redukcji i uproszczenia" mamy obecnie:

• kilkanaście niezależnych drzew certyfikacji dla certyfikatów SSL, spiętych przez parodie kotwicy zaufania jaka jest Internet Explorer czy też baza certyfikatów Windows (polecam ją [href="http://www.idg.pl/artty/S.Czarnecki%20Kup%20pan%20podpis"](http://www.idg.pl/artty/S.Czarnecki%20Kup%20pan%20podpis)),
• trzy niezależne drzewa stworzone przez każde z polskich centrów certyfikacji oraz jedno kwalifikowane, spięte przez NCC Contrast,
• Bóg jeden wie ile analogicznych drzew certyfikacji w każdym z 27 Państw Członkowskich Unii i na całym świecie
• jedna polska faktura elektroniczna, która zamiast obniżać koszty i ułatwiać na razie podraża, utrudnia i budzi wątpliwości,
• Bóg jeden wie ile analogicznych faktur elektronicznych w każdym z 27 Państw Członkowskich, a każda inna pomimo że wszystkie niby wywodzą się z tych samych Dyrektyw i tych samych standardów technicznych.

Komisja Europejska [href="http://www.theregister.co.uk/2007/03/06/ec_debates_id/"](http://www.theregister.co.uk/2007/03/06/ec_debates_id/) > *mającycycośonowym, paneu /a > .Wydamy się, że lepiej byłoby na papier skończyć jedną, raz zacząć i rzec, zamiast zadrukowywać kole jnetysiacel*

Osobiście od 1992 roku nieprzerwanie wykorzystuję niedoskonałe (bo nie wbudowane w popularne MUA) i nie pobłogosławione przez żadną świetną komisję OpenPGP. Dokładnie tak samo robi kilkadziesiąt znanych mi firm i instytucji (także państwowych!) Do przesyłania wstępnej wersji raportu z audytu bezpieczeństwa znajomi audytorzy używają PGP. Do poufnej komunikacji z klientami - PGP. Do publikacji dokumentów dla wąskiej grupy partnerów - PGP. Do szyfrowania backupów - PGP.

Przyznam szczerze, że próbowałem - wielokrotnie próbowałem - wdrażać rozwiązania oparte o X.509 w zastosowaniach własnych i w zewnętrznych instytucjach. Dopóki sprawa rozgrywa się w zamkniętym gronie korporacji da się nad tym zapanować. W momencie wyjścia poza granice firmy czy instytucji natychmiast zaczynają się problemy, które w końcu prowadzą do... uruchomienia PGP, szybkiej wymiany kluczy i robienia tego co należy zamiast zabaw z uruchamianiem kolejnych, wzajemnie nieuznawanych drzew certyfikacji. Albo porzucenia szyfrowania w ogóle.

Czy bezpieczeństwo opisanych przeze mnie w artykule [href="http://securitystandard.pl/news/107001/Po.co.nam.SS](http://securitystandard.pl/news/107001/Po.co.nam.SS) co nam SSL?" [i/a](#) stron e-Poltaxu jest wyższe, niż gdyby były one podpisane przez PGP (pomijając że SSL nie używa PGP)? Nie, zaufanie do tej strony jest dokładnie takie samo jak do pobranego ze strony klucza PGP. PKI pełni tutaj rolę kosztownego gadżetu.

Czy mail podpisany certyfikatem wystawionym przez Sigillum (proszę pamiętać, do S/MIME nie można użyć kwalifikowanego) jest bardziej godny zaufania od maila podpisanego PGP? Nie, bo jeśli sam nie mam certyfikatu Sigillum to i tak muszę zaufać certyfikatowi pobranemu z sieci.

Proszę pamiętać, że każde rozwiązanie techniczne służy jakiemuś konkretnemu, bardzo rzeczywistemu i zwykle przyziemnemu celowi, nawet jeśli jest ono tylko małym trybikiem w całym ciągu zdarzeń, które do tego celu prowadzi. Podpis elektroniczny miał zasadniczo uprościć komunikację w biznesie oraz obniżyć koszty fakturowania i kontaktów z administracją. Życie weryfikuje X.509 i jak na razie weryfikuje go negatywnie.

Europejski ped do stosowania rozwiązań w 100