

Uwagi do wywiadu z Elżbieta Włodarczyk w Naszym Dzienniku

<http://ipsec.pl/firmy/2008/uwagi-do-wywiadu-z-elzbieta-wlodarczyk-w-naszym-dzienniku.html>

{ W ja href="http://www.naszdziennik.pl/index.php?typ=poamp;dat=20080321amp;id=po12.txt" ;opublikowanym 21 marca w quot;Naszym Dziennikuquot; wywiadzie z pania Elżbieta Włodarczyk z KIR;|/a; pada kilka tez, które wymagają komentarza.

{ {quot;Proszę pamiętać, że podpisanego dokumentu nie możemy zakwestionować.quot;

{ Rozumiem, że autorka użyła skrótu myślowego. W rzeczywistości Dyrektywa i polska ustawa o podpisie elektronicznym robi wiele, by zapewnić dokumentowi podpisanemu podpisem kwalifikowanym maksymalna wartość dowodowa, pozwalająca zmniejszyć możliwość nieuzasadnionego wyparcia się go przed sadem.

{ ;strong;Nie jest jednak prawda, że quot;nie można zakwestionowaćquot;;/strong; takiego dokumentu - można, tak samo jak można skutecznie zakwestionować ważność dokumentu podpisanego z lufa pistoletu przy skroni, jak i zakwestionować w ogóle nawet bez pistoletu.

{ W kontekście docelowego wykorzystania w przypadku zakwestionowania podpisu kwalifikowanego złożonego na zawirusowanym komputerze kompetenty biegły - a za nim sad - ;strong;powinien wziąć pod uwagę możliwość manipulacji danymi w niezaufanym środowisku, jakim jest quot;bezpieczne urządzeniequot;;/strong; w obecnej definicji. Sad może uznać to za zasadne, albo i nie, ale twierdzenie że quot;podpisu elektronicznego nie można zakwestionowaćquot; jest w oczywisty sposób nieprecyzyjne i może co najwyżej zwiększyć obawy przed stosowaniem podpisu elektronicznego.

{ {span style="background-color: cffc" ;quot;W praktyce więc karta wykona nam operacje podpisywania przy użyciu klucza prywatnego zapisanego na niej, ale nie zapewni kontroli nad tym, co dokładnie podpisujemy. ;/span;{To jest rola aplikacji, która prezentuje dokument{span style="background-color: cffc" ;quot;;/span;

;strong; Aplikacja nie zapewnia pełnej kontroli nad podpisywanym skrótem;/strong; ;strong;i nie ma fizycznej możliwości;/strong; by to zrobić. Aplikacja otrzymuje treść podpisywanego pliku z API Windows i ma niewielką kontrolę nad oryginalnym źródłem tych danych.

{ Byłoby to możliwe gdyby:

- {system operacyjny był systemem klasy quot;trustedquot; i zapewniał mechanizmy bezpiecznej komunikacji wewnętrznej (takie jak quot;bezpieczny kanałquot;),
- {lub gdyby aplikacja uruchamiała się jako jedyna w komputerze w charakterze systemu operacyjnego i posiadała wbudowaną implementację systemu plików, na którym znajdują się podpisywane dane.

{ Warunki te są oczywiście całkowicie niepraktyczne dlatego się ich nie stosuje do popularnych aplikacji.

{ Dlatego podkreślę jeszcze raz: ;strong;aplikacja do składania podpisu, działająca w standardowym systemie Windows ;/strong;(czy Linux);strong; ma ograniczoną kontrolę nad tym, skąd faktycznie pochodzą dane podpisywane;/strong;. W praktyce możliwości kontroli nad przepływami tych danych są bardzo duże w takich systemach, zarówno za pomocą metod przewidzianych przez producenta (ja href="http://www.microsoft.com/whdc/driver/filterdrv/default.msp" ;filtry systemu plików;/a;) jak i tworzonych przez niezależnych badaczy i quot;podziemiequot; (ja href="http://www.idg.pl/news

{ Zostało to w praktyce ja href="http://www.computerworld.pl/news/news.asp?id=83636" ;zademonstrowane w 2005 roku przez firmę G DATA;/a;. Demonstracja ta wywołała szeroki oddźwięk i zaowocowała ja href="http://www.certum.pl/certum/47966.xml" ;dementi ze strony firmy Certum;/a;. Firma Certum ;strong;nie zakwestionowała jednak w żaden sposób praktyczności;/strong; tego ataku tylko terminologię i wnioski firmy G DATA.

{ Certum przyznało równocześnie że nazywanie quot;bezpiecznego podpisuquot; quot;bezpiecznym podpisemquot; jest niezbyt fortunne.

{ quot;{i zapewnia bezpieczna komunikacje z karta, spełniająca określone wymogi bezpieczeństwa.quot;}span style="background-color: cffcc" i /span i

{ W obecnym stanie prawnym istrong; aplikacja podpisująca nie zapewnia bezpiecznej komunikacji z karta! i/strong;Po pierwsze dlatego że istrong;nie może;/strong; - bo z karta komunikuje się znowu tylko przez pośredników (CSP, sterowniki czytnika) - a po drugie dlatego że istrong;nie musi;/strong;.

{ Rozporządzenie o warunkach technicznych dla bezpiecznego urządzenia wprowadziło kategorie istrong;quot;oprogramowania niepublicznegoquot;;/strong; dla którego wprost z istrong;nosi obowiązek stosowania quot;bezpiecznego kanałuquot; i quot;ścieżkiquot;;/strong; do komunikacji z karta i dokumentem. Można się zastanawiać, co powoduje że oprogramowanie jest quot;niepublicznequot;?

{ W definicji ustawowej niepubliczne jest system do którego w zwykłych warunkach {quot;nie ma dostępu każdyquot;. I tu następuje kuriozalne wyliczenie, że niepubliczne jest {quot;oprogramowanie w biurze, domu i telefonie komórkowymquot;. Kuriozalne, bo istrong;w XXI wieku do komputera podłączonego przez 24h do Internetu na publicznym adresie IP ma dostęp każdy, z całego świata;/strong;.

{ W praktyce więc główna podstawa dla której z prawnego punktu widzenia uznajemy dane oprogramowanie za niepubliczne jest... jedno zdanie z podrecznika, które mówi: {quot;aplikacja X istrong;nie jest;/strong; oprogramowaniem publicznym w rozumieniu rozporządzeniaquot;. Niewątpliwie taka klauzula zdejmuje odpowiedzialność z producenta, ale istrong;nie ma żadnego wpływu na faktyczne bezpieczeństwo końcowego użytkownika;/strong;.

{ Z równym powodzeniem można na czerwonej skrzynce na listy napisać {quot;ta skrzynka nie jest czerwona w rozumieniu rozporządzeniaquot; i efekt dla świata materialnego będzie ten sam.

{ {i span style="background-color: cffcc" i quot;Dlatego właśnie w Polsce quot;bezpiecznym urządzeniemquot; do składania e-podpisu jest całość: karta kryptograficzna wraz z certyfikatem kwalifikowanymquot;;/span i

To musi być błąd redakcyjny, bo istrong;albo i/strong;quot;całośćquot; istrong;albo i/strong;wymieniony jako rozwinięcie quot;komponent technicznyquot; czyli karta. Karta jest elementem, a nie całością quot;bezpiecznego urządzeniaquot;.

{ W świetle rozporządzenia o warunkach technicznych quot;bezpieczne urządzeniequot; składa się z quot;komponentu technicznegoquot; (karty) i quot;oprogramowania podpisującegoquot;, co zresztą jest już poprawnie ujęte w ja href="http://www.naszdziennik.pl/index.php?typ=poamp;dat=20080321amp;id=po11.t artykułej/a: {quot;bezpiecznego urządzenia do składania e-podpisu (na które składa się karta kryptograficzna wraz z oprogramowaniem oraz aplikacja podpisująca)quot;.

{ Niezależnie od tej definicji, istrong;twierdzenie że sama aplikacja zabezpieczy użytkownika przed atakami jest mylące;/strong;, czego dowodem była demonstracja G DATA.

{ i span style="background-color: cffcc" i quot;Wspomniana aplikacja powinna zabezpieczyć nas przed niepożądanymi ingerencjami osób trzecich w treść dokumentu.quot;;/span i

istrong;Może i powinna, ale tego nie gwarantuje i w standardowym systemie nigdy nie będzie gwarantować;/strong;, o czym pisałem wcześniej.

{ Myląca jest w ogóle sugestia, że quot;specjalna aplikacjaquot; zapewnia iu; radykalnie i/u; większy poziom bezpieczeństwa końcowemu użytkownikowi niż np. wbudowane w popularne aplikacje biurowe funkcje podpisu elektronicznego.

{ Rola karty kryptograficznej jest jednoznaczna bo chroni ona klucz prywatny przed skopiowaniem, co mogłoby mieć katastrofalne skutki.

{ Tymczasem rola „specjalnej aplikacji” jest znacznie mniej krytyczna - chroni ona przed pewnymi specyficznymi atakami, z naciskiem na „pewnymi” i „specyficznymi”. Inne wynikające z rozporządzenia i ustawy obowiązki to np. umożliwienie prezentacji (ale nieobowiązkowe) i wyświetlenie ostrzeżenia o możliwych konsekwencjach podpisu. Obie te funkcje są w jakimś stopniu obecne w każdej innej aplikacji podpisującej, tyle że „specjalne aplikacje” mają je zaimplementowane w sposób dosłowny.

{ Zaś z punktu widzenia użytkownika główna różnica jest taka, że złożenie podpisu w Wordzie to (przykładowo) trzy okienka i PIN, a w „specjalnej aplikacji” - sześć okienek i PIN, często dodatkowo ukraszone interfejsem użytkownika o ergonomii Windows 95. Dlatego proszę się nie dziwić, że ludzie nie chcą z nich korzystać, dopóki nie muszą.

{ To „nie jest strach przed nowym”, stosowany ostatnio jako dyżurny argument - to jest po prostu „niechęć do rozwiązań zaprojektowanych niemądrze, niewygodnie i w sposób utrudniający wykonywanie pracy zamiast ułatwiać”.

{ Rozumiem, że centra certyfikacji muszą poruszać się w ramach nakreślonych przez ustawę. Nie znaczy to jednak, że powinny tracić kontakt z rzeczywistością.

{ Najważniejsza rzecz, jaka odróżnia certyfikat zwykły e-podpisu od kwalifikowanego, jest dokładne sprawdzenie danych osobowych przed jego wydaniem

Jest to teza wprowadzająca w błąd użytkownika bo sugerująca, że istnieje coś takiego jak „silny” certyfikat kwalifikowany i „słaby” certyfikat zwykły. Tymczasem coś takiego jak „certyfikat zwykły” nie istnieje. Istnieje wiele certyfikatów niekwalifikowanych, wystawianych na bazie różnych polityk i o różnych poziomach bezpieczeństwa.

{ Niektóre z nich mają poziom bezpieczeństwa „prawie taki sam” jak certyfikat kwalifikowany. Certyfikat niekwalifikowany wydany w ramach polityki Certum IV jest niemal tak samo dokładnie zweryfikowany jak kwalifikowany.

{ Co je w takim razie różni? To, że certyfikatem niekwalifikowanym można złożyć podpis w Wordzie, Excelu czy OpenOffice, a kwalifikowanym - nie. A w każdym razie nie będzie to podpis kwalifikowany.

{ Banki „mBank” i „Multibank” co miesiąc wysyłają setki tysięcy sald kont podpisanych elektronicznie - oczywiście certyfikatem niekwalifikowanym, bo tylko tak mogą to robić z automatu. Tysiące sklepów internetowych i banków od lat korzysta z certyfikatów niekwalifikowanych do zapewnienia autentyczności swoich stron.

{ Czy jest to „niebezpieczne”? Czy tożsamość banków jest „niedokładnie sprawdzona”? Oczywiście że nie. Są to „wystarczająco bezpieczne” i „wystarczająco używalne” certyfikaty, by stać się rynkiem masowym.

{ Tylko w niewielu krajach na świecie (m.in. Polsce i Niemczech) udało się wytworzyć stan psychozy, w którym wobec bliżej niesprecyzowanego zagrożenia jako jedyny dopuszczalny stosuje się „bardzo” bezpieczny „i” (a w praktyce średnio) „ale i bardzo nieużywalny” podpis kwalifikowany, a gdy rynek odmawia jego stosowania to postuluje się stosowanie przymusu administracyjnego.