

Potrzeba różnych polityk uwierzytelnienia

<http://ipsec.pl/administracja-publiczna/2008/potrzeba-roznych-polityk-uwierzytelnienia.html>

{W toczącej się obecnie dyskusji na temat podpisu elektronicznego dominują dwa przeciwstawne stanowiska - według jednego z nich bezpieczny podpis jest za silny", według drugiego dla odmiany za słaby" jest podpis zwykły, cokolwiek przez niego rozumiemy.

{Dyskusja na ten temat jest całkowicie jałowa bez precyzyjne pytanie - silny, słaby, ale do czego konkretnie? Bez końca można bowiem debatować o tym czy jakieś zabezpieczenie jest za silne" czy za słabe", jeśli nie powie się jasno co ma być chronione i przed czym.

{Problem ten objawił się w ostatnich kontrowersjach dotyczących polityki autoryzacji certyfikatów przez Ministerstwo Finansów (rejestracja wymagana) i ZUS (rejestracja nie wymagana). Jeden obóz" dowodzi, że autoryzacja jest absolutnie konieczna, a drugi - że absolutnie zbędna.

{Przy takim postawieniu sprawy można pomyśleć, że błędzi albo MF albo ZUS. W rzeczywistości jednak wcale nie musi tutaj mieć miejsca tego typu konfrontacja. Racje może mieć każde z ministerstw z osobna, stosując taki model autoryzacji, jaki odpowiada jego wymaganiom i jego profilowi ryzyka.

{W całym sporze brakuje racjonalnej analizy ryzyka oraz odpowiadającej na nią gradacji zabezpieczeń. W świecie papierowym poziomów zaufania są listy polecone, faksy, poświadczony kopie dokumentów, weryfikacja przelewem i wreszcie, do najpoważniejszych spraw, notariusze.

{Zredukowanie wszystkich poziomów uwierzytelnienia w świecie elektronicznym do najdroższego i najtrudniejszego w stosowaniu podpisu kwalifikowanego musi powodować opór w jego wdrażaniu, ponieważ jest to narzędzie znacznie przerastające potrzeby.

{Żadnemu urzędnikowi nie przyszłoby do głowy zadać notarialnego poświadczenia wniosku w prostej sprawie administracyjnej, bo przesadne niedostosowanie tego mechanizmu do wymagań jest oczywiste. Tymczasem w świecie elektronicznym to niedostosowanie przyjmowane jest jako konieczność i na siłę uzasadniane względami bezpieczeństwa".

{Błędem jest sprowadzanie całej debaty do argumentu, że podpis kwalifikowany zapewnia wysoki poziom bezpieczeństwa" i dlatego musi być stosowany. Istotnie - zapewnia. Ale zabezpieczenie ma gwarantować, że wartość chroniona będzie używana w sposób bezpieczny - z akcentem na używana". Zabezpieczenie, które uniemożliwia korzystanie z chronionego zasobu powoduje skutek przeciwny do zamierzonego i zaczyna mieć więcej wspólnego z atakiem typu denial of service".

{Patrzac na pięcioprocentowe wykorzystanie faktury elektronicznej w Polsce (5

{Jednym z elementów zarządzania ryzykiem wskazywanym przez normę PN ISO/IEC 27001:2007 jest analiza kosztów i korzyści (za: {Krzysztof Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych", PWN 2008), polegająca na:

{1. Oszacowaniu możliwych strat, jeśli poziom zabezpieczeń będzie minimalny i zrealizują się wszystkie zagrożenia (co wymaga uprzedniego określenia zagrożeń),

{2. Obliczeniu kosztów technicznych i organizacyjnych (co powinno uwzględniać wszystkie koszty bezpośrednie i pośrednie, które szczególnie mocno ujawniają się w przypadku podpisu kwalifikowanego),

{3. Oszacowanie nakładów łącznych zabezpieczeń i sprawdzenie czy są akceptowalne przy zadanym wskaźniku nakładów na postępowanie z ryzykiem.

{Polskie prawodawstwo bardzo potrzebuje takiego procesu, wykonanego jako kluczowy element informatyzacji. Jego brak powoduje widoczne odrealnienie projektów informatycznych administracji publicznej, niejednokrotnie opóźnienia i pogłębianie wykluczenia informatycznego zamiast jego niwelowania.

{Postulowane niekiedy stosowanie przymusu administracyjnego w celu przekonania" obywateli i upowszechnienia" nieprzydatnych narzędzi wynika z mylenia skutków z przyczynami i może mieć jedynie efekt odwrotny do zamierzonego.

{Z dotychczasowych doświadczeń wylania się krytyczna potrzeba stworzenia polityki, określającej minimalne wymagania bezpieczeństwa dla procesów administracyjnych w zależności od ich konsekwencji prawnych.

{Pierwszym krokiem jest określenie wymagań bezpieczeństwa różnych procesów urzędowych

- { **Poziomy gwarancji tożsamości** osób lub podmiotów biorących udział w tych procesach (np. niski, średni, wysoki),
- { **Funkcje bezpieczeństwa**, które muszą być zapewnione w każdym procesie (np. autentyczność, integralność, niezaprzeczalność, poufność, anonimowość) oraz na jakich **poziomach** muszą być spełnione (np. niski, średni, wysoki).

{Następnie należy stworzyć **katalog mechanizmów uwierzytelniających** realizujących wyżej wymienione postulaty (ma to jednak sens dopiero po określeniu potrzeb). Znajda się tam różne formy podpisu elektronicznego (kwalifikowany, różne polityki komercyjne, na karcie lub bez karty, ze specjalną aplikacją lub bez), mechanizmy oparte o potwierdzone z różną ufnością dane oferowane przez protokoły federacji tożsamości (CardSpace, OpenID), mechanizmy oparte o pocztę lub kurierów i wiele innych. Katalog musi określać poziom realizacji gwarancji tożsamości oraz funkcji bezpieczeństwa przez dany mechanizm.

{Ostatnim krokiem jest **przyporządkowanie mechanizmów zapewniających poziomy bezpieczeństwa** odpowiednie dla poszczególnych procedur. Należy tutaj zwrócić uwagę na ryzyko asekuracyjnego i nieuzasadnionego zawyżania wymagań (podobnie jak w administracjach na całym świecie istnieje tendencja do zawyżania klasyfikacji informacji niejawniej nawet jeśli jest to konieczne), którego unikanie jest niezwykle ważne na etapie tworzenia specyfikacji.

{Dzięki takiemu przyporządkowaniu administracja publiczna realizując systemy teleinformatyczne nie będzie miała wątpliwości jaki mechanizm faktycznie musi (i może) zastosować, co pozwoli jej uniknąć stosowania mechanizmów niepotrzebnie zawyżonych na wszelki wypadek”.

{Gdyby dla faktur elektronicznych przeprowadzono racjonalną analizę ryzyka, to okazałoby się, że jedyne wymagane tutaj funkcje to autentyczność oraz integralność, oraz potwierdzona na średnim poziomie tożsamość podmiotu.

{Wynika to z faktu, że fakturowanie elektroniczne - jeśli ma istotnie zwiększać konkurencyjność firmy - powinno być prowadzone półautomatycznie. Rola osoby fizycznej powinna ograniczyć się do autoryzowania rozpoczęcia procesu wystawiania i wysyłki faktur. Ochrona autentyczności na średnim poziomie jest z kolei konieczna dla uniknięcia masowych wyłudzeń przez fałszowanie np. numerów kont.

{Mechanizmem zapewniającym **wystarczający poziom gwarancji** byłby tutaj komercyjny certyfikat SSL na serwerze udostępniającym faktury klientom po wejściu na ich konto, lub używany do podpisywania plików z fakturami za pomocą standardowego oprogramowania (praktyka taka od kilku lat stosują co najmniej dwa polskie banki do wysyłania wyciągów z kont w formacie PDF).

{Zastosowanie w tym przypadku podpisu kwalifikowanego oczywiście też zapewnia te funkcje i to nadmiarowo. Jednak zapewniane przez nie bardzo silne gwarancje tożsamości osoby fizycznej, silna funkcja niezaprzeczalności i ochrona przed wyrafinowanymi atakami są w tym konkretnym przypadku nie tylko zbędne, ale w dużym stopniu niweczą sens elektronicznego fakturowania.

{Dostrzegli to autorzy unijnej dyrektywy 2001/115, która wyraźnie mówi tylko o autentyczności i integralności. Dostrzega to biznes na całym świecie, który od ponad dekady zabezpiecza serwery SSL certyfikatami - niekwalifikowanymi przecież - wystawianymi na podstawie dokumentów przesłanych faksem.

{Dostrzegają to firmy polskie, które w kreatywny sposób radzą sobie z problemem potwierdzenia tożsamości użytkowników bez odstraszenia ich zbyt restrykcyjną procedurą - serwisy aukcyjne stosują kody przesyłane listem poleconym, przelewy na groszowe kwoty czy potwierdzenie tożsamości przez kuriera, realizowane przy doreczeniu pakietu startowego.

{Zaczyna to wreszcie dostrzegać administracja polska zapowiadając wprowadzenie podpisu zaawansowanego (certyfikat kwalifikowany, ale bez specjalnej aplikacji), pieczętarki cyfrowej” czy wreszcie zaufanych profili.

{Problem w tym, że samo w sobie udostępnienie takich mechanizmów niczego nie zmieni, jeśli nie będzie poparte racjonalnymi wytycznymi jasno określającymi, które z nich gdzie i na jakich zasadach można stosować, oraz jeśli ich katalog będzie zbudowany na oko”.