

Doghouse: skrzynka podawcza E-Studio

<http://ipsec.pl/podpis-elektroniczny/2008/doghouse-skrzynka-podawcza-e-studio.html>

{ Cześć druga cyklu `quot;Jak nie implementować elektronicznej skrzynki podawczej?quot;`, tym razem na podstawie skrzynki udostępnionej przez powiat mławski.

{ Skrzynka jest dostępna pod adresem `ja href="https://powiatmlawski.skrzynkapodawcza.pl/"` `;``https://powiatmlawski` ale jest to alias DNSowy koncentrujący wiele serwerów wirtualnych na jednym serwerze. `ih1;`Niezaufane certyfikaty `ih1;`

{ Pierwsze co zwraca uwagę po wejściu na stronę to ostrzeżenie o `istrong;niezaufanym` certyfikacie serwera SSL`istrong;`. I słusznie, bo jest to certyfikat samopodpisany wystawiony przez firmę `ja href="http://www.estudio.com.pl/index.php"` `;`E-Studio sp.j.`ia;` dla wszystkich poddomen `{skrzynkapodawcza.pl` (tzw. certyfikat `{wildcard`). W przypadku dowolnego produkcyjnego serwera SSL jest to błąd w sztuce. W przypadku serwera administracji publicznej jest to zbrodnia. Dlaczego?

{ Użycie niezaufanego, w tym przypadku samopodpisanego, certyfikatu `istrong;zmusza` `istrong;` użytkownika to `istrong;pominiecia` `istrong;` wszelkich ostrzeżeń i `istrong;zaakceptowania` `istrong;` niezaufanego certyfikatu bez żadnej pewności że jest to certyfikat autentyczny.

{ Po to przecież właśnie wprowadzono uwierzytelnienie serwera SSL certyfikatem poświadczonym przez zaufaną trzecią stronę, by użytkownik mógł z dużą dozą zaufania i bez konieczności zgadywania wysłać swoje dane do serwera.

{ Używanie na stronie niezaufanego certyfikatu `iu;` przez administrację publiczną`iu;` jest zbrodnia, bo dodatkowo `istrong;przyzwyczajaja` `istrong;` użytkownika do takiej praktyki i `istrong;poświadcza` `istrong;` ją autorytetem rządu. Naraża to użytkowników na późniejsze ataki ze strony cyberprzestępców.

{ Apeluje o niestosowanie takich certyfikatów przez administrację publiczną. Domagajcie się od dostawców certyfikatu weryfikującego się poprawnie co najmniej MSIE i Firefoksie.

{ Zdaje sobie sprawę że `ja href="http://www.idg.pl/news/93693.html"` `;`stajnia VeriSignu (czyli obecnie także Thawte i GeoTrust)`ia;` są drogie, ale przecież weryfikujący się poprawnie w Windows certyfikat SSL można kupić w `ja href="https://www.godaddy.com/gdshop/ssl/ssl.asp?check`

{ Proszę też pamiętać, że certyfikat wystawiony w dowolnym drzewie polskich centrów certyfikacji `istrong;KIR` i `Sigillumistrong;` jest z punktu widzenia SSL certyfikatem `istrong;niezaufanym` `istrong;` - z błędnym przekonaniem że jest inaczej można się zetknąć w serwisie `ja href="https://e-poltax.mf.gov.pl/"` `;`e-Poltax`ia;` (podpisany przez PWPW, wyskakuje ostrzeżenie), ale już e-`ja href="http://www.securitystandard.pl/artykuly/57285/Jak.rozliczyc.VAT.przez.Internet..html"` `;`Deklaracje `ia;` są podpisane przez VeriSign.

{ Warto zauważyć, że tak samo niezaufane certyfikaty są stosowane do podpisywania aplikacji Java opisywanych poniżej. `ih1;`Błędy w implementacji`ih1;`

{ Po wejściu dalej na stronę skrzynki i próbie wysłania czegokolwiek próbują się załadować applety Javy opisane jako SZAFIR, co sugeruje że skrzynka do podpisu kwalifikowanego wykorzystuje komponenty KIR.

{ Niestety, albo KIR nie dba o swoich klientów albo autor aplikacji wykazał się niedbalstwem, bo applet nie potrafi załadować bibliotek kryptograficznych ze strony KIR. Powód jest bardzo prosty - nie ma ich pod zakodowanym w appletcie linkiem! `ipre;` `java.io.FileNotFoundException: ja href="http://www.kir.com.pl/szafir/sdk/1.3.2-build051/cryptointerface.jar"` `;``http://www.kir.com.pl/szafir/sdk/1.3.2-build051/cryptointerface.jaria;` `ipre;`

{ Proszę kliknąć na ten link by zobaczyć to samo co widzi applet: `ipre;` `istrong;404 Not Foundistrong;` The requested URL `/szafir/sdk/1.3.2-build051/cryptointerface.jar` was not found on this server. `{Apache/1.3.34 Server at www.kir.com.pl Port 80 ipre;` `ih1;`In plus`ih1;`

{ Pluszem tej skrzynki podawczej - na ile możliwe było jej przetestowanie - jest fakt, że autor włożył sporo wysiłku w obsłużenie `ja href="http://blog.securitystandard.pl/news/143670.html"` `;`formatowego

chaosu wprowadzonego przez polskie firmy prowadzące informatyzację urzędów publicznych/a. Ponieważ nie udało mi się przetestować tego w praktyce, więc opieram się na opisach w plikach pomocy. Wynika z nich że skrzynka stara się obsłużyć maksymalną ilość komponentów tego grochu z kapusta:

- {skrzynka akceptuje formaty podpisu enkapsulujące dokument w środku, jak i sam dokument wraz z podpisem zewnętrznym (typowe opcje w aplikacjach proCertum SecureSign, Sigillum SignPro i KIR SZAFIR)
- {jspan style="background-color: 99cc00"}skrzynka umożliwia podpisanie dowolnego dokumentu tekstowego z poziomu strony WWW przy pomocy appletu Java, co byłoby rozwiązaniem maksymalnie otwartym i neutralnym technologicznie w ramach wiezów obecnej/prawiaj/spani, oczywiście gdyby tylko działało

{ Na pochwałę zasługują także jspan style="background-color: 99cc00"}przejrzyste pliki pomocy kontekstowej na każdej stroniej/spani.

{ Dodatkowo wygląda na to, że jspan style="background-color: 99cc00"}skrzynka zwraca UPO w formacie PDFi/spani (wnioskuję ze strony do jego weryfikacji). Jeśli tak, to jest to mentalna rewolucja w naszej administracji, która z uporem forsuje swoje prywatne formaty UPO, co ja href="/podpis/podpis-elektroniczny/2008/ekscytujaco-prosta-w-uzyciu-skrzynka-podawcza.html"}opisywałem już na przykładzie strony UMKi/a. Założyłem się jednak, że jspan style="background-color: ff0000"}PDF jest podpisany... znowuż tym nieszczęsnym, samopodpisanym certyfikatemj/spani o którym było wyżej.

{ nbsp;

{ nbsp;

{ P.S. nazwa quot;doghousequot; pochodzi od cyklu ja href="http://www.google.pl/search?hl=pl&client=firefox-a&rls=org.mozilla:pl:official&hs=On&q="+site:www.schneier.com+schneier+doghouse"}quot;Doghousequot; prowadzonego od lat przez Bruce Schneieraj/a, w którym pietnuje on firmy wprowadzające na rynek rozwiązania kryptograficzne zawierające fundamentalne błędy, zazwyczaj równocześnie w ekstatycznej otoczce marketingowej.