

Urzedowe poświadczenie odbioru w formacie PDF

<http://ipsec.pl/firmy/2008/urzedowe-poswiadczenie-odbioru-w-formacie-pdf.html>

{ W chwili obecnej Urzedowe poświadczenie odbioru (UPO) jest generowane przez skrzynki podawcze (ESP) różnych dostawców z tym samym zamiłowaniem do chaosu, jakie cechuje formaty podpisu elektronicznego od początków polskiej informatyzacji. W jaki sposób można to uporządkować pozostając w ramach obowiązującego prawa?

{ Otóż proszę pamiętać, że rozporządzenie które wprowadziło pojecie ESP i UPO [ja href="#">/podpis_elektroniczny/uo/1](#)

{ Co to znaczy w praktyce? Przede wszystkim to, że [jstrong;certyfi](#)kat użyty do złożenia podpisu pod UPO nie musi być kwalifikowany [i/strong; i](#) że podpis ten [jstrong;można](#) składać oraz weryfikować praktycznie w dowolnym oprogramowaniu [i/strong;.](#)

{ Autorzy znanych mi skrzynek podawczych poszli w kierunku tradycyjnie [ja href="#">"http://blog.securitystandard.pl/new](#) pojętej innowacyjności [i/a; -](#) każdy wymyślił to po swojemu. I tak, skrzynka podawcza [jstrong;Zeto](#) Białostok [i/strong;](#) zwraca UPO jako wymyślony przez siebie XML z podpisem w formacie XML-DSig i rozszerzeniem [jstrong;ZSI/strong;.](#)

{ Skrzynka podawcza [jstrong;Certum](#) [i/strong;](#) zwraca z kolei plik w formacie S/MIME z podpisem PKCS7 i rozszerzeniem [jstrong;EML/strong;.](#) To ostatnie można uznać za rozwiązanie przenośne, bo plik taki weryfikuje bez problemu Outlook lub Thunderbird.

{ Ale inne rozwiązanie jest stosowane... przez banki - mBank i MultiBank od dawna wysyła ją klientom mailem [ja href="#">"http://multibank.pl/images/MultiBank2/Portal/BinaryPL/83888/przykladowy_wyciag83888.pdf](#) [saldarachunków w postaci < strong > dokumentu PDF podpisanego certyfikatem VeriSign . *Taki plik otwierasz bez problemu w Acrobatcie – co najważniejsze – automatycznie weryfikuje się i boczny certyfik h1 > W kontekście – faktury dla zwolenników* *quot; bezpiecznego podpisu* *quot; ; ... </h1 >*](#)

{ Przechodząc od UPO do e-faktur, proszę się zastanowić, które z poniższych zapewni odbiorcy końcowemu [jstrong;wyższy](#) poziom bezpieczeństwa [i/strong;](#) już [jstrong;faktycznego](#) [i/strong; ;/u;](#)

- [jstrong;automatycznie](#) [i/strong;](#) weryfikujący się podpis w jednym pliku PDF (złożony przy pomocy certyfikatu VeriSign, GoDaddy czy innego znanego Windows),
- [jstrong;niepodpisany](#) plik PDF z e-faktura, do którego dołączony jest [jstrong;drugi](#) [i/strong;](#) plik z podpisem, który trzeba [jstrong;recznie](#) [i/strong;](#) weryfikować [jstrong;oddzielna](#) [i/strong;](#) aplikacja (tak to jest zrobione w e-fakturze Sigillum)

{ Pytam, bo wczoraj na konferencji [ja href="#">" /podpis/firmy/2008/konferencja-quote-dokumentquot-13-marca-2008.html"](#) [;e-Dokument/;a;](#) przedstawiciel PWPW/Sigillum bez żadnego skrepowania mówił, że *quot;oczywiście mało kto taki podpis faktycznie weryfikuje, co najwyżej za pierwszym razem* *quot; ;.*

{ Na moje pytanie czy biorą pod uwagę możliwość masowej wysyłki fałszywych faktur z podmiennym numerem konta np. gdy taki system stanie się masowy (wdraża go TPSA, Tele2) odpowiedziano że *quot;to wina użytkownika, że nie korzysta z dostarczonego zabezpieczenia* *quot; ; (wszystkie cytaty z pamięci).*

{ Moje kolejne pytanie o sensowność zabezpieczenia, które wprost [jstrong;zniechca](#) [i/strong;](#) do korzystania z niego pozostało bez odpowiedzi...