

## Czy nie należy odesłać DER na emeryture?

<http://ipsec.pl/x509/czy-nie-nalezey-odeslac-der-na-emeryture.html>

Czy dzisiaj, wobec dominacji XML wśród formatów dokumentu elektronicznego i protokołów sieciowych, nie należałoby stopniowo odchodzić od pochodzących z innego świata wtrąceń kodowanych w DER?

Mamy `<a href="http://ipsec.pl/podpis-elektroniczny/openxml">OOXML</a>`, `<a href="http://ipsec.pl/podpis-elektroniczny/odf">ODF</a>`. Mamy też `<a href="http://ipsec.pl/podpis-elektroniczny/dokument-elektroniczny/standardy`

`>` `<a href="http://ipsec.pl/files/ipsec/Archiwum/test_files/sigillumpro`

W strukturze XML pole X509Data to wtret z innego świata i z punktu widzenia aplikacji przetwarzającej dokument jest to struktura nieprzezroczysta. Żeby trochę ułatwić aplikacji wgląd w tę strukturę do drzewa XML skopiowane zostało kilka pól z certyfikatu (`{X509IssuerSerial, {X509SubjectName` itd) ale to tylko półśrodek.

Wgląd w pozostałe pola certyfikatu jest możliwy tylko w jeden sposób - przez odtworzenie takiego `<a href="http://en.wikipedia.org/wiki/Binary_large_object">bloba</a>` *izdekodowanie DER. Wady takiego podejścia:*

• *niższa efektywność* - aplikacja przetwarzająca drzewo XML musi uruchamiać dodatkowy dekodery DER • *większa złożoność* - poza jednym modulem do przetwarzania XML aplikacja musi używać drugiego - do DER; złożoność ma konsekwencje dla bezpieczeństwa - zamiast jednej `<a href="http://secunia.com/advisories/31558">` dziury w parserze XML `</a>` aplikacja będzie mieć ich dwie - `<a href="http://secunia.com/advisories/18794">` druga w parserze DER `</a>`; oba dekodery są bardzo złożone, mają inną filozofię, inne standardy, API itd. • *mniejsza funkcjonalność* - ponieważ certyfikat nie jest integralną częścią drzewa XML, nie jest możliwe przeszukiwanie go za pomocą XPath i inne formy szybkiego przetwarzania

W jakim kierunku powinna pójść zatem ewolucja standardów elektronicznej tożsamości i podpisu elektronicznego?

Teoretycznie nic nie stoi na przeszkodzie by X.509 kodować jako XML, bo standard wyraźnie oddziela opis struktur (ASN.1) od kodowania (BER, DER). Istnieje nawet mało znane kodowanie XML Encoding Rules - XER (`<a href="http://www.itu.int/ITU-T/studygroups/com17/languages/X.693-0112.pdf">` X.693 `</a>`) lub nowsze Robust XML Encoding Rules - RXER (`<a href="http://www.faqs.org/rfcs/rfc4910.html">` 4910 `</a>`), które można zastosować do zapisania certyfikatu X.509 jako struktury XML. Zachowują one jednak filozofię X.509.

W nieco szerszej perspektywie wydaje mi się jednak, że czas X.509 powoli przemija. Architektura X.509 ma wiele wad, z których głównymi są `<a href="http://ipsec.pl/x509/2006/x509-keyusage-mylace-rozszerzenie.html">` hermetyczność standardów `</a>`, `<a href="http://blog.securitystandard.pl/news/347769.html">` architektury `</a>` oraz `<a href="http://ipsec.pl/kwalifikowany-podpis-elektroniczny/2008/co-poswiadcza-certyfikat-czyli-brak-autoryzacji-w-zus.html">` ograniczona funkcjonalność `</a>`, łataną później za pomocą certyfikatów atrybutów i innych dodatków.

Być może rozwiązaniem byłaby filozofia `<a href="http://pl.wikipedia.org/wiki/SPKI">` SPKI/SDSI `</a>`, opakowana w XML zamiast nieco archaicznych s-wyrażeń i pozbawiona `<a href="http://www.cs.auckland.ac.nz/pgut00">` wad `</a>` XML-DSig?