

X.509 keyUsage - mylące rozszerzenie

<http://ipsec.pl/x509/2006/x509-keyusage-mylace-rozszerzenie.html>

Jednym z podstawowych rozszerzeń certyfikatu ({certificate extension} wprowadzonych przez standard X.509v3 było rozszerzenie {keyUsage}. Przypomnijmy, że w X.509v1 certyfikat był - w skrócie - po prostu kluczem publicznym podmiotu ({code;subjectPublicKeyInfo;/code;}) z jego opisem ({code;Subject;/code;}) oraz podpisem wystawcy ({code;signatureValue;/code;}). Tak opisany klucz mógł być więc wykorzystywany do dowolnego celu niezależnie od intencji wystawcy lub właściciela. A to jest niebezpieczne...

Aby dać osobie weryfikującej cudzy certyfikat możliwość sprawdzenia czy został on zastosowany zgodnie z przeznaczeniem certyfikat X.509 zawiera dwa ważne rozszerzenia:

 |li;{keyUsage - rozszerzenie określające dopuszczalny zakres zastosowań klucza prywatnego
 |li;{basicConstraints - rozszerzenie określające czy dany klucz prywatny może podpisywać inne certyfikaty

{keyUsage

Rozszerzenie keyUsage określa funkcjonalnie zakres zastosowań danego klucza prywatnego. W X.509v3 (ja href="http://tools.ietf.org/html/rfc3280section-4.2.1.3";RFC 3280 4.2.1.3;/a;) sa zdefiniowane następujące zastosowania i odpowiednie wartości - każda z nich mówi do czego może być wykorzystany klucz prywatny lub publiczny związany z certyfikatem:

 |li;{digitalSignature (0) - opis poniżej |li;{nonRepudiation (1) - opis poniżej |li;{keyEncipherment (2) - deszyfrowanie kluczy sesyjnych inne niż wymiana klucza (od tego jest 4) |li;{dataEncipherment (3) - szyfrowanie danych inne niż 2 i 4 |li;{keyAgreement (4) - szyfrowanie/deszyfrowanie kluczy sesyjnych w protokołach wymiany klucza |li;{keyCertSign (5) - podpisywanie certyfikatów przez CA ("poświadczanie zaświadczeń certyfikacyjnych" wg polskiej Ustawy) |li;{cRLSign (6) - podpisywanie list CRL przez CA ("poświadczanie list CRL") |li;{encipherOnly (7) - flaga ograniczająca zakres stosowania klucza w keyAgreement (4) tylko do szyfrowania |li;{decipherOnly (8) - flaga ograniczająca zakres stosowania klucza w keyAgreement (4) tylko do deszyfrowania

Szczególne uwagi należy poświęcić flagom {code;digitalSignature;/code; i {code;nonRepudiation;/code;. W rzeczywistości ich nazwy nie oznaczają tego co sugerowałyby ich dosłowne znaczenie. I tak:

 |li;Flaga {digitalSignature oznacza wykorzystanie klucza prywatnego do operacji uwierzytelnienia {opartych o matematyczna operacje podpisania jednej liczby przez druga, co wynika także z różnicy między definicją {podpisu elektronicznego i {podpisu cyfrowego. W szczególności dotyczy to operacji, w których klucz prywatny "podpisuje" różne wartości losowe, tymczasowe itd. |li;Flaga {nonRepudiation - wbrew nazwie - nie musi realizować usługi niezaprzeczalności. Flaga ta odnosi się do operacji {podpisu elektronicznego (nie "cyfrowego") czyli podpisania określonej treści, znanej osobie podpisującej.

Nazwy te są jak widać nieco mylące, co wynika głównie ze specyficznej terminologii stosowanej w Unii Europejskiej ({podpis cyfrowy vs {elektroniczny).

Oczywiście, nie wszystkie kombinacje flag keyUsage mają sens techniczny. Np. flagi encipherOnly i decipherOnly mogą występować tylko z flagą keyAgreement.

O tym jakie flagi powinny się znajdować w jakich certyfikatach mówi nam ja href="/podpis_elektroniczny/cwa14365-01-2004-Mar.pdf"; > CWA14365 - 1 March 2004 {"Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects" . Jest to dokument zalecający stosowanie tylko określonych kombinacji flag. [ahref = "http://ipsec.pl/x509/2006/europejski-profil-certyfikatu-x509.html"](http://ipsec.pl/x509/2006/europejski-profil-certyfikatu-x509.html) > "Europejski profil certyfikatu").

{Ryzyko niewłaściwego użycia klucza

Niewłaściwe zastosowanie klucza prywatnego zagraża użytkownikowi. Z danym kluczem prywatnym powiązana jest określona odpowiedzialność prawna - m.in. niezaprzeczalność podpisu elektronicznego opiera się o założenie, że klucz występuje w jednej i tylko jednej kopii („pozostaje w wyłącznej dyspozycji właściciela”) podczas gdy klucze używane do szyfrowania są często dublowane na wypadek utraty oryginału.

Inny przypadek niewłaściwego zastosowania klucza to złożenie kwalifikowanego podpisu elektronicznego pod liczbą losową (nonce) w niektórych protokołach uwierzytelnienia (np. `ISAKMP` `RSA_SIG`). Użytkownikowi wydaje się, że podpisuje liczbę losową, a w rzeczywistości może to być skrót niekorzystny