System Podpisów Cyfrowych z Mediatorem

Opis wykorzystanych pól w żądaniu certyfikatu oraz w wystawionym certyfikacie

grupa „piątek 7:30”

Bartosz Chodorowski <chomzee@ethernet.pl>

Wrocław, 30 października 2009

1 Wstęp

Dokument ten definiuje sposób wytwarzania żądania certyfikatu przez Klienta oraz samego certyfikatu wystawianego przez CA.

2 Żądanie certyfikatu

Klient wypełnia strukturę żądania zdefiniowaną przez RSA Security w standardzie PKCS#10:

```
CertificationRequest ::= SEQUENCE {
     certificationRequestInfo CertificationRequestInfo,
     signatureAlgorithm AlgorithmIdentifier,
     signature          BIT STRING }
}


CertificationRequestInfo ::= SEQUENCE {
     version       INTEGER { v1(0) } (v1,...),
     subject       Name,
     subjectPKInfo SubjectPublicKeyInfo,
     attributes    [0] Attributes }
}
```

By wypełnić pole `subject`, Klient musi znać następujące dane przyszłego właściciela klucza:

- Miejsce zamieszkania:
  - Państwo (C)
  - Województwo, stan lub prowincja (ST)
  - Miasto (L)
- Miejsce pracy:
  - Organizacja (O)
  - Jednostka organizacyjna (OU)
- Imię, nazwisko oraz adres e-mail (CN)

Poniżej znajduje się przykładowe, poprawnie wypełnione pole `subject`:

```
C=PL, ST=Dolnośląskie, L=Wrocław, O=Politechnika Wrocławska, OU=Wydział
    Podstawowych Problemów Techniki, CN=Bartosz Chodorowski/emailAddress=bartosz
    .chodorowski@student.pwr.wroc.pl
```

Klucz szyfrujący wymieniony w żądaniu (z racji zastosowania architektury szyfrowania z mediatorem), którym całe żądanie zostaje też podpisane, jest pozornym kluczem RSA wytworzonym w następujący sposób:

- $e = 1$
- $d = 1$
- $N = 2^{1024}$

Podpis zostaje wykonany algorytmem `sha512WithRSAEncryption`.

Pozostałe pola wypełniane są zgodnie z zasadami ściśle określonymi w standardzie PKCS#10. Żadne opcjonalne atrybuty nie zostają wykorzystane.

3 Certyfikat X.509

CA generuje certyfikat w wersji 3 zgodnie ze standardem X.509:

```
1  Certificate ::= SEQUENCE {
2        tbsCertificate TBSCertificate,
3        signatureAlgorithm AlgorithmIdentifier,
4        signatureValue BIT STRING }
5
6  TBSCertificate ::= SEQUENCE {
7        version [0] EXPLICIT Version DEFAULT v1,
8        serialNumber CertificateSerialNumber,
9        signature AlgorithmIdentifier,
10       issuer Name,
11       validity Validity,
12       subject Name,
13       subjectPublicKeyInfo SubjectPublicKeyInfo }
```

Zasady jakich musi trzymać się CA są następujące:

- Pole `version` określa wersję trzecią certyfikatu X.509
- Pole `subject` kopiowane jest z danych obecnych w żądaniu certyfikatu wypełnionym przez Klienta
- Pole `issuer` zawiera dane dotyczące CA w formacie identycznym z danymi właściciela klucza (opisane w sekcji 2 tego dokumentu)
- Pole `subjectPublicKeyInfo` zawiera dane dotyczące certyfikowanego klucza publicznego wytworzonego przez Dealera
- Pole `validity` wypełniane jest tak, aby początek obowiązywania certyfikatu był obecną datą, a okres trwania certyfikatu wynosił jeden rok
- CA składa podpis algorytmem `sha512WithRSAEncryption`

Pozostałe pola wypełniane są według ścisłych reguł określonych w standardzie X.509. Opcjonalne pola nie zostają wykorzystane.