PROFILI CERTIFIKATA, CRL LISTE I OCSP RESPONDERA OVJERITELJA IDDEEA BIH

Ovjerilac IDDEEA izdaje certifikate u X.509v3 formatu i u skladu sa RFC 5280, EN 319 412-2, EN 319 412-3 i EN 319 412-5. Sljedeća osnovna polja X.509 se koriste:

Ekstenzija X.509	Opis
Potpis	TSP potpis za autentifikaciju certifikata
Izdavalac	TSP naziv
Period važenja	Datum aktivacije i isteka važenja certifikata
Subjekat	Prepoznatljivo ime korisnika
Informacije o javnom ključu korisnika	Algoritam ID, ključ
Verzija	Verzija certifikata X.509, verzija 3 (2)
Serijski broj	Jedinstveni serijski broj certifikata

7.1.2 Ekstenzije certifikata

Sljedeća polja osnovne ekstenzije X.509 se koriste

Ekstenzija X.509	Opis
Potpis	TSP potpis za autentifikaciju certifikata
Izdavalac	TSP naziv
Period važenja	Datum aktivacije i isteka važenja certifikata
Subjekat	Određeno ime korisnika
Informacije o javnom ključu korisnika	Algoritam ID, ključ
Verzija	Verzija Certifikata X.509, verzija 3 (2)
Serijski broj	Jedinstveni serijski broj certifikata

Certifikati TSP-a sadrže sljedeće kritične ekstenzije:

Ekstenzija X.509	Opis
keyUsage	keyCertSign, cRLSign
basicConstraints	CA=TRUE, pathLenConstraint

Korisnički i certifikati usluga mogu sadržavati sljedeće ekstenzije:

Ekstenzija X.509	Opis
authorityKeyIdentifier	Hash ključa izdavaoca
subjectKeyIdentifier	Hash ključa nosioca
keyUsage	Kao što je definisano u odjeljku 6.1.7 Namjena ekstenzije "keyUsage" Ekstenzije su uvijek označene kao kritične.
extendedKeyUsage	Kao što je definisano u odjeljku 6.1.7 Namjena ekstenzije "keyUsage"
privateKeyUsagePeriod	Kao što je definisano u odjeljku 6.3.2. Periodi važenja certifikata i parova ključeva
certificatePolicies:	Politika certifikacije OID = OID kao što je definisano u 1.2 Naziv dokumenta i identifikacija
CertPolicyID	
CPS URI	
CRLDistributionPoints	CRL lokacije

subjectAlternativeName	Alternativno ime korisnika
basicConstraints	CA=false
Authority Information Access	accessMethod=caIssuers; and accessMethod=OCSP
qcStatement	According to ETSI EN 319 412-5

7.1.3 Ekstenzije privatnih certifikata

X.509	OID
Key Usage: digitalSignature,nonRepudiation,keyEncipherment	2.5.29.15
extendedKeyUsage: Document Signing,	1.3.6.1.4.1.311.10.3.12
extendedKeyUsage: PDF Signing	1.2.840.113583.1.1.5

7.1.4 Identifikator objekta (OID) algoritama

Algoritam	Identifikacioni broj
RSA	1.2.840.113549.1.1.1
SHA512 with RSA	1.2.840.113549.1.1.13

7.1.5 Oblici naziva

U sve certifikate koje izdaje Ovjerilac IDDEEA se upisuje puno prepoznatljivo ime certifikacionog tijela i subjekta certifikata u polja ime izdavaoca odnosno ime korisnika. Kodiranje tih imena se vrši u UTF8 string ili PrintableString formatu.

7.1.6 Ograničenja imena

Nije primjenjivo.

7.1.7 Identifikator objekta politike certifikacije

Svi certifikati koje izdaje TSP sadrže OID politike certifikacije po kojoj se izdaje certifikat. OID za svaki certifikat je definisan u odjeljku 1.2 Naziv dokumenta i identifikacija.

7.1.8 Upotreba "Policy Constraints" ekstenzija

Nije primjenjivo.

7.1.9 Sintaksa i semantika kvalifikatora politike

Kvalifikatori politike se koriste u skladu sa RFC5280.

7.1.10 Semantika procesiranja kritične ekstenzije "Certificate Policies"

Korisničke aplikacije PKI-a moraju obraditi ekstenziju certifikata kao kritičnu u skladu sa RFC 5280.

7.2 Profil spiska opozvanih certifikata

7.2.1 Broj verzije certifikata

TSP izdaje spiskove opozvanih certifikata u X.509 v2 formatu koristeći niz distribucionih tačaka u okviru LDAP direktorija i http web servera.

Sljedeća osnovna polja ekstenzije X.509 se koriste:

Ekstenzija X.509	Opis
Verzija	Set to v2
Potpis	Algoritam identifikatora koji se koristi za potpisivanje spiska

	opozvanih certifikata
Izdavalac	Određeno ime CA
thisUpdate	Datum izdavanja spiska opozvanih certifikata
nextUpdate	Datum narednog izdavanja spiska opozvanih certifikata
revokedCertificate	Serijski brojevi opozvanih certifikata

7.2.2 CRL i CRL "entry" ekstenzije

Ekstenzija X.509	Opis
CRLNumber	Redni broj spiska opozvanih certifikata
authorityKeyIdentifier	"Hash" ključa izdavaoca
reasonCode	TSP može sadržavati vrijednosti u skladu sa RFC5280
invalidityDate	Popunjava TSP aplikacija kako je operater odredio
expiredCertsOnCRL	Spisak opozvanih certifikata koji sadrži ovu ekstenziju uključuje informacije o statusu opoziva za certifikate koji su već istekli.

7.3 OCSP profil

Profil OCSP koji se koristi definisan je u RFC 6960.

7.3.1 Broj verzije certifikata

Verzija OSCP v1 u skladu sa RFC 6960 se koristi.

7.3.2 Ekstenzije OCSP

Ekstenzije OCSP zahtjeva su:

Ekstenzija	Opis
nonce	Vrijednost "nonce" povezuje zahtjev i odgovor kako bi se spriječili napadi ponavljanja. Vrijednost će biti u skladu sa RFC6280

Ekstenzije OCSP odgovora su :

Ekstenzija	Opis
nonce	Ista vrijednost kao u zahtjevu ukoliko se traži tako u zahtjevu.
ArchiveCutoff	Vremenski period koji OCSP čuva informacije o opozivu nakon isteka certifikata.