Profil kvalifikovanog elektronskog sertifikata

Mr Dragan Spasić, dipl. inž.

***Sadržaj* — U radu je opisan profil kvalifikovanog elektronskog sertifikata X.509 verzije 3 i definisana su neophodna polja kvalifikovanog sertifikata.**

***Ključne reči* — Kvalifikovani elektronski sertifikat, Sertifikaciono telo - CA, Evropska Direktiva o elektronskom potpisu 1999/93/EC.**

I. Uvod

Sertifikaciono telo (Certification Authority - CA ili Certification Service Provider - CSP) je institucija koja izdaje elektronske (digitalne) sertifikate X.509 verzije 3 zainteresovanim korisnicima. Elektronski sertifikati (electronic certificates) i pripadajući tajni (privatni) kriptografski ključevi mogu da se koriste za autentifikaciju tj. predstavljanje korisnika na Internetu, šifrovanje / dešifrovanje i elektronsko potpisivanje / verifikovanje potpisanih datoteka, elektronskih pisama i transakcija, u okviru aplikacija koje podržavaju rad sa elektronskim sertifikatima. Namena kvalifikovanih elektronskih sertifikata (qualified electronic certificates) je verifikovanje kvalifikovanog elektronskog potpisa, koji ima isto pravno dejstvo kao i svojeručni potpis.

Prema Evropskoj Direktivi o elektronskom potpisu 1999/93/EC [1], Aneks 1 i prema Zakonu o elektronskom potpisu [2], član 17, kvalifikovani elektronski sertifikat mora da sadrži:

1. oznaku da je sertifikat izdat kao kvalifikovani sertifikat,
2. skup podataka koji jedinstveno identifikuju sertifikaciono telo koje je izdalo sertifikat,
3. skup podataka koji jedinstveno identifikuju korisnika kome je izdat sertifikat,
4. specifične atribute korisnika, ako su važni, u zavisnosti od namene sertifikata,
5. podatke za proveru elektronskog potpisa (javni kriptografski ključ korisnika), koji odgovaraju podacima za izradu elektronskog potpisa (tajni kriptografski ključ korisnika), a koji su pod kontrolom korisnika,
6. podatke o početku i kraju važenja sertifikata (rok važnosti sertifikata),
7. identifikacionu oznaku sertifikata,
8. napredni (advanced) elektronski potpis sertifikacionog tela koje je izdalo sertifikat,
9. ograničena koja se odnose na korišćenje sertifikata, ako ih ima,
10. ograničenja koje se odnose na vrednost transakcija za koje sertifikat može da se koristi, ako ih ima.

Dragan Spasić, GIAC GSEC Certified Professional, JP PTT saobraćaja "Srbija", Katićeva 14-18, 11000 Beograd (telefon: 381-11-3607896; faks: 381-11-3651412; e-mail: dspasic@ptt.rs).

II. Oznaka da je sertifikat kvalifikovan

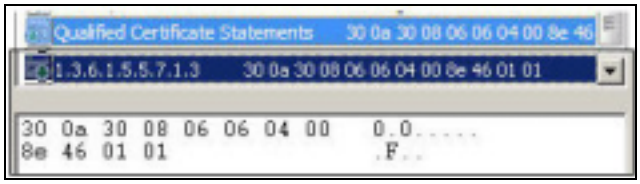
Prema dokumentu ETSI TS 101 862 "Qualified Certificate profile" [3], moguće je na dva (2) načina definisati oznaku koja ukazuje da je sertifikat kvalifikovan:

- Korišćenjem polja "Certificate Policies" u kome postoji oznaka vrste sertifikata (Policy Identifier) i Web strana na kojoj se nalazi dokument "Certification Practice Statement - CPS" sertifikacionog tela, a iz koga se može pročitati da je sertifikat kvalifikovan, kao i detaljne karakteristike sertifikata. Moguće je za isti Policy Identifier staviti i "User Notice" (na primer: Ovo je kvalifikovani sertifikat). U isto polje "Certificate Policies" moguće je, ali nije neophodno, staviti i dodatni Policy Identifier, koji prema dokumentu ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates" [4] može da bude **0.4.0.1456.1.1** (QCP public + SSCD (Secure Signature Creation Device), kada je kvalifikovani sertifikat na smart kartici ili USB smart tokenu koji je sredstvo za kreiranje kvalifikovanog potpisa tj. SSCD) ili **0.4.0.1456.1.2** (QCP public, kada kvalifikovani sertifikat nije na SSCD-u), kao što je prikazano na slikama 1. i 2., respektivno.
- Korišćenjem polja "Qualified Certificate Statements" sa objektom **id-etsi-qcs-QcCompliance** čiji je OID = **0.4.0.1862.1.1** (slika 3.). Ukoliko je kvalifikovani sertifikat na smart kartici ili USB smart tokenu koji je SSCD, moguće je dodati i objekat **id-etsi-qcs-QcSSCD** čiji je OID = **0.4.0.1862.1.4** (slika 4.).

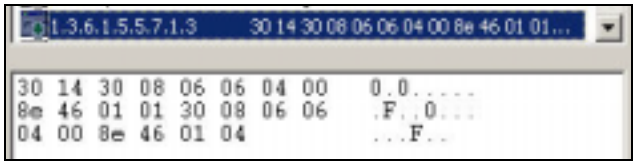
Sl. 1. Primer polja "Certificate Policies", QCP public + SSCD (0.4.0.1456.1.1)

Sl. 2. Primer polja "Certificate Policies", QCP public (0.4.0.1456.1.2)

Kvalifikovani sertifikati izdati posle 30.6.2005. godine moraju da imaju polje "Qualified Certificate Statements" sa objektom **id-etsi-qcs-QcCompliance** [3]. Microsoft Windows Vista program za pregled sertifikata prikazuje u sertifikatu ime polja "Qualified Certificate Statements" (slika 3.), a Windows XP i prethodne verzije Windows operativnog sistema umesto imena tog polja prikazuju njegov OID = **1.3.6.1.5.5.7.1.3**. Microsoft Windows program za pregled sertifikata prikazuje sadržaj polja "Qualified Certificate Statements" isključivo u formi HEX i ASCII vrednosti, što nije čitljivo za korisnike.



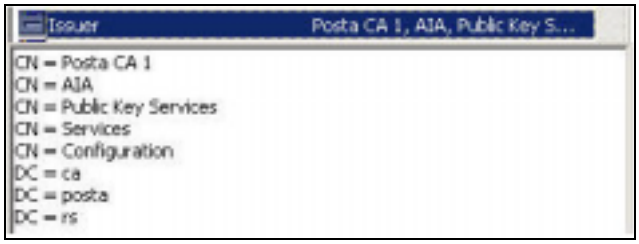
Sl. 3. Primer polja "Qualified Certificate Statements", id-etsi-qcs-QcCompliance



Sl. 4. Primer polja "Qualified Certificate Statements", id-etsi-qcs-QcCompliance + id-etsi-qcs-QcSSCD

III. PODACI KOJI JEDINSTVENO IDENTIFIKUJU SERTIFIKACIONO TELO KOJE JE IZDALO SERTIFIKAT

Podaci koji jedinstveno identifikuju sertifikaciono telo koje je izdalo sertifikat upisuju se u polje "Issuer" sertifikata (slika 5.). Prema dokumentu RFC 3739 "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile" [5], jedinstveno ime (Distinguished Name) sertifikacionog tela može da sadrži podskup sledećih atributa: domainComponent (DC), countryName (C), stateOrProvinceName (ST), organizationName (O), localityName (L) i serialNumber. Moguće je korišćenje i dodatnih atributa (na primer: commonName (CN)).

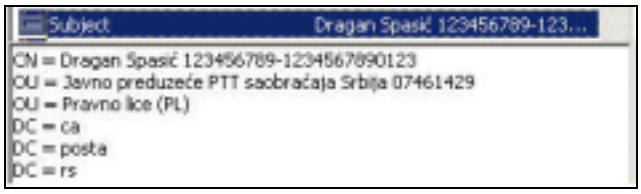


Sl. 5. Primer polja "Issuer" sertifikata

IV. PODACI KOJI JEDINSTVENO IDENTIFIKUJU KORISNIKA KOME JE IZDAT SERTIFIKAT

Podaci koji jedinstveno identifikuju korisnika kome je izdat sertifikat upisuju se u polje "Subject" sertifikata (slika 6.). Prema dokumentu RFC 3739 [5], jedinstveno ime (Distinguished Name) korisnika sertifikata može da sadrži podskup sledećih atributa: domainComponent (DC), countryName (C), commonName (CN), surname (SN), givenName (G), pseudonym, serialNumber, title, organizationName (O), organizationalUnitName (OU), stateOrProvinceName (ST) i localityName (L). Moguće je korišćenje i dodatnih atributa, ali nije neophodno.

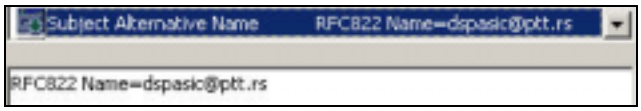
Najvažniji atribut korisnika je "**Common Name - CN**" u koji se upisuju ime i prezime korisnika sertifikata, a po potrebi i drugi podaci korisnika (slika 6.) Prema [6], U atribut "Common Name - CN" korisnika treba da je upisano puno ime i prezime korisnika, jedinstveni identifikator korisnika unutar sertifikacionog tela i opciono JMBG. Da bi srpska tj. YU slova (Č, č, Ć, ć, Đ, đ , Š, š, Ž, ž) mogla ispravno da se prikažu u atributu "Common Name - CN", neophodno je da taj atribut bude "**UTF8String**" kodiran prema [6] i [7].



Sl. 6. Primer polja "Subject" sertifikata

V. SPECIFIČNI ATRIBUTI KORISNIKA

Specifični atributi korisnika sertifikata upisuju se u polje "Subject" i polje "Subject Alternative Name" sertifikata. Polje "Subject Alternative Name" može da sadrži sledeće atribute korisnika [7]: otherName, rfc822Name (slika 7.), dNSName, x400Address, directoryName, ediPartyName, uniformResourceIdentifier, iPAddress i registeredID.

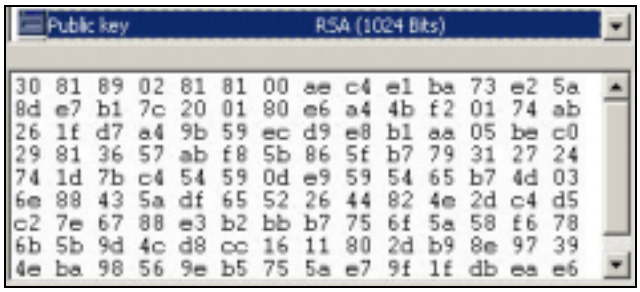


Sl. 7. Primer polja "Subject Alternative Name" sertifikata

VI. PODACI ZA PROVERU ELEKTRONSKOG POTPISA

Podaci za proveru elektronskog potpisa tj. javni kriptografski ključ korisnika sertifikata upisuje se u polje "Public Key" ("Subject Public Key Info" [7]) sertifikata (slika 8.). Primenom softverskog alata OpenSSL moguće je dobiti detaljan sadržaj polja "Public Key" sertifikata

(tabela 1.). Kod korisničkih sertifikata dužina RSA ključeva treba da bude minimalno 1024 bita, a kod sertifikata sertifikacionih tela minimalno 2048 bita.



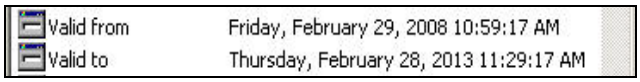
Sl. 8. Primer polja "Public Key" sertifikata

TABELA 1: OPENSSL PRIKAZ SADRŽAJA POLJA "PUBLIC KEY" SERTIFIKATA SA SLIKE 8.

Public Key Algorithm:	rsaEncryption
RSA Public Key:	(1024 bit)
Modulus (1024 bit):	00:ae:c4:e1:ba:73:e2:5a:8d:e7:b1:7c:20:01:80: e6:a4:4b:f2:01:74:ab:26:1f:d7:a4:9b:59:ec:d9: e8:b1:aa:05:be:c0:29:81:36:57:ab:f8:5b:86:5f: b7:79:31:27:24:74:1d:7b:c4:54:59:0d:e9:59:54: 65:b7:4d:03:6e:88:43:5a:df:65:52:26:44:82:4e: 2d:c4:d5:c2:7e:67:88:e3:b2:bb:b7:75:6f:5a:58: f6:78:6b:5b:9d:4c:d8:cc:16:11:80:2d:b9:8e:97: 39:4e:ba:98:56:9e:b5:75:5a:e7:9f:1f:db:ea:e6: e2:5a:49:42:7a:fe:d4:75:bf
Exponent:	65537 (0x10001)

VII. PODACI O POČETKU I KRAJU VAŽENJA SERTIFIKATA (ROK VAŽNOSTI SERTIFIKATA)

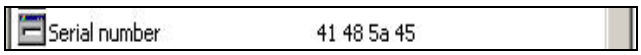
Podaci o početku i kraju važenja sertifikata upisuju se u polje "Valid From" i polje "Valid To" sertifikata (slika 9.). Rok važnosti korisničkih sertifikata je najčešće od jedne (1) do pet (5) godina, a kod sertifikata sertifikacionih tela je najčešće 20 godina.



Sl. 9. Primer polja "Valid From" i "Valid To" sertifikata

VIII. IDENTIFIKACIONA OZNAKA SERTIFIKATA

Identifikaciona oznaka sertifikata upisuju se u polje "Serial Number" sertifikata (slika 10.).



Sl. 10. Primer polja "Serial Number" sertifikata

IX. NAPREDNI ELEKTRONSKI POTPIS SERTIFIKACIONOG TELA KOJE JE IZDALO SERTIFIKAT

Poslednji korak prilikom generisanja kvalifikovanog sertifikata korisnika je elektronsko potpisivanje podataka iz svih polja sertifikata od strane sertifikacionog tela, korišćenjem tajnog kriptografskog ključa sertifikacionog tela. Elektronski potpis iz sertifikata se koristi za proveru integriteta svih podataka sertifikata. Ukoliko je iz bilo kog razloga narušen integritet sertifikata, dobiće se sledeća poruka: "The integrity of this certificate cannot be guaranteed. The certificate may be corrupted or has been tampered with.", a takav sertifikat **ne** može da se koristi.

Iako je elektronski potpis sertifikata sastavni deo sertifikata, Microsoft Windows program za pregled sertifikata ni u jednom polju sertifikata ne prikazuje vrednost elektronskog potpisa (Signature Value). Primenom softverskog alata OpenSSL moguće je dobiti vrednost elektronskog potpisa sertifikata (tabela 2.).

TABELA 2: PRIMER OPENSSL PRIKAZA ELEKTRONSKOG POTPISA IZ SERTIFIKATA

Sign. Algo:	sha1WithRSAEncryption
Sign. Value:	06:77:4b:3c:5f:14:19:d0:5e:a7:43:a7:68:1f:6b:c6:9a:c6: 18:f4:a5:73:16:5a:ce:a3:6a:08:29:d2:b5:cf:87:1b:c9:88: 36:a4:4d:50:e4:04:6c:54:2c:b1:02:1e:df:1e:29:c7:79:c4: 0e:6f:7c:2c:e9:59:83:7c:a8:38:39:8d:11:cd:70:e9:a3:ce: 9d:6a:97:d9:71:95:4f:04:de:aa:cc:55:e0:74:83:83:e6:78: 68:87:07:0b:0b:e6:f2:95:e4:6d:f6:c2:4c:c6:74:62:e2:2c: 82:19:3e:35:2f:45:17:4a:50:00:74:58:35:e5:fe:7b:e7:a2: 5c:b3:76:f8:1a:8e:a7:a3:f1:fc:9a:ec:a8:c0:15:6c:8e:04: 11:56:d9:fd:af:4f:94:ad:1e:39:ff:a7:dc:6d:55:5a:f6:96: c0:c3:4b:a2:36:56:d1:23:3a:a4:86:a3:e8:a9:da:25:40:37: b4:67:59:02:67:02:28:65:8a:94:00:d4:6f:99:b3:7b:40:13: e3:2b:06:5e:0a:09:4e:74:c6:00:8c:d9:9d:d0:56:63:b5:4c: 99:e2:bf:8a:8d:64:57:ef:2b:83:0f:7e:f7:01:6b:8a:f7:0f: 1a:bf:d0:ed:d2:56:64:6a:b7:fa:63:4d:e8:84:1c:fa:10:28: ff:d5:8b:15

Elektronski potpis sertifikacionog tela je napredni (advanced) elektronski potpis, a **ne** kvalifikovani (qualified) elektronski potpis, kako je greškom navedeno u Zakonu o elektronskom potpisu [2], član 17. Naime, kvalifikovani elektronski potpis je napredni elektronski potpis kod koga su ispunjena dva (2) dodatna uslova:

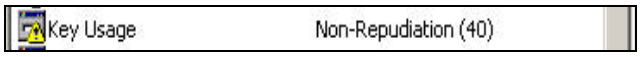
1. Zasniva se na korišćenju kvalifikovanog elektronskog sertifikata.
2. Kreira se primenom sredstva za kreiranje kvalifikovanog elektronskog potpisa - SSCD.

S obzirom na to da se kvalifikovani elektronski sertifikati izdaju ljudima (RFC 3739 [5]: The Qualified Certificate is issued to a natural person (living human being).), i namenjeni su za elektronsko potpisivanje dokumenata koje je jednako svojeručnom potpisivanju, a **nisu** namenjeni serverima ili drugim uređajima, to znači da ih serveri sertifikacionih tela **ne** mogu imati. Iz tog razloga, serveri sertifikacionih tela koji izdaju kvalifikovane elektronske sertifikate korisnicima, **ne** mogu da kreiraju kvalifikovan elektronski potpis sertifikata, već samo napredni elektronski potpis.

X. OGRANIČENA KOJA SE ODNOSE NA KORIŠĆENJE SERTIFIKATA

Ograničena koja se odnose na korišćenje kvalifikovanog elektronskog sertifikata definišu se na dva (2) načina:

- Korišćenjem polja "Certificate Policies" u kome postoji oznaka vrste sertifikata (Policy Identifier) i Web strana na kojoj se nalazi dokument "Certification Practice Statement - CPS" sertifikacionog tela, a iz koga se mogu pročitati ograničena koja se odnose na korišćenje sertifikata, kao i detaljne karakteristike sertifikata.
- Korišćenjem polja "Key Usage". Prema dokumentu ETSI TS 102 280 "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" [8], sadržaj polja "Key Usage" kvalifikovanog sertifikata može da bude **samo** "**Non-Repudiation**" (slika 11.) ili "**Digital Signature, Non-Repudiation**" (slika 12.), pri čemu bi polje "Key Usage" trebalo da bude "Critical" [5], [7].

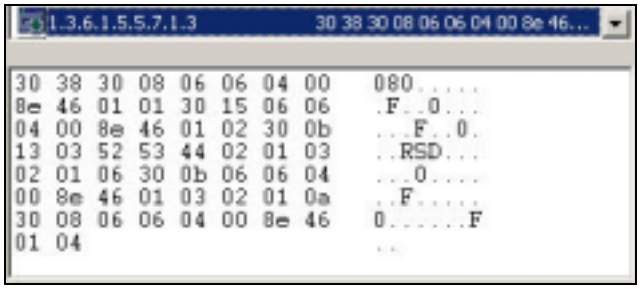


Sl. 11. Polje "Key Usage=Non-Repudiation"

Sl. 12. Polje "Key Usage=Digital Signature, Non-Repudiation"

XI. OGRANIČENJA KOJE SE ODNOSE NA VREDNOST TRANSAKCIJA ZA KOJE SERTIFIKAT MOŽE DA SE KORISTI

Prema dokumentu ETSI TS 101 862 "Qualified Certificate profile" [3], za definisanje maksimalne novčane vrednosti transakcije za koju kvalifikovani elektronski sertifikat može da se koristi, upotrebljava se polje "Qualified Certificate Statements" sa objektom **id-etsi-qcs-QcLimitValue** čiji je OID = **0.4.0.1862.1.2** (slika 13. i tabela 3.). Maksimalna novčana vrednost se izračunava prema formuli: QcEuLimitValue = amount * 10^exponent (currency). Prema primeru iz tabele 3., QcEuLimitValue = 3 * 10^6 (RSD) = 3.000.000 RSD.



Sl. 13. Primer polja "Qualified Certificate Statements", id-etsi-qcs-QcCompliance + id-etsi-qcs-QcLimitValue + id-etsi-qcs-QcRetentionPeriod + id-etsi-qcs-QcSSCD

TABELA 3: ASN.1 TEKSTUALNI PRIKAZ POLJA "QUALIFIED CERTIFICATE STATEMENTS" SERTIFIKATA SA SLIKE 13.

Len	Content
70	SEQUENCE :
8	OBJECT IDENTIFIER : [1.3.6.1.5.5.7.1.3]
58	OCTET STRING :
56	SEQUENCE :
8	SEQUENCE :
6	OBJECT IDENTIFIER : [0.4.0.1862.1.1]
21	SEQUENCE :
6	OBJECT IDENTIFIER : [0.4.0.1862.1.2]
11	SEQUENCE :
3	PRINTABLE STRING : 'RSD'
1	INTEGER : 3
1	INTEGER : 6
11	SEQUENCE :
6	OBJECT IDENTIFIER : [0.4.0.1862.1.3]
1	INTEGER : 10
8	SEQUENCE :
6	OBJECT IDENTIFIER : [0.4.0.1862.1.4]

U primeru polja "Qualified Certificate Statements" sertifikata koje je prikazano na slici 13. i tabeli 3., postoji i objekat **id-etsi-qcs-QcRetentionPeriod** čiji je OID = **0.4.0.1862.1.3**. Taj objekat predstavlja izjavu sertifikacionog tela da će svi materijalni podaci koji se odnose na sertifikat biti arhivirani i dostupni po zahtevu, posle isteka roka važnosti sertifikata za onoliko godina koliko je navedeno u polju QcEuRetentionPeriod. Prema primeru iz tabele 3., QcEuRetentionPeriod = 10 godina.

XII. ZAKLJUČAK

Kreiranje i provera (verifikacija) kvalifikovanog elektronskog potpisa vrši se korišćenjem:

1. kvalifikovanog elektronskog sertifikata (Aneks 1 Evropske Direktive o elektronskom potpisu 1999/93/EC) kojeg je izdalo registrovano (akreditovano) sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata (Aneks 2 Direktive 1999/93/EC),
2. sredstva za kreiranje kvalifikovanog elektronskog potpisa (Secure Signature Creation Device - SSCD, Aneks 3 Direktive 1999/93/EC),
3. bezbedne aplikacije za kreiranje (Secure Signature Creation Application - SSCA) i za proveru (Secure Signature Verification Application - SSVA) kvalifikovanog elektronskog potpisa (Aneks 4 Direktive 1999/93/EC).

Profil kvalifikovanog elektronskog sertifikata X.509 verzije 3 mora da bude u skladu sa Aneksom 1 Evropske Direktive o elektronskom potpisu 1999/93/EC, odgovarajućim dokumentima ETSI TS (European Telecommunications Standards Institute, Technical Specification) i IETF RFC (Internet Engineering Task Force, Request for Comments).

LITERATURA

[1] "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures", Official Journal of the European Communities, L 13/12, 19.1.2000.

[2] Zakon o elektronskom potpisu, "Službeni glasnik Republike Srbije", broj 135, 21.12.2004. godine.

[3] ETSI TS 101 862, V1.3.3 (2006-01), "Qualified Certificate profile".

[4] ETSI TS 101 456, V1.4.3 (2007-05), "Policy requirements for certification authorities issuing qualified certificates".

[5] S. Santesson, M. Nystrom, T. Polk, RFC 3739, "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile", March 2004.

[6] Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa ("Sl. glasnik RS", br. 26/2008).

[7] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008. (Obsoletes RFC 3280).

[8] ETSI TS 102 280, V1.1.1 (2004-03), "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons".

ABSTRACT

The X.509 version 3 qualified electronic certificate profile is described in detail, and required fields are defined in this paper.

QUALIFIED ELECTRONIC CERTIFICATE PROFILE

Dragan Spasić