GOSPODARSKA ZBORNICA SLOVENIJE

Center Vlade RS za informatiko
SIGEN-CA SIGOV-CA SI-TSA

Projekt *e*-SLOG

Elektronsko poslovanje slovenskega gospodarstva

VARNOSTNE ZAHTEVE ZA OVERITELJE KVALIFICIRANIH DIGITALNIH POTRDIL

v. 1.0
november 2003

STANJE DOKUMENTA

Namen dokumenta:	Priporočila za prepoznavanje overiteljev kvalificiranih digitalnih potrdil
Kratek naziv projekta:	e-SLOG – e-podpis
Vsebina:	*Glej "Vsebina"*
Status:	dokončna
Verzija:	1.0
Datum verzije:	november 2003
Avtorji:	Center vlade RS za informatiko
Naslovniki:	člani delovne skupine, ostali
Zgodovina verzij:	*Glej "Verzija"*

Verzija	Datum spremembe	Opombe
0.9	september 2003	
1.0	november 2003	

VSEBINA

1. UVOD

Elektronski način opravljanja storitev in poslovanja postaja prevladujoč način našega vsakdana. Slovenija se že vseskozi zaveda pomena sodobnih informacijskih tehnologij in se na tem področju vsekakor uvršča med razvitejše države. Bila je med prvimi državami s sprejeto zakonodajo, ki ureja to področje, razvija nove elektronske storitve v privatnem sektorju in v okviru javne uprave, omogoča dostop in povezovanje različnih podatkov ter integracijo elektronskih storitev z različnimi družbenimi subjekti, zagotavlja zakonske in podzakonske akte ter tehnične standarde kot pogoje razvoja elektronskega poslovanja in komuniciranja, ter sodeluje v svetovnih in evropskih integracijah na področjih povezovanja administrativnih podatkovnih baz.

Za zagotovitev vsaj take varnosti in zaupanja, kot jo lahko pričakujemo v klasičnem načinu komuniciranja in poslovanja, pa je ključno, da elektronski način postane prevladujoč in da resnično zaživi. Omogočiti je potrebno mehanizme za nedvoumno ugotavljanje identitete, zaupnost pri izmenjavi občutljivih podatkov, avtenticiran dostop do podatkovnih baz, obstajajo pa tudi številne aplikacije, ki so povezane z elektronskimi podpisi oziroma potrebujejo le-te za delovanje. Zagotavljanje ustrezne varnosti podatkov in resnične identitete oseb v medsebojnem komuniciranju na elektronski način v evropskem prostoru ureja Direktiva 1999/93/EC, 13 December 1999 on a Community framework for electronic signatures. Na podlagi le-te in na podlagi drugih dokumentov (podrobneje o tem v pravnem delu priporočil) področje v Republiki Sloveniji urejata predvsem Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000) in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur. l. RS, št. 77/2000 in 2/2001). Bistveni pomen zakona je, da pod posebnimi pogoji elektronskemu podpisu priznava enako veljavo kot jo ima v papirnatem svetu lastnoročni podpis (15. člen ZEPEP).

Najbolj razširjen način za zagotavljanje varnosti in zaupnosti zagotovi infrastruktura javnih ključev (PKI, angl. *Public Key Infrastructure*) oz. overitelj digitalnih potrdil javnih ključev (CA, angl. *Certification Authority*).

Digitalno potrdilo (angl.: *digital certificate*) je najbolj razširjena sodobna alternativa klasičnim osebnim identifikatorjem (osebna ali zdravstvena izkaznica, potni list, bančna kartica, ...), s specifičnim namenom - zagotavljanju varnega in legitimnega e-poslovanja.

Digitalna potrdila so sestavni del tehnoloških rešitev, ki nudijo dve osnovni možnosti za zasebnost v elektronskem poslovanju in komuniciranju:
1. šifriranje podatkov, ki zagotavlja zaupnost, in
2. digitalni podpis, ki predstavlja sodobno alternativo klasičnemu podpisu, zagotavlja pa:
    - identiteto imetnika digitalnega potrdila
    - nezatajljivost lastništva poslanih e-podatkov, in
    - celovitost (integriteto) sporočila, kar pomeni, da samo del podatkov ni mogoče spremeniti ali drugače popraviti brez (vednosti) podpisnika.

Slika 1 – Vzpostavitev zaupanja preko overitelja

Overitelj tako predstavlja ustanovo, ki ji njegovi komitenti - imetniki digitalnih potrdil - zaupajo. S tem overitelja tudi pooblaščajo, da upravlja z njihovimi digitalnimi potrdili. Slika 1 prikazuje princip zaupanja med lastniki digitalnih potrdil preko tretje osebe – t.j. overitelja.

1.1. Namen in obseg priporočil

Uspešnost prenosa pravnih okvirjev, ki ga določata tako evropska direktiva kot slovenska zakonodaja, zahteva standarde za storitve, procese, sisteme in produkte, ki se nanašajo na infrastrukturo overitelja, digitalnih potrdil, elektronski podpis kot tudi za sama priporočila za upoštevanje predpisanih standardov pri implementacijah vseh teh elementov, ki omogočajo legitimen in varen način elektronskega poslovanja.

V dokumentu je zbrana pravna podlaga, ki določa delovanje overiteljev kvalificiranih digitalnih potrdil kot tudi standardov za njihovo uspešno implementacijo. V dokumentu so tudi opozorila za tretje osebe oz. za razvijalce aplikacij v zvezi z različnostjo implementacije posameznih elementov infrastrukture overiteljev.

1.2. Osnovne varnostne zahteve za overitelje kvalificiranih digitalnih potrdil

V skladu s slovensko in evropsko zakonodajo razlikujemo med:
- overitelji, ki izdajajo nekvalificirana potrdila in
- overitelji, ki izdajajo kvalificirana potrdila.

Kvalificiranost digitalnih potrdili nasproti nekvalificiranim potrdilom pomeni razlikovanje tako v pravni veljavnosti teh potrdil kot tudi v njihovih tehničnih lastnostih. Enako pa seveda velja tudi za overitelje, ki izdajajo taka potrdila. V skladu z ZEPEP so razlike med kvalificiranimi in nekvalificiranimi digitalnimi potrdili v:
1. vsebini: minimalni nabor podatkov je v primeru kvalificiranih digitalnih potrdil določen z zakonodajo,
2. načinu izdaje: za pridobitev kvalificiranega digitalnega potrdila se zahteva osebna identifikacija osebe – bodočega imetnika takega potrdila,
3. zahtevah za overitelja: overitelj, ki izdaja kvalificirana digitalna potrdila mora izpolnjevati strožje pogoje glede svojega delovanja, visokih zahtev po varnosti njegove infrastrukture, programske opreme, osebja itd.
4. pravnih posledicah uporabe: uporaba kvalificiranih potrdil lahko ob izpolnjenih zahtevah glede izvedbe varnega elektronskega podpisa in uporabo sredstev za varno hranjenje pomeni enakost z lastnoročnim podpisom.

1.3. Mednarodni standardi

Obstaja vrsta mednarodnih in nacionalnih standardov, ki jim lahko sledijo tako overitelji kot tudi inšpekcijske/akreditacijske službe, ki preverjajo posamezne implementacije overiteljev. Osnovni, v EU uveljavljeni mednarodni standardi za delovanje overiteljev, varnostnih zahtev infrastrukture, politiko delovanja, vsebino kvalificiranih digitalnih potrdil:
- priporočilo RFC 2527 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework",
- priporočilo RFC 3039: "Internet X.509 Public Key Infrastructure Qualified Certificates Profile",
- priporočilo RFC3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Eden izmed najbolj razširjenih ameriških standardov za delovanje overiteljev je ANS (angl. American National Standard) X9.79:2000 “PKI Practices and Policy Framework”, ki vključuje kriterije za overitelje, oblikovane na podlagi mednarodnih standardov – ISO, IETF, BSI, ANSI, FIPS, ABA – za upravljanje s potrdili, kriptografskimi ključi, in varnostno politiko. Ta standard pa je tudi osnova za kriterije WebTrust, AICPA/CICA (angl. E-Commerce Assurance Task Force), ki je razširjen pri izvajanju inšpekcijskega nadzora pri številnih poslovnih organizacijah.

Ostala priporočila so sledeča:

- priporočilo ETSI*, Policy requirements for certification authorities issuing qualified certificates* - TS 101 456 v 1.2.1 (april 2002),
- priporočilo ETSI*, International Harmonization of Policy Requirements for CAs issuing Certificates* - TR 102040 (marec 2002),
- priporočilo CEN/CWA 14172-1,-2,-3 Conformity Assessment Guidance,
- priporočilo CEN/CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part1: System Security Requirements,
- priporočilo CEN/CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2 Cryptographic Module for CSP Signing Operation – Protection Profile (MCSO-PP),
- priporočilo ETSI*, Qualified Certificate Profile* - TS 101 862 v 1.2.1 (junij 2001),priporočilo ITU-T X.509 (1997) | ISO/IEC 9594-8: "Information technology – O Systems Interconnection - The directory: Public-key and attribute certificate frameworks",
- priporočilo RFC 2459: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Posamezni sklopi so podrobneje opisani v naslednjih poglavjih.

2. PRAVNA PODLAGA ZA DELOVANJE OVERITELJA KVALIFICIRANIH DIGITALNIH POTRDIL

2.1. Zakonodaja

Pravna podlaga delovanja overiteljev kvalificiranih digitalnih potrdil v RS zajema:

- Zakon o elektronskem poslovanju in elektronskem podpisu – ZEPEP (Uradni list RS, št. 57/2000),
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001),
- Zakon o varstvu osebnih podatkov – ZVOP (Uradni list RS, št. 59/99 in 57/2001),
- in druge veljavne predpise.

S pristopom Slovenije k EU je potrebno predvideti tudi druge evropske predpise, ki določajo pravne in tehnične okvire delovanja overiteljev, ki konkurenčno nastopajo na evropskem trgu kot tudi tisti, ki se povezujejo z overitelji drugih držav. Slovenija že sedaj sodeluje pri oblikovanju nove evropske direktive, ki bo na novo uredila področje e-poslovanja in e-podpisa. Slovenska vlada pa tudi že sodeluje pri oblikovanju tehničnih standardov kot podlago za izmenjavo podatkov med vladnimi državami EU-ja (projekt IDA, angl. Interchange of data between administration. Leta 2005 bo program razširjen tudi na področje zasebnega sektorja in državljanov).

2.1.1 Notranja pravila overitelja

Overitelj mora v skladu z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje delovati v skladu s svojimi notranjimi pravili. Le-ta so sestavljena iz javnega in zaupnega dela.

Javni del notranjih pravil overitelja:

- določa namen uporabe,
- določa varnostne zahteve na višjem nivoju,
- določa odgovornosti in obveznosti vseh strank,
- je netehničen dokument
- je javno objavljen.

Zaupni del notranjih pravil overitelja je:

- podroben tehničen dokument o postopkih in operacijah overitelja in njegove infrastrukture

- navadno je zaupni dokument.

2.2. Status overiteljev v RS

V skladu s trenutno veljavno zakonodajo (ZEPEP) ločimo med naslednjimi statusi overitelja:
- overitelji nekvalificiranih potrdil
- overitelji kvalificiranih potrdil,
- akreditiran overitelj (lahko je overitelj kvalificiranih ali nekvalificiranih potrdil).

2.2.1 Register overiteljev (40. člen ZEPEP)

Register overiteljev je v pristojnosti Ministrstva za informacijsko družbo (MID). Po trenutno veljavni zakonodaji se v register overiteljev vpiše overitelj, ki v skladu s pravilnikom MID predloži ustrezno dokumentacijo o izpolnjevanju zakonskih zahtev. V register se vpišejo tako overitelji, ki izdajajo kvalificirana ali nekvalificirana potrdila. V register overiteljev se na njihovo zahtevo vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz zakona ZEPEP za veljavnost njihovih potrdil v Republiki Sloveniji. Objava registra je v pristojnosti MID.

2.2.2 Register akreditiranih overiteljev (42. – 45. člen ZEPEP).

Overitelji, ki dokažejo, da izpolnjujejo vse z zakonom in na njegovi podlagi izdanimi podzakonskimi predpisi predpisane pogoje za svoje delovanje, lahko zahtevajo, da jih akreditacijski organ vpiše v register akreditiranih overiteljev. Na njihovo zahtevo se lahko vpišejo tudi tuji overitelji, če izpolnjujejo pogoje iz tega zakona za veljavnost njihovih potrdil v Sloveniji. Prostovoljno akreditirani overitelji lahko to dejstvo označijo v izdanih potrdilih. Naloge akreditacijskega organa opravlja Agencija za telekomunikacije po trenutno veljavni zakonodaji.

2.3. Kvalificirana in nekvalificirana digitalna potrdila

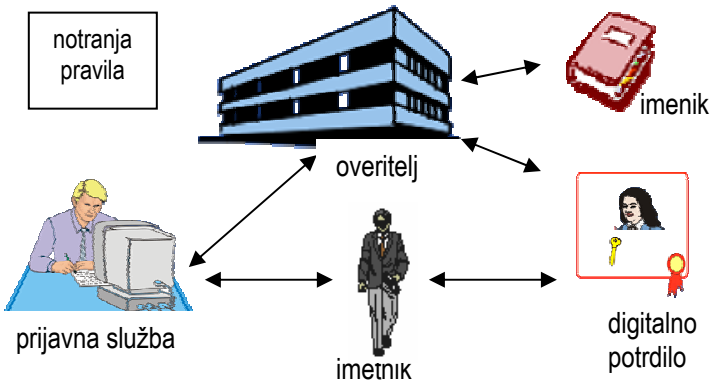
V skladu z ZEPEP in tudi direktivo se kvalificirana in nekvalificirana digitalna potrdila načelno razlikujejo po:
- vsebini: minimalni nabor podatkov je v primeru kvalificiranih digitalnih potrdil določen z zakonom
- načinu izdaje: za pridobitev kvalificiranega digitalnega potrdila se zahteva osebna identifikacija osebe – bodočega imetnika takega potrdila
- zahtevah za overitelja: overitelj, ki izdaja kvalificirana digitalna potrdila mora izpolnjevati strožje pogoje glede same infrastrukture, programske opreme, osebja itd.

Posamezni sklopi so podrobneje opisani v nadaljevanju.

3. PRAKTIČNA PRIPOROČILA S KONTROLNO LISTO

Delovanje overitelja je kombinacija tehnologije (programske in strojne opreme), poslovnih procesov (notranja pravila delovanja - politika delovanja, procesi) in pravnih elementov (dogovori, pogodbe), kar je zajeto z naslednjimi osnovnimi gradniki:
- infrastruktura overitelja
- njegova notranja pravila
- prijavna služba
- imenik potrdil in register preklicanih potrdil
- digitalna potrdila
- imetniki digitalnih potrdil

- in tretje osebe, ki se na potrdila zanašajo.



Slika 2 – Elementi infrastrukture overitelja

V okviru namena teh priporočil so v nadaljevanju zbrane zahteve v obliki kontrolnega seznama, ki jih morajo po trenutno veljavni zakonodaji izpolnjevati overitelji, ki izdajajo kvalificirana digitalna potrdila. Nazadnje pa so podana tudi praktična priporočila, ki jih morajo upoštevati tretje osebe, ki se odločijo za uporabo kvalificiranih potrdil izbranega overitelja.

3.1. Zahteve za kvalificirana digitalna potrdila

3.1.1 Zahteve po veljavni zakonodaji

Kvalificirano potrdilo mora vsebovati najmanj naslednje podatke (28. člen ZEPEP):		
1.	• navedbo, da gre za kvalificirano potrdilo	☐
2.	• identiteto overitelja in njegov podpis	☐
3.	• identiteta imetnika	☐
4.	• podatke za preverjanje elektronskega podpisa, ki ustrezajo podatkom za elektronsko podpisovanje pod nadzorom imetnika potrdila;	☐
5.	• varen elektronski podpis overitelja, ki je potrdilo izdal	☐
6.	• morebitne omejitve v zvezi z uporabo in transakcijami potrdila	☐
7.	• začetek in konec veljavnosti potrdila	☐
Kvalificirano potrdilo mora imeti ustrezno veljavnost:		
8.	• časovna veljavnost kvalificiranega potrdila razen lastnega kvalificiranega potrdila overitelja je največ pet let od dneva njegove izdaje (32. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje)	☐
Sredstva za varno elektronsko podpisovanje morajo zagotoviti, da:		
9.	• podatki za elektronsko podpisovanje (zasebni ključ) morajo biti edinstveni in njihova zaupnost zagotovljena	☐
10.	• podatkov za elektronsko podpisovanje (zasebni ključ) ni mogoče v razumnem času ali z razumnimi sredstvi ugotoviti iz podatkov za preverjanje elektronskega podpisa, elektronski podpis pa je učinkovito zaščiten pred poneverjanjem z uporabo trenutno dostopne tehnologije	☐
11.	• podpisnik lahko zanesljivo varuje svoje podatke za elektronsko podpisovanje (zasebni ključ) pred nepooblaščenim dostopom	☐

3.1.2 Uveljavljeni standardi

Kvalificirano potrdilo:		
12.	• je v skladu s standardom X.509 v 3 priporočil PKIX	☐
13.	• je v skladu s priporočili Qualified Certificate Profile – ETSI TS 101 862 v 1.2.1 (junij 2001)	☐
14.	• kriptografski ključi RSA min. dolžine 1024 bitov	☐
15.	• je v skladu s priporočili RFC3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"	☐
16.	• je v skladu s priporočili RFC 3039 "Internet X.509 Public Key Infrastructure Qualified Certificates Profile"	☐
Standardi za sredstva za varno elektronsko podpisovanje:		
17.	• morajo ustrezati EAL 4+ ali FIPS le v.2	☐

3.2. Zahteve za prijavne službe

Zahteve za prijavne službe:		
18.	• potrebna je fizična prisotnost bodočega imetnika	☐
19.	• potrebno je nedvoumno preveriti istovetnost imetnika kvalificiranega potrdila na podlagi uradnega in veljavnega osebnega dokumenta	☐
20.	• potrebno je nedvoumno preveriti istovetnost pravne osebe z uradno potrjenimi dokumenti za pravne osebe	☐
21.	• pooblaščene osebe prijavne službe overitelja sporočajo tiste podatke o osebah, ki so potrebni za izdajo kvalificiranega potrdila overitelja (31. člen ZEPEP, 20. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje)	☐

3.3. Zahteve za overitelje

3.3.1 Zahteve po veljavni zakonodaji

Vpis v register overiteljev		
22.	• overitelj mora bit vpisan v register overiteljev (s tem overitelj zagotovlja, da ustreza vsem zahtevam iz ZEPEP in Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje)	☐
23.	• podatki o opravljenem inšpekcijskem nadzoru	☐
Preklic in register preklicanih potrdil		
24.	• overitelj mora zagotavljati takojšen in varen preklic (39. člen ZEPEP)	☐
25.	• overitelj mora voditi register preklicanih potrdil, ki mora vsebovati zlasti identifikacijsko oznako preklicanega potrdila in čas preklica (30. člen ZEPEP)	☐
26.	• register mora biti varno elektronsko podpisan s kvalificiranim potrdilom (30. člen ZEPEP)	☐
27.	• register ne sme vsebovati podatkov o vzrokih za preklic (30. člen ZEPEP)	☐

Imenik kvalificiranih potrdil		
28.	• overitelj mora zagotavljati zanesljiv in ažuren imenik potrdil (overitelj mora uporabljati zanesljive sisteme za shranjevanje potrdil – imenik potrdil (spremembe možne samo pooblaščenim osebam, avtentičnost podatkov, javna dostopnost, zaznava tehnične spremembe, ki bi ogrozile varnost in zanesljivost)	☐
Obvestilo imetniku pred izdajo kvalificiranega digitalnega potrdila		
29.	• overitelj mora obvestiti imetnika o vseh ključnih zadevah v zvezi s potrdilom (podroben povzetek vsebine veljavnih predpisov ter notranjih pravil in drugih pogojev, ki se nanašajo na uporabo potrdila, podatke o morebitnih omejitvah uporabe potrdila, podatke o ukrepih imetnika potrdila, potrebnih za varnost elektronskega podpisovanja in preverjanja elektronskih podpisov, ter o ustrezni tehnologiji , ...)	☐
Zahteve po delovanju overitelja:		
30.	• overitelj ne sme hraniti podatkov za imetnikov podpis	☐
31.	• overitelj mora imeti zavarovano svojo škodno odgovornost. (34. člen ZEPEP)	☐
32.	• overitelj mora uporabljati zanesljive sisteme in opremo, ki so zaščiteni pred spreminjanjem in ki zagotavljajo tehnično in kriptografsko varnost postopkov, v katerih se uporabljajo (33. člen ZEPEP)	☐
33.	• overitelj mora zaposlovati osebje s potrebnim strokovnim znanjem, izkušnjami in usposobljenostjo na področju opravljanih storitev, še posebej na področju upravljanja ter poznavanja tehnologije elektronskega poslovanja in ustreznih varnostnih postopkov, da zagotovi izpolnjevanje vseh določb veljavne zakonodaje (32. člen ZEPEP).	☐
34.	• overitelj mora shranjevati vsa pomembna dokazila o načinu ugotovitve istovetnosti imetnika potrdila in načinu izdaje potrdila, vzroku, času in načinu morebitnega preklica potrdila, roku veljavnosti potrdila ter vseh sporočilih, ki se nanašajo na veljavnost potrdila, izmenjanih med overiteljem in imetnikom (35. člen ZEPEP)	☐
Javni del notranjih pravil overitelja (29. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje):		
35.	• določila o infrastrukturi overitelja, ki obsegajo osnovne tehnične in postopkovne lastnosti ter podatke o nivoju varnosti in zanesljivosti infrastrukture	☐
36.	• določila o številu, sestavi in usposobljenosti zaposlenih overitelja - overitelj, ki izdaja kvalificirana potrdila, mora zaposlovati osebje s potrebnim strokovnim znanjem, izkušnjami in usposobljenostjo na področju opravljanih storitev, še posebej na področju upravljanja ter poznavanja tehnologije elektronskega poslovanja in ustreznih varnostnih postopkov, da zagotovi izpolnjevanje vseh določb tega zakona (32. člen Uredbe)	☐
37.	• določila glede zahteve za morebitne podrejene overitelje, zahteve pri medsebojnem priznavanju overiteljev	☐
38.	• določila glede varnostnih zahtev in obveznosti imetnika kvalificiranih potrdil in tretje stranke, ki se zanašajo na kvalificirana potrdila	☐
39.	• določila glede osnovnih lastnosti in vsebine kvalificiranih potrdil, ki jih izdaja overitelj	☐
40.	• določila glede upravljanja s kvalificiranimi potrdili, kar obsega predvsem določila glede vloge za izdajo in preverjanja istovetnosti oseb ter določila glede izdaje, podaljševanja veljavnosti in preklica kvalificiranih potrdil	☐
41.	• določila glede odgovornosti overitelja in višini sklenjenega zavarovanja	☐
42.	• podatke o istovetnosti overitelja in njegove infrastrukture	☐
43.	• določila o postopkih pri prenehanju delovanja overitelja	☐
44.	• mora biti javno dostopen v elektronski obliki na internetu in na trajnem nosilcu podatkov v elektronski ali klasični obliki	☐
45.	• podatke o istovetnosti overitelja in njegove infrastrukture	☐
46.	• določila o postopkih pri prenehanju delovanja overitelja	☐

47.	• mora biti javno dostopen v elektronski obliki na internetu in na trajnem nosilcu podatkov v elektronski ali klasični obliki	☐
Zaupni del notranjih pravil overitelja (30. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje):		
48.	• določila, ki so določena z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje	☐

3.3.2 Uveljavljeni standardi

Infrastruktura overitelja:		
49.	• FIPS 140-1 za kriptografske module (18. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje)	☐
50.	• priporočljivo EAL5 oziroma najmanj EAL3 Skupnih meril - Common Criteria /ISO 15408 (18. člen Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje)	☐
51.	• CWA14172-2 EESSI Conformity Assessment Guidance – Part: 2: Certification Authority services and processes,	☐
52.	• CWA14172-3 EESSI Conformity Assessment Guidance – Part: 3: Trustworthy systems managing certificates for electronic signatures	☐
Register preklicanih potrdil:		
53.	• je v skladu s priporočili ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, ver. 2.	☐
54.	• je v skladu s priporočili RFC3280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"	☐
Imenik kvalificiranih potrdil:		
55.	• mora biti dostopen vsaj po protokolu LDAP	☐
56.	• dostopen tudi preko spletnih strani overitelja	☐
Priporočeni protokoli za izmenjavo ključev in kvalificiranih potrdil:		
57.	• Public Key Cryptography Standards PKCS#7, PKCS#10	☐
58.	• Public Key Infrastructure (based on) X.509 Certificate Management Protocols	☐
Javni del notranjih pravil overitelja:		
59.	• so v skladu z RFC 2527: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"	☐
60.	• so v skladu s Policy requirements for certification authorities issuing public key certificates - TS 102 042 (april 2002)	☐

3.4. Priznavanje različnih overiteljev

Tretje osebe, ki se zanašajo na potrdila overitelja kvalificiranih potrdil, morajo pri tehnični izvedbi upoštevati specifičnosti posameznih izdajateljev.

Tehnična raznolikosti profila potrdil	
1.	• namen uporabe
2.	• razširitve
3.	• število ključev

Dostopnost potrdila	
4.	• ali je javno dostopen ali ne, mesto dostopa
5.	• protokoli za dostop (LDAP, HTTP, HTTPS,…)
Dostopnost registra preklicanih potrdil	
6.	• objava CRL – angl.certificate revocation list (delna, celotna, …)
7.	• dostop OCSP – angl. *on-line certificate status protocol*
8.	• protokoli za dostop (LDAP, HTTP, HTTPS…)
9.	• časovne lastnosti izdajanja CRL
Istovetnosti imetnika potrdila	
10.	• način za ugotavljanje istovetnosti imetnika kvalificiranega potrdila

4. SLOVAR IN POJMOVNIK

CA: (angl. Certification Authority) overitelj je fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi, glej tudi Overitelj.

CEN: (fr. *Comite European de Normalisation*) je organizacija, ki pripravlja evropske standarde s področij informatike, ki pa ne sodijo v področji elektrotehnike in telekomunikacij. CEN je ustanovila t.i. standardizacijski sistem informacijske družbe (angl. *Information Society Standardization System* oz. CEN/ISSS) prek katerega se odvijajo delavnice, ki so odprtega tipa. Rezultati teh delavnic so objavljeni pod oznako CWA (angl*. CEN Workshop Agreements*).

CRL: Je seznam preklicanih potrdil s časom preklica, ki ga overitelj objavlja on-line in ki se osvežuje v kratkih, rednih časovnih razmikih (angl. *Certification Revocation List*).

CWA: (angl*. CEN Workshop Agreements*), je dokument s priporočili, izoblikovani kot rezultat delavnic CEN.

ETSI: (angl. *European Telecommunications Standards Institute*) je neprofitna organizacija, katere poslanstvo je priprava telekomunikacijskih standardov za področje Evrope, ki bodo služili kot smernice razvoja telekomunikacijskih storitev v prihodnje.

IDA: (angl. Interchange of data between administration), pod pokroviteljstvom komisije EU program projektov za določanje priporočil za izmenjavo podatkov med vladami. Leta 2005 bo program razširjen tudi na področje zasebnega sektorja in državljanov.

Kvalificirano potrdilo je potrdilo, ki izpolnjuje posebne zakonske zahteve glede oblike in vsebine potrdila.

LDAP: (angl.: Leightweight Directory Access Protocol) je protokol, ki določa dostop do imenika in je specificiran po IETF (angl.: Internet Engineering Task Force) priporočilu RFC 1777.

OCSP: Je s strani overitelja elektronsko podpisana izjava o veljavnosti oz. neveljavnosti določenega potrdila v določenem trenutku. (angl. *on-line certificate status protocol)*

Overitelj: Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. (CA, angl*. Certification Authority*).

PKI: Infrastruktura javnih ključev (angl. *Public Key Infrastructure*).

Politika delovanja overitelja je množica pravil overitelja digitalnih potrdil, ki se nanašajo na izdajanje digitalnih potrdil,

delovanje overitelja in načinov njihove uporabe pri verifikaciji elektronskih podpisov, je javni del notranjih pravil overitelja.

Potrdilo je z zasebnim ključem overitelja podpisano elektronsko potrdilo, ki jamči, da je javni ključ uporabnika, ki ga potrdilo vsebuje kot enega izmed podpisanih podatkov (poleg imena overitelja, obdobja veljavnosti potrdila, politike potrdila itd.) povezano s tem uporabnikom oz. identificira podpisnika na podlagi njegovega javnega ključa.

Prijavna služba: Služba za sprejem zahtevkov za potrdila in preverjanje istovetnosti bodočih imetnikov (*RA,* angl. *Registration Authority)*.

RFC: (angl. Request for Comment) splošno sprejeta priporočila "Internet research and development community". Priporočila so javno dostopna in brezplačna. Večina standardov RFC pomeni predloge ali sprejete standarde organizacije IETF.

SSL: angl. Secure Sockets Layer, je protokol, ki ga je Netscape predstavil leta 1994, omogoča šifrirano povezavo med strežnikom in odjemalcem in zagotavlja varnost za spletne aplikacije.

X.509: priporočila ITU-T, ki določajo digitalna potrdila.

X.500: priporočila ITU-T za privatne in javne storitve direktorijev, glej tudi LDAP.

ZEPEP: Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000).

Ostali pojmi so razloženi v dokumentu Pravnih vprašanj e-poslovanja in v drugih priporočilih

5. PRILOGE S POVZETKI OZ. TEORIJO POSAMEZNIH PRIPOROČIL

5.1. Priporočila ETSI

ETSI (angl. *European Telecommunications Standards Institute*) je neprofitna organizacija, katere poslanstvo je priprava telekomunikacijskih standardov za področje Evrope, ki bodo služili kot smernice razvoja telekomunikacijskih storitev v prihodnje. To so predstavniki uprave, operaterji, podjetja, ponudniki storitev, raziskovalne ustanove in uporabniki. ETSI igra pomembno vlogo pri razvoju širokega spektra standardov in tehnične dokumentacije, ki predstavlja evropski prispevek k svetovni standardizaciji na področju telekomunikacijske in informacijske tehnologije. ETSI je uradno priznan s strani Evropske komisije in sekretariata EFTA. V nadaljevanju so podana relevantna priporočila, ki določajo overitelje kvalificiranih potrdil je naštetih nekaj ETSI priporočil s področja Elektronskega poslovanja.

Priporočila za overitelje kvalificranih potrdil in upravljanje infrastrukture digitalnih potrdil:
- *Policy requirements for certification authorities issuing qualified certificates* - TS 101 456 v 1.2.1 (april 2002),
- *Qualified Certificate Profile* - TS 101 862 v 1.2.1 (junij 2001),
- *Policy requirements for certification authorities issuing public key certificates* - TS 102 042 (april 2002),
- *International Harmonization of Policy Requirements for CAs issuing Certificates* - TR 102040 (marec 2002).

5.2. Priporočila CEN

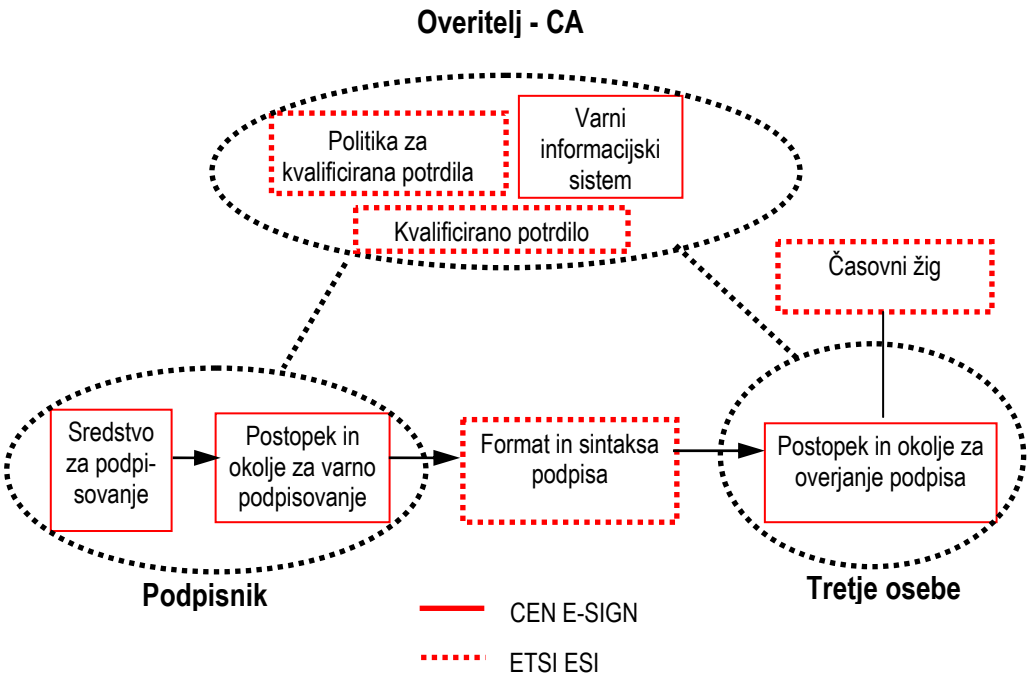
CEN (fr. *Comite European de Normalisation*) je organizacija, ki pripravlja evropske standarde s področij informatike, ki pa ne sodijo v področji elektrotehnike in telekomunikacij. CEN je ustanovila t.i. standardizacijski sistem informacijske družbe (angl. *Information Society Standardization System* oz. CEN/ISSS) prek katerega se odvijajo delavnice, ki so odprtega tipa. Rezultati teh delavnic so objavljeni pod oznako CWA (angl. *CEN Workshop Agreements*).

Delavnica CEN/ISSS E-SIGN je odgovorna za del EESSI delovnega programa, ki se nanaša na kvalitativne in funkcijske standarde za sredstva za elektronsko podpisovanje in sredstva za overjanje elektronskega podpisa ter tudi za kvalitativne

in funkcijske standarde za Overitelje. Doslej so bili pod okriljem CEN/ISSS s teh področij pripravljeni naslednji dokumenti:

- CWA14172-1 EESSI Conformity Assessment Guidance – Part: 1: General,
- CWA14172-2 EESSI Conformity Assessment Guidance – Part: 2: Certification Authority services and processes,
- CWA14172-3 EESSI Conformity Assessment Guidance – Part: 3: Trustworthy systems managing certificates for electronic signatures,
- CWA14172-4 EESSI Conformity Assessment Guidance – Part: 4: Signature Creation Application and Procedures for Electronic Signature Verification,
- CWA14172-5 EESSI Conformity Assessment Guidance – Part: 5: Secure signature creation devices,
- CWA14171 Procedures for Electronic Signature Verification,
- CWA 14170 Security Requirements for Signature Creation Systems,
- CWA 14169 Secure Signature-Creation Dvices, version 'EAL 4+',
- CWA 14168 Secure Signature-Creation Devices, version 'EAL 4',
- CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part1: System Security Requirements,
- CWA 14167-2 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2 Cryptographic Module for CSP Signing Operation – Protection Profile (MCSO-PP).

Naslednja slika (slika 3) prikazuje elemente, ki so vključeni v postopek pridobitve digitalnega potrdila in njegove uporabe za elektronski podpis ter za katere teh elementov pripravlja standarde posamezna organizacija t.j. CEN/ISSE ali ETSI.



Slika 3 – Razdelitev področij standardizacije ETSI in CEN