UREDBA

o pogojih za elektronsko poslovanje in elektronsko podpisovanje

1. Splošne določbe

1. člen

Ta uredba določa:

- merila, ki se uporabljajo za presojanje izpolnjevanja zahtev za delovanje overiteljev, ki izdajajo kvalificirana potrdila,
- podrobnejšo vsebino notranjih pravil overiteljev, ki izdajajo kvalificirana potrdila,
- podrobnejše tehnične pogoje za elektronsko podpisovanje in preverjanje varnih elektronskih podpisov,
- časovno veljavnost kvalificiranih potrdil,
- podrobnejše pogoje glede uporabe varnih časovnih žigov,
- vrsto in uporabo označbe akreditiranih overiteljev,
- pogoje za elektronsko poslovanje v javni upravi.

2. člen

Ne glede na določbe drugih členov te uredbe, strojna in programska oprema ter postopki izpolnjujejo merila in pogoje po tej uredbi, če so v skladu s standardi, merili ali pogoji, ki so splošno priznani v Evropski uniji in objavljeni v Uradnem listu Evropskih skupnosti.

2. Splošno o varovanju infrastrukture overitelja

3. člen

Overiteljevi prostori in infrastruktura morajo biti v skladu s pravili stroke ustrezno elektronsko in fizično varovani pred nepooblaščenimi vdori.

4. člen

(1) Overitelj mora opravljati redne varnostne preglede svoje infrastrukture vsak delovni dan. Če zagotavlja svoje storitve 24 ur na dan 365 dni na leto, pa vsak dan. Overitelj mora v dnevnik vpisovati vse svoje ugotovitve in posege.

(2) Pri tem mora preveriti, ali je njegova infrastruktura varna in ali vsi varnostni sistemi nemoteno delujejo in ali je v vmesnem času prišlo do vdora ali poskusa vdora nepooblaščenih oseb do overiteljeve opreme ali podatkov.

5. člen

S podatki za elektronsko podpisovanje overitelja morata upravljati vsaj dva overiteljeva zaposlena hkrati. V ta namen mora overitelj zagotoviti, da nihče ne more imeti sam vseh potrebnih podatkov in orodij, s katerimi je možen dostop do opreme, kjer so shranjeni podatki za elektronsko podpisovanje overitelja.

6. člen

Overitelj mora zagotoviti varno shranjevanje najmanj dveh varnostnih kopij in drugih medijev za prenos podatkov na tak način, da se prepreči izguba podatkov ali uporaba podatkov s strani nepooblaščenih oseb. Varnostne kopije morajo biti shranjene ločeno od overiteljevega informacijskega sistema za upravljanje kvalificiranih potrdil na drugi varni lokaciji. Overitelj mora v dnevnik zapisovati podatke o shranjevanju varnostnih kopij.

7. člen

Overitelj mora svoje podatke za elektronsko podpisovanje kvalificiranih potrdil uporabljati in varovati kot dober strokovnjak ter jih fizično in elektronsko varovati v skladu z uveljavljenimi pravili stroke, da se onemogoči fizični ali elektronski vdor oziroma nepooblaščen dostop do teh podatkov.

8. člen

Overitelj mora voditi enega ali več ločenih dnevnikov v pisni obliki, kamor morajo biti vpisani vsi podatki predpisani s to uredbo in drugi podatki o postopkih in posegih v infrastrukturo, ki vplivajo na zanesljivost delovanja overitelja. Dnevnik mora biti dostopen in hranjen za dobo vsaj 5 let.

9. člen

(1) Overitelj mora sestaviti poseben zapisnik o vseh začetnih avtorizacijah in vseh postopkih, uporabljenih pri vzpostavitvi svojega informacijskega sistema za upravljanje kvalificiranih potrdil. Zapisnik mora biti podpisan s strani vseh udeleženih v teh postopkih in trajno shranjen.

(2) Če pride kasneje do sprememb v avtorizacijah ali do pomembnih sprememb nastavitev informacijskega sistema za upravljanje kvalificiranih potrdil, ki so bile opravljene ob vzpostavitvi sistema, morajo biti vse omenjene spremembe dokumentirane v zapisniku.

3. Fizično varovanje infrastrukture overitelja

10. člen

Overitelj mora zagotavljati ustrezno fizično varovanje svoje strojne opreme in nadzor fizičnega dostopa do svojega informacijskega sistem za upravljanje kvalificiranih potrdil. V dnevnik mora ažurno zapisovati vse fizične dostope do tega informacijskega sistema.

11. člen

(1) Za fizični dostop do informacijskega sistema overitelja za upravljanje kvalificiranih potrdil se zahteva sočasna prisotnost vsaj dveh oseb, ki imata dovoljenje za dostop do tega sistema.

(2) Vstop v overiteljeve prostore, kjer se nahaja informacijski sistem overitelja za upravljanje kvalificiranih potrdil, mora biti omejen zgolj na osebe, ki v teh prostorih opravljajo svoja dela in naloge za overitelja. Dostop mora biti v skladu s pisnim seznamom oseb, ki imajo dovoljen reden vstop v posamezne prostore. Osebe, ki nimajo dovoljenega rednega vstopa, morajo biti vpisane na poseben seznam s strani oseb, ki imajo dovoljenje za reden vstop in morajo biti ves čas v spremstvu oseb z rednim vstopom.

4. Elektronsko varovanje infrastrukture overitelja

12. člen

(1)Overiteljeva informacijsko telekomunikacijska infrastruktura, ki je povezana v drugo informacijsko telekomunikacijsko omrežje, mora biti varovana z zanesljivimi varnostnimi mehanizmi (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada in podobno), ki preprečujejo nedovoljene dostope prek tega omrežja in omejujejo dostop samo po protokolih, ki so nujno potrebni za upravljanje s kvalificiranimi potrdili, vsi drugi protokoli pa morajo biti onemogočeni.

(2)Če je sistem zasnovan tako, da obstaja komunikacija preko drugega omrežja do overiteljevega sistema za upravljanje kvalificiranih potrdil, mora le-ta potekati po šifrirani poti.

13. člen

Informacijski sistem overitelja za upravljanje kvalificiranih potrdil mora biti sestavljen zgolj iz strojne in programske opreme, ki je potrebna za upravljanje kvalificiranih potrdil.

14. člen

Po poteku veljavnosti overiteljevih podatkov za elektronsko podpisovanje, ki niso nujno potrebni za preverjanje podatkov za nazaj, mora overitelj vse izvode varno in zanesljivo uničiti.

15. člen

Podatki overitelja, ki vplivajo na zanesljivost in varnost delovanja overitelja, ne smejo zapustiti sistema na nenadzorovani način, ki lahko ogrozi delovanje v skladu z veljavnimi predpisi in notranjimi pravili overitelja. Po poteku uporabe morajo biti nosilci podatkov odstranjeni ter nato varno in zanesljivo uničeni.

16. člen

(1) Overiteljev informacijski sistem za upravljanje kvalificiranih potrdil mora imeti vgrajene zadostne varnostne mehanizme, ki preprečujejo zlorabo s strani zaposlenih in omogočajo jasno ločitev nalog na področja iz 21. člena te uredbe.

(2) Varnostni ukrepi informacijskega sistema za upravljanje kvalificiranih potrdil morajo zagotavljati nadzorovan dostop do podatkov in sledljivost dostopa do ravni posameznika in sicer za vse posege in funkcije, ki vplivajo na overiteljevo upravljanje kvalificiranih potrdil.

5. Tehnične zahteve na strani overitelja

17. člen

Overitelj mora v okviru svoje tehnologije in postopkov zagotavljati edinstvenost podatkov za preverjanje elektronskega podpisa, kar pomeni, da mora omogočati nedvoumno in varno ugotavljanje istovetnosti imetnika iz podatkov za elektronsko podpisovanje.

18. člen

(1) Programska oprema, ki jo uporablja overitelj mora ustrezati svetovno uveljavljenim varnostnim in tehničnim standardom (FIPS 140-1 za kriptografske module, priporočljivo EAL5 oziroma najmanj EAL3 Skupnih meril - Common Criteria /ISO 15408/, priporočila izvedenske skupine Evropske iniciative za standardizacijo elektronskih podpisov - EESSI in drugo).

(2) Programska oprema, ki generira podatke za elektronsko podpisovanje, mora zagotavljati najmanjšo možnost poneverbe teh podatkov z uporabo trenutno razpoložljivih tehnologij.

19. člen

Overitelj mora zagotoviti zaupnost in enkratnost uporabe podatkov za generiranje kvalificiranega potrdila.

6. Prijavna služba

20. člen

(1) Zaposleni v prijavni službi overitelja osebno in z uporabo uradnih dokumentov s fotografijo imetnika zanesljivo ugotovijo istovetnost oseb ter zbirajo in sporočajo tiste podatke o osebah, ki so potrebni za izdajo kvalificiranega potrdila overitelja.

(2)Prijavna služba overitelja mora sporočati tako pridobljene podatke o osebah drugim službam overitelja na način, kot je to predpisano za zavarovanje osebnih podatkov z zakonom, ki ureja varstvo osebnih podatkov.

7. Overiteljevi zaposleni

21. člen

(1)Overitelj mora zaposlovati najmanj tri osebe z univerzitetno izobrazbo, od tega morata biti najmanj dve osebi z univerzitetno diplomo tehnične oziroma naravoslovne smeri, najmanj dve osebi pa morata imeti tudi dve leti delovnih izkušenj s področja delovanja overiteljev ali sorodnega področja.

(2) Zadolžitve zaposlenih za opravljanje nalog pri overitelju morajo biti porazdeljene med več oseb tako, da se prepreči možnost zlorab s strani zaposlenih. Zadolžitve zaposlenih overitelja morajo biti določene tako, da so med seboj jasno ločena področje upravljanja s kvalificiranimi potrdili, področje upravljanja z informacijskim sistemom overitelja in področje varovanja in kontrole.

22. člen

Overitelj mora zaposlovati ali imeti sklenjeno ustrezno svetovalno pogodbo z univerzitetnim diplomiranim pravnikom z opravljenim pravniškim državnim izpitom.

23. člen

(1) Vse osebe iz prejšnjih dveh členov morajo imeti posebna strokovna znanja glede upravljanja in poznavanja tehnologije, varnostnih postopkov in pravnih zahtev s področja elektronskega poslovanja in delovanja overiteljev pridobljena na strokovnih usposabljanjih.

(2)Zaposleni v prijavni službi morajo biti usposobljeni za zanesljivo ugotavljanje istovetnosti oseb.

24. člen

(1)Zaposleni overitelja ne smejo poleg svojega dela opravljati enakih oziroma podobnih del, kot jih opravljajo na svojem delovnem mestu, pri drugih overiteljih, če to niso podrejeni overitelji, ali opravljati del, ki so nezdružljiva z njihovimi delovnimi zadolžitvami in odgovornostmi pri overitelju.

(2) Ne glede na določbo prejšnjega odstavka sme zaposleni overitelja opravljati samostojno znanstveno in pedagoško delo, delo v kulturnih, umetniških, športnih, humanitarnih in drugih podobnih društvih in organizacijah ter delo na publicističnem področju.

8. Tehnične zahteve za varno elektronsko podpisovanje in preverjanje varnega elektronskega podpisa

25. člen

Vsaka uporaba podatkov za varno elektronsko podpisovanje mora od podpisnika zahtevati zavestno in zanesljivo dejanje za predstavitev sredstvu za varno elektronsko podpisovanje (npr. vnos gesla, prstni odtis in podobno) razen v primeru, da gre za samodejno odzivanje vnaprej programiranega informacijskega sistema.

26. člen

(1) Uporabnik mora vedno preveriti elektronski podpis v skladu z navodili podpisnika. Če je podpisnik podpisu priložil tudi potrdilo overitelja, pa mora elektronski podpis preveriti tudi v skladu z navodili overitelja, ki je potrdilo izdal, ali overitelja, ki je nadrejen ali priznava overitelja, ki je potrdilo izdal.

(2) Pri preverjanju elektronskega podpisa s pomočjo potrdila overitelja mora uporabnik vedno preveriti veljavnost potrdila v skladu z navodili overitelja, ki je izdal potrdilo. Uporabnik mora preveriti tudi, ali je potrdilo navedeno v registru preklicanih potrdil, če overitelj, ki je izdal potrdilo, vodi tak register.

(3) Sredstvo za preverjanje varnega elektronskega podpisa mora uporabniku omogočati, da jasno ugotovi, kateri podatki in v kakšnem obsegu so bili podpisani. Če so podpisani podatki povezani z drugimi podatki ali se na druge podatke sklicujejo ter je uporabniku omogočen samodejen preskok na te podatke, mora sredstvo jasno opozoriti uporabnika, če ti podatki niso zajeti s preverjenim elektronskim podpisom.

9. Zavarovanje odgovornosti

27. člen

Najnižji znesek zavarovalne vsote, za katero overitelj, ki izdaja kvalificirana potrdila, zavaruje svojo škodno odgovornost, znaša 50.000.000,00 tolarjev.

10. Notranja pravila overiteljev

28. člen

Notranja pravila overiteljev, ki izdajajo kvalificirana potrdila, morajo vsebovati javni in zaupni del. Vse bistvene določbe notranjih pravil, ki vplivajo na odnos med overiteljem in imetniki od njega izdanih kvalificiranih potrdil ter tretjimi osebami, ki se zanašajo na ta potrdila, morajo biti vsebovani v javnem delu notranjih pravil.

29. člen

Notranja pravila morajo v svojem javnem delu vsebovati najmanj:

- določila o infrastrukturi overitelja, ki obsegajo osnovne tehnične in postopkovne lastnosti ter podatke o nivoju varnosti in zanesljivosti infrastrukture;
- določila o številu, sestavi in usposobljenosti zaposlenih overitelja;
- določila glede zahteve za morebitne podrejene overitelje, zahteve pri medsebojnem priznavanju overiteljev;
- določila glede varnostnih zahtev in obveznosti imetnika kvalificiranih potrdil in tretje stranke, ki se zanašajo na kvalificirana potrdila;
- določila glede osnovnih lastnosti in vsebine kvalificiranih potrdil, ki jih izdaja overitelj;
- 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;
- določila glede odgovornosti overitelja in višini sklenjenega zavarovanja;
- podatke o istovetnosti overitelja in njegove infrastrukture;
- določila o postopkih pri prenehanju delovanja overitelja.

30. člen

Notranja pravila morajo v svojem zaupnem delu vsebovati najmanj:

- določila glede prostorov overitelja;
- dodatna določila glede osebja overitelja, kar obsega predvsem pristojnosti in naloge posameznih članov osebja, določila glede posebnih pooblastil članov osebja, zahtevani pogoji za osebje in določila glede morebitnih zunanjih sodelavcev;
- določila glede fizičnega varovanja infrastrukture overitelja, kar obsega predvsem določila glede dostopa v prostore overitelja (vstopne pravice, avtentikacijski sistem,...), glede ravnanja s strojno opremo in odpadki ter glede vnosa in iznosa opreme in materiala;
- določila glede elektronskega oziroma programskega varovanja, kar obsega predvsem določila glede varnostnih nastavitev strežnikov, uporabe telekomunikacijskih sredstev in opreme ter določil glede prijave v sistem, varnostnih kopij in podobno;
- določila glede notranjega nadzora, kar obsega predvsem operativno izvedbo in spremljanje dogodkov (kontrola fizičnega dostopa, kontrola pooblastil, poročanje o varnostnih problemih in podobno);
- določila glede ukrepov ob nepredvidenih dogodkih;
- določila glede vodenje dnevnikov in sestave zapisnikov, vključno z določili glede morebitne elektronske oblike zapisa.

31. člen

Javni del notranjih pravil overiteljev mora biti javno dostopen v elektronski obliki na internetu in na trajnem nosilcu podatkov v elektronski ali klasični obliki.

11. Časovna veljavnost kvalificiranih potrdil

32. člen

Časovna veljavnost kvalificiranega potrdila razen lastnega kvalificiranega potrdila overitelja je največ pet let od dneva njegove izdaje.

33. člen

(1) Kdor hrani elektronsko podpisane podatke, mora najkasneje en mesec pred iztekom roka, ki ga je za veljavnost podatkov za elektronski podpis določil overitelj v javnem delu notranjih pravil, če tega roka ni, pa z dnem konca veljavnosti kvalificiranega potrdila, zagotoviti ponoven elektronski podpis teh podatkov s strani vseh oseb, ki so podatke elektronsko podpisale prvič, ali s strani notarja ali potrditev teh podatkov z varnim časovnim žigom overitelja.

(2) Overitelj je dolžan ob izdaji kvalificiranega potrdila opozoriti imetnika potrdila o ponovnem elektronskem podpisu podatkov iz prejšnjega odstavka.

12. Varni časovni žig

34. člen

(1) Varni časovni žig mora vsebovati nedvoumne in pravilne podatke o datumu, točnemu času najmanj na sekundo natančno in overitelju, ki je varni časovni žig ustvaril.

(2) Varni časovni žig je lahko dokumentu dodan ali priložen in z njim povezan, vendar morajo biti pri tem vedno izpolnjene enake zahteve kot za varen elektronski podpis s kvalificiranim potrdilom.

35. člen

Overitelj, ki izdaja varne časovne žige, mora uporabljati informacijski sistem, ki je sinhroniziran z virom točnega časa.

13. Označba akreditiranega overitelja

36. člen

(1) Znak za akreditiranega overitelja je okrogle oblike, z veliko tiskano črko "A" v sredini in napisom "AKREDITIRANI OVERITELJ V REPUBLIKI SLOVENIJI" v slovenski različici ter napisom "ACCREDITED CERTIFICATION SERVICE IN THE REPUBLIC OF SLOVENIA" v angleški različici (Priloga 1) ob celotnem robu kroga.

(2) Znak se lahko uporablja v poljubni velikosti ob ohranitvi enakih razmerij (Priloga 1).

37. člen

(1) Akreditirani overitelj lahko znak iz prejšnjega člena uporablja pri svojem poslovanju na dokumentih v klasični ali elektronski obliki.

(2) Pri poslovanju v slovenskem jeziku mora overitelj vedno uporabljati znak v slovenski različici, pri poslovanju v drugih jezikih lahko uporablja znak v angleški različici.

14. Elektronsko poslovanje v javni upravi

38. člen

Vse informacijske rešitve za elektronsko poslovanje v javni upravi morajo, če vsebujejo tudi uporabo elektronskega podpisa, uporabljati izključno potrdila overitelja SIGOV-CA Centra Vlade za informatiko ali njemu podrejenih ali od njega potrjenih drugih overiteljev. Center Vlade za informatiko razvije hierarhično porazdeljeni model zaupanja.

39. člen

Upravne enote opravljajo naloge v zvezi s prijavo in ugotavljanjem istovetnosti oseb za uporabo elektronskega poslovanja z institucijami javne uprave. Pooblastilo se lahko izda tudi drugim institucijam.

40. člen

(1) Pri Centru Vlade RS za informatiko deluje komisija kot svetovalno telo za vprašanja uporabe elektronskega poslovanja in podpisovanja v javni upravi, predvsem za pregledovanje varnostnih, tehničnih in pravnih zahtev ter druga vprašanja.

(2) Komisija daje Vladi Republike Slovenije in ministru, pristojnemu za gospodarstvo, na podlagi zakona o elektronskem poslovanju in elektronskem podpisu predloge za sprejem podzakonskih aktov iz njune pristojnosti ter inšpekcijskemu in akreditacijskemu organu priporočila glede oblikovanja varnostnih in tehničnih meril za opravljanje nadzora nad delovanjem overiteljev.

41. člen

Člane komisije imenuje Vlada Republike Slovenije izmed naravoslovnih, tehničnih in pravnih strokovnjakov v državni upravi in izven nje na predlog direktorja Centra Vlade Republike Slovenije za informatiko.

15. Prehodni in končni določbi

42. člen

(1) Zaposleni in pogodbeni sodelavci overiteljev, ki bodo začeli delovati pred 1. januarjem 2002, morajo izpolniti zahteve iz 23. člena te uredbe najkasneje do tega datuma.

(2) Dokler zavarovalnice na trgu Republike Slovenije ne ponudijo možnosti sklenitve zavarovanja iz 27. člena te uredbe, se šteje, da overitelj, ki izdaja kvalificirana potrdila, izpolnjuje pogoj iz 27. člena:

- če pridobi drug ustrezen finančni instrument (npr. bančna garancija), s katerim se finančna institucija zaveže, da bo v primeru škodnega dogodka oškodovancu v imenu overitelja izplačala odškodnino v višini, ki ne sme biti manjša od zneska iz 27. člena, ali
- če vrednost obveznosti prostega premoženja overitelja ali pravne osebe, ki solidarno jamči za overiteljevo odgovornost, znaša najmanj trikratni znesek iz 27. člena te uredbe.

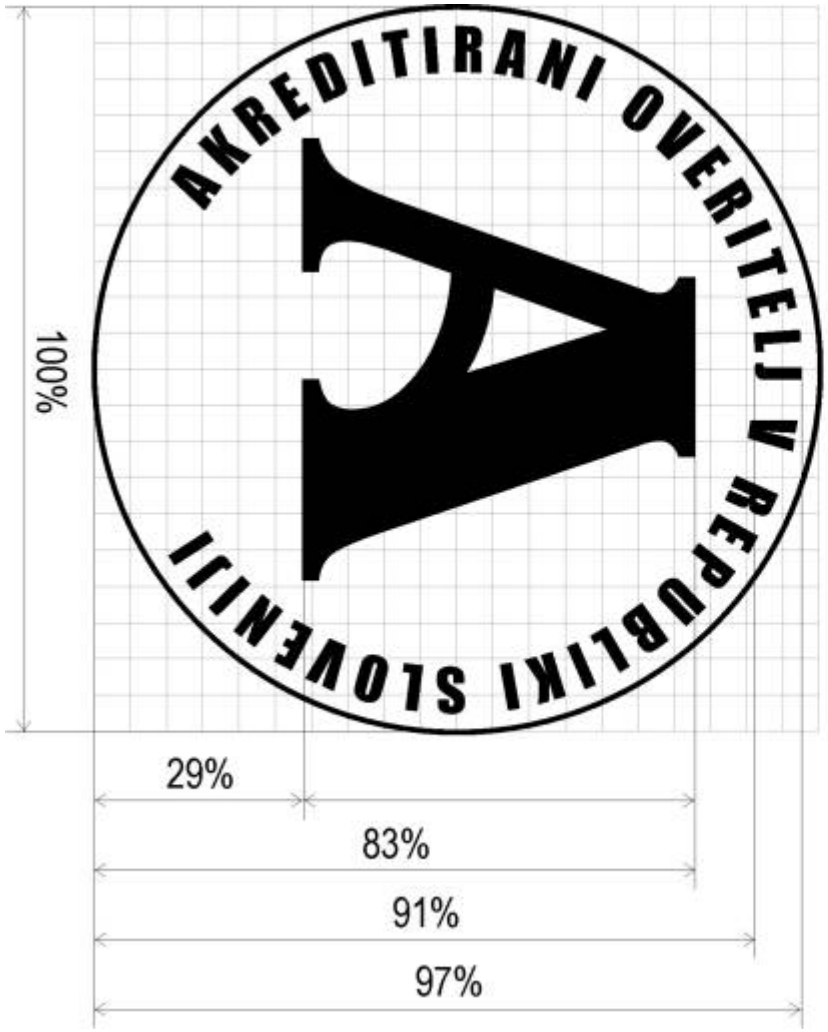
42.a člen

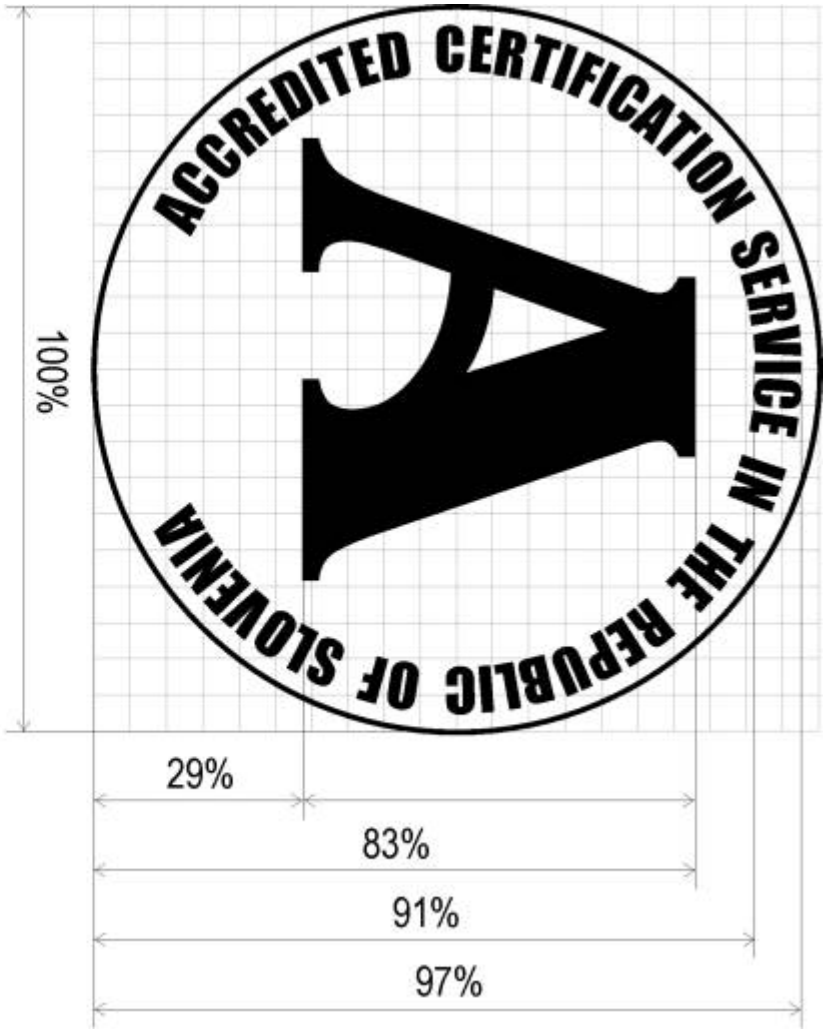
Potrdila, ki jih je izdal overitelj, ki je deloval pred uveljavitvijo te uredbe, se štejejo za kvalificirana potrdila, če potrdila in overitelj ob prijavi pristojnemu ministrstvu izpolnjujejo pogoje iz te uredbe.

43. člen

Uredba začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije.

PRILOGA 1:


AKREDITIRANI OVERITELJ V REPUBLIKI SLOVENIJI
100%
29%
83%
91%
97%


ACCREDITED CERTIFICATION SERVICE IN THE REPUBLIC OF SLOVENIA
100%
29%
83%
91%
97%