

# Politika HALCOM-CA

Javni del notranjih pravil HALCOM-CA

za poslovna in strežniška  
kvalificirana digitalna potrdila

CPName: HALCOM CA PO 2

CPoID: 1.3.6.1.4.1.5939.1.2.4

Dokument je veljaven od: 05.03.2007

## Kazalo

Kazalo .....	2
1. UVOD .....	3
2. SPLOŠNE DOLOČBE .....	3
2.1 NAMEN IN UPORABA POTRDIL .....	3
2.2 STROŠKI UPORABE INFRASTRUKTURE .....	4
3. INFRASTRUKTURA HALCOM-CA .....	4
3.1 SPLOŠNE ZNAČILNOSTI .....	4
3.1.1 Osnovni podatki o HALCOM-CA .....	4
3.1.2 Lastno potrdilo glavnega overitelja .....	5
3.1.3 Šifrirni algoritmi, formati podatkov in protokoli .....	5
3.1.4 Imenik .....	5
3.1.5 Register preklicanih potrdil.....	5
3.1.6 Morebitno prenehanje delovanja HALCOM-CA .....	6
3.2 VARNOSTNE ZAHTEVE IN ZANESLJIVOST .....	6
3.2.1 Varnostne zahteve in zanesljivost .....	6
3.2.2 Osebjje .....	6
3.2.3 Nadzor .....	8
3.3 ODGOVORNOST .....	8
3.3.1 Odgovornost .....	8
3.3.2 Zavarovanje odgovornosti.....	8
3.4 PODREJENI OVERITELJI .....	8
3.4.1 Varnostne zahteve in zanesljivost .....	8
3.4.2 Zahteve glede osebjja .....	9
3.4.3 Medsebojno priznavanje .....	9
3.4.4 Odgovornost .....	9
3.5 MEDSEBOJNO PRIZNAVANJE Z DRUGIMI OVERITELJI ALI MREŽAMI OVERITELJEV. 9	
4. UPRAVLJANJE POTRDIL .....	10
4.1 OSNOVNA PRAVILA ZA UPRAVLJANJE S POTRDILI.....	10
4.2 IZDAJA POTRDILA .....	11
4.2.1 Naročilnica za izdajo potrdila .....	11
4.2.2 Izdaja poslovnega potrdila .....	11
4.2.3 Izdaja in prevzem strežniškega potrdila .....	12
4.3 OBDOBJE VELJAVNOSTI POTRDILA IN PODPISA .....	12
4.4 PODALJŠANJE VELJAVNOSTI POTRDILA.....	12
4.5 PREKLIC POTRDILA IN OBJAVA V REGISTRU PREKLICANIH POTRDIL .....	13
5. IMETNIKI POTRDIL .....	13
5.1 VARNOSTNE ZAHTEVE .....	13
5.2 PRAVICE IMETNIKA POTRDILA .....	13
6. PRAVNE OSEBE .....	14
6.1 VARNOSTNE ZAHTEVE .....	14
6.2 PRAVICE PRAVNE OSEBE.....	14
7. TRETJE OSEBE .....	14
7.1 VARNOSTNE ZAHTEVE .....	14
7.2 PRAVICE TRETJE OSEBE.....	15
8. KONČNE IN PREHODNE DOLOČBE .....	15
8.1 SPLOŠNO.....	15
8.2 REŠEVANJE SPOROV .....	15
8.3 VELJAVNOST .....	15
TERMINOLOŠKI SLOVAR IN KRATICE .....	16

## 1. UVOD

(1) Ta politika, ki predstavlja nedeljivo celoto javnega dela notranjih pravil overitelja HALCOM-CA glede izdaje kvalificiranih poslovnih potrdil in kvalificiranih strežniških potrdil, ureja namen, delovanje in metodologijo upravljanja kvalificiranih poslovnih potrdil ter varnostne zahteve, ki jih morajo izpolnjevati overitelji HALCOM-CA, imetniki in tretje osebe, ki se zanašajo na ta potrdila, ter odgovornost vseh naštetih oseb.

(2) HALCOM-CA je overitelj, ki izdaja in upravlja s kvalificiranimi poslovnimi potrdili in kvalificiranimi strežniškimi potrdili za overjanje varnega elektronskega podpisa. HALCOM-CA deluje tudi kot glavni overitelj, ki skupaj s svojimi podrejenimi overitelji sestavlja hierarhično mrežo overiteljev, ki je namenjena izdajanju kvalificiranih osebnih in spletnih potrdil in opravljanju tehnoloških storitev v zvezi z varnimi elektronskimi podpisi.

(3) HALCOM-CA izdaja potrdila v skladu z veljavnimi nacionalnimi predpisi s področja elektronskega poslovanja in elektronskega podpisa ter z direktivo Evropskega parlamenta in Sveta Evropske unije z dne 13. decembra 1999 o skupnem okviru Skupnosti za elektronske podpise.

(4) Vse določbe te politike glede ravnanja HALCOM-CA so ustrezno prenesene in podrobneje opredeljene v določbah notranje politike, ki predstavlja zaupni del notranjih pravil in jo sestavljajo dokumenti zaupne narave, ki definirajo infrastrukturo, določila glede osebja HALCOM-CA (pristojnosti, naloge, pooblastila in zahtevani pogoji posameznih članov osebja), fizično varovanje (dostop do prostorov, ravnanje s strojno in programsko opremo), programsko varovanje (varnostne nastavitve strežnikov, varnostne kopije...) in notranji nadzor (kontrola fizičnih dostopov, pooblastil,...) ter so v skladu s tehničnimi zahtevami Evropskega inštituta za telekomunikacijske standarde (*European Telecommunications Standards Institute*) ETSI TS 101 456 (*Policy requirements for certification authorities issuing qualified certificates*) in ETSI TS 101 862 (*Qualified certificate profile*).

(5) Overitelj HALCOM-CA se lahko povezuje z drugimi overitelji na horizontalni (bilateralni) ravni.

## 2. SPLOŠNE DOLOČBE

### 2.1 NAMEN IN UPORABA POTRDIL

(1) HALCOM-CA upravlja (izdaja in overja, preklicuje, podaljšuje, hrani in objavlja) s kvalificiranimi poslovnimi potrdili za overjanje elektronskega podpisa (v nadaljevanju poslovna potrdila), ki so namenjena pooblaščenim oz. zaposlenim osebam (v nadaljevanju imetniki potrdil) pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti (v nadaljevanju pravnih oseb), in s kvalificiranimi poslovnimi potrdili za overjanje elektronskega podpisa, ki so namenjena uporabi na strežnikih pravnih ali fizičnih oseb, registriranih za opravljanje dejavnosti. (v nadaljevanju strežniška potrdila).

(2) Poslovna in strežniška potrdila so namenjena za elektronsko podpisovanje enostranskih ali medsebojnih komunikacij imetnikov potrdil ter za uporabo v različnih aplikacijah in za različne namene, ki se pojavljajo na tržišču. Med drugim se lahko ta potrdila uporabljajo v aplikacijah in namenih kot so:

- 1) elektronsko bančništvo
- 2) aplikacije E uprave
- 3) podpisovanje elektronskih obrazcev

- 4) elektronsko shranjevanje podatkov
- 5) varovanje omrežnih povezav
- 6) druge vrste uporabe, ki jih določi in javno objavi Halcom-CA

Potrdila se lahko uporabijo za:

- šifriranje podatkov in sporočil v elektronski obliki,
- digitalno podpisovanje podatkov in sporočil v elektronski obliki ter overjanje identitete podpisnika,
- varovanje podatkov med prenosi po nezaščitenih kanalih
- varno brisanje podatkov v elektronski obliki.

Ti načini uporabe omogočajo:

- 1) elektronsko bančništvo za hkratno delo z več bankami;
- 2) varno elektronsko podpisovanje E obrazcev;
- 3) varno poslovanje pravnih oseb z javnim sektorjem;
- 4) varno poslovanje med pravnimi osebami.

## **2.2 STROŠKI UPORABE INFRASTRUKTURE**

(1) HALCOM-CA določi cenik uporabe poslovnih in strežniških potrdil ter svojih storitev ter cenik objavi na svojih spletnih straneh.

## **3. INFRASTRUKTURA HALCOM-CA**

### **3.1 SPLOŠNE ZNAČILNOSTI**

#### **3.1.1 Osnovni podatki o HALCOM-CA**

Naslov HALCOM-CA: **HALCOM-CA**

**Tržaška 118  
1000 LJUBLJANA  
Slovenija  
Tel.: (+386) 01 200 33 40  
Fax: (+386) 01 200 33 56  
E-pošta: ca@halcom.si**

Osnovne informacije o glavnem overitelju so na voljo tudi na spletnem strežniku z naslovom:

**<http://www.halcom.si/>**

### **Identiteta**

HALCOM-CA predstavljajo naslednji podatki:

C=SI, O=Halcom, CN=Halcom CA PO 2  
CPName HALCOM CA PO 2  
CPOID 1.3.6.1.4.1.5939.1.2.4

(1) Infrastrukturo HALCOM-CA sestavljajo:

- notranji in zunanji prostori HALCOM-CA;
- strojna in programska oprema, ki jo HALCOM-CA uporablja za upravljanje s potrdili ali opravljanje drugih storitev v zvezi z elektronskim podpisovanjem;
- osebje HALCOM-CA;
- metode in postopki pri upravljanju s potrdili in drugih storitev v zvezi z elektronskim podpisovanjem.

### 3.1.2 Lastno potrdilo glavnega overitelja

(1) HALCOM-CA je oblikoval svoje lastno kvalificirano digitalno potrdilo (potrdilo HALCOM CA PO 2), serijska številka 79074 (01 34 e2), ki je namenjeno podpisovanju potrdil drugih imetnikov, podpisovanju registra preklicanih potrdil ter preverjanju podpisa oz. veljavnosti overitelja.

(2) Potrdilo HALCOM CA PO 2 vsebuje naslednje podatke:

Serijska številka	79074 (01 34 e2)
Overitelj potrdila	HALCOM CA PO 2, Halcom, SI
Imetnik potrdila	HALCOM CA PO 2, Halcom, SI
Veljavnost potrdila	7.2. 2004 – 7.2.2019
Dolžina ključa	1024 bitov
SHA-1	7f bb 6a cd 7e 0a b4 38 da af 6f d5 02 10 d0 07 c6 c0 82 9c

### 3.1.3 Šifrirni algoritmi, formati podatkov in protokoli

(1) HALCOM-CA uporablja:

- za podpisovanje potrdil algoritem RSA s parom ključev dolžine 1024 bitov,
- za šifriranje podatkov algoritme Triple DES,
- zgostitveni algoritem SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in MD5 (RFC 1321),
- format potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:2001 ter X.509 ver. 3 (v3),
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:2001,
- protokol LDAP ustreza priporočilu RFC 1777,

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri HALCOM-CA.

### 3.1.4 Imenik

(1) Vsa potrdila overiteljev temeljijo na standardu X.509 in so lahko javno objavljena v centralnem imeniku, ki je v skrbništvu HALCOM-CA, v tem imeniku pa je tudi javni centralni register preklicanih potrdil.

(2) Dostop do imenika je možen po protokolu LDAP.

### 3.1.5 Register preklicanih potrdil

(1) Register preklicanih potrdil HALCOM-CA je seznam preklicanih potrdil (CRL) in se nahaja v veji:

CN= Halcom CA PO 2  
 O = Halcom  
 C = SI

(2) Register preklicanih potrdil se osvežuje po vsakem preklicu potrdila oziroma najmanj enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil (24 ur po zadnjem osveževanju).

(3) Register preklicanih potrdil vsebuje enolično interno serijsko številko preklicanega potrdila in čas ter datum preklica.

### **3.1.6 Morebitno prenehanje delovanja HALCOM-CA**

(1) Če HALCOM-CA preneha z delovanjem, prekliče vsa potrdila, ki jih je do tedaj izdal, vodenje njegovega registra preklicanih potrdil pa preda drugemu overitelju ali pristojnemu ministrstvu.

## **3.2 VARNOSTNE ZAHTEVE IN ZANESLJIVOST**

### **3.2.1 Varnostne zahteve in zanesljivost**

(1) HALCOM-CA načrtuje in izvaja vse varnostne ukrepe v skladu s standardi ISO/IEC 17799:2005 (Code of practice for information security management), ISO/IEC 27001:2005 (Information security management systems – Requirements) in BS 7799-3:2005 (Information Security Management Systems - Guidelines for Information Security Risk Management), FIPS 140-1 level 3 ter tehničnimi zahtevami ETSI TS 101 456 - Policy requirements for certification authorities issuing qualified certificates

(2) Oprema HALCOM-CA je postavljena v posebnih, ločenih prostorih in je zavarovana z večnivojskim sistemom fizičnega in protivlomnega tehničnega varovanja. Oprema je varovana proti nepooblaščenemu dostopu. Prav tako je zavarovana in zaščitena s protipožarnim sistemom, s sistemom proti izlitju vode, sistemom za prezračevanje in večnivojskim sistemom neprekinjenega napajanja.

(3) HALCOM-CA shranjuje rezervne in distribucijske medije tako, da je v največji meri preprečena izguba, vdor ali nepooblaščen uporaba ali spreminjanje shranjenih informacij. Tako za obnovitev podatkov kot za arhiviranje pomembnih informacij so zagotovljene rezervne kopije, ki so shranjene na drugem mestu, kot je shranjena programska oprema za upravljanje s potrdili, za zagotovitev ponovnega delovanja v primerih, ko bi bili uničeni podatki na osnovni lokaciji.

(4) Podroben opis infrastrukture HALCOM-CA, operativno delovanje, postopki upravljanja z infrastrukturo ter nadzor nad varnostno politiko njegovega delovanja je določen z njegovo interno politiko.

### **3.2.2 Osebj**

(1) HALCOM-CA zaposluje zanesljivo in strokovno usposobljeno osebje, ki preverjeno ni bilo kaznovano za kakršnokoli kaznivo dejanje. Vse osebe se redno usposablja in pridobiva dodatna znanja s svojega strokovnega področja.

(2) Operativne delovne vloge so načrtovane tako, da v največji možni meri preprečujejo možnosti zlorab in so razdeljene med posamezne, med seboj nezdržljive organizacijske skupine:

**Organizacijska skupina:** Upravljanje z informacijskim sistemom

**Vloga:** upravljalca informacijskega sistema

**Število oseb:** 2

**Naloge:**

1. Priprava začetne konfiguracije sistema, vključno z varnim zagonom in ustavitvijo delovanja sistema
2. Začetna nastavitve parametrov novih podrejenih overiteljev
3. Postavitve začetne konfiguracije omrežja
4. Priprava medijev za zasilni ponovni start sistema v primeru katastrofalne izgube sistema
5. Priprava sistemskih kopij, nadgradnja in obnovitev programske opreme, varno shranjevanje in distribucija kopij in nadgradenj na ločeno lokacijo
6. Administrativne funkcije, ki so povezane z vzdrževanjem baze podatkov overitelja in ki pomagajo pri raziskavah odstopanj od pravil
7. Spremembe imena strežnika in/ali omrežnega naslova
8. Izvajanje arhiviranja zahtevanih sistemskih zapisov

**Organizacijska skupina:** Varovanje in kontrola

**Vloga:** Prvi varnostni inženir

**Število oseb:** 2

**Naloge:**

1. Upravljanje postopkov za izdajo potrdil
2. Pomoč podrejenim overiteljem
3. Pooblaščenje podrejenih overiteljev
4. Izpis PIN kod
5. Dostop do protokola podpisovanja potrdil

**Organizacijska skupina:** Upravljanje s potrdili

**Vloga:** drugi varnostni inženir

**Število oseb:** 2

**Naloge:**

1. Priprava potrdil (obdelava podpisanih zahtev za potrdila)
2. Poosebljanje (izdelava potrdil, zapis na medij, tiskanje imetnikovih podatkov na medij)
3. Preklic potrdil

**Organizacijska skupina:** Upravljanje s potrdili

**Vloga:** administrator potrdil

**Število oseb:** 2

**Naloge:**

1. Identifikacija imetnikov potrdil oziroma pooblaščene osebe pravnih oseb
2. Varna distribucija potrdil imetnikom
3. priprava zahtev za preklic potrdil

**Organizacijska skupina:** Upravljanje s potrdili

**Vloga:** administrator PIN kod

**Število oseb:** 2

**Naloge:**

1. Distribucija PIN kod

**Organizacijska skupina:** Varovanje in kontrola

**Vloga:** Uslužbenec za varnost informacijskega sistema

**Število oseb:** 2

**Naloge:**

1. Določanje varnostnih pravil in nadzor njihovega upoštevanja
2. Pregledovanje sistemske dokumentacije in kontrolnih dnevnikov za nadzor dela
3. Osebno sodelovanje in pomoč pri letni inventuri dokumentacije podrejenih overiteljev

(3) Navedeno je minimalno število zaposlenih za posamezne vloge.

(4) Za vsako vlogo je v interni politiki HALCOM-CA natančno določeno, s katero sme oz. ne sme biti združljiva. Za nekatere je potrebna prisotnost vsaj dveh za to pooblaščenih

oseb. V primeru nepredvidene odsotnosti določenih zaposlenih, njihove vloge prevzamejo drugi zaposleni, če to po interni politiki ni nezdružljivo.

### **3.2.3 Nadzor**

(1) Pri HALCOM-CA deluje tričlanska nadzorna skupina, ki jo sestavljajo strokovnjaki z ustreznimi tehnološkimi in pravnimi znanji, ki ne opravljajo nalog v zvezi z upravljanjem potrdil.

(2) Nadzorna skupina nadzoruje delo HALCOM-CA. Nadzorna skupina v primeru odkritih pomanjkljivosti odredi ustrezne ukrepe za odpravo teh pomanjkljivosti, ki jih je HALCOM-CA dolžan izvesti, ter nadzoruje izvedbo odrejenih ukrepov.

## **3.3 ODGOVORNOST**

### **3.3.1 Odgovornost**

(1) HALCOM-CA ne prevzema nobene odgovornosti za podatke, ki jih imetnik potrdila elektronsko šifrira ali podpisuje in sicer tudi v primeru, da je imetnik ali tretja oseba spoštoval vse veljavne predpise, vsa določila te politike in drugih pravil HALCOM-CA oziroma upošteval vsa njegova navodila.

(2) HALCOM-CA ne prevzema nobene odgovornosti za posledice, ki nastanejo, ker imetnik potrdila ni ravnal v skladu z varnostnimi zahtevami iz točke 5.1 te politike.

### **3.3.2 Zavarovanje odgovornosti**

(1) HALCOM-CA ima ustrezno zavarovano svojo odgovornost. Podrobnejše informacije so objavljene na spletnih straneh.

## **3.4 PODREJENI OVERITELJI**

(1) Podrejeni overitelji so tiste pravne osebe, ki opravljajo dejavnost overiteljev in so vključeni v mrežo overiteljev HALCOM-CA in jim glavni overitelj izda kvalificirano potrdilo za izdajanje potrdil drugim imetnikom.

(2) HALCOM-CA kot glavni overitelj lahko, če določbe veljavnih predpisov držav podrejenih overiteljev po mnenju glavnega overitelja ne zadoščajo za zagotavljanje varnosti in zanesljivosti, sprejme in javno objavi Pogoje za podrejene overitelje, ki natančneje določajo varnostne zahteve, zahteve glede osebja in druge ustrezne zahteve za podrejene overitelje.

(3) Podrejeni overitelji ravnajo v skladu z nacionalnimi predpisi in s to politiko ter s svojo interno politiko, katere določbe so v primeru, da gre za državo, ki je harmonizirala predpise s področja elektronskega podpisovanja s pravnim redom Evropske unije, v skladu z interno politiko HALCOM-CA, sicer pa so smiselno v skladu z interno politiko HALCOM-CA. V kolikor so sprejeti Pogoji za podrejene overitelje, ravnajo overitelji tudi v skladu z določbami teh pogojev.

### **3.4.1 Varnostne zahteve in zanesljivost**

(1) Podrejeni overitelji izpolnjujejo nivo varnostnih zahtev, ki je določen z veljavnimi predpisi njihove države in drugimi pravili, navedenimi v tretjem odstavku točke 3.4. Če glavni overitelj sprejme Pogoje za podrejene overitelje iz drugega odstavka točke 3.4, so podrejeni overitelji dolžni ravnati tudi v skladu s temi pogoji.

(2) Nadzorna skupina iz HALCOM-CA redno pregleduje izpolnjevanje varnostnih zahtev in postopkov pri upravljanju s potrdili podrejenih overiteljev.

#### **3.4.2 Zahteve glede osebja**

(1) Osebje podrejenih overiteljev je strokovno usposobljeno za delo z infrastrukturo HALCOM-CA pri podrejenih overiteljih.

(2) Podrejeni overitelji izpolnjujejo nivo varnostnih zahtev, ki je določen v zgoraj navedenih virih pravil za podrejene overitelje (točka 3.4).

#### **3.4.3 Medsebojno priznavanje**

(1) Podrejeni overitelji priznavajo potrdila, ki jih je izdal glavni overitelj HALCOM-CA, kot svoja. Glavni overitelj praviloma ne priznava potrdil podrejenih overiteljev kot svoja.

(2) Glavni overitelj lahko prizna potrdila posameznega podrejenega overitelja kot svoja. V tem primeru obvestilo objavi na način iz petega odstavka točke 3.5. Enako ravna podrejeni overitelj, če prizna potrdila drugega podrejenega overitelja, ki jih ni priznal glavni overitelj.

#### **3.4.4 Odgovornost**

(1) Podrejeni overitelji prevzemajo popolno odgovornost za identificiranje vlagateljev zahtevkov, za pridobitev dokumentov, potrebnih za pridobitev posameznega potrdila in za preverjanje pristnosti teh dokumentov ter za izdajanje in upravljanje izdanih potrdil v skladu s svojimi notranjimi pravili in določbami te politike.

(2) Podrejeni overitelj je samostojno odgovoren za svoje delovanje in upoštevanje vseh pravil, ki urejajo delovanje infrastrukture mreže overiteljev HALCOM-CA in podrejenih overiteljev.

(3) Podrejeni overitelji jamčijo za potrdila glavnega overitelja kot za svoja. Glavni overitelj jamči za potrdila podrejenih potrdil samo, če jih prizna kot svoja. Glavni overitelj pa v nobenem primeru ne odgovarja za druge vidike delovanja posameznih podrejenih overiteljev, prav tako tudi ne podrejeni overitelji med seboj.

### **3.5 MEDSEBOJNO PRIZNAVANJE Z DRUGIMI OVERITELJI ALI MREŽAMI OVERITELJEV**

(1) Glavni overitelj se lahko ob soglasju večine podrejenih overiteljev povezuje in priznava z domačimi in tujimi overitelji ali mrežami overiteljev, vendar ni dolžan priznati drugih overiteljev tudi, če ima drugi overitelj status akreditiranega overitelja.

(2) Medsebojno priznavanje se izvaja na osnovi pisne dvostranske pogodbe. V kolikor posamezna pogodba o medsebojnem priznavanju ne vsebuje vseh potrebnih določb, veljajo namesto njih smiselno določbe nacionalne zakonodaje, te politike ter notranje politike HALCOM-CA, v kolikor pa to ni ustrezno, pogodba ni veljavna. Glavni overitelj zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu medsebojne pogodbe o priznavanju.

(3) Drugi overitelji oziroma mreže overiteljev morajo vsebovati vsaj minimalni nivo varnostnih zahtev, ki veljajo za podrejene overitelje v mreži overiteljev HALCOM-CA.

(4) HALCOM-CA kot glavni overitelj lahko sprejme in javno objavi Pogoje za medsebojno priznavanje overiteljev z mrežo overiteljev HALCOM-CA, ki natančneje določajo pogoje in način medsebojnega priznavanja drugih overiteljev ali mrež overiteljev.

(5) Bistvene dele pogodb o medsebojnem priznavanju, ki se nanašajo na lastnosti potrdil enega ali obeh overiteljev ali na pravice in obveznosti imetnikov potrdil ali tretjih oseb, objavijo glavni overitelj HALCOM-CA in podrejeni overitelji na svoji spletnih straneh.

(6) Podrejeni overitelji v mreži overiteljev HALCOM-CA, ki niso dali soglasja za medsebojno priznavanje z drugim overiteljem, lahko določijo, da za njih oziroma za aplikacije pod njihovo kontrolo medsebojno priznanje ne velja. Obvestilo o takšni izjemi objavijo glavni overitelj HALCOM-CA in podrejeni overitelji na svoji spletnih straneh.

## **4. UPRAVLJANJE POTRDIL**

### **4.1 OSNOVNA PRAVILA ZA UPRAVLJANJE S POTRDILI**

(1) Izdajanje in osnovne lastnosti potrdila:

- izdaja se na osnovi podpisanega obrazca s strani pooblaščenice osebe pravne osebe in bodočega imetnika potrdila;
- v primeru strežniških potrdil se za imetnika potrdila smatra systemskega skrbnika pravne osebe;
- HALCOM-CA je odgovoren samo za upravljanje z izdanimi potrdili ter za hranjenje in objavljanje potrdil v javno dostopnem imeniku po protokolu LDAP;
- HALCOM-CA ne odgovarja za dogodke, do katerih bi prišlo zaradi napačne uporabe potrdil, kot npr.:
  - o uporabe potrdil za namene, ki niso predvideni v tej politiki,
  - o nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev, izdajanje zaupnih podatkov ali ključev tretjim osebam,
  - o kakršnekoli zlorabe oz. vdora v informacijsko-komunikacijski sistem imetnika potrdila in s tem do podatkov s strani tretje osebe,
  - o nedelovanja ali slabega delovanja informacijsko-komunikacijske infrastrukture imetnika potrdila ali tretjih oseb,
  - o nepreverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
  - o zaradi uporabe potrdil na nestandardni način ali na nelicenčni programski opremi;
- HALCOM-CA ni odgovoren za vsebino podatkov, ki se šifrirajo ali podpisujejo z njegovimi potrdili ali za obnašanje imetnikov pri uporabi le-teh;
- infrastruktura HALCOM-CA ustreza najvišjim stopnjam varovanja in zaščite potrdil in ključev; veljavnost izdanih potrdil je zagotovljena le, če imetnik upošteva in deluje v skladu s priporočili in standardi, ki jih predlaga HALCOM-CA.

(2) Vsak imetnik potrdila ima par ključev za digitalno podpisovanje oziroma šifriranje:

- zasebni ključ za podpisovanje (v nadaljevanju ključ za podpisovanje) ter
- javni ključ za overjanje podpisa (v nadaljevanju ključ za overjanje podpisa).

(3) Ključ za podpisovanje ima samo imetnik.

(4) Javno dostopni podatki iz potrdila so:

- različica,
- enolična serijska številka,
- identiteta HALCOM-CA,
- rok veljavnosti potrdila,
- identiteta imetnika potrdila in njegove pravne osebe,

- davčna številka pravne osebe,
- davčna številka imetnika potrdila (ne velja za strežniška potrdila),
- javni ključ imetnika,
- številka politike, pod katero je bilo izdano potrdilo (CPOID),
- drugi podatki, za katere tako določi ta politika ali veljaven predpis.

(5) Strežniška potrdila poleg podatkov iz točke (4) vsebujejo tudi:

- ime strežnika in domena strežnika
- administratorski elektronski naslov strežnika
- navedba, da gre za strežniško potrdilo (OU = server certificates)

(6) V primeru, da podatki iz šeste, sedme ali desete alineje četrtega odstavka te točke politike imetniku potrdila ali pravni osebi v skladu z veljavnimi predpisi niso dodeljeni, se teh podatkov v potrdilo ne vključi.

(7) Vsak imetnik poslovnega potrdila ima lahko pod istimi naštetimi podatki le eno samo potrdilo. Imetnik strežniških potrdil ima lahko pod istimi naštetimi podatki več potrdil.

(8) HALCOM-CA pridobljene osebne podatke hrani trajno.

(9) HALCOM-CA ne posreduje osebnih podatkov o imetnikih potrdil, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih funkcij oz. aplikacij, povezanih z potrdili ter je to odobril imetnik potrdila, ali na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa.

## **4.2 IZDAJA POTRDILA**

### **4.2.1 Naročilnica za izdajo potrdila**

(1) Poslovno ali strežniško potrdilo se izda na osnovi pravilno izpolnjene in podpisane naročilnice za potrdilo (v nadaljevanju naročilnice) s strani pravne osebe in bodočega imetnika. Naročilnice so dostopne pri HALCOM-CA ter na spletni strani HALCOM-CA. Zakoniti zastopnik pravne osebe lahko, če že ima veljavno digitalno potrdilo izdano s strani overitelja HALCOM-CA, digitalno podpisano vlogo za generiranje strežniškega potrdila odda tudi preko spleta ([www.halcom-ca.si](http://www.halcom-ca.si)).

(2) Pred izdajo naročilnice HALCOM-CA pravno osebo in bodočega imetnika natančno seznanj s to politiko in obvestilom o elektronskem podpisovanju in delovanju overitelja HALCOM-CA.

(3) Ob sprejemu naročilnice prijavna služba HALCOM-CA s pomočjo uradno potrjene dokumentacije ali podatkov iz uradnih evidenc preveri istovetnost pravne osebe in s pomočjo uradnega dokumenta s sliko istovetnost pooblaščenega osebe pravne osebe, ki je podpisala naročilnico.

(4) Prijavne službe preverijo izpolnjene vloge in sprejemajo originalno dokumentacijo ter jo na varen način posredujejo na HALCOM-CA.

### **4.2.2 Izdaja poslovnega potrdila**

(1) Proizvodni postopek za potrdila in za par ključev na napravi za varno tvorjenje podpisa je sestavljen iz petih, jasno ločenih delov (ali funkcij), z njihovimi ustreznimi ločenimi podsistemi:

1. predpoosebljanje (generiranje in shranjevanje ključev, generiranje in shranjevanje kodiranega osebnega gesla (PIN kode));

2. priprava potrdila;
3. poosebljanje (izdaja in zapis potrdila, tiskanje imetnikovih podatkov);
4. izpis osebnega gesla (PIN kode);
5. posredovanje potrdila in osebnega gesla (PIN kode) ter obvestila imetniku.

(2) Opisani postopek je zasnovan tako, da ga ne more opraviti posamezna oseba sama.

(3) HALCOM-CA posreduje imetniku potrdilo na napravi za varno tvorjenje podpisa in osebno geslo (PIN kodo) ločeno.

(4) Imetnik potrdila mora ob prevzemu potrdila na napravi za varno tvorjenje podpisa nemudoma preveriti podatke v potrdilu in ob morebitnih napakah ali težavah takoj obvestiti HALCOM-CA.

#### **4.2.3 Izdaja in prevzem strežniškega potrdila**

(1) HALCOM-CA na podlagi vloge za strežniško potrdilo pri pooblaščenem registrarju domen preveri lastništvo domene, katero je pooblaščen osebna pravne osebe navedla na zahtevku in za katero pravni osebi izdaja potrdilo.

(2) HALCOM-CA po uspešni avtorizaciji s strani pooblaščenega registrarja domen za vsako vlogo za izdajo potrdila pripravi potrdilo.

(3) HALCOM-CA posreduje pooblaščen osebni pravne osebe referenčno številko naročila ter geslo za prevzem potrdila po dveh ločenih poteh. Z geslom in referenčno številko pravna oseba prevzame digitalno potrdilo na spletnih straneh overitelja ali preko varovane elektronske pošte.

(4) Pooblaščen osebna pravne osebe mora ob prevzemu potrdila nemudoma preveriti podatke v potrdilu in ob morebitnih napakah ali težavah takoj obvestiti HALCOM-CA.

#### **4.3 OBDOBJE VELJAVNOSTI POTRDILA IN PODPISA**

(1) Običajna veljavnost poslovnega potrdila je tri (3) leta od izdaje potrdila.

(2) Običajna veljavnost strežniškega potrdila je pet (5) let od izdaje potrdila.

(3) HALCOM-CA lahko za posamezno potrdilo določi tudi krajši rok veljavnosti potrdila.

(4) Veljavnost varnega elektronskega podpisa je 5 let od trenutka podpisa.

#### **4.4 PODALJŠANJE VELJAVNOSTI POTRDILA**

(1) Podaljševanje veljavnosti potrdila je mogoče samo za poslovna potrdila, na prošnjo imetnika.

(2) Po preteku veljavnosti potrdila mora imetnik po enkratnem (1x) podaljšanju ponovno zaprositi za izdajo potrdila.

(3) Imetnik potrdila lahko pred iztekom veljavnosti potrdila po elektronski poti zaprosi za izdajo novega digitalnega potrdila, ki ga podpiše s še veljavnim potrdilom.

## **4.5 PREKLIC POTRDILA IN OBJAVA V REGISTRU PREKLICANIH POTRDIL**

(1) Preklic potrdila lahko imetnik potrdila zahteva kadarkoli, mora pa ga zahtevati v primeru:

1. spremembe razločevalnega imena (DN),
2. ko imetnik potrdila zamenja ključne podatke, povezane s potrdilom (ime ali priimek, elektronski naslov, zaposlitev in podobno),
3. ko se ugotovi ali sumi, da je prišlo bodisi do razkritja ključa za podpisovanje bodisi do zlorabe potrdila,
4. nadomestitve potrdila z drugim potrdilom, (npr. ob izgubi pametne kartice, izgubi gesel za dostop do podatkov na kartici in podobno),
5. prenehanja lastništva domene, za katero je izdano strežniško potrdilo.

(2) HALCOM-CA lahko prekliče potrdilo tudi brez zahteve imetnika v primerih iz prvega odstavka ali na podlagi zahteve pristojnega sodišča ali upravnega organa.

(3) Preklic potrdila je mogoč 24 ur dnevno. Točna navodila za preklic potrdila HALCOM-CA javno objavi.

(4) HALCOM-CA bo na podlagi pravilne zahteve za preklic potrdila potrdilo preklical najkasneje v štirih (4) urah. V primeru nastanka nepredvidljivih okoliščin bo HALCOM-CA izjemoma preklical potrdilo najkasneje v 8 (osmih) urah po prejemu pravilne zahteve za preklic potrdila. V tem času bo preklicano potrdilo v imeniku označeno kot preklicano in dodano v register preklicanih potrdil.

## **5. IMETNIKI POTRDIL**

### **5.1 VARNOSTNE ZAHTEVE**

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

1. skrbno prebrati to politiko pred podpisom naročilnice za potrdilo ter spremljati vsa obvestila HALCOM-CA in ravnati v skladu z njimi in to politiko,
2. spremljati razvoj tehnologije oziroma obvestila HALCOM-CA in ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
3. uporabljati programsko opremo, ki je v skladu z obvestili HALCOM-CA,
4. vse spremembe, ki so povezane s časovnim žigom, nemudoma sporočiti HALCOM-CA,

(2) Imetnik potrdila mora izpolnjevati vse zahteve iz te politike in veljavnih predpisov.

(3) Imetnik potrdila se zavezuje, da bo uporabljal svoj par ključev le v obdobju veljavnosti svojega potrdila.

### **5.2 PRAVICE IMETNIKA POTRDILA**

(1) Imetnik potrdila lahko kadarkoli zahteva vse informacije glede veljavnosti potrdila, glede določb te politike ter glede obvestil HALCOM-CA.

(2) Imetnik lahko kadarkoli zahteva preklic svojega potrdila.

## **6. PRAVNE OSEBE**

### **6.1 VARNOSTNE ZAHTEVE**

(1) Pravna oseba se zavezuje, da bodo imetniki znotraj nje izpolnjevali vse določbe te politike in veljavnih predpisov.

(2) Pravna oseba je dolžna:

1. zagotoviti, da imetniki skrbno preberejo to politiko pred podpisom naročilnice za potrdilo ter spremljajo vsa obvestila HALCOM-CA in ravnati v skladu z njimi in to politiko,
2. zagotoviti nesporno ugotavljanje istovetnosti imetnikov potrdil znotraj nje v skladu z veljavnimi predpisi (uradni dokument s sliko),
3. spremljati razvoj tehnologije oziroma obvestila HALCOM-CA in ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili ter uporabljati tako programsko opremo, ki je v skladu z obvestili HALCOM-CA,
4. vse spremembe, ki so povezane s potrdilom kateregakoli imetnika znotraj nje, nemudoma sporočiti HALCOM-CA,
5. zahtevati preklic potrdila, če so se spremenili podatki, ki so navedeni v potrdilu.

(3) Stroške potrebne strojne ali programske opreme, ki jo predlaga HALCOM-CA za varno shranjevanje in uporabo potrebnih podatkov za potrdilo na strani imetnika potrdila, krije pravna oseba.

### **6.2 PRAVICE PRAVNE OSEBE**

(1) Pravna oseba lahko kadarkoli zahteva vse informacije glede veljavnosti potrdila, glede določb te politike ter glede obvestil HALCOM-CA.

(2) Pravna oseba ima enake pravice kot imetnik poslovnega potrdila znotraj nje, vključno s pravico zahtevati preklic potrdila, razen pravic do ključa za podpisovanje in drugih pravic, za katere tako določajo veljavni predpisi. Če imetnik poslovnega potrdila in pravna oseba izvršujeta pravice medsebojno nasprotujoče, prevladajo pravice pravne osebe.

(3) Pravna oseba ima enake pravice kot imetnik strežniškega potrdila znotraj nje, vključno s pravico zahtevati preklic potrdila. Če imetnik strežniškega potrdila in pravna oseba izvršujeta pravice medsebojno nasprotujoče, prevladajo pravice pravne osebe.

## **7. TRETJE OSEBE**

### **7.1 VARNOSTNE ZAHTEVE**

(1) Ob prvi uporabi potrdil HALCOM-CA po tej politiki mora tretja oseba, ki se zanaša na potrdilo, skrbno prebrati to politiko in od tedaj redno spremljati vsa obvestila HALCOM-CA.

(2) Tretja oseba mora vedno v času uporabe potrdila natančno preveriti, če potrdilo ni v registru preklicanih potrdil.

(3) Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

## **7.2 PRAVICE TRETJE OSEBE**

(1) Tretja oseba se lahko do preklica potrdila zanese na takšno potrdilo.

(2) Tretja oseba lahko kadarkoli zahteva vse informacije glede veljavnosti kateregakoli izdanega potrdila, glede določb te politike ter glede obvestil HALCOM-CA.

## **8. KONČNE IN PREHODNE DOLOČBE**

### **8.1 SPLOŠNO**

(1) Določbe glede avtorskih, sorodnih in drugih pravic:

- na ključu za podpisovanje pripadajo vse pravice imetniku potrdila;
- na potrdilu in drugih ključih ter vseh ostalih podatkih vse pravice pripadajo HALCOM-CA.

### **8.2 REŠEVANJE SPOROV**

(1) Vse pritožbe imetnikov potrdil rešuje nadzorna skupina HALCOM-CA (podpoglavje 3.2.3).

(2) Morebitne spore med imetnikom potrdila ali tretjo osebo in HALCOM-CA rešuje stvarno pristojno sodišče v Ljubljani ob uporabi materialnega prava Republike Slovenije.

### **8.3 VELJAVNOST**

(1) HALCOM-CA si pridržuje pravico do spremembe politike delovanja in nadgradnje infrastrukture brez predhodnega obveščanja imetnikov potrdil. Veljavna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti in po stari politiki delovanja. Vsa potrdila izdana po začetku veljavnosti nove politike se obravnavajo po novi politiki delovanja.

(2) Ta politika začne veljati z dnem, ko jo sprejme HALCOM-CA.

## TERMINOLOŠKI SLOVAR IN KRATICE

<b>CA</b>	Overitelj potrdil. <i>Angl.: Certification Authority ali Certification Agency</i>
<b>CCPS</b>	Certificate and Card Production Service – storitev izdelave potrdil in kartic in zajema: <ol style="list-style-type: none"> <li>1. Izdajo CA ključa za vsakega podrejenega overitelja</li> <li>2. Postavitev CA parametrov v CCPS za vsakega podrejenega overitelja</li> <li>3. Predpoosebljanje pametnih kartic, v skladu z nizom standardiziranih izdelkov</li> <li>4. Izdelavo visoko kakovostnih ključev RSA z najmanj 1024 biti</li> <li>5. Varovanje integritete predpoosebljenih inteligentnih kartic s transportnim PIN-om</li> <li>6. Dobavo predpoosebljenih pametnih kartic za podrejene overitelje z LCM</li> <li>7. Poosebljanje kartic končne entitete s povezovanjem podatkov imetnika in javnega ključa, torej izdajo potrdil x509 v3 in njihovo nalaganje v pametne kartice</li> <li>8. Dobavo kartic končne entitete podrejenim overiteljem, ki nimajo LCM</li> </ol>
<b>CPName</b>	Ime politike delovanja overitelja ( <i>Angl.: Certification Policy Name</i> ), enolično povezano z mednarodno številko politike delovanja CPOID ( <i>Angl.: Certification Policy Object Identifier</i> )
<b>CPOID</b>	Mednarodna številka, ki enolično določa politiko delovanja ( <i>Angl.: Certification Policy Object Identifier</i> ).
<b>CRL</b>	Certificate Revocation List – seznam preklicanih digitalnih potrdil
<b>DN</b>	Enolično razločevalno ime (prim. definicijo Razločevalno ime). <i>Angl.: Distinguished Name</i>
<b>Imenik potrdil</b>	Imenik potrdil po priporočilu X.500, kjer so shranjena potrdila po priporočilu X.509 ver. 3, do katerih je možen dostop po protokolu LDAP
<b>SSCD</b>	Secure Signature Creation Device - naprava za varno tvorjenje podpisa
<b>LDAP</b>	Leightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu RFC 1777
<b>Nedvoumna identifikacija</b>	Preverjanje istovetnosti je osebno preverjanje istovetnosti osebe s pomočjo veljavnega osebnega dokumenta ali elektronsko dokazovanje istovetnosti z veljavnim potrdilom overjenim s strani HALCOM-CA ali s strani HALCOM-CA priznanih overiteljev.
<b>Overitelj potrdila</b>	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. <i>Angl.: Certification service provider (CSP) v Evropski uniji oziroma Certification Authority (CA) v Združenih državah Amerike.</i>
<b>Potrdilo</b>	Kvalificirano potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo ter potrjuje njeno identiteto. <i>Angl.: Certificate</i>
<b>Prijavna služba</b>	Služba ali oseba, ki sprejema vloge za potrdila in prevzema identificiranje in preverjanje istovetnosti bodočih imetnikov v imenu overitelja potrdil. <i>Angl.: Registration Authority (RA).</i>
<b>Razločevalno ime</b>	Enolično ime (prim. definicijo DN) v potrdilu, ki nedvoumno in enolično definira uporabnika v strukturi imenika.  Primer za osebo, zaposleno v Halcom informatika d.o.o.: <i>cn=ime priimek%serijska številka, ou=Support, o=Halcom, c=SI</i>
<b>S/MIME</b>	Secure Multipurpose Internet Mail Extensions

<b>SSL</b>	Secure Sockets Layer
<b>TLS</b>	Transport Layer Security

Kraj in datum: Ljubljana, 05.03.2007

Direktor  
Matjaž Čadež