

# Politika HALCOM-CA

Javni del notranjih pravil HALCOM-CA

za kvalificirana digitalna potrdila

za fizične osebe

CPName: HALCOM CA FO

Mobilno kvalificirano digitalno potrdilo z obvezno uporabo  
varnega nosilca

CPOID:1.3.6.1.4.1.5939.1.6.1

Dokument je veljaven od: 04.12.2006

## Kazalo

|   |    |
|---|----|
| 1. UVOD.....  | 3  |
| 2. SPLOŠNE DOLOČBE .....  | 3  |
| 2.1 NAMEN IN UPORABA POTRDIL .....  | 3  |
| 2.1.1 Kvalificirana digitalna potrdila z dvema paroma ključev in z obvezno uporabo<br>varnega nosilca (mobilno kvalificirano digitalno potrdilo)..... | 4  |
| 2.2 STROŠKI.....  | 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 .....  | 6  |
| 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 Osebje .....  | 7  |
| 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 Lastno potrdilo podrejenega overitelja.....   | 9  |
| 3.4.2 Varnostne zahteve in zanesljivost .....   | 9  |
| 3.4.3 Zahteve glede osebja .....  | 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 OSNOVNE LASTNOSTI POTRDIL .....   | 11 |
| 4.3 VLOGA ZA IZDAJO POTRDILA .....  | 11 |
| 4.4 IZDAJA POTRDILA .....   | 12 |
| 4.4.1 Mobilno kvalificirano digitalno potrdilo .....  | 12 |
| 4.5 PREVZEM POTRDILA .....  | 12 |
| 4.5.1 Mobilno kvalificirano digitalno potrdilo .....  | 12 |
| 4.6 OBDOBJE VELJAVNOSTI POTRDILA.....   | 12 |
| 4.7 PREKLIC POTRDILA IN OBJAVA V REGISTRU PREKLICANIH POTRDIL .....   | 13 |
| 5. IMETNIKI POTRDIL .....   | 13 |
| 5.1 VARNOSTNE ZAHTEVE .....   | 13 |
| 5.2 PRAVICE IMETNIKA POTRDILA .....   | 14 |
| 6. TRETJE OSEBE .....   | 14 |
| 6.1 VARNOSTNE ZAHTEVE .....   | 14 |
| 6.2 PRAVICE TRETJE OSEBE.....   | 14 |
| 7. OPERATER .....   | 15 |
| 7.1. VARNOSTNE ZAHTEVE .....  | 15 |
| 7.2 PRAVICE OPERATERJA .....  | 15 |
| 8. PREHODNE IN KONČNE 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 digitalnih potrdil, ureja namen, delovanje in metodologijo upravljanja kvalificiranih digitalnih potrdil ter varnostne zahteve, ki jih morajo izpolnjevati overitelji HALCOM-CA, imetniki potrdil, tretje osebe in operaterji, ki se zanašajo na ta potrdila, ter odgovornost vseh naštetih oseb.

(2) HALCOM-CA je overitelj, ki izdaja in upravlja s kvalificiranimi digitalnimi potrdili za overjanje 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 potrdil in opravljanju tehnoloških storitev v zvezi z varnimi elektronskimi podpisi. Overitelj HALCOM-CA deluje v okviru Halcom, d.d., Ljubljana.

(3) HALCOM-CA izdaja kvalificirana digitalna potrdila z dvema paroma ključev in z obvezno uporabo varnega nosilca (mobilno kvalificirano digitalno potrdilo) za fizične osebe.

(4) Vse določbe te politike glede ravnanja HALCOM-CA so ustrezno prenesene in podrobneje opredeljene v določbah notranjega dela politike, ki predstavlja zaupni del notranjih pravil in ga sestavljajo dokumenti zaupne narave, ki opredeljujejo 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,...).

(5) HALCOM-CA izdaja potrdila in opravlja druge dejavnosti overitelja v skladu z veljavnim pravnim redom Republike Slovenije, v skladu z nacionalnimi predpisi s področja elektronskega poslovanja in elektronskega podpisa, v skladu z direktivo Evropskega parlamenta in Sveta Evropske unije z dne 13. decembra 1999 o skupnem okviru Skupnosti za elektronske podpise ter v skladu s tehničnimi zahtevami ETSI TS 101 456 (*Policy requirements for certification authorities issuing qualified certificates*) in veljavnimi aneksi in ETSI TS 101 862 (*Qualified certificate profile*), standardom RFC 3647 (*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*) in standardom ISO/IEC 17799, BS 7799-1 (*Code of practice for information security management*).

(6) Seznam operaterjev, ki omogočajo pridobitev mobilnega kvalificiranega digitalnega potrdila, HALCOM-CA objavi na svetovnem spletu.

## 2. SPLOŠNE DOLOČBE

### 2.1 NAMEN IN UPORABA POTRDIL

(1) HALCOM-CA upravlja (izdaja in overja, preklicuje, podaljšuje, hrani, objavlja) s kvalificiranimi digitalnimi potrdili za overjanje elektronskega podpisa (v nadaljevanju potrdila), ki so namenjena fizičnim osebam (v nadaljevanju imetniki potrdil).

(2) 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 potrdila uporabljajo v namenih kot so npr.:

- 1) identifikacija imetnika
- 2) izkazovanje istovetnosti imetnika
- 3) podpisovanje dokumentov v elektronski obliki
- 4) šifriranje in dešifriranje dokumentov v elektronski obliki.

Elektronski podpis se lahko uporablja v aplikacijah kot so npr.:

- 1) elektronsko oz. mobilno bančništvo
- 2) aplikacije e-uprave ali m-uprave
- 3) podpisovanje elektronskih ali mobilnih obrazcev
- 4) varno poslovanje z organi in organizacijami javnega sektorja ter z drugimi pravnimi ali fizičnimi osebami
- 5) druge aplikacije oziroma storitve, v katerih se zahteva uporaba kvalificiranega digitalnega potrdila.

### **2.1.1 Kvalificirana digitalna potrdila z dvema paroma ključev in z obvezno uporabo varnega nosilca (mobilno kvalificirano digitalno potrdilo)**

Mobilna kvalificirana digitalna potrdila z dvema paroma ključev in z obvezno uporabo varnega nosilca se lahko uporabljajo za varen elektronski podpis, za šifriranje in kontrolo dostopa.

## **2.2 STROŠKI**

HALCOM-CA določi cenik uporabe potrdil, svojih storitev, potrebne opreme in infrastrukture 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-ca.si/>**

## Identiteta

HALCOM-CA predstavljajo naslednji podatki:

C=SI, O=Halcom, CN=Halcom CA FO

CPName HALCOM CA FO

Kvalificirana digitalna potrdila pod točko 2.1.1 se izdajajo pod oznako Mobilno kvalificirano digitalno potrdilo

CPOID: 1.3.6.1.4.1.5939.1.6.1

(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 potrdilo (potrdilo HALCOM CA FO), serijska številka 113253 (01 ba 65), ki je namenjeno podpisovanju potrdil drugih imetnikov, podpisovanju registra preklicanih potrdil ter preverjanju podpisa oz. veljavnosti overitelja.

(2) Potrdilo HALCOM CA FO vsebuje naslednje podatke:

|                     |   |
|---------------------|---|
| Serijska številka   | 113253 (01 ba 65)   |
| Overitelj potrdila  | HALCOM CA FO, Halcom, SI                                    |
| Imetnik potrdila    | HALCOM CA FO, Halcom, SI                                    |
| Veljavnost potrdila | 5.6.2005 – 5.6.2020   |
| Dolžina ključa      | 2048 bitov  |
| SHA-1               | 04 09 56 5b 77 da 58 2e 64 95 ac 00 60 a7 23 54 e6 4b 01 92 |

### 3.1.3 Šifrirni algoritmi, formati podatkov in protokoli

(1) HALCOM-CA uporablja:

- za podpisovanje potrdil algoritem RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme Triple DES (3 DES) in Advanced Encryption Standard (AES),
- algoritem SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in zgoščevalne funkcije iz družine SHA-2 (FIPS PUB 180-2),
- format potrdil ustreza priporočilu ITU-T za X.509 in ISO/IEC 9594-8 ter X.509 ver. 3 (v3),
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 in ISO/IEC 9594-8,
- 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 FO

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 ter čas in 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 standardoma ISO/IEC 17799, BS 7799-1 (*Code of practice for information security management*) in s FIPS 140-1 level 3 ter s 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 osebo, 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:** upravljavec 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. Postavitev 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
2. Varna distribucija potrdil imetnikom
3. Priprava zahtev za preklic potrdil

**Organizacijska skupina:** Upravljanje s potrdili

**Vloga:** administrator PIN kod

**Število oseb:** 2

**Naloge:**

← Formatted: Bullets and Numbering

## 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 nezdržljivo.

### 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 vsebino podatkov, 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 fizične ali 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 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 ravnaajo v skladu z nacionalnimi predpisi in s to politiko ter s svojo interno politiko, čigar določbe so v primeru, da gre za državo članico, 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, ravnaajo overitelji tudi v skladu z določbami teh pogojev.

#### **3.4.1 Lastno potrdilo podrejenega overitelja**

V javnem delu notranjih pravil podrejenega overitelja je med drugim navedena država overitelja.

#### **3.4.2 Varnostne zahteve in zanesljivost**

(1) Podrejeni overitelji izpolnjujejo nivo varnostnih zahtev, ki je določen v zgoraj navedenih virih pravil za podrejene overitelje (točka 3.4, 3. odstavek).

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

#### **3.4.3 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 (3. odstavek točke 3.4).

#### **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 dobavo ustreznih potrdil in dogovorjenih nosilcev podatkov.

(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) Glavni overitelj ne odgovarja za delovanje posameznih podrejenih overiteljev, prav tako tudi ne podrejeni overitelji med seboj.

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

(1) Overitelj HALCOM-CA se lahko povezuje z drugimi overitelji. HALCOM-CA se lahko kot glavni overitelj 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. HALCOM-CA 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, objavi glavni overitelj HALCOM-CA.

(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.

## **4. UPRAVLJANJE POTRDIL**

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

(1) Na podlagi te politike HALCOM-CA izdaja mobilna kvalificirana digitalna potrdila fizičnim osebam na varni nosilec, ki ga priskrbi mobilni operater, in opravlja druge storitve, povezane z izdajo in upravljanjem z digitalnimi potrdili.

(2) Potrdilo se izdaja na osnovi odobrenega zahtevka za izdajo potrdila.

(3) 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.

(4) Odgovornost overitelja:

- 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 ravnanje imetnikov pri uporabi le-teh.

(5) HALCOM-CA poleg podatkov, ki so vključeni v potrdilo, hrani ostale potrebne podatke o imetniku za namen elektronskega poslovanja v skladu z veljavnimi predpisi.

(6) HALCOM-CA pridobljene osebne podatke hrani pet let po prenehanju veljavnosti potrdila oziroma po preklicu potrdila.

(7) 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 in je to odobril imetnik potrdila. Osebni podatki o imetnikih potrdil se lahko posredujejo tudi na podlagi zahteve pristojnega sodišča, prekrškovnega ali upravnega organa ter na podlagi drugega obvezujočega pravnega akta.

(8) HALCOM-CA na svojih spletnih straneh objavi navodila za uporabo digitalnih kvalificiranih potrdil, ki so izdana na podlagi te politike, ter skrbi za ažurnost in pravilnost objavljenih navodil.

#### **4.2 OSNOVNE LASTNOSTI POTRDIL**

(1) Vsak imetnik potrdila ima dva para ključev za digitalno podpisovanje oziroma šifriranje:

- zasebni ključ za podpisovanje (v nadaljevanju ključ za podpisovanje);
- zasebni ključ za potrjevanje identitete (v nadaljevanju ključ za potrjevanje identitete);
- javni ključ za overjanje podpisa (v nadaljevanju ključ za overjanje podpisa) in
- javni ključ za preverjanje identitete (v nadaljevanju ključ za preverjanje identitete).

(2) Ključ za podpisovanje ima samo imetnik.

(3) Vsak imetnik potrdila ima lahko pod istimi naštetimi podatki le eno samo potrdilo.

(4) V potrdilu so navedeni podatki o imetniku in izdajatelju. Javno dostopni podatki iz potrdila so:

- različica standarda x.509,
- enolična serijska številka potrdila,
- rok veljavnosti potrdila,
- identiteta imetnika potrdila (ime, priimek, država in neobvezno elektronski naslov),
- identifikacijska številka imetnika potrdila (za davčne zavezance je obvezna osebna davčna številka),
- javni ključ potrdila,
- številka politike, pod katero je bilo izdano potrdilo (CPOID),
- drugi podatki, za katere tako določi ta politika ali veljaven predpis.

#### **4.3 VLOGA ZA IZDAJO POTRDILA**

(1) Bodoči imetnik poda vlogo za izdajo potrdila tako, da izpolni in lastnoročno podpiše zahtevek za izdajo digitalnega potrdila, vlogo odda prijavnih službi HALCOM-CA ter poravnava finančne obveznosti v zvezi z izdajo potrdila. Obrazci za zahtevek za izdajo digitalnega potrdila so na voljo pri prijavnih službah HALCOM-CA in na spletni strani HALCOM-CA. Cenik storitev je javno objavljen na spletnih straneh HALCOM-CA.

(2) Bodoči imetnik poda vlogo v pisni obliki.

(3) Pred izdajo naročilnice HALCOM-CA bodočega imetnika seznanjeni s to politiko in obvestilom o elektronskem podpisovanju in delovanju overitelja HALCOM-CA.

(4) Ob sprejemu vloge pooblaščen osebna v prijavnih službah HALCOM-CA ugotovi identiteto bodočega imetnika potrdila s pomočjo njegovega osebnega dokumenta ob njegovi fizični prisotnosti.

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

(6) HALCOM-CA si pridružuje pravico do zavrnitve vloge za izdajo potrdila brez obrazložitve.

#### **4.4 IZDAJA POTRDILA**

##### **4.4.1 Mobilno kvalificirano digitalno potrdilo**

(1) Pri izdaji potrdila sodeluje tudi mobilni operater, ki preskrbi varen nosilec.

(2) Operater mora omogočiti HALCOM-CA pridobitev podatkov, ki so potrebni za preverjanje kompletnosti podatkov elektronskega podpisovanja in podatkov za preverjanje elektronskega podpisa.

(3) Proizvodni postopek za potrdila in za oba para ključev na pametnih karticah je sestavljen iz jasno ločenih delov (ali funkcij), z njihovimi ustrezno ločenimi podsistemi:

1. obravnava vloge za izdajo potrdila,
2. tiskanje enkratnega gesla za prevzem potrdila,
3. posredovanje enkratnega gesla za prevzem potrdila imetnikom,
4. predpoosebljanje varnega nosilca na uporabnikovem mobilnem telefonu (generiranje ključev na kartici, izbira gesla za zaščito potrdila),
5. priprava elektronskega zahtevka za prevzem potrdil na uporabnikovem mobilnem telefonu (angl. »*certificate request*«),
6. posredovanje elektronskega zahtevka za prevzem potrdil do overitelja,
7. priprava potrdil,
8. posredovanje obvestila o zaključenem postopku imetniku.

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

#### **4.5 PREVZEM POTRDILA**

##### **4.5.1 Mobilno kvalificirano digitalno potrdilo**

Enkratno geslo za prevzem mobilnega kvalificiranega digitalnega potrdila izda operater in ga ločeno posreduje imetniku potrdila na naslov, ki je naveden na vlogi za pridobitev kvalificiranega digitalnega potrdila. Imetnik potrdila na telefonu sproži generacijo ključev. V telefon vnese enkratno geslo za prevzem potrdila in si izmisli geslo za zaščito privatnega ključa ter ga potrdi. Ključi se samogenerirajo na varnem nosilcu. Javni ključ se posreduje preko operaterja na HALCOM-CA, ki izda potrdilo. Po končanem postopku je uporabnik obveščen o uspehu namestitve.

#### **4.6 OBDOBJE VELJAVNOSTI POTRDILA**

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

(2) HALCOM-CA lahko v posebnih primerih za posamezno potrdilo določi tudi krajši rok veljavnosti potrdila.

#### **4.7 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)
3. ko se ugotovi ali sumi, da je prišlo bodisi do razkritja ključa za podpisovanje bodisi do zlorabe potrdila,
4. nadomestitvi potrdila z drugim potrdilom (npr. ob izgubi varnega nosilca, izgubi mobilnega telefona, izgubi gesel za dostop do podatkov na kartici in podobno).

(2) HALCOM-CA lahko prekliče potrdilo tudi brez zahteve imetnika v primerih iz prvega odstavka ali na podlagi zahteve pristojnega sodišča, prekrškovnih organov ali upravnega organa. Preklic potrdila je v skladu s sedmo točko te politike možen tudi na zahtevo operaterja.

(3) Preklic potrdila je mogoč 24 ur dnevno. Natančna navodila za preklic potrdila so objavljena na spletnih straneh HALCOM-CA in operaterja.

(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. Če bo imetnik potrdila HALCOM-CA posredoval nepravilno zahtevo za preklic potrdila, mu bo poslano opozorilo o nepravilni zahtevi za preklic potrdila in bo seznanjen z navodili za vložitev pravilne zahteve za preklic.

## **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 s to politiko,
2. spremljati razvoj tehnologije in obvestila HALCOM-CA ter ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
3. uporabljati tako programsko opremo, ki je v skladu z obvestili HALCOM-CA (npr. z dovolj močnimi kriptografskimi moduli),
4. uporabljati varni nosilec v namene, ki so v skladu s to politiko
5. varni nosilec ščititi s primernim geslom ali na drug način tako, da jo lahko uporablja samo imetnik,
6. vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti HALCOM-CA ali operaterju, ki je dolžan o tem obvestiti HALCOM-CA,
7. zahtevati preklic potrdila, če je bil ključ za podpisovanje ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

- (2) Imetnik potrdila mora izpolnjevati vse zahteve iz te politike in iz veljavnih predpisov.
- (3) Imetnik potrdila krije stroške potrebne strojne ali programske opreme za varno uporabo potrdila glede na vrsto potrdila. Stroške strojne ali programske opreme določi HALCOM-CA v soglasju z operaterjem in jih objavi v svojem ceniku.
- (4) Imetnik potrdila je odgovoren za varno in pravilno uporabo kvalificiranega digitalnega potrdila.
- (5) Imetnik dovoljuje operaterju in HALCOM-CA obdelavo, vključno z medsebojnim obveščanjem, vseh nanj nanašajočih se osebnih podatkov, ki so potrebni za upravljanje potrdil in s tem povezano izpolnjevanje veljavnih predpisov in te politike.
- (6) V primeru, da uporaba kvalificiranega digitalnega potrdila iz kakršnihkoli razlogov ni možna, razen iz razlogov za katere je odgovoren HALCOM-CA, imetnik kvalificiranega digitalnega potrdila ni upravičen do povračila nadomestila ali kakršnegakoli drugega zahtevka, kljub neuporabnosti kvalificiranega digitalnega potrdila pred pretekom roka 3 let (npr. kraja mobilnega telefona, izguba mobilnega telefona, prenehanje naročniškega razmerja...). HALCOM-CA imetniku v primeru izgube, kraje ali odtujitve varnega nosilca ali v drugih primerih, ko uporaba varnega nosilca ni več mogoča, imetniku omogoči izdajo potrdila na nov varni nosilec.

## **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 brez navedbe razloga zahteva preklic svojega potrdila.

## **6. TRETJE OSEBE**

### **6.1 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.

### **6.2 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.

## **7. OPERATER**

### **7.1. VARNOSTNE ZAHTEVE**

(1) Operater je dolžan:

1. Redno in vestno obveščati HALCOM-CA o tem, katero kvalificirano digitalno potrdilo je potrebno preklicati. To mora storiti v vsakem primeru, ko je ogrožena zanesljivost oblikovanja elektronskega podpisa (izguba mobilnega telefona, kraja mobilnega telefona, zamenjava SIM kartice, ipd.).
2. Uporabljati ustrezno programsko in strojno opremo, s katero se omogoči izpolnjevanje veljavnih predpisov ter izvajanje določb te politike. Med drugim mora operater spremljati razvoj tehnologije in obvestila HALCOM-CA ter ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
3. Skrbeti za ustrezno fizično in elektronsko varovanje programske in strojne opreme, tako da imajo do kritičnih strojnih in programskih komponent ter podatkovnih zbirk s podatki o imetnikih potrdil dostop le pooblaščen osebe po natančno določenih procedurah.

### **7.2 PRAVICE OPERATERJA**

(1) Operater lahko zahteva vse informacije glede preklicanih digitalnih potrdil, določb te politik in obvestil HALCOM-CA.

## **8. PREHODNE IN KONČNE DOLOČBE**

### **8.1 SPLOŠNO**

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

- na zasebnem ključu pripadajo vse pravice imetniku potrdila,
- na javnih ključih, vseh podatkih na potrdilu, na javnem imeniku potrdil in registru preklicanih potrdil ter na tej politiki pripadajo vse pravice 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 zanje še naprej velja tista politika delovanja, ki je veljala ob njihovi izdaji. Za vsa potrdila, izdana po začetku veljavnosti nove politike, velja nova politika.

(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</i> ali <i>Certification Agency</i> ).   |
| <b>CCPS</b>               | <i>Certificate and Card Production Service</i> – storitev izdelave potrdil in kartic in zajema:<br><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 pametnih kartic</li> <li>6. Poosebljanje kartic končne entitete s povezovanjem podatkov imetnika in javnega ključa, torej izdajo potrdil x509 v3 in njihovo nalaganje v pametne kartice</li> <li>7.</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>                | <i>Certificate Revocation List</i> – seznam preklicanih digitalnih potrdil.  |
| <b>DN</b>                 | Enolično razločevalno ime (prim. opredelitev razločevalnega imena) ( <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>LDAP</b>               | <i>Lightweight Directory Access Protocol</i> je protokol, ki določa dostop do imenika in je specificiran po IETF ( <i>Internet Engineering Task Force</i> ) priporočilu RFC 1777.  |
| <b>Identifikacija</b>     | Identifikacija je ugotavljanje identitete osebe, ki se izvaja osebno s pomočjo veljavnega osebnega dokumenta ali v elektronski obliki s pomočjo veljavnega digitalnega potrdila.   |
| <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 Authority - CA</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 v potrdilu (prim. opredelitev DN), ki nedvoumno in enolično definira uporabnika v strukturi imenika.  |
| <b>S/MIME</b>             | <i>Secure Multipurpose Internet Mail Extensions</i>  |
| <b>SSL</b>                | <i>Secure Sockets Layer</i>  |

|                      |   |
|----------------------|---|
| <b>TLS</b>           | <i>Transport Layer Security</i>   |
| <b>WPKI</b>          | <i>Wireless Public Key Infrastructure</i> je infrastruktura javnih ključev, ki deluje preko brezžičnih povezav (npr. GSM telefonov).  |
| <b>varni nosilec</b> | SIM (angl.: <i>Subscriber Identity Module</i> ) pametna kartica, ki ima vgrajen poseben pomnilnik za varno hranjenje zasebnih ključev ter matematični procesor za izvajanje operacij s temi ključi. Namenjena je varni uporabi in hranjenju ključev. Najpogostejša je uporaba WPKI (ang. <i>wireless public key infrastructure</i> ) SIM kartice. |

Kraj in datum: Ljubljana, 24.11.2006

Direktor  
Matjaž Čadež