

Politika HALCOM-CA

Javni del notranjih pravil HALCOM-CA

za storitve varnega časovnega žigosanja

CPName (RFC 3161, SHA-1): HALCOM CA TS RFC 1

CPName (RFC 3161, SHA-256): HALCOM CA TS RFC 2

CPName (DSS XML, SHA-1): HALCOM CA TS DSS 1

CPName (DSS XML, SHA-256): HALCOM CA TS DSS 2

Varno časovno žigosanje

CPOID (RFC 3161, SHA-1): 1.3.6.1.4.1.5939.3.1.1.1

CPOID (RFC 3161, SHA-256): 1.3.6.1.4.1.5939.3.1.2.1

CPOID (DSS XML, SHA-1): 1.3.6.1.4.1.5939.3.2.1.1

CPOID (DSS XML, SHA-256): 1.3.6.1.4.1.5939.3.2.2.1

Dokument je veljaven od: 15.08.2006

1 UVOD	3
2 SPLOŠNE DOLOČBE	3
2.1 NAMEN IN UPORABA VARNIH ČASOVNIH ŽIGOV	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
3.2 VARNOSTNE ZAHTEVE IN ZANESLJIVOST	6
3.2.1 Varnostne zahteve in zanesljivost	6
3.2.2 Nadzor	6
3.3 ODGOVORNOST	6
3.3.1 Odgovornost	6
3.3.2 Zavarovanje odgovornosti	7
4 DEJAVNOST IZDAJANJA VARNIH ČASOVNIH ŽIGOV	7
4.1 UPRAVLJANJE S KLJUČI ZA VARNO ČASOVNO ŽIGOSANJE	7
4.1.1 Generiranje ključev	7
4.1.2 Zasebni ključi overitelja	7
4.1.3 Dostopnost digitalnega potrdila overitelja	7
4.1.4 Veljavnost digitalnega potrdila	8
4.1.5 Podaljšanje veljavnosti digitalnega potrdila overitelja	8
4.1.6 Upravljanje kriptografskih modulov	8
4.2 VARNO ČASOVNO ŽIGOSANJE	8
4.2.1 Varni časovni žig	8
4.2.2 Sinhronizacija ure s časovnim virom	9
4.3 NAROČILNICA ZA VARNI ČASOVNI ŽIG	9
4.4 POSTOPEK IZDAJE VARNEGA ČASOVNEGA ŽIGA	10
5 UPORABNIKI VARNIH ČASOVNIH ŽIGOV	10
5.1 VARNOSTNE ZAHTEVE	10
5.2 PRAVICE UPORABNIKA VARNEGA ČASOVNEGA ŽIGA	10
6 TRETJE OSEBE	11
6.1 VARNOSTNE ZAHTEVE	11
6.2 PRAVICE TRETJE OSEBE	11
6.3 OBVEZNOSTI TRETJE OSEBE	11
8. KONČNE IN PREHODNE DOLOČBE	11
8.1 SPLOŠNO	11
8.2 REŠEVANJE SPOROV	11
8.3 VELJAVNOST	11
TERMINOLOŠKI SLOVAR IN KRATICE	12

1 UVOD

(1) Ta politika, ki predstavlja nedeljivo celoto javnega dela notranjih pravil overitelja HALCOM-CA glede izdaje varnih časovnih žigov, ureja namen, delovanje in metodologijo upravljanja varnih časovnih žigov ter varnostne zahteve, ki jih morajo izpolnjevati overitelji HALCOM-CA, uporabniki varnih časovnih žigov in tretje osebe, ki se zanašajo na te časovne žige, ter odgovornost vseh naštetih oseb.

(2) HALCOM-CA je overitelj, ki izdaja in upravlja s kvalificiranimi digitalnimi potrdili za overjanje elektronskega podpisa in izdaja ter upravlja z varnimi časovnimi žigi. HALCOM-CA deluje tudi kot glavni overitelj, ki skupaj s svojimi podrejenimi overitelji sestavlja hierarhično mrežo overiteljev, ki je namenjena izdajanju kvalificiranih digitalnih potrdil in varnih časovnih žigov ter opravljanju tehnoloških storitev v zvezi z varnimi elektronskimi podpisi in varnimi časovnimi žigi.

(3) HALCOM-CA izdaja kvalificirana digitalna potrdila in varne časovne žige 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*), ETSI TS 101 862 (*Qualified certificate profile*) in ETSI TS 101 023 (*Policy requirements for time-stamping authorities*).

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

2 SPLOŠNE DOLOČBE

2.1 NAMEN IN UPORABA VARNIH ČASOVNIH ŽIGOV

(1) HALCOM-CA izdaja in dodeljuje varne časovne žige, ki so namenjeni uporabi pri storitvah v povezavi s kvalificiranimi digitalnimi potrdili za overjanje elektronskega podpisa ali drugih storitvah, kjer se podatkom v elektronski obliki dodaja varni časovni žig.

(2) Namen varnih časovnih žigov je na kriptografsko varen način zagotavljati povezljivost elektronsko podpisanih dokumentov in drugih elektronskih podatkov z datumom in časom, v katerem so bili elektronski dokumenti ali podatki elektronsko podpisani. Z varnim časovnim žigom se zagotovi tudi, da je bilo digitalno potrdilo veljavno v času elektronskega podpisa dokumenta.

Varni časovni žigi se uporabljajo v različnih aplikacijah in za različne namene, ki se pojavljajo na tržišču. Med drugim se varni časovni žigi uporabljajo v aplikacijah in namenih kot so:

- 1) elektronsko bančništvo
- 2) elektronska hramba podatkov, dokumentarnega ali arhivskega gradiva

- 3) aplikacije E-uprave
- 4) druge aplikacije, kjer je treba zagotoviti povezljivost določenega dejanja ali dejstva s točnim časovnim virom.

(3) Varno časovno žigosanje je del infrastrukture javnih ključev pri overitelju HALCOM-CA. Za uporabo varnega časovnega žiga HALCOM-CA mora imeti uporabnik programsko opremo, ki omogoča časovno žigosanje. Preko nje uporabnik izdajatelju varnih časovnih žigov pri overitelju HALCOM-CA posreduje zgostitveno vrednost elektronskih podatkov ali elektronskega dokumenta, katerega želi časovno žigosati. Zgostitvena vrednost je »povzetek« dokumenta fiksne dolžine, katero izdajatelj časovnih žigov digitalno podpiše s svojim zasebnim ključem, pred tem pa ji doda podatke o točnem času podpisa. S tem je zagotovljeno, da so žigosani elektronski podatki ali elektronski dokument nastali pred tem časom.

2.2 STROŠKI UPORABE INFRASTRUKTURE

(1) HALCOM-CA določi cenik storitev varnega časovnega žiga in drugih 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

Storitev časovnega žigosanja overitelja HALCOM-CA predstavljajo naslednji podatki:

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

1. Za RFC 3161 časovne žige in zgostitveno funkcijo SHA-1:

CPName HALCOM CA TS RFC 1
CPOID 1.3.6.1.4.1.5939.3.1.1.1

2. Za RFC 3161 časovne žige in zgostitveno funkcijo SHA-256:

CPName HALCOM CA TS RFC 2
CPOID 1.3.6.1.4.1.5939.3.1.2.1

3. Za OASIS DSS XML časovne žige in zgostitveno funkcijo SHA-1:

CPName HALCOM CA TS DSS 1

CPOID 1.3.6.1.4.1.5939.3.2.1.1

4. Za OASIS DSS XML časovne žige in zgostitveno funkcijo SHA-256:

CPName HALCOM CA TS DSS 2

CPOID 1.3.6.1.4.1.5939.3.2.2.1

(1) Infrastrukturo HALCOM-CA sestavljajo:

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

3.1.2 Lastno potrdilo glavnega overitelja

(1) HALCOM-CA je za storitev varnega časovnega žigosanja oblikoval svoje lastno potrdilo (potrdilo HALCOM CA TS 1), serijska številka 169355 (02 95 8b), ki je namenjeno elektronskemu podpisovanju časovnih žigov, ki so izdani pri HALCOM-CA.

(2) Potrdilo HALCOM CA TS 1 vsebuje naslednje podatke:

Serijska številka	169355 (02 95 8b)
Overitelj potrdila	HALCOM CA PO 2, Halcom, SI
Imetnik potrdila	HALCOM CA TS 1, TSA, Halcom, SI
Veljavnost potrdila	3.8.2006 – 3.8.2011
Dolžina ključa	1024 bitov
SHA-1	93 3b 05 5d d5 58 c2 29 30 4b 18 89 2c 4a b8 c0 fe 81 0d c2

3.1.3 Šifrirni algoritmi, formati podatkov in protokoli

(1) HALCOM-CA uporablja:

- za podpisovanje varnega časovnega žiga algoritem RSA s parom ključev dolžine 1024 bitov;
- za šifriranje podatkov algoritme Triple DES in AES;
- zgostitveni algoritem SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)), MD5 (RFC 1321), SHA-256 (FIPS PUB 180-2) in RIPEMD-160 (ISO/IEC 10118-3:2003);
- za sinhronizacijo ure protokol NTP v4 z IFF autokey obojestransko avtentikacijo,
- format digitalnih potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:2001 ter X.509 ver. 3 (v3);
- format varnega časovnega žiga ustreza priporočilu RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) in standardu OASIS Digital Signature Service (DSS Core specification);
- 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.

3.2 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 in ETSI TS 101 023 Policy requirements for time-stamping authorities.

(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 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 in izdajanjem varnih časovnih žigov.

(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 je zavezan delovati in izdajati varne časovne žige v skladu s to politiko, z zaupnim delom notranjih pravil, ter z drugimi predpisi, na katere se ta politika sklicuje.

(2) HALCOM-CA ne prevzema nobene odgovornosti za podatke, ki jih naročnik varnega časovnega žiga elektronsko šifrira, podpisuje ali varno časovno žigosa. HALCOM-CA ne prevzema odgovornosti za te podatke 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.

(3) HALCOM-CA ne prevzema nobene odgovornosti za posledice, ki nastanejo, ker uporabnik varnega časovnega žiga 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.

4 DEJAVNOST IZDAJANJA VARNIH ČASOVNIH ŽIGOV

4.1 UPRAVLJANJE S KLJUČI ZA VARNO ČASOVNO ŽIGOSANJE

4.1.1 Generiranje ključev

(1) Par ključev overitelja HALCOM-CA za izdajo varnih časovnih žigov se generira v fizično in elektronsko varnem okolju overitelja ob prisotnosti overiteljevega osebja v zaupanja vrednih vlogah po posebnem postopku generiranja ključev pod vsaj dvojnimi nadzorom.

(2) Generiranje ključev overitelja HALCOM-CA za izdajo varnih časovnih žigov se izvede v varnih strojnih kriptografskih modulih (HSM), ki izpolnjujejo vse zahteve določil standarda NIST FIPS PUB 140-2 nivo 3 ali višji.

(3) Algoritem za generiranje ključev, dolžina ključev ter algoritem za podpisovanje podatkov ustrezajo mednarodno uveljavljenim priporočilom in standardom ter varnostnim zahtevam overitelja HALCOM-CA in so primerni za uporabo v namene izdajanja varnih časovnih žigov v okviru overitelja HALCOM-CA.

4.1.2 Varovanje zasebnih ključev za izdajo varnih časovnih žigov

(1) Overitelj HALCOM-CA skrbi za varovanje zaupnosti in celovitosti zasebnih ključev za izdajo varnih časovnih žigov.

(2) Zasebni ključi overitelja HALCOM-CA so varovani v varnih strojnih kriptografskih modulih (HSM), ki izpolnjujejo vse zahteve določil standarda NIST FIPS PUB 140-2 nivo 3 ali višji.

(3) Programska oprema za izdajo varnih časovnih žigov overitelja HALCOM-CA uporablja zasebne ključe v skladu z mednarodno priznanimi standardi, algoritmi ter veljavno zakonodajo.

4.1.3 Dostopnost javnega ključa za preverjanje veljavnosti varnih časovnih žigov

(1) Javni ključi za preverjanje veljavnosti varnih časovnih žigov overitelja HALCOM-CA so dosegljivi izključno v obliki digitalnega potrdila za časovno žigosanje, ki ga v skladu z veljavno politiko za izdajanje kvalificiranih digitalnih potrdil izda overitelj HALCOM-CA.

(2) Digitalna potrdila overitelja HALCOM-CA za časovno žigosanje so izdana v skladu s politiko, ki po varnostnih zahtevah ustreza ali presega varnostne zahteve politike za izdajo varnih časovnih žigov overitelja HALCOM-CA.

(3) Digitalna potrdila overitelja HALCOM-CA za časovno žigosanje so skupaj s podatki o potrdilu dosegljiva na spletnih straneh overitelja.

4.1.4 Veljavnost digitalnega potrdila za časovno žigovanje

(1) Veljavnost digitalnega potrdila overitelja HALCOM-CA za časovno žigovanje je določena v politiki overitelja HALCOM-CA za izdajo kvalificiranih digitalnih potrdil in ne presega zakonskih omejitev ter priporočil mednarodno uveljavljenih standardov.

(2) Veljavnost digitalnega potrdila overitelja HALCOM-CA za časovno žigovanje je omejena na vrednost, ki skozi vso življenjsko dobo digitalnega potrdila nudi dovolj visok nivo zaščite za namene uporabe izdaje časovnih žigov. Oceno stopnje varnosti posameznih algoritmov in vrst ključev redno podaja organizacija European Electronic Signature Standardization Initiative Steering Group (EESSI) ali druga primerljiva mednarodno priznana organizacija.

4.1.5 Podaljšanje veljavnosti digitalnega potrdila za časovno žigovanje

(1) Programska in strojna oprema za izdajo varnih časovnih žigov ter postopki overitelja HALCOM-CA imajo vgrajene varovala in mehanizme, ki preprečujejo uporabo zasebnih ključev po poteku njihove časovne veljavnosti.

(2) Novi ključi overitelja HALCOM-CA za izdajo varnih časovnih žigov se izdelajo ter aktivirajo v skladu z veljavno politiko overitelja še pred potekom časovne veljavnosti starih ključev.

(3) Poseben postopek za uničenje zasebnih ključev overitelja HALCOM-CA za izdajo varnih časovnih žigov zagotavlja, da uničenih ključev ni mogoče obnoviti.

4.1.6 Upravljanje kriptografskih modulov

(1) Overitelj HALCOM-CA zagotavlja ustrezno varovanje strojnih kriptografskih modulov ter podatkov v moduli v celotnem življenjskem ciklu le-teh, konkretno:

- uporablja postopke, ki preprečujejo oziroma odkrivajo morebitne nepooblaščen posege v kriptografske module med prevozom le-teh od proizvajalca do overitelja,
- uporablja elektronsko in fizično varovanje za preprečevanje nepooblaščenih posegov v module in povezano programsko opremo med njihovo uporabo,
- za namestitvev, aktivacijo ter izdelavo varnostnih kopij ključev za podpisovanje in kriptografskih modulov se uporabljajo posebni, zakonodajo in z mednarodnimi standardi in predpisani postopki, ki se izvajajo ob prisotnosti zaupanja vrednega osebjia overitelja ter verodostojnih prič v fizično in elektronsko varovanih prostorih overitelja,
- izvaja redne nadzore pravilnega delovanja in obnašanja strojnih kriptografskih modulov ter povezane programske opreme,
- uporablja posebne postopke za zamenjavo oziroma nadgradnjo strojnih kriptografskih modulov, ki poskrbijo za uničenje podpisnih ključev v zamenjanih moduli.

4.2 VARNO ČASOVNO ŽIGOVANJE

4.2.1 Varni časovni žig

(1) Časovni žigi, ki jih izdaja overitelj HALCOM-CA, so izdani na varen način in vsebujejo točen čas nastanka žiga.

(2) Oblika časovnega žiga je v skladu z mednarodnim standardom RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), kadar gre za binarne

časovne žige, in standardom OASIS Digital Signature Service (DSS Core specification) kadar gre za časovne žige v obliki XML.

(3) Časovni žigi overitelja HALCOM-CA vsebujejo naslednje podatke:

- oznako CP_{OID} politike, po kateri je bil žig izdan,
- enolično serijsko številko, ki ga razlikuje od vseh ostalih časovnih žigov, izdanih pri tem overitelju,
- čas nastanka žiga, ki je na varen način sledljivo usklajen z enim od uradnih UTC laboratorijev na svetu, seznam katerih določa organizacija Bureau International des Poids et Mesures (BIPM),
- natančnost ure, ki določa čas nastanka posameznega časovnega žiga, omejene s to politiko,
- oznaka algoritma in zgoščitveno vrednost podatkov, ki se časovno žigosajo,
- oznaka overitelja HALCOM-TSA, država, kjer se overitelj nahaja (SI) ter oznaka logične enote, ki je časovni žig izdala (npr. oznaka strežnika),
- ostale podatke, ki jih predpiše overitelj HALCOM-CA.

(4) Programska oprema za izdajo časovnih žigov overitelja HALCOM-CA ima vgrajene metode in postopke za ugotavljanje odstopanja lokalne ure od ure UTC laboratorija, ki v primeru prevelikega odstopanja preprečijo izdajo časovnih žigov.

(5) Časovni žigi overitelja HALCOM-CA se podpisujejo s ključem, ki se uporablja izključno za namene časovnega žigosanja.

4.2.2 Sinhronizacija ure s časovnim virom

(1) Referenčna ura, ki se uporablja za določanje časa nastanka časovnih žigov overitelja HALCOM-CA, se redno na varen način po protokolu NTP z obojestransko avtentikacijo usklajuje z uro enega od uradno priznanih UTC laboratorijev s seznama organizacije Bureau International des Poids et Mesures (BIPM).

(2) Referenčna ura, ki se uporablja za določanje časa nastanka časovnih žigov overitelja HALCOM-CA, se nahaja v elektronsko in fizično varovanih prostorih overitelja, do katerih ima dostop le pooblaščen osebje overitelja.

(3) Programska oprema za nadzor referenčne ure overitelja HALCOM-CA izklopi sistem za izdajo časovnih žigov v primeru, da zazna odstopanje referenčne ure od ure UTC laboratorija, ki presega v tej politiki deklarirano natančnost izdanih časovnih žigov overitelja HALCOM-CA v velikosti +/- 1 sekunde.

(4) Referenčna ura, ki se uporablja za določanje časa nastanka časovnih žigov overitelja HALCOM-CA, skrbi za upoštevanje prestopne sekunde (angl. »leap second«), kot jo določi ustrezna mednarodna meroslovna organizacija.

4.3 NAROČILNICA ZA VARNI ČASOVNI ŽIG

(1) Bodoči uporabnik storitve varnega časovnega žigosanja overitelja HALCOM-CA se na storitev prijavi z oddajo in podpisom naročilnice za vklop storitve varnega časovnega žigosanja overitelja HALCOM-CA.

(2) Bodoči uporabnik na naročilnici poleg osebnih podatkov in, če je uporabnik pravna oseba, podatkov o pravni osebi, navede tudi podatke o kvalificiranem digitalnem potrdilu, uporabljenem za dostop do servisa varnega časovnega žigosanja overitelja HALCOM-CA.

(3) S podpisom naročilnice za storitev varnega časovnega žigosanja overitelja HALCOM-CA se uporabnik zavezuje, da bo spoštoval vse pogoje in zahteve overitelja HALCOM-CA iz te politike in določila veljavnih predpisov ter zakonodaje.

4.4 POSTOPEK IZDAJE VARNEGA ČASOVNEGA ŽIGA

(1) Uporabnik storitve varnega časovnega žigosanja overitelja HALCOM-CA strežniku za žigosanje posreduje zahtevek za žigosanje preko varne povezave SSL oziroma TLS. Uporabnik (fizična oseba ali informacijski sistem) se na strežnik prijavi s svojim kvalificiranim digitalnim potrdilom.

(2) Programska oprema za izdajo varnega časovnega žiga overitelja HALCOM-CA samodejno preveri, ali je uporabnik storitve registriran za uporabo storitve varnega časovnega žigosanja po ustrezni politiki overitelja HALCOM-CA za izdajo varnega časovnega žiga.

(3) Zahtevek za časovno žigosanje se v programski opremi overitelja HALCOM-CA preveri, tako da vsebuje pravilne podatke in zgostitveno vrednost pravilne vrste in dolžine glede na uporabljeno politiko varnega časovnega žigosanja.

(4) Preverjeni zahtevek za časovno žigosanje se vpiše v dnevnik zahtevkov za žigosanje.

(5) Za zgostitveno vrednost dokumenta iz zahtevka se izdelava nov varen časovni žig overitelja HALCOM-CA, ki vsebuje vse podatke iz 3. odstavka podpoglavja 4.2.1 in je digitalno podpisan v varovani strojni opremi v varnem okolju overitelja z namenskim zasebnim ključem za časovno žigosanje.

(6) Varni časovni žig overitelja HALCOM-CA se zapiše v dnevnik izdanih časovnih žigov in se posreduje uporabniku, ki je zahtevek za žigosanje poslal.

5 UPORABNIKI VARNIH ČASOVNIH ŽIGOV

5.1 VARNOSTNE ZAHTEVE

(1) Uporabnik oziroma bodoči uporabnik varnega časovnega žiga je dolžan:

1. skrbno prebrati to politiko pred podpisom naročilnice za varni časovni žig ter spremljati vsa obvestila HALCOM-CA in ravnati v skladu z njimi in to politiko;
2. spremljati razvoj tehnologije oziroma obvestila HALCOM-CA in ravnati v skladu s priporočili HALCOM-CA glede zanesljive uporabe varnih časovnih žigov.

(2) Uporabnik varnega časovnega žiga mora izpolnjevati vse zahteve iz te politike in veljavnih predpisov.

5.2 PRAVICE UPORABNIKA VARNEGA ČASOVNEGA ŽIGA

(1) Uporabnik časovnega žiga lahko kadarkoli zahteva vse informacije glede veljavnosti varnega časovnega žiga, glede določb te politike ter glede obvestil HALCOM-CA.

6 TRETJE OSEBE

6.1 VARNOSTNE ZAHTEVE

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

6.2 PRAVICE TRETJE OSEBE

(1) Tretja oseba se lahko zanese na varni časovni žig.

(2) Tretja oseba lahko kadarkoli zahteva vse informacije glede veljavnosti varnega časovnega žiga, glede določb te politike ter glede obvestil HALCOM-CA.

6.3 OBVEZNOSTI TRETJE OSEBE

(1) Tretje osebe, ki se zanašajo na varni časovni žig, morajo:

1. preveriti pravilnost zapisa varnega časovnega žiga;
2. preveriti veljavnosti varnega časovnega žiga in veljavnost lastnega digitalnega potrdila HALCOM-CA, s katerim so elektronsko podpisani javni ključi varnih časovnih žigov;
3. seznaniti se s to politiko;
4. upoštevati morebitne omejitve pri uporabi varnih časovnih žigov, določene s to politiko.

8. KONČNE IN PREHODNE DOLOČBE

8.1 SPLOŠNO

(1) Vse avtorske, sorodne in druge pravice na varnem časovnem žigu in na drugih ključih ter vseh ostalih podatkih vse pravice pripadajo HALCOM-CA.

8.2 REŠEVANJE SPOROV

(1) Vse pritožbe uporabnikov varnih časovnih žigov rešuje nadzorna skupina HALCOM-CA (podpoglavje 3.2.2).

(2) Morebitne spore med uporabnikom varnega časovnega žiga 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. Veljavni varni časovni žigi pri tem ostanejo v veljavi do konca preteka veljavnosti in po stari politiki delovanja. Vsi časovni žigi izdani 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

CA	Overitelj potrdil. <i>Angl.: Certification Authority ali Certification Agency</i>
CCPS	Certificate and Card Production Service – storitev izdelave potrdil in kartic in zajema: <ol style="list-style-type: none"> 1. Izdajo CA ključa za vsakega podrejenega overitelja 2. Postavitev CA parametrov v CCPS za vsakega podrejenega overitelja 3. Predpoosebljanje pametnih kartic, v skladu z nizom standardiziranih izdelkov 4. Izdelavo visoko kakovostnih ključev RSA z najmanj 1024 biti 5. Varovanje integritete predpoosebljenih inteligentnih kartic s transportnim PIN-om 6. Dobavo predpoosebljenih pametnih kartic za podrejene overitelje z LCM 7. Poosebljanje kartic končne entitete s povezovanjem podatkov imetnika in javnega ključa, torej izdajo potrdil x509 v3 in njihovo nalaganje v pametne kartice 8. Dobavo kartic končne entitete podrejenim overiteljem, ki nimajo LCM
CPName	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>)
CPOID	Mednarodna številka, ki enolično določa politiko delovanja (<i>Angl.: Certification Policy Object Identifier</i>).
CRL	Certificate Revocation List – seznam preklicanih digitalnih potrdil
DN	Enolično razločevalno ime (prim. definicijo Razločevalno ime). <i>Angl.: Distinguished Name</i>
Imenik potrdil	Imenik potrdil po priporočilu X.500, kjer so shranjena potrdila po priporočilu X.509 ver. 3, do katerih je možen dostop po protokolu LDAP
LCM	Local Certificate Manager – sistem za upravljanje s potrdili pri podrejenem overitelju
LDAP	Leightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu RFC 1777
Nedvoumna identifikacija	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.
NTP	Protokol za sinhronizacijo časa; <i>Angl.: Network Time Protocol</i>
Overitelj potrdila	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>
Overitelj varnega časovnega žiga	Fizična ali pravna oseba, ki izdaja varne časovne žige in opravlja druge storitve v zvezi z izdajanjem časovnih žigov. <i>Angl: Time stamp authority (TSA).</i>
Potrdilo	Kvalificirano potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo ter potrjuje njeno identiteto. <i>Angl.: Certificate</i>

Razločevalno ime	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>
SSL	Kriptografski protokol za varen prenos podatkov preko interneta; <i>Ang.: Secure Sockets Layer</i>
TLS	Kriptografski protokol za varen prenos podatkov preko interneta; <i>Ang.: Transport Layer Security</i>
TSA	Overitelj ali izdajatelj časovnih žigov; <i>Ang.: Time-Stamping Authority</i>
TSP	Protokol za izdajanje časovnih žigov; <i>Ang.: Time-Stamping Protocol</i>
UTC	Koordinirani univerzalni čas – mednarodni standard za merjenje časa, kii temelji na atomski uri; <i>Ang.: Coordinated Universal Time</i>
Varni časovni žig	Varni časovni žig (ang. <i>Time stamp</i>) je elektronsko podpisano kvalificirano potrdilo overitelja, s katerim se zagotovi povezljivost elektronskih dokumentom z datumom in časom, do sekunde natančno, v katerem so bili ti elektronsko podpisani. Glede izdajanja varnega časovnega žiga veljajo enake zakonske zahteve kot glede izdajanja kvalificiranih digitalnih potrdil.

Kraj in datum: Ljubljana, 07.08.2006

Direktor
Matjaž Čadež