# AS Sertifitseerimiskeskuse ajatempliteenuse ajatembelduspõhimõtted

Versioon 1.0

OID: 1.3.6.1.4.1.10015.4.1.1

7.10.2002

Versioonid ja muudatused:

| Versioon | Kuupäev | Kommentaarid |
|---|---|---|
| 1.0 | 7.10.2002 | Esimene versioon |

# 1. Sissejuhatus

AS Sertifitseerimiskeskus osutab Digitaalallkirja seaduse (DAS) nõuetele vastavat ajatempliteenust, mis tagab digitaalselt allkirjastatud dokumentide tõestusväärtuse pikaajalise säilimise.

Käesolev dokument kirjeldab pakutavat ajatempliteenust ning esitab selle ajatembelduspõhimõtted (ATP).

## 1.1 Terminid ja lühendid

ajatempel – elektrooniline andmekogum, mille otstarve on tõestada mingi teise andmekogumi (dokumendi) tekkehetke ajalist seost (enne, pärast) muude sündmustega

ajaallikas - seade, programm või süsteem, mille väljundsuurus on teatud kriteeriumidele vastavuse mõttes õige ajanäit. Kriteeriumiks võib olla näiteks maailmaaeg.

ajanäit – ajaallika väljundsuuruse väärtus

ATO – ajatempliteenuse osutaja: digitaalallkirja seaduse alusel ajatempliteenust andev organisatsioon

ATP – ajatembelduspõhimõtted

CISA – infosüsteemide sertifitseeritud audiitor (Certified Information Systems Auditor)

DAS – digitaalallkirja seadus (Eesti)

GPS – globaalne positsioneerimissüsteem

kehtivuskinnitus – andmete kogum, mis seob digitaalselt allkirjastatud dokumendi ajahetkega, mil digitaalallkirja andmiseks kasutatud sertifikaat oli kehtiv

SK – AS Sertifitseerimiskeskus

SRR – Sertifitseerimise Riiklik Register

UPS – puhvertoiteallikas

UTC – maailmaaeg ("universaalne ajakoordinaat")

## 1.2 Viited


1. Digitaalallkirja seadus // RT I 2000, 92, 597; RT I 2001, 56, 338; RT I 2002, 53, 336; RT I 2002, 61, 375 (WWW) https://www.riigiteataja.ee/ert/act.jsp?id=184502 (30.08.2002)
2. Sertifitseerimise Riiklik Register // Sideameti koduleht (WWW) http://web.sa.ee/est/keskmine.php?GID=6&MID=329 (30.08.2002)
3. Teenuse osutajate infosüsteemide auditeerimise kord // RTL 2000, 108, 1655 (WWW) https://www.riigiteataja.ee/ert/act.jsp?id=26553 (30.08.2002)
4. Sertifitseerimise riikliku registri volitatud töötleja avalikud võtmed ja neile vastavate isiklike võtmete kasutusala // RTL 2001, 110, 1545 (WWW) https://www.riigiteataja.ee/ert/act.jsp?id=27249 (30.08.2002)
5. RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Service Protocol - OCSP http://www.ietf.org/rfc/rfc2560.txt (06.1999)
6. AS Sertifitseerimiskeskuse sertifitseerimispõhimõtted – CPS http://www.sk.ee/cps/


# 2. Ajatempliteenuse osutaja

Ajatempliteenuse osutaja on AS Sertifitseerimiskeskus (edaspidi SK). SK asutasid 2001. aasta veebruaris võrdse osalusega Hansapank, Ühispank, Eesti Telefon ja EMT. SK missioon on turvalist ja usaldusväärset elektroonilist äritegevust, asjaajamist ning suhtlemist võimaldava keskkonna loomine ja arendamine Eestis. SK on registreeritud SRR-is sertifitseerimisteenuse pakkujana ning väljastab sertifikaate Eesti ID-kaartidele. Kõigis ajatempliteenusega seotud küsimustes võib teavet saada järgmistelt aadressidelt (eelistatav on elektrooniline infovahetus):

AS Sertifitseerimiskeskus
Äriregistri kood 10747013
Aadress: Pärnu mnt 12, 10148 Tallinn
Tel +372 610 1880
Faks +372 610 1881
E-post: info@sk.ee
http://www.sk.ee/

Kontaktandmete muutumisel teatatakse sellest kohe SK veebilehel.

Kõik SK ajatembelduste enusega seotud avalikud dokumendid, teenuse kasutamiseks vajalikud tehnilised parameetrid ning klienditarkvara on kättesaadavad avalikus andmesidevõrgus aadressil http://www.sk.ee/ajatempel/.

# 3. Ajatempliteenuse osutamiseks kasutatavad vahendid

SK ajatempliteenus on vormistatud üldisema, nn. „kehtivuskinnituse“ teenusena. Kehtivuskinnituse teenuse abil on võimalik jagada infot nii sertifikaadi kehtivuse kohta kui ka kehtivuskinnituse väljastamise aja kohta. Kehtivuskinnituse teenusega järgib SK muuhulgas ka DAS §22 lg.5 esitatud nõuet „tõendada huvitatud isiku nõudmisel oma esindaja digitaalallkirjaga enda poolt väljaantud sertifikaadis sisalduvale avalikule võtmele vastava isikliku võtmega antud digitaalallkirja kehtivust“.

Teenus põhineb OCSP-protokollil, mis on kirjeldatud Interneti standardis RFC 2560. OCSP kujutab endast lihtsat klient-server süsteemi, kus OCSP klient saadab OCSP responderile (serverile) päringu mingi sertifikaadi kohta ning responder annab selle sertifikaadi kohta kinnituse, mis sisaldab selle sertifikaadi (mitte)kehtivust ja kinnituse andmise aega. Responderi poolt antud vastus on digitaalselt signeeritud.

OCSP responderi vastused sertifikaadi kohta võivad olla kolmelaadsed:

- sertifikaat kehtib
- sertifikaat ei kehti
- informatsioon küsitava sertifikaadi kohta puudub (OCSP responder ei serveeri infot sellise väljaandja poolt välja antud sertifikaatide kohta)

Standardikohane OCSP positiivne vastus sertifikaadi kohta ei tähenda seda, et küsitav sertifikaat üldse kunagi välja antud on. SK OCSP positiivne vastus tähendab aga, et sertifikaat on välja antud ning ta oli kinnituse väljastamise hetkel kehtiv.

SK OCSP saab sertifikaatide kehtivusinformatsiooni otse sertifikaatide andmebaasist, kuhu laekuvad operatiivselt ka kõik sertifikaatide olekumuutused. See kindlustab, et OCSP vastused näitavad maksimaalselt ajakohast sertifikaatide olekut.

SK OCSP juurdepääsul kontrollitakse OCSP kliendi identiteeti. Kasutada on kaks meetodit – kas lubatakse juurdepääs kliendi IP-aadressi järgi või saata signeeritud OCSP-päring. SK väljastab eraldi sertifikaate (juurdepääsutõendeid) OCSP-päringute signeerimiseks. Erinevatele klientidele on võimalik kehtestada ka piiranguid selle kohta, milliste sertifikaatide kohta ta saab kehtivusinfot pärida.

<u>Digitaalallkirja kinnitamine OCSP-teenuse abil</u>

OCSP-standard näeb ette protokolli standardlaiendust nimega „nonss“ (*nonce*). Tegemist on juhuslikult genereeritud baidijadaga, mis pannakse kaasa OCSP-päringusse ning mis kaasatakse signeerituna OCSP-vastusesse. Algselt on nonss mõeldud taasesitusrünnete kaitseks.

SK OCSP-teenus ei piira tehniliselt  nonsi sisu ega pikkust ning seetõttu võib seda käsitleda kui digitaalselt allkirjastatud dokumenti või selle sõnumilühendit.

Nonsiga laiendatud OCSP-päringut võib seega käsitleda järgnevalt:

- klient saadab OCSP responderile allkirjastatud dokumendi ning vastava sertifikaadi, mille alusel ta selle dokumendi allkirjastas
- OCSP responder väljastab digitaalselt allkirjastatud kinnituse semantikaga „hetkel, kui ma selle sertifikaadi alusel allkirjastatud dokumenti nägin, oli see sertifikaat kehtiv“

Signeeritud OCSP-päringus sisaldub ka aeg, mistõttu saab OCSP-kinnitust digitaalselt allkirjastatud dokumendile pidada vajalikuks ja piisavaks lisandiks selleks, et allkirjastatud ja OCSP-kinnitusega varustatud dokumenti pidada kõigiti pädevaks DAS mõttes. SK võtab endale vastutuse OCSP-kinnituste eest, k.a. seal sisalduva ajakomponendi õigsuse eest.

<u>Pikaajalise tõestusväärtuse tagamine, dispuutide lahendamine</u>

Selleks, et tagada tõestusväärtuse järjepidevus võimalike turvaintsidentide (võtmete vahetus või korrumpeerumine, signeerimisalgoritmi murdmine jne.) korral ning võimaldada SK poolt väljastatud kinnituste auditeerimist, kasutab SK sisemiselt CPS-s p.4.7.3 kirjeldatud turvalist logimissüsteemi, kuhu logitakse kõik sertifikaatide olekumuutused ning väljastatud OCSP-kinnitused.

Turvalogi seob logitavad kirjed üksteisega ajalises järjekorras, kasutades krüptograafilisi linkimismeetodeid. Arusaamise lihtsustamiseks võib turvalogi vaadelda ka kui „registripäevikut“, kus kanded kirjutatakse üksteise alla, leheküljed nummerdatakse ning pärastine vahelekirjutamise võimalus või kannete kustutamise võimalus puudub (kui just ei hävitata tervet registripäevikut).

Sertifikaadi olekut SK andmebaasis ei muudeta ning OCSP-kinnitusi ei väljastata juhul, kui sisemine logimine turvalogisse ei õnnestu. See tagab, et väljastatud OCSP-kinnituse kohta on alati olemas turvaline jälg SK infosüsteemis ning ka vastupidi – kui leidub kinnitus, mille kohta SK infosüsteemis jälge pole, on see kinnitus võltsitud.

Turvalisuse tõstmiseks publitseeritakse ajakirjanduses perioodiliselt turvalogi kirjeid. Kuna kõik turvalogi kirjed on omavahelises sõltuvuses, siis saab põhimõtteliselt iga kinnituse omaja kontrollida, kas tema kinnitus on seotud publitseeritud kirjega.

Publitseeritud turvalogi kirjed avaldatakse ka SK koduleheküljel. Koduleheküljel on ka info selle kohta, millal ja millises ajakirjandusväljaandes on sama turvalogi kirje publitseeritud.

Turvalogi funktsioonid kasutajale on:

- Kinnituse leidmine andmebaasist – kasutaja sisestab oma saadud kinnituse ning veendub, kas see kinnitus on SK infosüsteemis logitud

- Kahe kinnituse omavaheline võrdlemine – sisestatakse kaks kinnitust ning (positiivsel juhul) leitakse nendevaheline seos. Kinnitus võib olla ka publitseeritud kinnitus.

Turvalogi järjestab turvaliselt kõik sertifikaatide kehtivusega seonduva ning tagab seetõttu:

- võimaluse omavahel võrrelda sertifikaatide olekumuutuseid ja/või väljastatud kinnitusi,
- kindlustunde, et SK ei saa teha toiminguid tagantjärele,
- auditeeritavuse,
- digitaalselt allkirjastatud dokumentide pikaajalise tõestusväärtuse, kuna tagasiulatuvaid kinnitusi pole võimalik tekitada isegi siis, kui OCSP kinnitusvõti korrumpeerub.

Kasutatavad vahendid:

Teenuse osutamiseks vajaliku infosüsteemi on loonud AS Privador, kasutades alltöövõtjate Cybernetica AS ja SEB IT Partner Estonia abi. Turvalogi on loodud firma Tietoenator Eesti AS poolt.

Teenust osutatakse üldkasutatava sidevõrgu (Interneti) kaudu.

Ajatempliteenuse osutamiseks kasutatav riistvara koosneb ajatempliserveri arvutist, FIPS 140-1 Level 2 sertifitseeritud riistvaralisest turvamoodulist ning serverisüsteemi kella sünkroniseerimiseks kasutatavast GPS-seadmest. Serveris kasutatavad kõvakettad on dubleeritud. Kui GPS-seadmega kella sünkroniseerimisega tekib tõrkeid, siis minnakse automaatselt üle sünkroniseerimisele NTP (*Network Time Protocol*) protokolli abil.

Turvalogist tehakse regulaarselt varukoopiad ühekordselt kirjutatavatele laserketastele (CDR) kahes eksemplaris. Varukoopia teine eksemplar deponeeritakse SRR-s.

Süsteemi töö jätkumise voolutõrgete korral tagavad vajaliku võimsusega puhvertoiteallikad (UPS).

Kehtivuskinnituse server asub kõrge turvalisusega serveriruumis.

# 4. Ajatemplite kinnitamise ning ajatempliserveri avaliku võtme avalikustamise kord

OCSP-serveri poolt väljastatud kehtivuskinnitused kinnitatakse serveri poolt, kasutades ainult kehtivuskinnituste kinnitamiseks mõeldud RSA privaatvõtit, mida hoitakse ja kasutatakse FIPS 140-1 Level 2 sertifitseeritud riistvaralises turvamoodulis.

Kehtivuskinnituste kinnitamiseks kasutatavale privaatvõtmele vastav avalik võti on Digitaalallkirja seaduse kohaselt registreeritud Sertifitseerimise Riiklikus Registris, võimaldamaks ajatempliteenuse osutaja poolt väljastatud ajatemplite kontrollimist.

Teenuse osutaja poolt teenuse osutamiseks kasutatavad avalikud võtmed on kättesaadavad SRR-i kodulehelt (http://register.srr.ee/). Võtmete kehtivust saab

kontrollida Riigi Teatajas avaldatud SRR-i avaliku võtme ning SRR-i poolt välja antava tühistusnimekirja abil. Kehtivuskinnituste kontrollimiseks ei tohi kasutada mittekehtivat avalikku võtit.

# 5. Ajatempli võtmine ja kontrollimine

Ajatemplit sisaldava kehtivuskinnituse vorming ja protokoll on määratud ära IETF-i standardiga RFC 2560 [5].

Kehtivuskinnitusse kantava ajanäidu määrab OCSP-responder, päringu esitaja ei saa serveri poolt ajatemplile lisatavat ajanäitu kuidagi mõjutada. Serveri kell sünkroniseeritakse automaatselt GPS-seadme abil maailmaajaga (UTC), välistades niiviisi ajatemplite võtmise taotletavast ajahetkest varasemale või hilisemale ajale.

Ajanäit tuuakse ära kehtivuskinnituse väljal *ProducedAt*.

Kehtivuskinnituse kontrollimine on võimalik vallasresiimis, kasutades OCSP-responderi sertifikaati (ajatempliserveri avalikku võtit). Kehtiva ja varem kehtinud OCSP-responderi sertifikaatide kohta saab informatsiooni SK koduleheküljelt.

Kehtivuskinnituse täiendavaks kontrolliks on võimalik kontrollida kehtivuskinnituse olemasolu SK turvalogis. Seda saab teha SK kodulehel oleva rakenduse kaudu. Sama rakenduse kaudu saab kontrollida turvalogi krüptograafilise linkimisahela olemasolu ja verifitseeruvust ajakirjanduses avaldatud turvalogi kirje ja vaadeldava kehtivuskinnituse vahel.

Publitseeritud turvalogi kirjete avaldamiskoha informatsioon on SK koduleheküljel.

# 6. Väljaantud ajatemplite arvestuse pidamine

Kõik väljastatud kehtivuskinnitused salvestatakse SK turvalogisse. SK garanteerib turvalogi andmebaasi tervikluse ning ei väljasta kehtivuskinnitusi juhul, kui logimine ei tööta.

Eri ajatempliteenuse osutajate poolt välja antud ajatemplite võrreldavuse tagamiseks annab SK perioodiliselt kehtivuskinnitusi SRR-i ajatemplite andmebaasi.

# 7. Andmete väljastamine ajatemplite kohta

Väljastatud kehtivuskinnitused logitakse SK turvalogisse, mida on kõigil soovijatel võimalik kasutada SK kodulehel oleva rakenduse kaudu.

Turvalogi säilitatakse kuni SK tegevuse lõpetamiseni. Turvalogi deponeeritakse perioodiliselt SRR-i.

# 8. Teenuseosutaja vastutus

SK vastutus lepinguliste klientide ees sätestatakse kliendilepingutega.

SK vastutus kehtivuskinnituste tõestusväärtuse säilimisest huvitatud kolmandate osapoolte ees sätestatakse käesolevas peatükis.

SK tegevus kehtivuskinnitusteenuse pakkumisel on suunatud väljastatud digitaalselt allkirjastatud dokumentide pikaajalise tõestusväärtuse tagamisele.

SK tagab:

1. Valitud ajatemplite sõnumilühendite perioodilise avaldamise ajakirjanduses.
2. Väljastatud kehtivuskinnituste arhiveerimise ja säilimise turvalogis.

SK kontrollib omapoolselt täiendavalt ajakirjanduses avaldatud turvalogi kirje õigsust ning vea leidmisel avaldab vastavasisulise õiendi.

SK ei vastuta kolmandate osapoolte poolt ajatemplite kehtivuse kontrollil tehtud vigadest või tegematajätmistest tingitud valeotsuste ja nende valeotsuste tagajärgede eest.

SK ei vastuta kehtivuskinnituste tõestusväärtuse kao eest vääramatu jõu (Force Majeure) tõttu.

# 9. Teenuse osutamise lõpetamise kord

Teenuse osutamine lõpetatakse vastavalt DAS 5. ptk nõuetele. Teenuse osutamise lõpetamisel antakse ajatemplite ja dokumentatsiooni arhiivid üle SRR-ile.

Lõpetamisel hävitatakse kõik kasutusel olnud privaatvõtmed: riistvaralisele turvamoodulile tehakse alglaadimine vastavalt tootja juhendile, teised privaatvõtmete või selle osade säilitamiseks kasutatud andmekandjad hävitatakse füüsiliselt.

Lepinguliste suhete lõpetamine reguleeritakse täpsemalt klientidega sõlmitavates teenuse osutamise lepingutes. Kliente ja SRR-i volitatud töötlejat teavitatakse teenuse osutamise lõpetamisest ning seniste ajatemplite edasise kasutamise võimalustest vähemalt 2 kuud ette.

# 10. Tegevuskava eriolukordade puhuks

Juhul, kui on saanud võimalikuks ajatempliteenuse osutaja või tema tegevuse jäljendamine teenuse osutamisel, on tegu eriolukorraga. Käesolev tegevuskava kirjeldab SK tegevuskava eriolukordade puhul.

Et kõik SK kehtivuskinnituse osutamisega seotud tegevused toimuvad elektrooniliselt ning on autenditud ajatemplite kinnitamiseks kasutatava privaatvõtmega, siis võib eriolukord tekkida vaid juhul, kui teenuse osutamiseks kasutatav privaatvõti on väljunud SK kontrolli alt ning ebaseaduslikult selle võtme omandanud isik on suutnud lisada kirjeid SK turvalogisse.

Järgnev tegevuskava on mõeldud juhuks, kui SK ajatempliteenuse andmiseks kasutatav privaatvõti väljub teenuseosutaja kontrolli alt.

1. määratakse võimalikult suure täpsusega privaatvõtme lekke ja esimeste turvalogisse kantud võltskirjete aeg;
2. võtme turvarikkest teatatakse massiteabevahendite kaudu, avaldades ajavahemiku, mille jooksul väljastatud kehtivuskinnitused kuulutatakse kehtetuks;
3. vastav info saadetakse ka kõigi lepinguliste klientide kontaktaadressidele;
4. kehtivuskinnituse infosüsteem isoleeritakse avalikust võrgust;
5. SK juhataja moodustab erikomisjoni, kes tuvastab võtme turvarikke põhjused;
6. turvarikke põhjus kõrvaldatakse;
7. kehtivuskinnituse teenuse osutamiseks kasutatav süsteem initsialiseeritakse;
8. turvalogist kustutatakse kõik kirjed alates sissemurdmisest kuni antud hetkeni;
9. juhul, kui asjaolud seda võimaldavad annab komisjon loa alustada teenuse osutamist varem ettevalmistatud varuvõtmega. Juhul, kui turvarikke asjaolud annavad alust oletada, et ka varuvõti võib olla väljunud SK kontrolli alt, genereeritakse teenuse osutamiseks uus võti, mis registreeritakse enne teenuse osutamise algust SRR-is.

# 11. Vastavus teenuseosutajale esitatud nõuetele

Ajatempliteenus vastab DAS §24 ajatempliteenusele esitatud nõuetele.

Ajatempliteenuse organisatsioon ja infosüsteem vastavad DAS §25 ning dokumendis "Teenuseosutajate infosüsteemide auditeerimise kord" (kehtestatud teede- ja sideministri määrusega nr.83 3.oktoobrist 2000) ajatempliteenuse osutajatele esitatud nõuetele.

Ajatembeldusteenus töötab SK organisatsioonilises ja tehnoloogilises keskkonnas, mille turvapoliitika on välja töötatud vastavuses standardiga EVS ISO/IEC TR 13335 osad 1,2,3,4 ja 5.

# 12. Audit

Ajatembeldusteenuse andmiseks kasutatavate infotehnoloogiliste süsteemide ning organisatsiooni vastavust esitatud nõuetele kontrollitakse regulaarselt sise- ja välisaudititega. Siseaudit toimub vähemalt kord aastas, välisaudit vastavalt kehtestatud nõuetele. Välisauditi tulemused avaldatakse SRR-i ja SK veebilehtedel.

Välisauditi läbiviimiseks kasutatakse ainult rahvusvaheliselt sertifitseeritud (CISA) audiitoreid.

# 13. Ajatembelduspõhimõtete haldus

Ajatembelduspõhimõtete sisulist tähendust mitte muutvate paranduste puhul, nagu õigekirjavigade parandamine, tõlkimine ja kontaktandmete ajakohastamine, tuleb muudatused dokumenteerida käesoleva dokumendi Versioonid-muudatused sektsioonis ning suurendada dokumendi versiooninumbri murdarvulist osa.

Sisuliste muudatuste puhul peab uus sertifitseerimispõhimõtete versioon olema eelnevatest selgelt eristatav. Uus versioon peab kandma ühe võrra suurendatud versiooninumbrit. Muudetud ajatembelduspõhimõtted koos kehtima hakkamise päevaga, mis ei või olla varasem kui 30 päeva avaldamisest, tuleb avaldada elektrooniliselt SK koduleheküljel.

Kõik muudatused kooskõlastatakse SRR-iga.