Sertifitseerimiskeskuse OCSP-teenus SK-OCSP

Käesolev dokument tutvustab Sertifitseerimiskeskuse (SK) poolt pakutavat laiendatud sertifikaatide kehtivuskinnituste ning digitaalselt allkirjastatud dokumentide kehtivuskinnituste teenust, mida edaspidi nimetame SK-OCSP (SK *Online Certificate Status Protocol*) teenuseks.

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.

SK-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.

Standardijärgne OCSP-teenus on ideoloogiliselt sobivaim autentimissertifikaatide siduskontrolliks (*online*). SK-OCSP serveerib mõlemate (s.t. ka digitaalallkirja sertifikaatide) ID-kaartidele salvestatud sertifikaatide kehtivusinfot.

Tagasiulatuvad päringud

SK -OCSP teenusel on realiseeritud ebastandardne laiendus, mis lubab esitada päringuid stiilis "kas antud sertifikaat eksisteeris SK andmebaasis päringus näidatud ajahetkel ja kas ta oli kehtiv". Päringus näidatud ajahetk saab olla ainult varasem päringu esitamise hetkest, tulevikupäringute kohta vastab responder „teadmata".

Digitaalallkirja kinnitamine SK-OCSP teenuse abil

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

Signeeritud SK-OCSP päringus sisaldub ka aeg, mistõttu saab SK-OCSP kinnitust digitaalselt allkirjastatud dokumendile pidada vajalikuks ja piisavaks lisandiks selleks, et allkirjastatud ja SK-

OCSP kinnitusega varustatud dokumenti pidada kõigiti pädevaks EV Digitaalallkirja Seaduse mõttes. SK võtab endale vastutuse SK-OCSP kinnituste eest, k.a. seal sisalduva ajakomponendi õigsuse eest.

Pikaajalise tõestusväärtuse tagamine, dispuutide lahendamine

Selleks, et tagada tõestusväärtuse järjepidevus võimalike turvaintsidentide (võtmete vahetus või korrumpeerumine, signeerimisalgoritmi murdmine jne.) korral ning võimaldaks SK poolt väljastatud kinnituste auditeerimist, kasutab SK sisemiselt turvalist logimissüsteemi (edaspidi: SeqLog), kuhu logitakse kõik sertifikaatide olekumuutused ning väljastatud SK-OCSP kinnitused.

SeqLog on turvaline logimissüsteem, mis seob logitavad kirjed üksteisega ajalises järjekorras kasutades krüptograafilisi linkimismeetodeid. Arusaamise lihtsustamiseks võib SeqLog-i vaadelda ka kui „registripäevikut“ kus kanded kirjutatakse üksteise alla, leheküljed nummerdatakse ning pärastine vahelekirjutamise võimalus või kannete kustutamise võimalus puudub (kui just ei hävita tervet registripäevikut).

Sertifikaadi olekut SK andmebaasis ei muudeta ning SK-OCSP kinnitusi ei väljastata juhul, kui sisemine logimine SeqLog-i süsteemi ei õnnestu. See tagab, et väljastatud SK-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 (st trükitakse ajalehes) perioodiliselt SeqLog-i kirjeid. Kuna kõik SeqLog-i kirjed on omavahelises sõltuvuses, siis saab põhimõtteliselt iga kinnituse omaja kontrollida, kas tema kinnitus on seotud publitseeritud kirjega.

SeqLog-i 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.

SeqLog 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 SK-OCSP kinnitusvõti korrumpeerub.