SPOF2.2 – Kehtivuskinnituse puhverteenuse analüüs

Aivo Kalu
Aleksander Kamenik
Triin Siil

20.09.2022

Euroopa Liit
Euroopa struktuuri- ja investeerimisfondid

Eesti
tuleviku heaks

CYBERNETICA

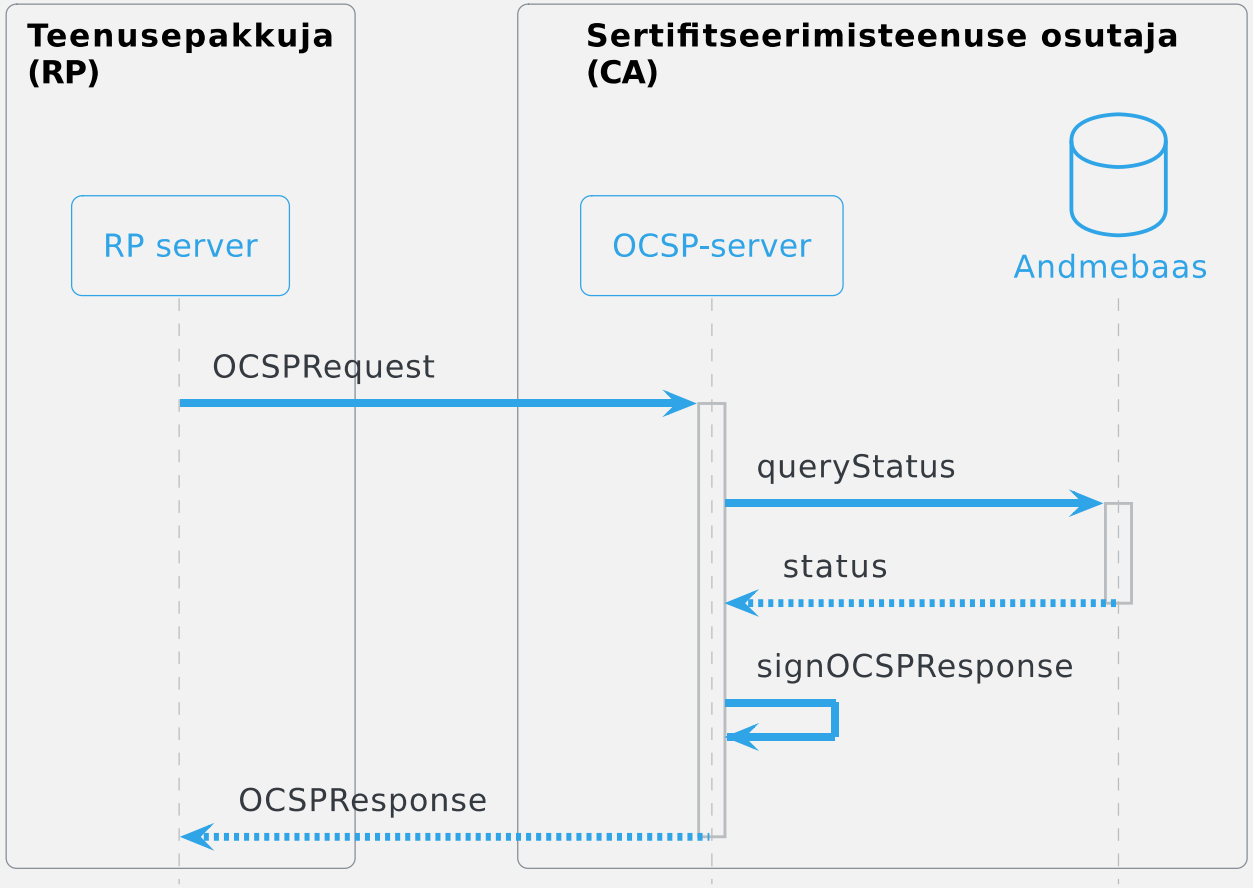
Seminari kava

- Projekti eesmärk
- Käsitletavad riskid
- Lahendusvariantide ülevaade
- Lahendusvariantide võrdlus
- Juriidiline analüüs
- Kokkuvõte

Projekti eesmärk

- Kehtivusinfo teenus (üldjuhul ocsp.ca.ee) on kriitiline teenus eID vahenditega autentimiseks ning digiallkirjade andmiseks.
- Lihtsustatult vaadates, kui teenus ocsp.ca.ee ei tööta, siis ei tööta mitte midagi.
- Analüüsime, kas teenust ocsp.ca.ee on tehniliselt ja juriidiliselt võimalik puhverdada?
- Millised tehnilised võimalused selleks on ning millised riskid vähenevad või suurenevad?

OCSP-teenuse tavapärane kasutamine



CYBERNETICA

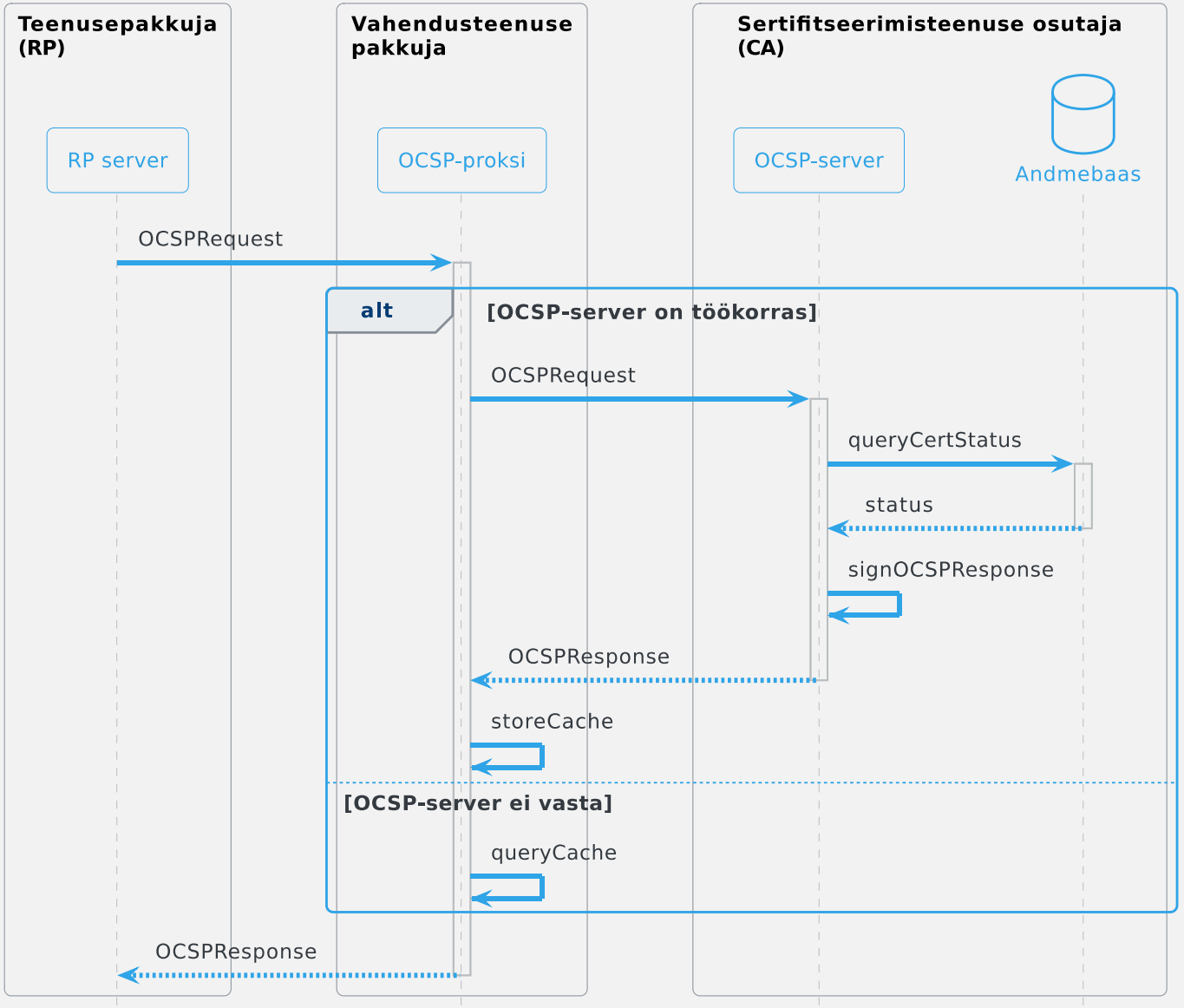
Analüüsitavad riskid

Riski ID	Riski kirjeldus
R1	Kehtivuskinnitusinfo ei ole kättesaadav ning autentimist ei saa kasutada
R2	Kehtivuskinnitusinfo ei ole kättesaadav ning allkirjastamist ei saa kasutada
R3	Kehtivuskinnitusinfot ei kasutata ning aktsepteeritakse ründaja autentimiskatse
R4	Kasutatakse aegunud kehtivuskinnitusinfot ning aktsepteeritakse ründaja autentimiskatse
R5	Kasutatakse ründaja ülevõetud kehtivuskinnitusteenust ning aktsepteeritakse ründaja autentimiskatse

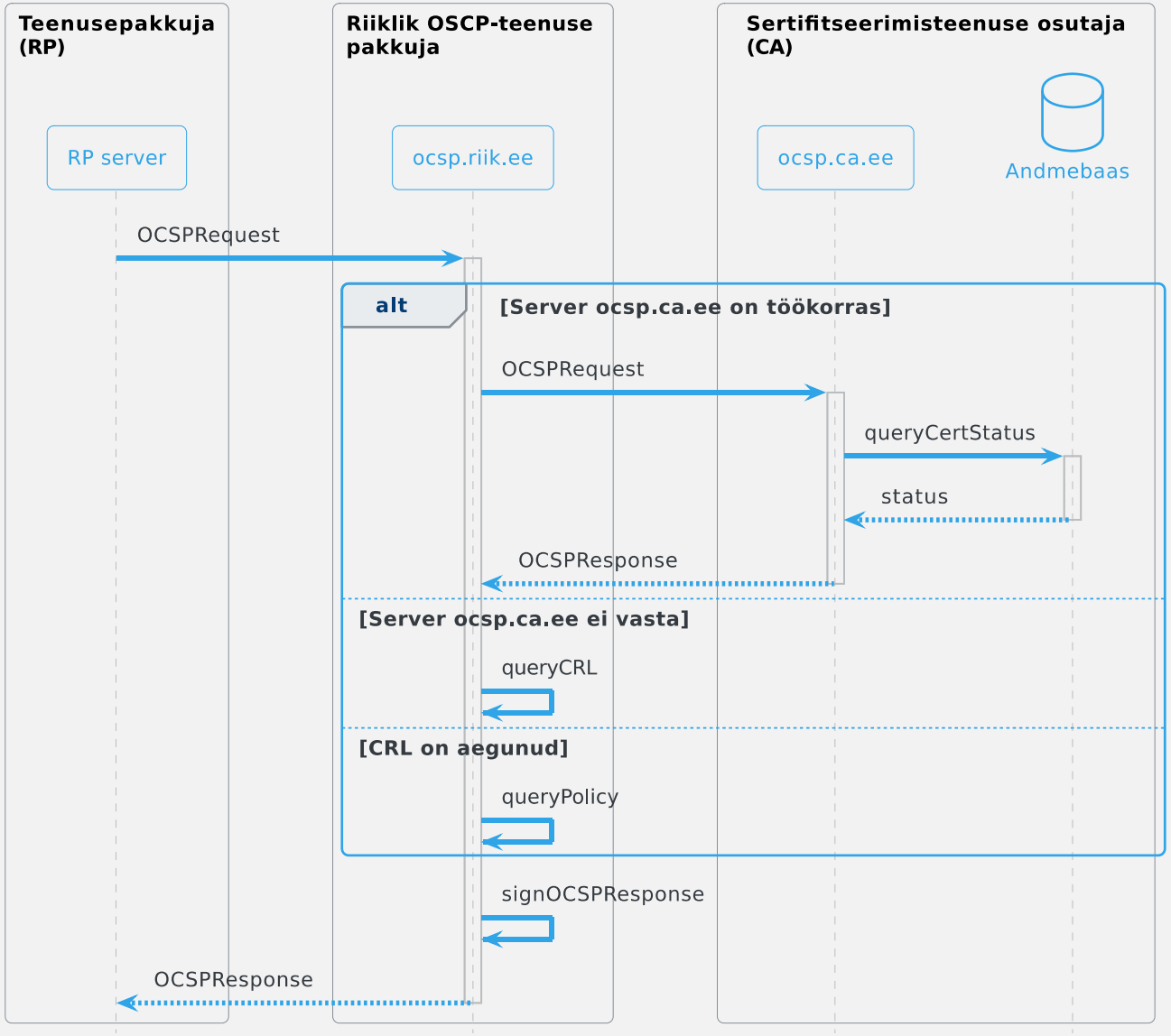
Analüüsitud lahendusvariandid

1. Vahendusteenus OCSP-proksi
2. Riiklik OCSP-teenus
3. Kõrgkäideldav CA OCSP-teenus
4. Autentimisteenuse TARA kehtivuskontrollide juhtimine

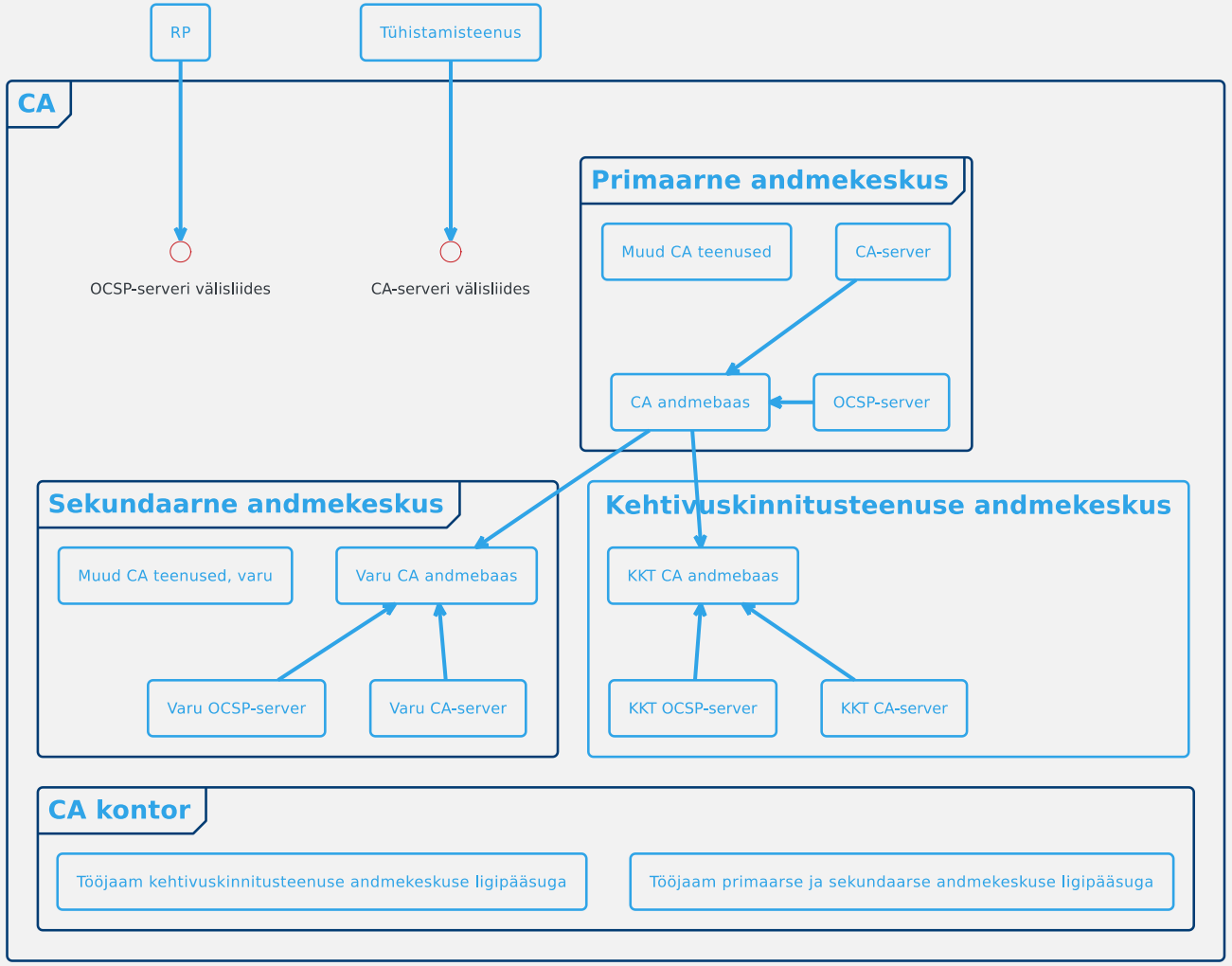
Lahendusvariant 1: vahendusteenus OCSP-proksi



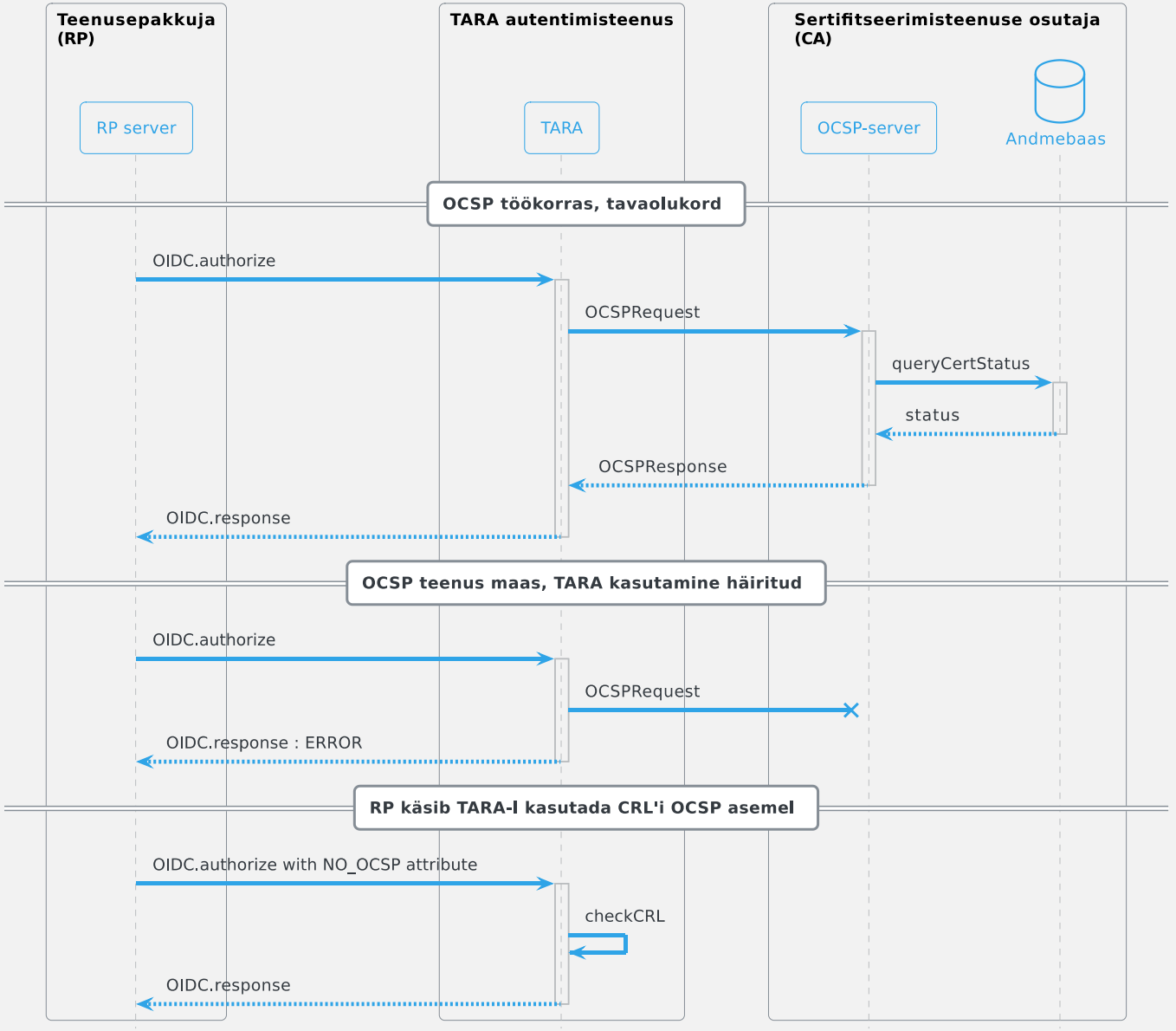
Lahendusvariant 2: riigi kehtivuskinnitusteenus



Lahendusvariant 3: kõrgkäideldav ocsp.ca.ee



Lahendusvariant 4: TARA kontrollide juhtimine



Riskide muutumise kokkuvõte

Risk	proxy.riik.ee	ocsp.riik.ee	Kõrg-käideldav ocsp.ca.ee	TARA kontrollide juhtimine
R1				
R2				
R3				
R4				
R5				

CYBERNETICA

Juriidiline analüüs

- Võrdlesime 4 lahendusvarianti lähtuvalt kehtivuskinnitusteenuse pakkuja isikust:
  - **riik** (1. ja 2. lahendusvariant)
  - **CA** ehk kvalifitseeritud sertifikaate väljastav kvalifitseeritud usaldusteenuse pakkuja (3. ja 4. lahendusvariant)

Juriidiline analüüs

- Eristame kehtivuskinnitusteenust kahel otstarbel:
  - **digitaalne tuvastamine** (autentimine)
    - digitaalset tuvastamist võimaldava sertifikaadi kehtivuse kontrollimiseks RP poolt
    - kehtivuskinnitust ei salvestata
    - põhineb siseriiklikul õigusel (praktiliselt puudub, sestap kohaldatakse analoogia korras eIDASt)
  - **digitaalne allkirjastamine**
    - digitaalset allkirjastamist võimaldava sertifikaadi kehtivuse kontrollimiseks RP poolt
    - kehtivuskinnitus salvestatakse
    - põhineb ELi õigusel (eIDAS)

Juriidiline analüüs

- eIDASe järgi on kehtivusinfo väljastamise kohustus üksnes kvalifitseeritud sertifikaate (ingl k *Qualified Certificates*, QC) väljastaval kvalifitseeritud usaldusteenuse pakkujal (ingl k *Qualified Trust Servise Provider*, QTSP)
  - P.S: eIDASe jõustumisega kaotas kehtivuse selle eelkäija, direktiiv Euroopa parlamendi ja nõukogu direktiiv 1999/93/EÜ elektroonilisi allkirju käsitleva ühenduse raamistiku kohta – sellega seoses kadus käibelt termin “sertifitseerimisteenuse osutaja”.

- Teisisõnu, kehtivusinfo väljastamist ei saa lahutada kvalifitseeritud sertifikaadi väljastanud QTSPst (vähemalt mitte digitaalse allkirjastamise puhul).

Juriidiline analüüs

- **Digitaalne allkirjastamine** – kui riik ei ole ise QTSP ega paku e-allkirja kvalifitseeritud sertifikaatide väljastamise usaldusteenust, ei saa ta kehtivusinfot ise väljastada.
  - Järeldus: 1. ja 2. lahendusvariant ei ole kooskõlas eIDASega.

- **Digitaalne tuvastamine** – kuna autentimine ei ole eIDASe kohaselt usaldusteenus ja autentimise teostamiseks ei nõuta ELi õiguse järgi QC olemasolu, siis on võimalik Eesti õiguse alusel lubada kehtivusinfo väljastamist ka riigi poolt, kes ei ole QTSP.
  - Järeldus: 1. ja 2. lahendusvariant on õiguslikult teostatavad, aga vajavad uue regulatsiooni kehtestamist.
  - Tuleks edasi analüüsida, kas riik suudab ilma QTSP staatuse, sertifikaatide andmebaasi ja vajaliku infrastruktuurita garanteerida eduka autentimise kõrgel tasemel vastavalt eIDASele.

Juriidiline analüüs

- **Kehtivuskinnitus kui elutähtis teenus** – Eesti õiguses eeldatakse, et kehtivuskinnitusteenuse pakkuja on elutähtsa teenuse pakkuja, kui ta on QTSP.
  - Järeldus: 1. ja 2. lahendusvariandi puhul ei saa riik olla elutähtsa teenuse pakkuja ilma QTSP staatuseta.

- **3. ja 4. lahendusvariant** – muudatusi pole võrreldes praeguse olukorraga, sest praegune CA on QTSP ning jätkab kehtivuskinnitusteenuse pakkumist samadel tingimustel.
  - Järeldus: pole vaja põhjalikumalt käsitleda.

Kokkuvõte

- Me ei leidnud häid ning lihtsaid tehnilisi lahendusi, mis töötaksid üldjuhul ning igast aspektist laitmatult.
- Esialgne analüüs näitab, et kõigi riskide riskitaseme vähendamine üheainsa meetmega ei ole võimalik.
- Täiendavate puhver- või vahendus-teenuste loomine riigis eeldab usaldusteenuste turvanõuetega arvestamist.
- Analüüsitud lahendusvariantide või muude üksikute turvameetmete mingis konkreetses piiratud situatsioonis rakendamine võib aga endiselt olla otstarbekas,
    - kui kõik osapooled on riskianalüüsi läbi teinud ning oskavad arvestada muutuvaid või täiendavalt tekkivate riskidega.

Täname!

cybernetica

CyberneticaAS

cybernetica_ee

Cybernetica