EESTI VABARIIK
RIIGI INFOSÜSTEEMI AMET

eID arhitektuurinõukogu

Priit Raspel

RIA arhitektuurinõukogude metsaseminar
20 aprill 2016. a.

Millest räägime?

- Töökorraldus ja muutused eID valdkonnas
- Isikukoodist
- eIDAS autentimismehhanismist
- MOPP, TeRa, KONT
- E-teenuste üldine UX (Martin Paljak)
- Java teegid: DigiDoc4J (Martin Paljak)

Töökorraldusja muutused eID valdkonnas

- AN kokkukutsumisega on olnud probleeme
- Uus kord
  - pikalt ette planeeritud koosolekute ajad
  - koosolekute päevakordade määramise kord
  - koosolekutest teavitamise kord
- Kaadri muudatused
  - analüütik
  - uued projektijuhid
  - SCRUM-master
- Confluence kui koht kus kogu info „saab kokku“

Mis on Confluence's?

- Strateegia
- Riskianalüüs
- Ülevaade kasutatavatest tehnoloogiatest (eesmärgiga jälgida nende arengut)
- Tööplaan
- Koosolekute protokollid/kokkuvõtted
- Arhitektuurinõukogu liikmed, ajagraafik ja protokollid
- Tarkvara dokumendid
- Käimas olevad projektid
- Käitatavad teenused

ISIKUKOOD

- Rootsis juba sai isikukoodi piirkond mõnedel kuupäevadel täis

Küsimuse on päevakorrale toonud sisserände kasv, vahendab DN.

Paljud sünnikuupäevad on juba kasutusel, seega tähendab see maksuametile antud mudeli muutmist. Hetkel on nn libasünnikuupäevaga isikut tõendava dokumendi saanud 2561 inimest.

«Me kutsume üles teisi riike Rootsi süsteemi mitte kasutama,» ütles Ingegerd Widell Rootsi maksuametist.

7. aprill 2016

- EU-s „potensiaalsed 500 milj.“ kodanikku, kes võivad tahta meie infosüsteemidesse siseneda
- Isikukood on sisuliselt viitenumber - viitenumber ei pea sisaldama sisulisi andmeid vaid kõigest järjenumbrit ja kontrolljärku
- Praegune struktuur ajaloolistel põhjustel

Isikukoodi muutmine

- Praegu igas kuupäevas võimalik 999 isikukoodi
- Juba välja antud isikukoodid ei muutu – sellel pole mõtet, pigem tekitab segadust
- Teha muudatus võimalikult väikse mõjuga infosüsteemidele kus neid kasutatakse
- Suurem probleem nende infosüsteemide jaoks, mis eraldavad isikukoodist sugu ja sünnikuupäeva
- Isikukood peab jääma endiselt muutumatuks

1. (lühiajaline) lahendus

- Muudame kuu esitust:
  - Jaanuar 01, 13, 25, 37, 49, 61, 73, 85
  - Veebruar 02, 14, 26, 38, 50, 62, 74, 86
  - …
  - Detsember 12, 24, 36, 48, 60, 72, 84, 96
- Saame igasse päeva juurde 7*999 = 6993 koodi
- Need kes soovivad kuupäeva isikukoodist välja võtta peavad kuu numbrit käsitlema valemiga

IF (mod(<kuu isikukoodis>; 12)=0;12;mod(<kuu isikukoodis>;12))

2. (pikaajaline) lahendus

- Isikukood peab endiselt j
- Muuta isikukood järjenumbriks alates näiteks 9000000001X ja mitte piirata enam isikukoodi pikkust 11-ga. Ainuke piirang on kontrolljärk viimases positsioonis.
- Kehtib reegel, et alates numbriga 9 algavatest koodidest ei sisalda isikukood enam mingit informatsiooni.
- Kõik tuleviku isikukoodid antakse välja sellest piirkonnast
- Ei ole mõtet teha nii, et kodanikele anda koode vanast piirkonnast ja teistele uuest piirkonnast – vastuolu mitte-kodaniku „muutumisel“ kodanikuks.

eIDAS ja piiride ülesus

- EU parlamendi eIDAS määruse eesmärk on suurendada usaldust elektroonsete tehingute vastu EU siseturul, luues ühise aluse riigipiirideülese turvalisele elektroonsele suhtlusele kodanike, ettevõtjate ja ametiasutuste vahel, suurendades sellega avaliku ja erasektori internetipõhiste teenuste, e-äri ja e-kaubanduse tõhusust liidus.

eIDAS skoop ja mõju

- Elektrooniliste allkirjade vastastikune tunnustamine (01.07.2016)
- Piiride ülene autentimine (CEF, 18.09.2018)
- Mõjutab kõiki avalikke e-teenuseid:
  - Teenused mida pakutakse enda kodanikele/ residentidele tuleb avada ka teistele EL kodanikele/residentidele võrdsetel tingimustel.
  - Digiallkirjadest peab aksepteerima kõiki. Kui nõutakse käsitsi antud allkirja siis saab nõuda vaid kvalifitseeritud digiallkirju.

Autentimisvahendite usaldustasemed

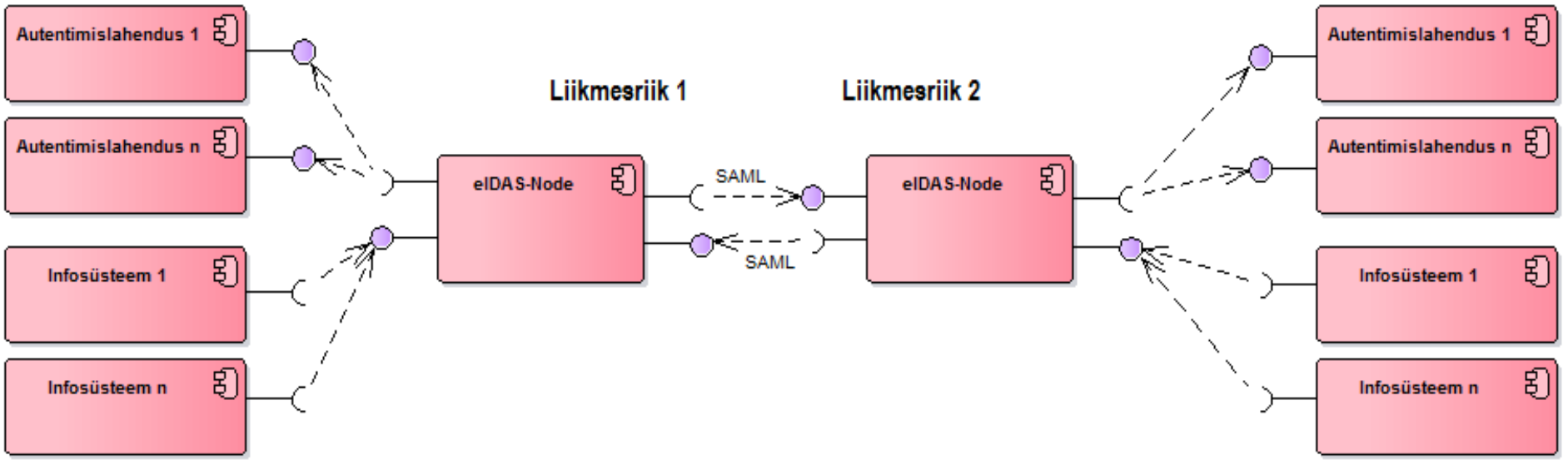
- **Kõrge** – isik on füüsiliselt ja pädevalt tuvastatud, ta omab ja teab (või on) midagi (nt. ID-kaart, m-ID + PIN kood vmt).
- **Märkimisväärne** – isik on enam-vähem tuvastatud, tal on mingi enam-vähem identimise vahend (soft sert, parooli tapeet jms).
- **Madal** – isik on esitanud usutavana tunduvad andmed ja saanud näiteks püsiparooli või korduvate paroolidega paroolikaardi.

CEF eID

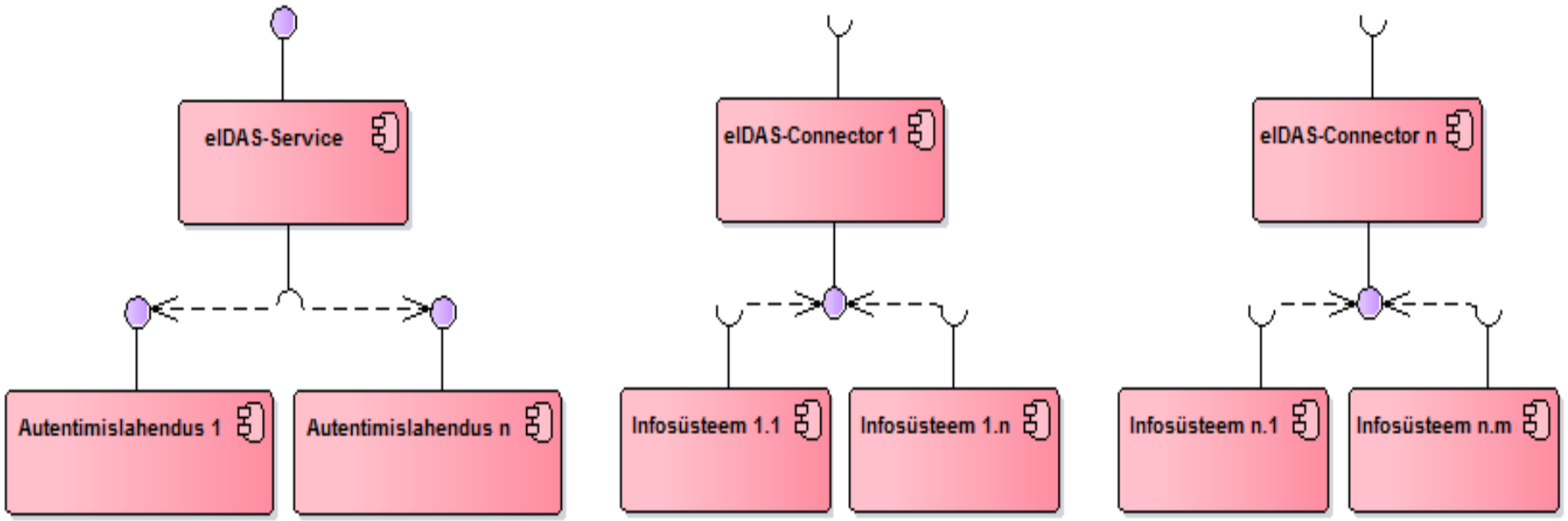
- ISA programmi alla kuuluva CEF eID projekti raames on Euroopa Liidu poolt välja töötatud tuumlahendus liikmesriikide vahelise autentimisvõrgustiku loomiseks ja tarkvaralised komponendid selleks, et luua liikmesriikide halduses oleva tarkvara seoseid tuumlahendusega:
  - Tomcat 6 and 7;
  - JBoss 6 and 7;
  - GlassFish v3,v4;
  - WebLogic 10.3.6, 12.1.2;
  - WebSphere Application Server v. 8.5.5

  https://joinup.ec.europa.eu/software/cefeid/asset_release/cef-eid-ms-integration-package-v10

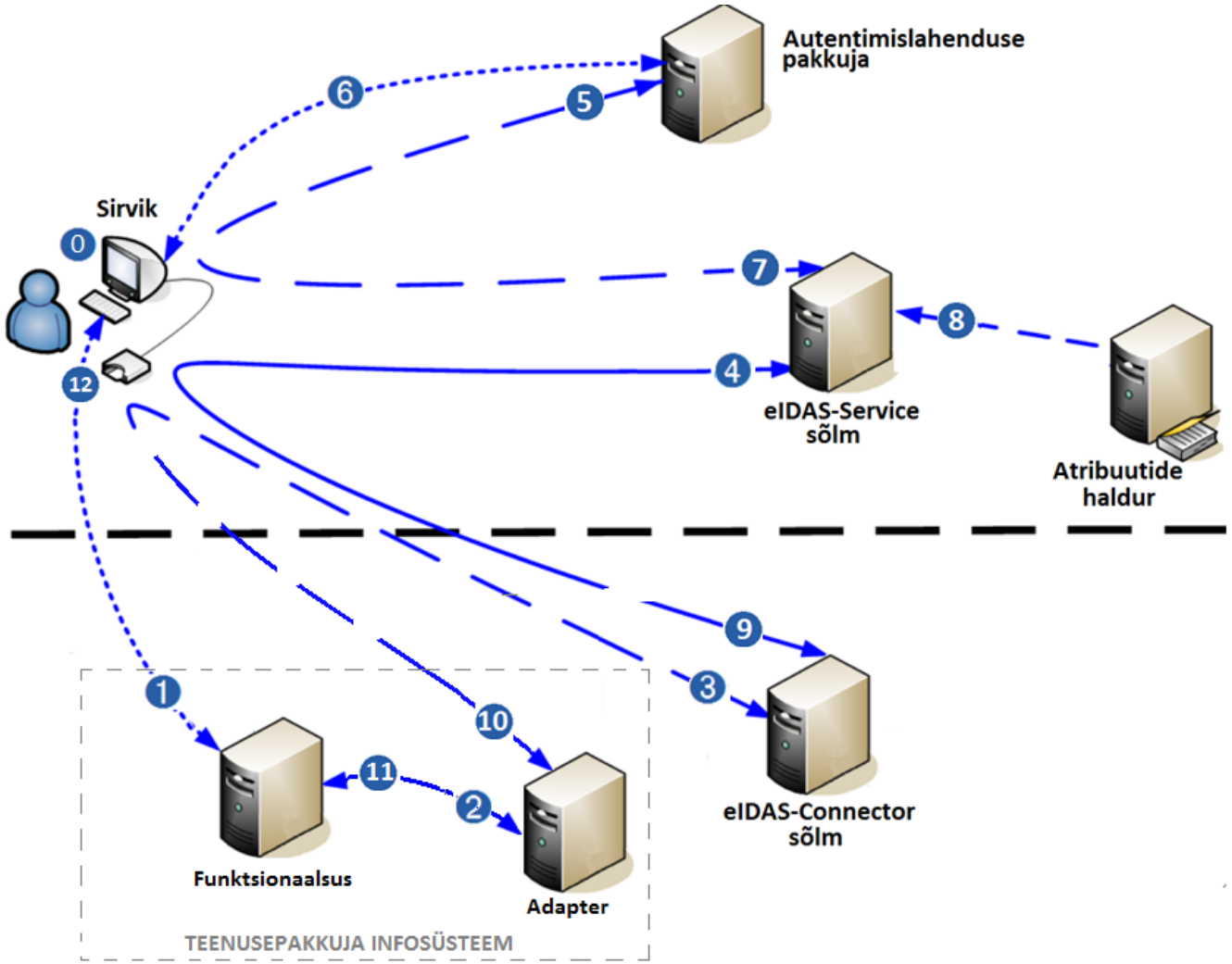
CEF arhitektuur (tsentraalne lahendus)



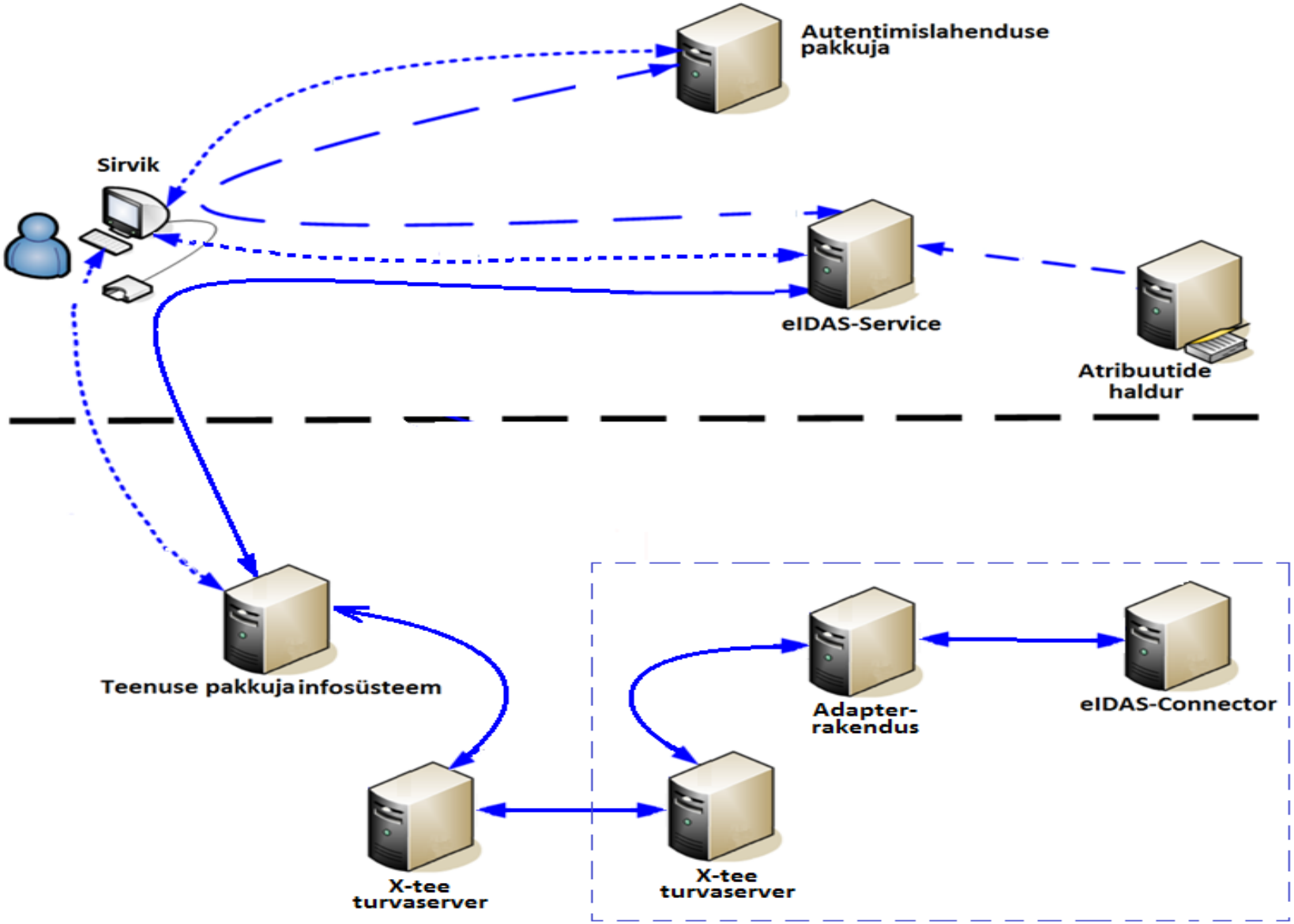
CEF arhitektuur (hajus lahendus)



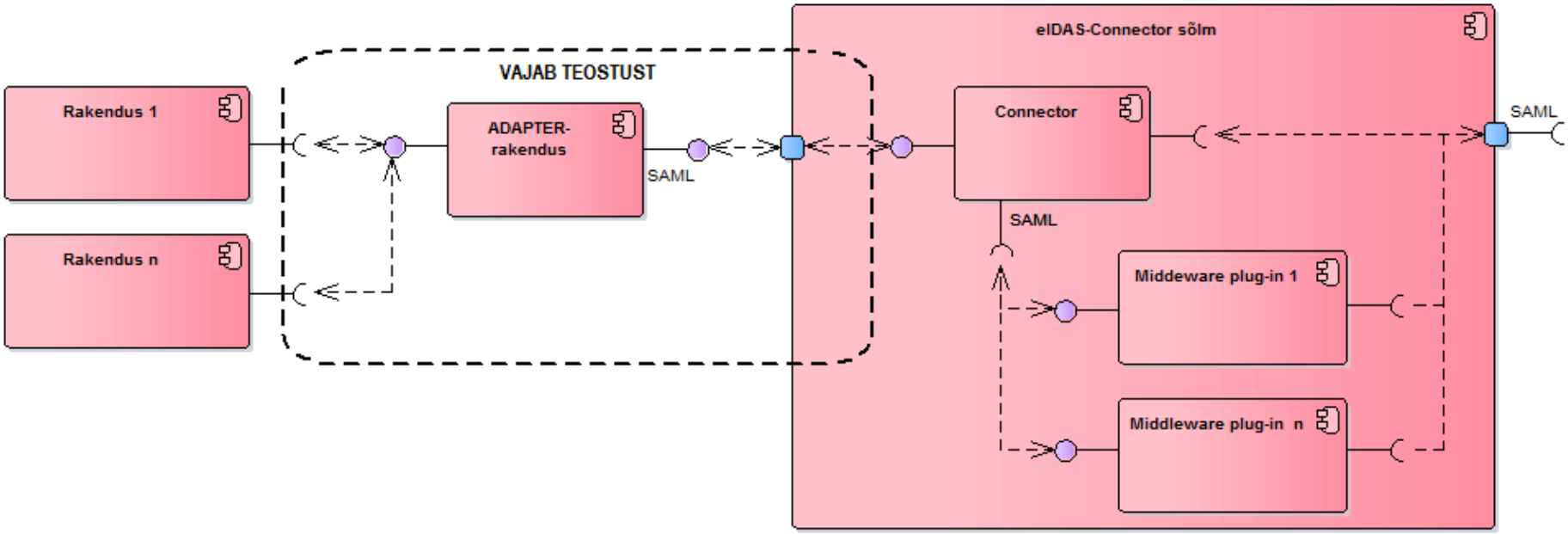
Autentimisprotseduuri andmevoog (1)



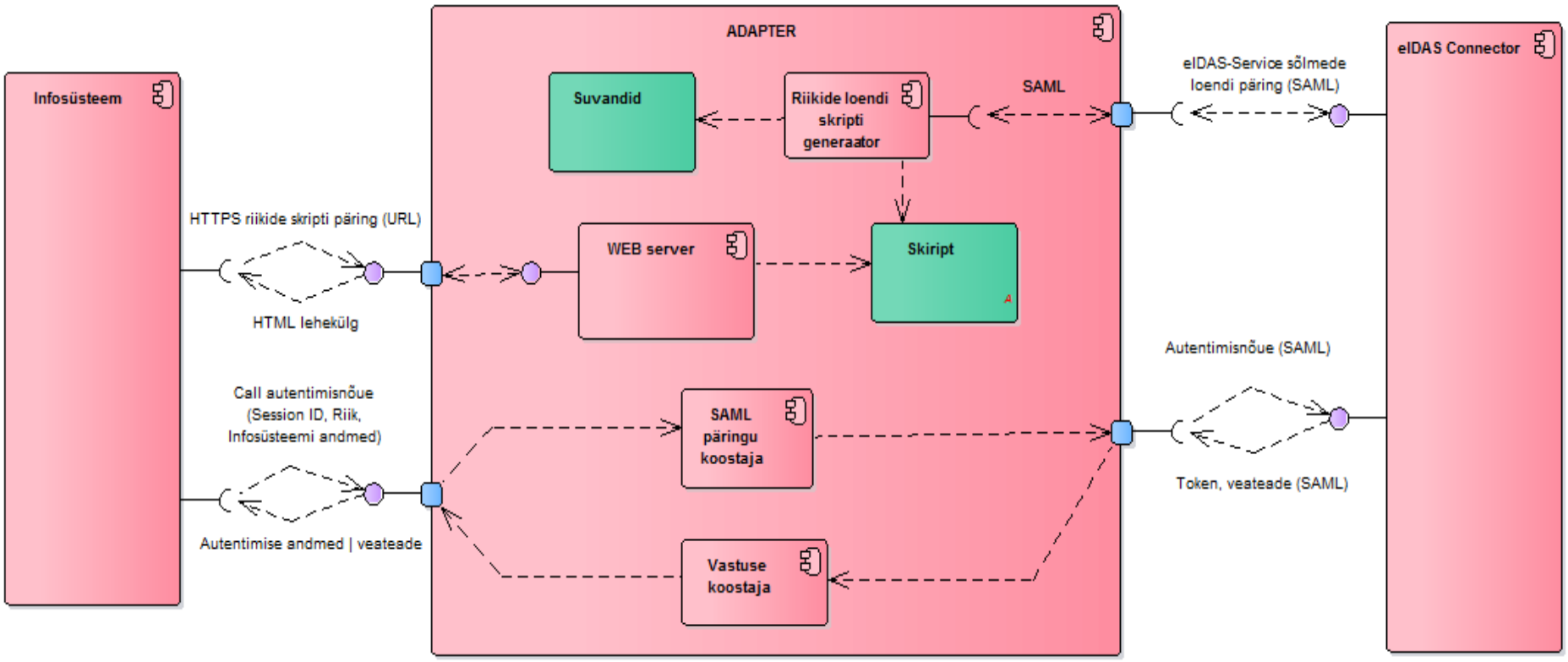
Autentimisprotseduuri andmevoog (2)



eIDAS-Connector sõlme liides



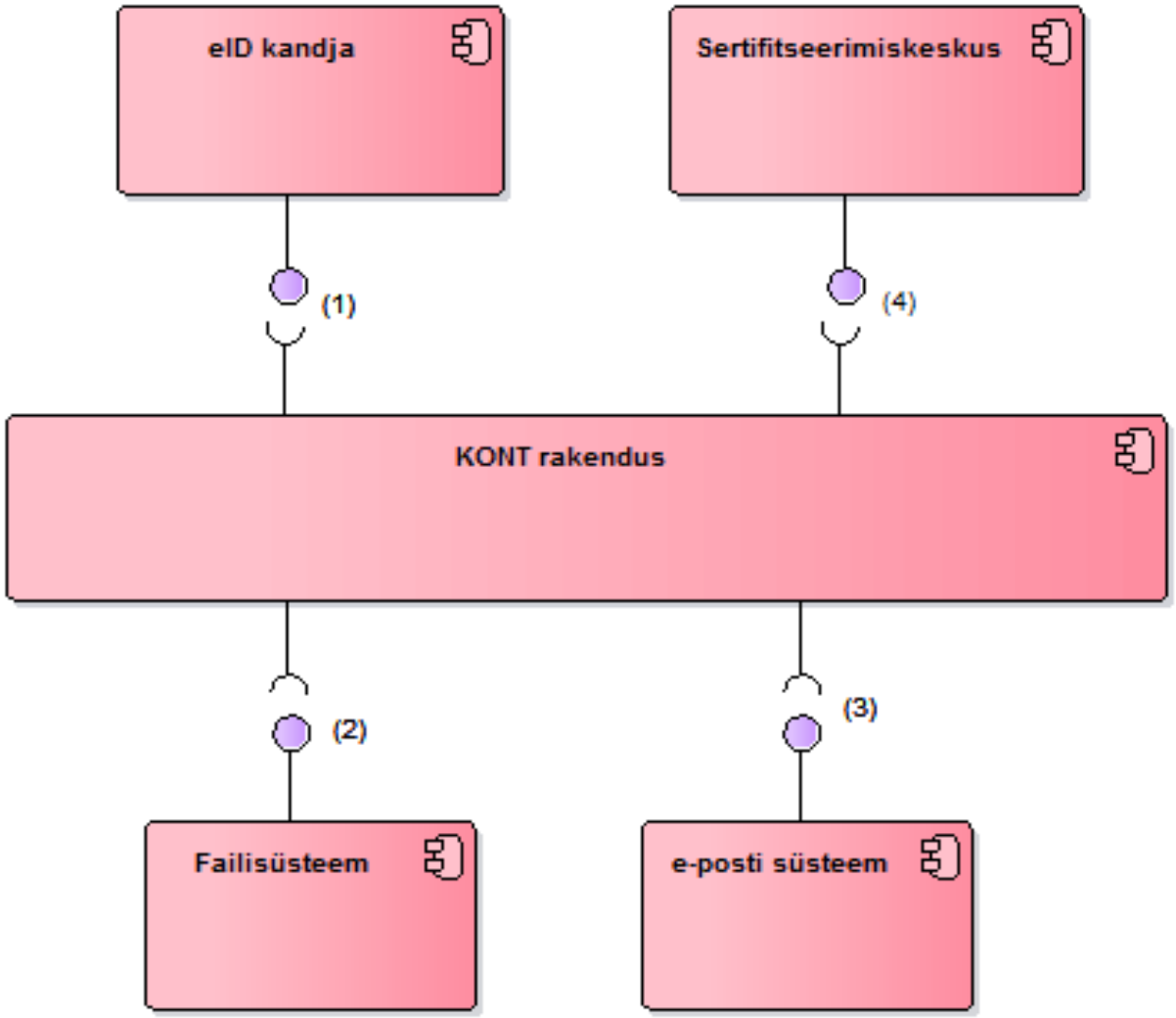
eIDAS eID adapter



eIDAS Node (EiNo) ajakava

- Aprilli lõpuks pakkumiskutse valmis
- Mai lõpuks hanke pakkumuskutse väljas
- Juuni keskpaik leping sõlmitud
- Novembri keskpaigaks eIDAS sõlmed kasutuses

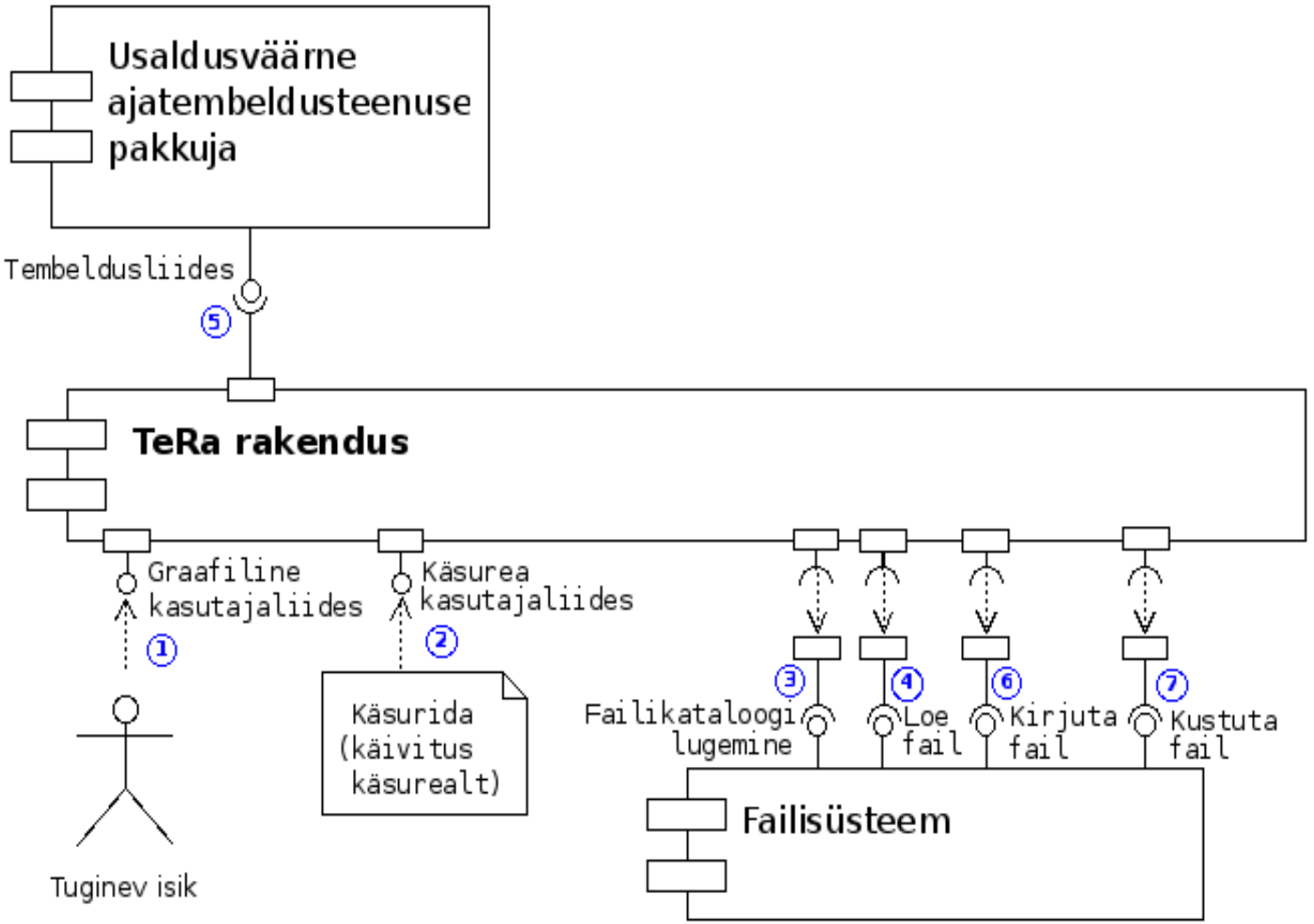
KONT – krüptokonteiner CDOC-na



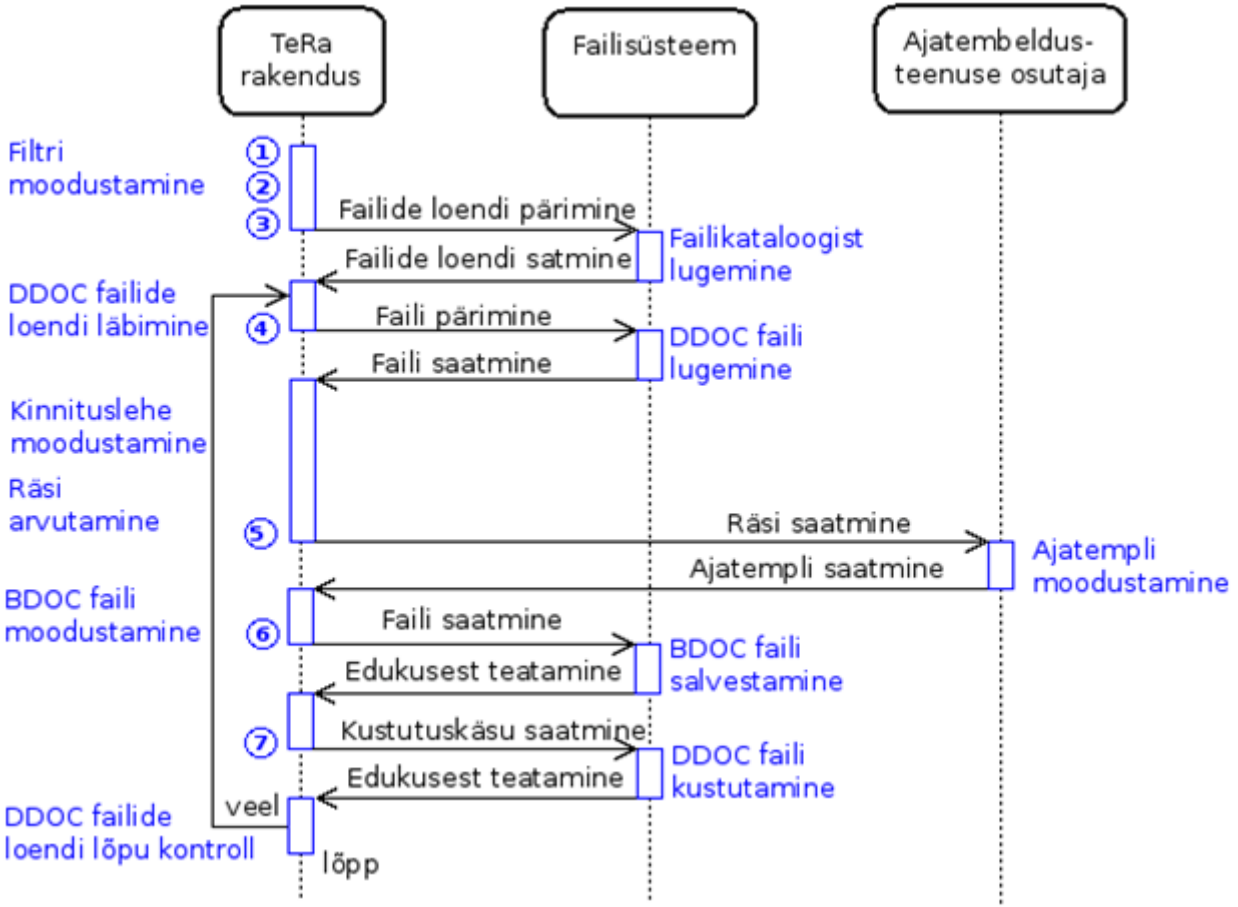
KONT tööd

- Tahame luua kasutajale mugava krüptokonteineri tarkvara
- SDK loomine (Java, C++)
- Analüüs käimas
  - lahendada allika autentsus
- Plaan lõpetada analüüs mai lõpuks
- Esitleme arhitektuurinõukogus
- Arendus raamhanke arenduspartnerite abil

TeRa – ületembeldamise rakendus



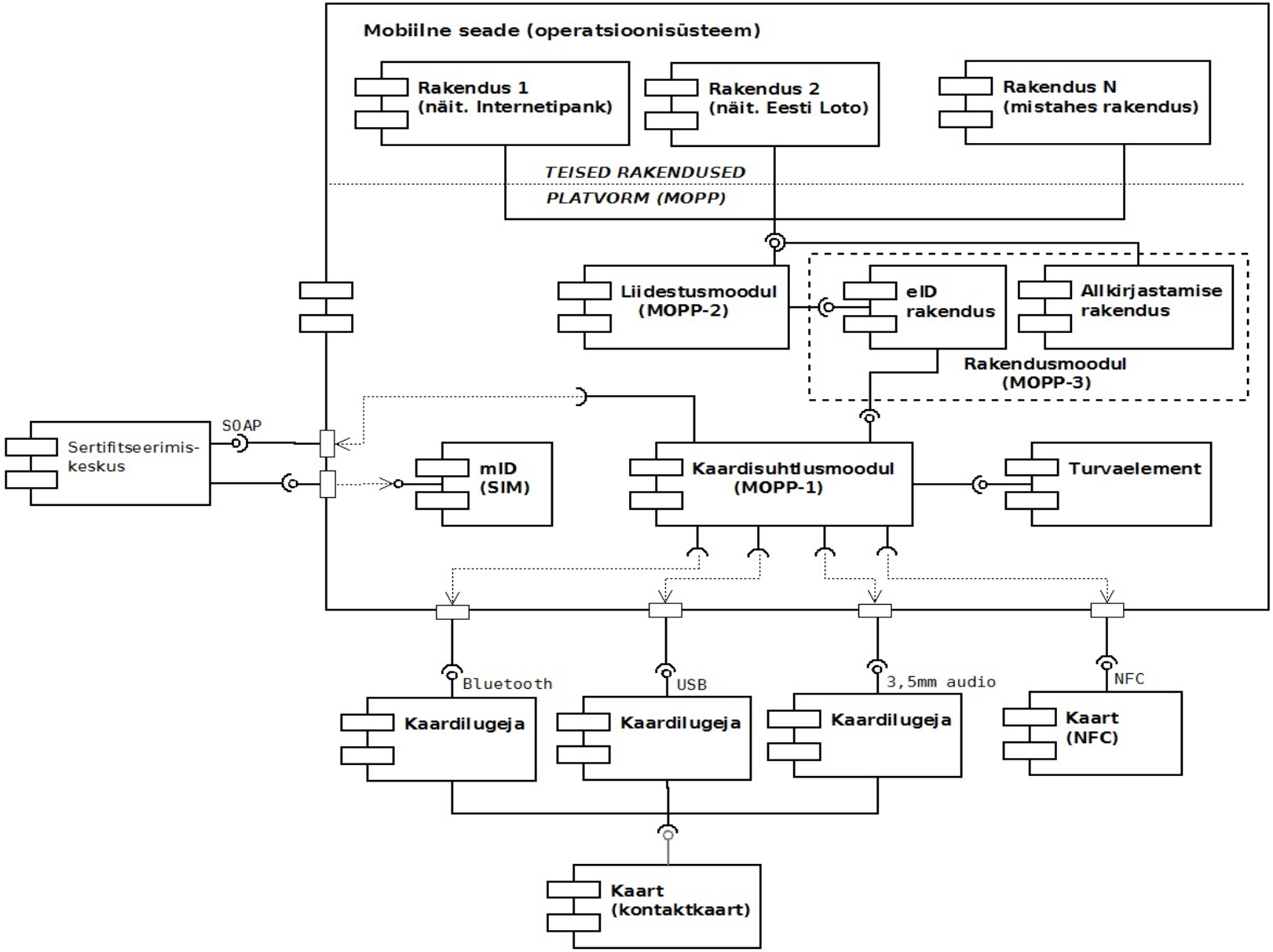
TeRa protsessi voog



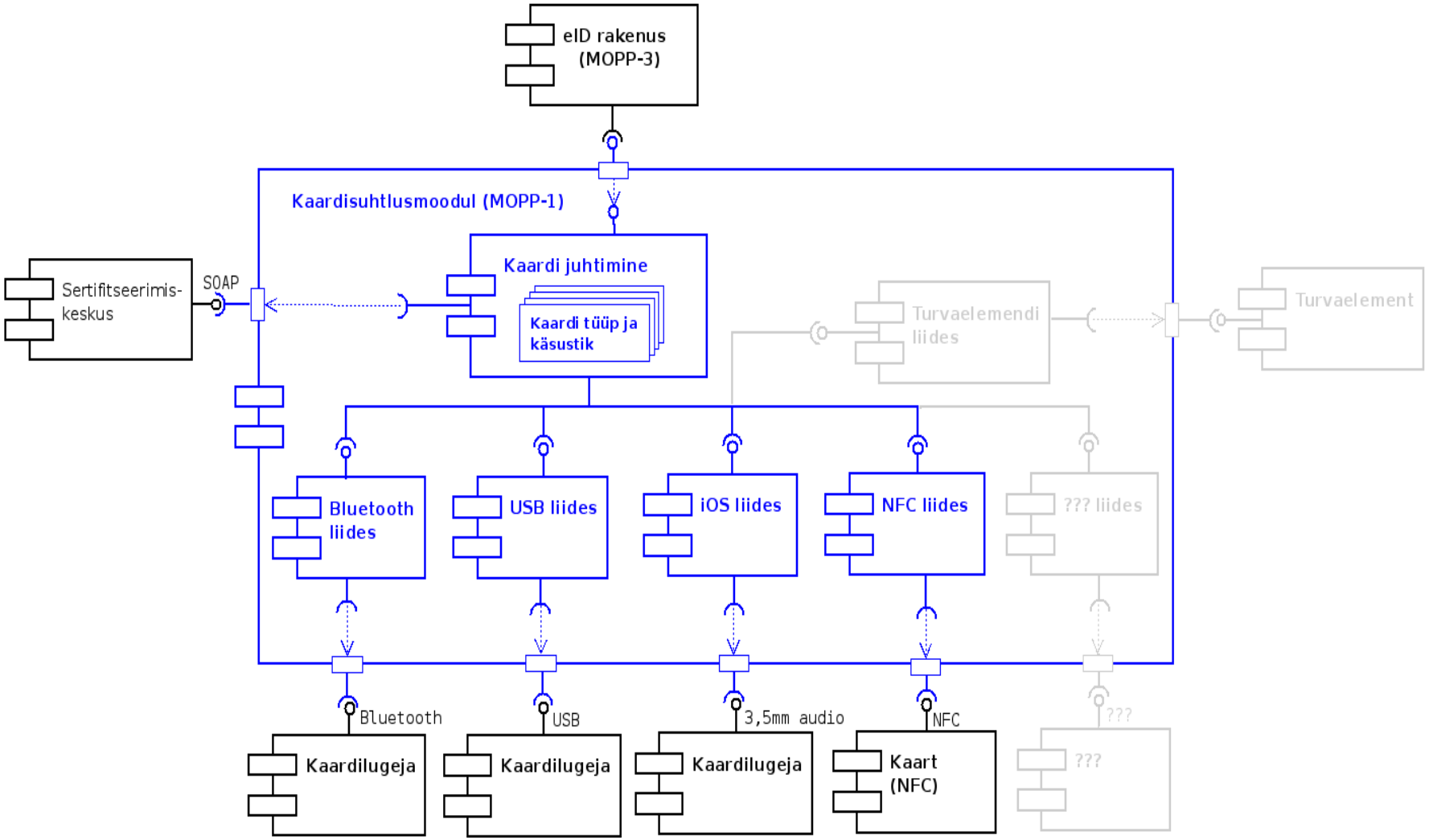
TeRa tööd

- Hange kestab; staatus: kvalifitseerimsprotokoll allkirjastatud
- Hankelepingu sõlmimine mais
- Hanke lõpp sügisel

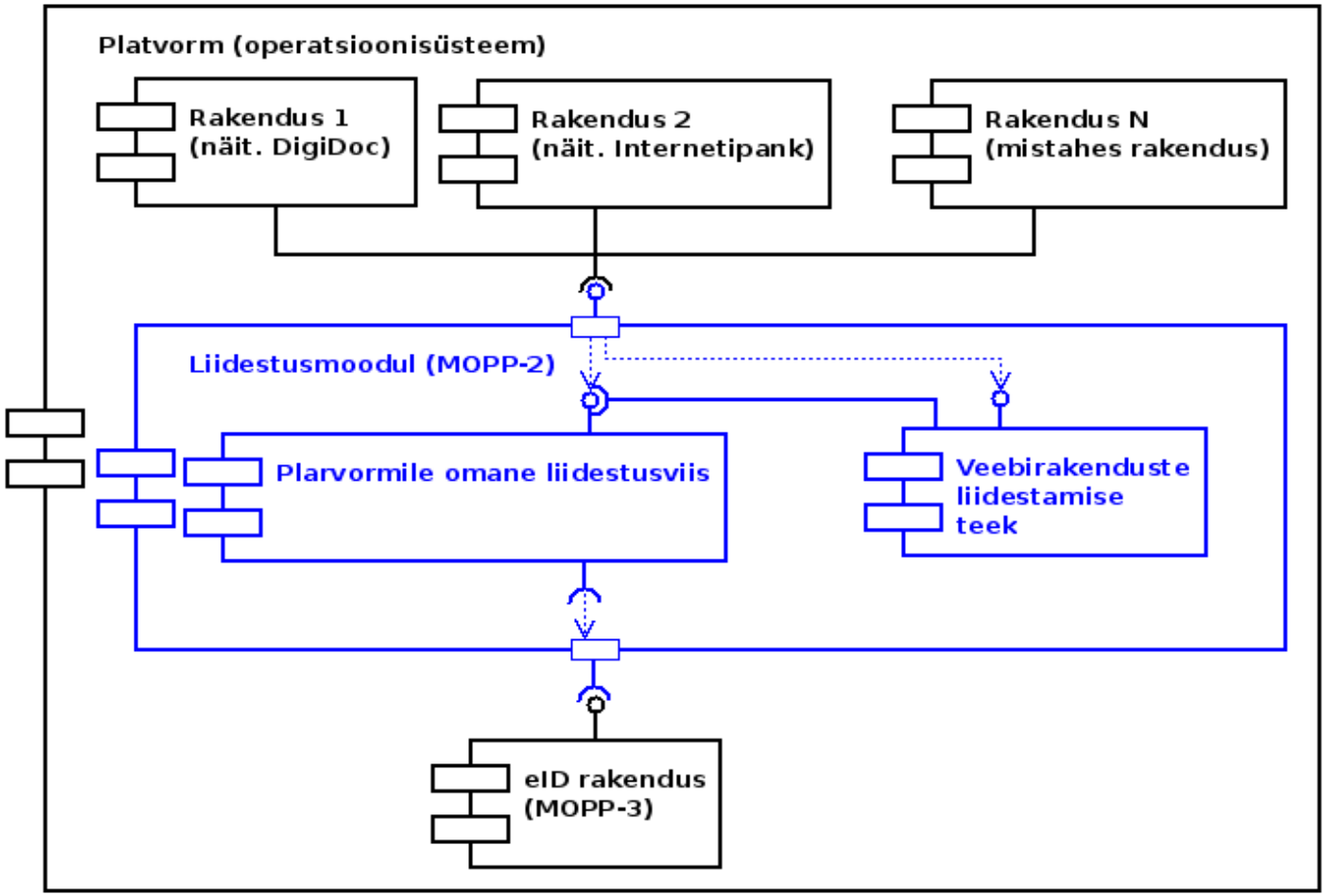
MOPP – ID-kaart mobiilsetes seadmetes



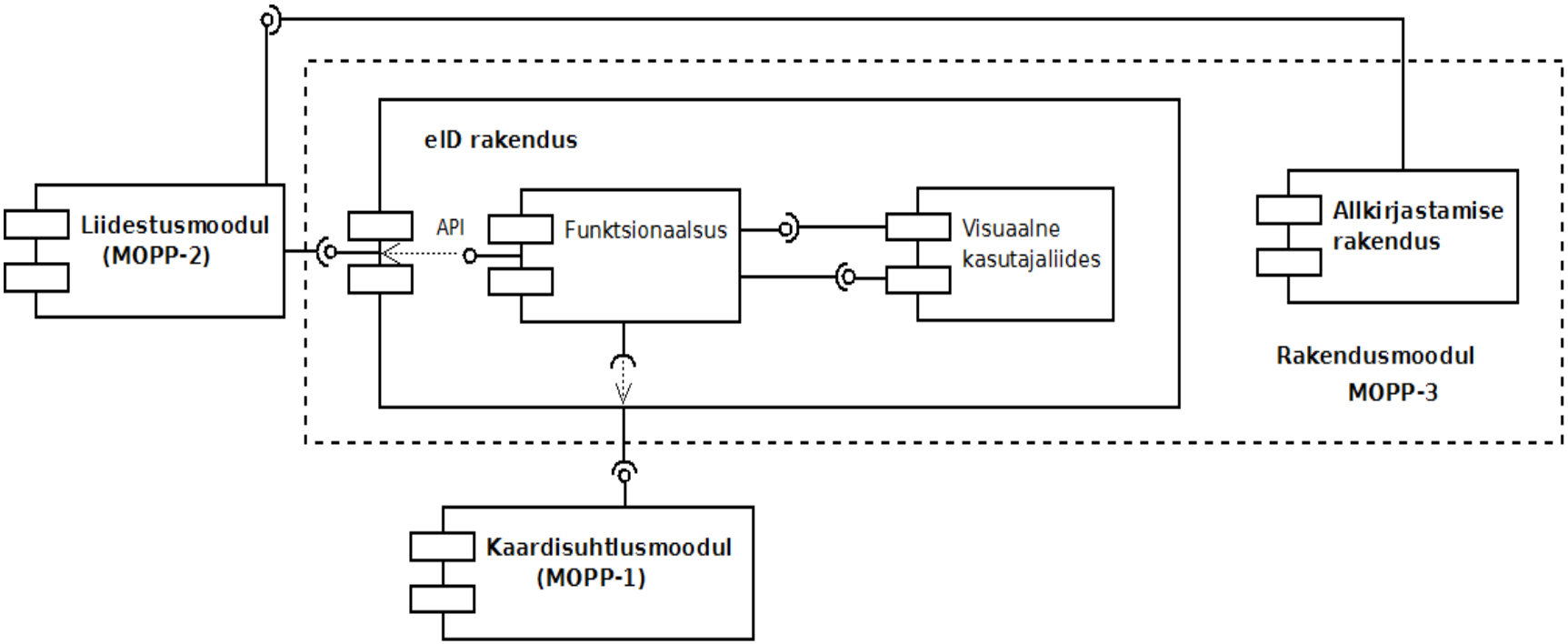
MOPP-1 (kaardisuhtlusmoodul)



MOPP-2 (liidestusmoodul)



MOPP- 3 (rakendusmoodul)



MOPP tööd

- Hanked ebaõnnestusid, kuna raha küsiti 4-5 korda rohkem kui olime planeerinud
- Arendus raamhanke arenduspartnerite abil