



www.sk.ee

Mobiil-ID teenusega seotud uuendused

Liisa Lukin

Lisateenuste ärijuht

Sertifitseerimiskeskus AS

2014. aasta märksõnad:



- Uus Mobiil-ID teenusplatvorm (DigiDocService)
- Mobiil-ID sertifikaatide kehtivusaja pikendamine
- Uus SIM rakendus, uus krüptoalgoritm
- Turvadomeeniga SIM kaart
- Üleminek operaatoripõhiselt lahenduselt tsentraalsele SK taristule



Uus DDS teenusplatvorm



- DigiDocService't kasutab IGA e-teenus, mis toetab Mobiil-ID'd
- Eeldame, et muudatus on vaid SK poolel.
- Testige, et veenduda ühilduvuses!
- Juba novembri jooksul viime üle enamus e-teenuseid
- Kui leiate mitteühilduvuse andke teada!
- Detailsem info Arendusessioonil kl 14:40



MID sertifikaatide pikendamine



- Al 02.2011 väljastatakse 3a sertifikaate
- PPAga on eelkokkulepe, et 2014 aeguvate sertifikaatide kehtivusaega pikendatakse
 - 1K RSA sertifikaadid lõppevad 31.12.2016
- Lõppkasutaja ei pea midagi tegema
- Võimaldab sujuvama ülemineku järgmise generatsiooni SIMile ja sertifikaatidele



Uus SIM rakendus, uus krüptoalgoritm



- 1K RSA → ECC (või 2K RSA)
 - DDOC standard ei toeta ECC
 - Keskkonnad ei toeta ECC ega BDOC
 - 2K RSA pärsib kasutajakogemust
 - SIMil 3 võtmepaari
 - 1K RSA
 - 2K RSA
 - ECC



ECC tulek – mis juhtub?



- BDOC 2.1 formaat kinnitatud 12.2013
 - Teegid
 - Lõppkasutaja tarkvara
- BDOC ja ECC tugi DDS-is IQ 2014
- Testkeskkond 01.2014
 - Testnumbrid
- Väljastamine mitte enne 07.2014



Turvadomeeniga SIM kaart



Operaatori
teenused



Operaatori
turvadomeen

SIM
profiil

USIM
profiil

Mobiil-ID
turvadomeen

Mobiil-ID
rakendus

UICC platform

GlobalPlatform 2.2

JavaCard

Hardware

Mobiil-ID
OTA
platvorm



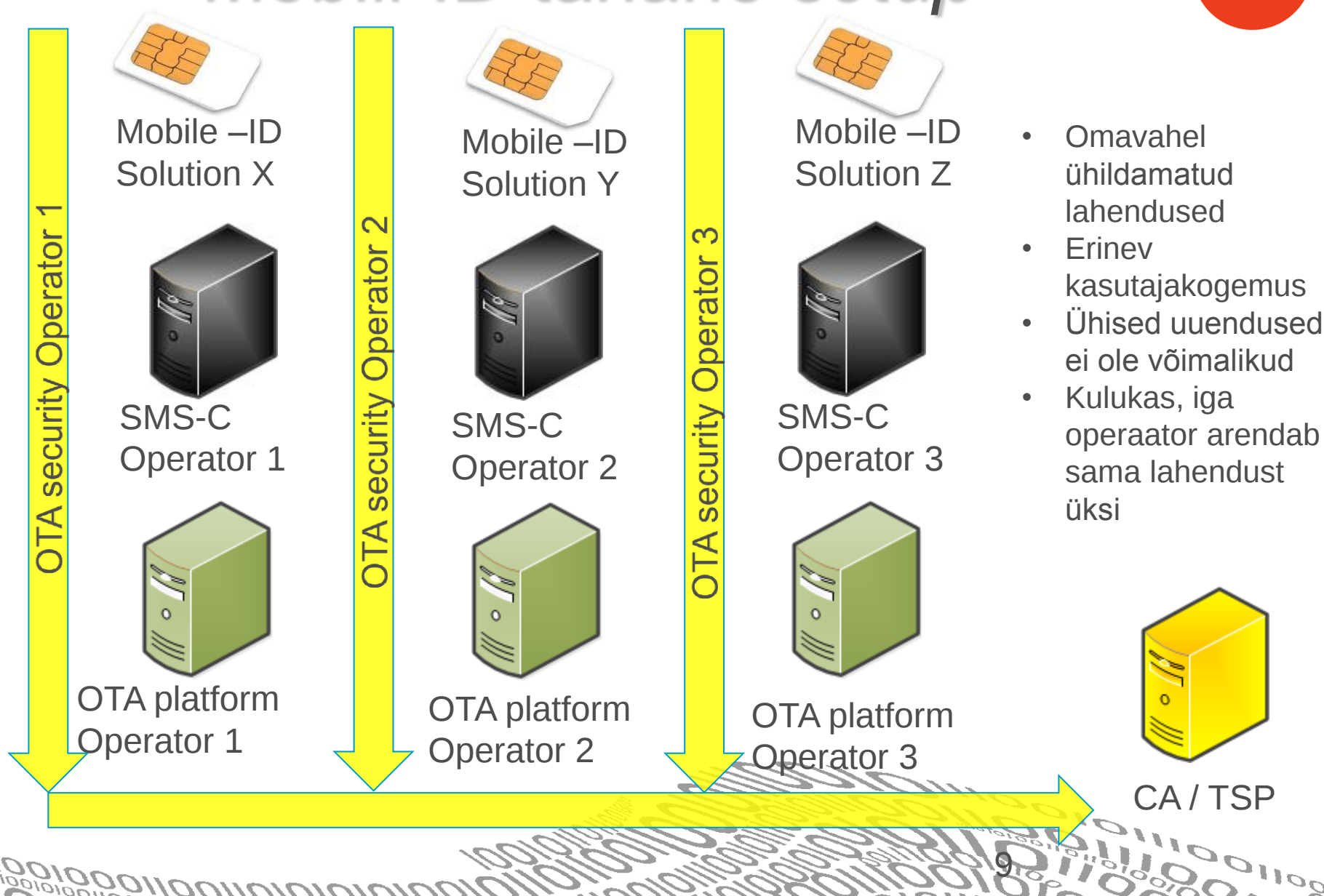
SK OTA platvorm



- Üleminek operaatoripõhiselt lahenduselt tsentraalsele SK taristule
- Tsentraliseeritud lahendus Eesti turule. Kõik operaatorid on potentsiaalsed kliendid.
- Annab võimaluse pakkuda Mobiil-ID teenust või tervikplatvormi välisriikides.



Mobiil-ID tänane setup



- Omavahel ühildamatud lahendused
- Erinev kasutajakogemus
- Ühised uuendused ei ole võimalikud
- Kulukas, iga operaator arendab sama lahendust üksi

Mobiil-ID 2014



Generic
Mobile –ID
SIM application



SMS-C

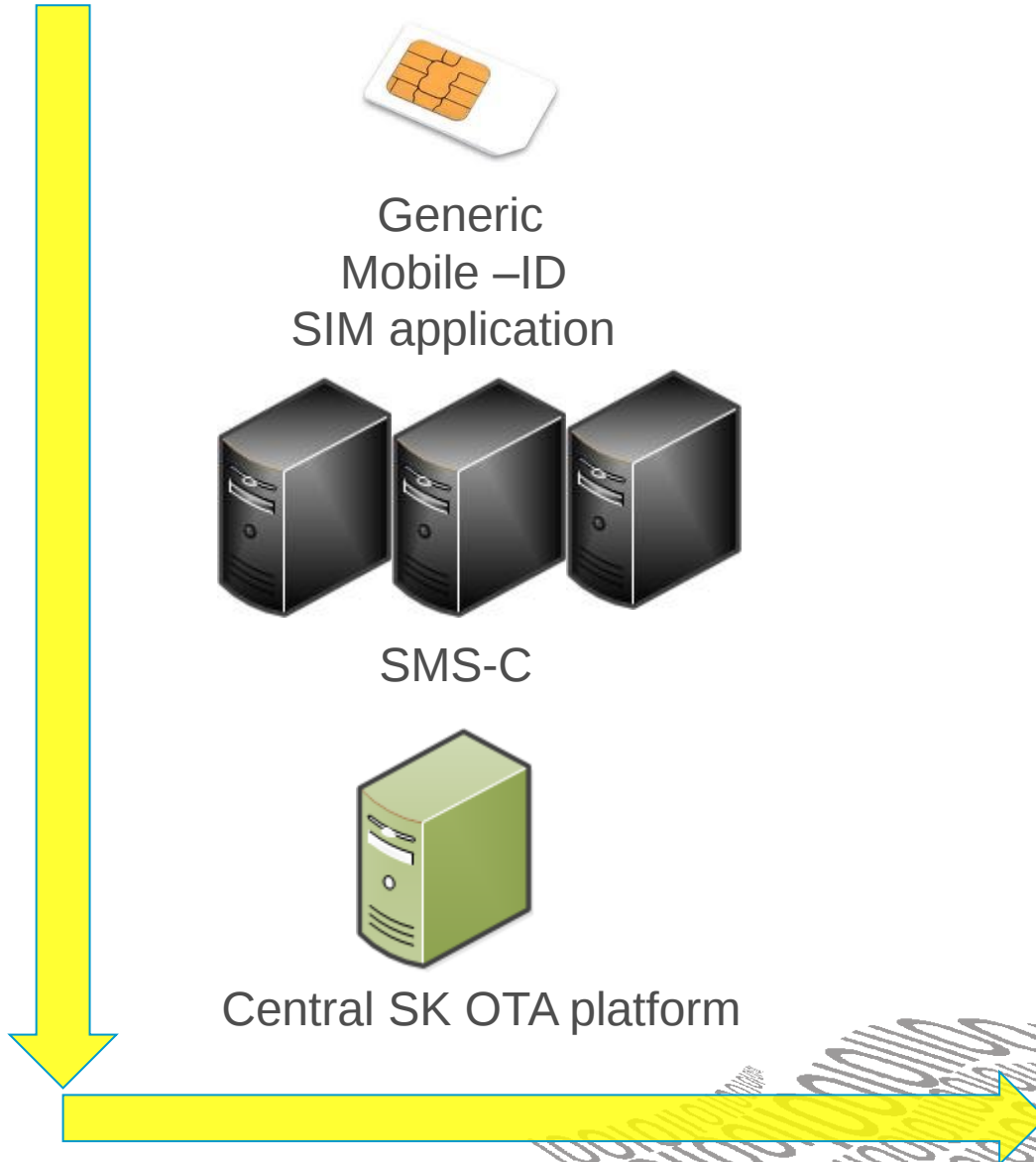


Central SK OTA platform

- Üks lahendus
- Üks SIMi rakendus
- Kergelt uuendatav
- Jagatud arendus- ja halduskulud
- Vähem väliseid sõltuvusi. Lihtsam kontrollida kogu ahelat



CA / TSP





www.sk.ee

Liisa Lukin

Sertifitseerimiskeskus AS