

UUS MOBIIL-ID JA ALTERNATIIVID

URMO KESKEL



TERE!





MOBIIL-ID TAGASIVAADE

2007 ESIMESE
MOBIIL-ID
VÄLJASTUS

2009 ELISA JA
TELE2

2011 RIIKLIK
MOBIIL-ID

2015 UUS SIM JA
MOBIIL-ID
PLATVORM

NUMBRID

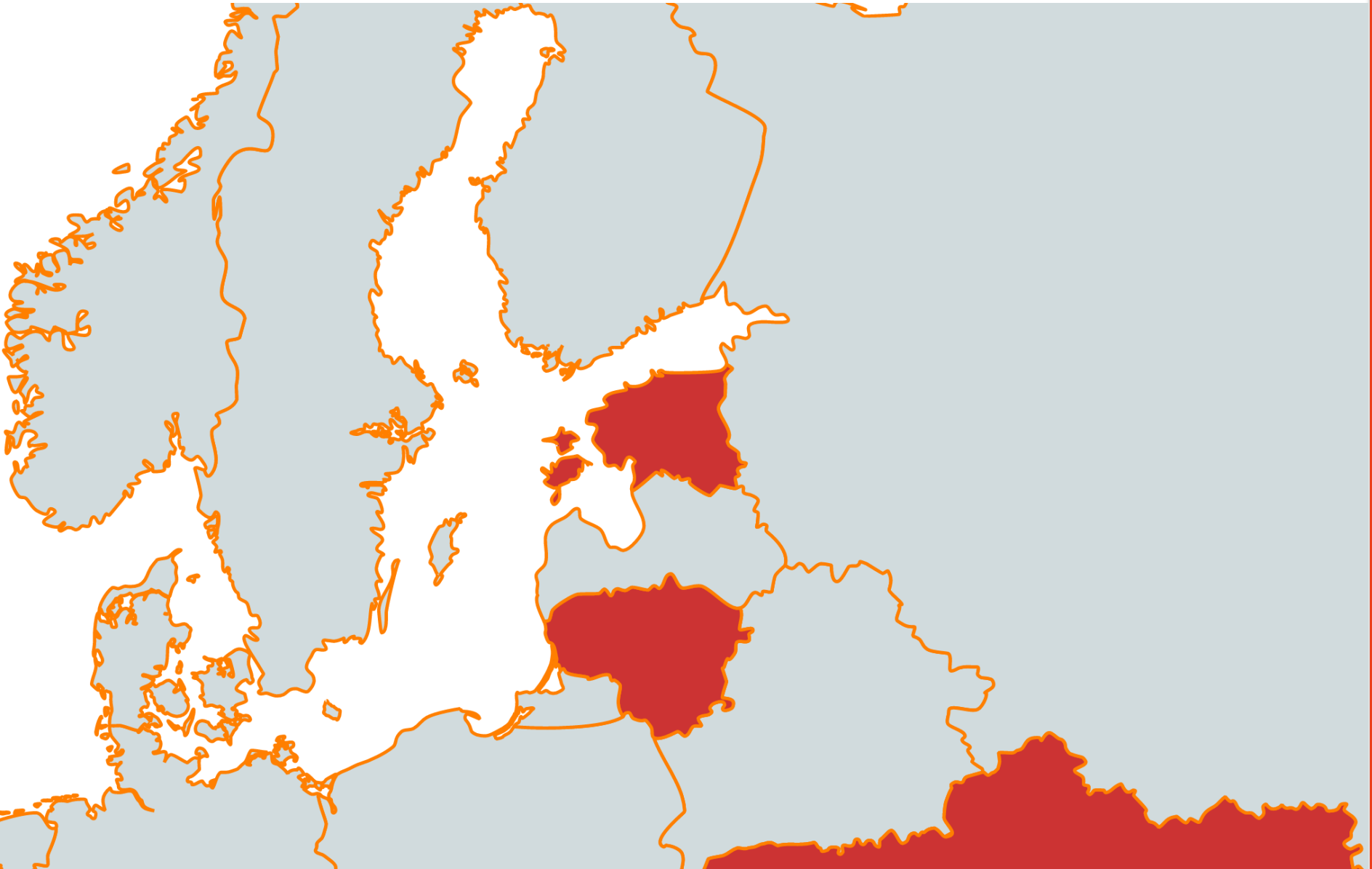
- + Kasutajaid: 69000+
- + Toiminguid kuus 2M+
- + 30 toimingut kasutaja kohta kuus
- + Liidestatud e-teenuseid: 300+
- + 70% kasutajatest kiidab!



VAATAME KAUGEMALE

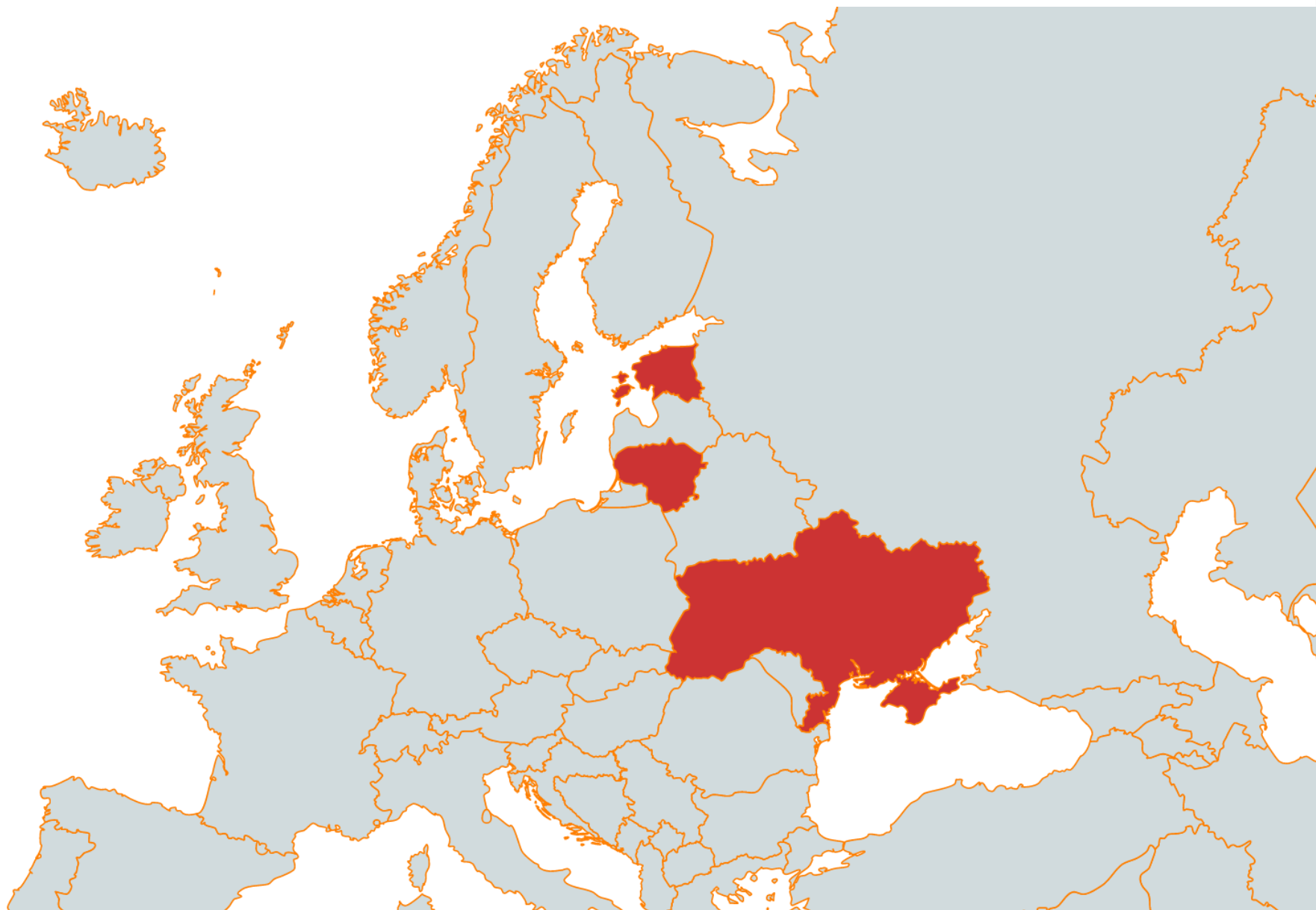


LÄHIREGIOONI



KAUGEMALE

SK



VEEL KAUGEMALE





EXMID PROJEKT

- + Teha Mobiil-ID lihtsamini juurutatavaks
- + Standardsem integratsioon e-teenusega
- + Tulevikukindel Mobiil-ID lahendus



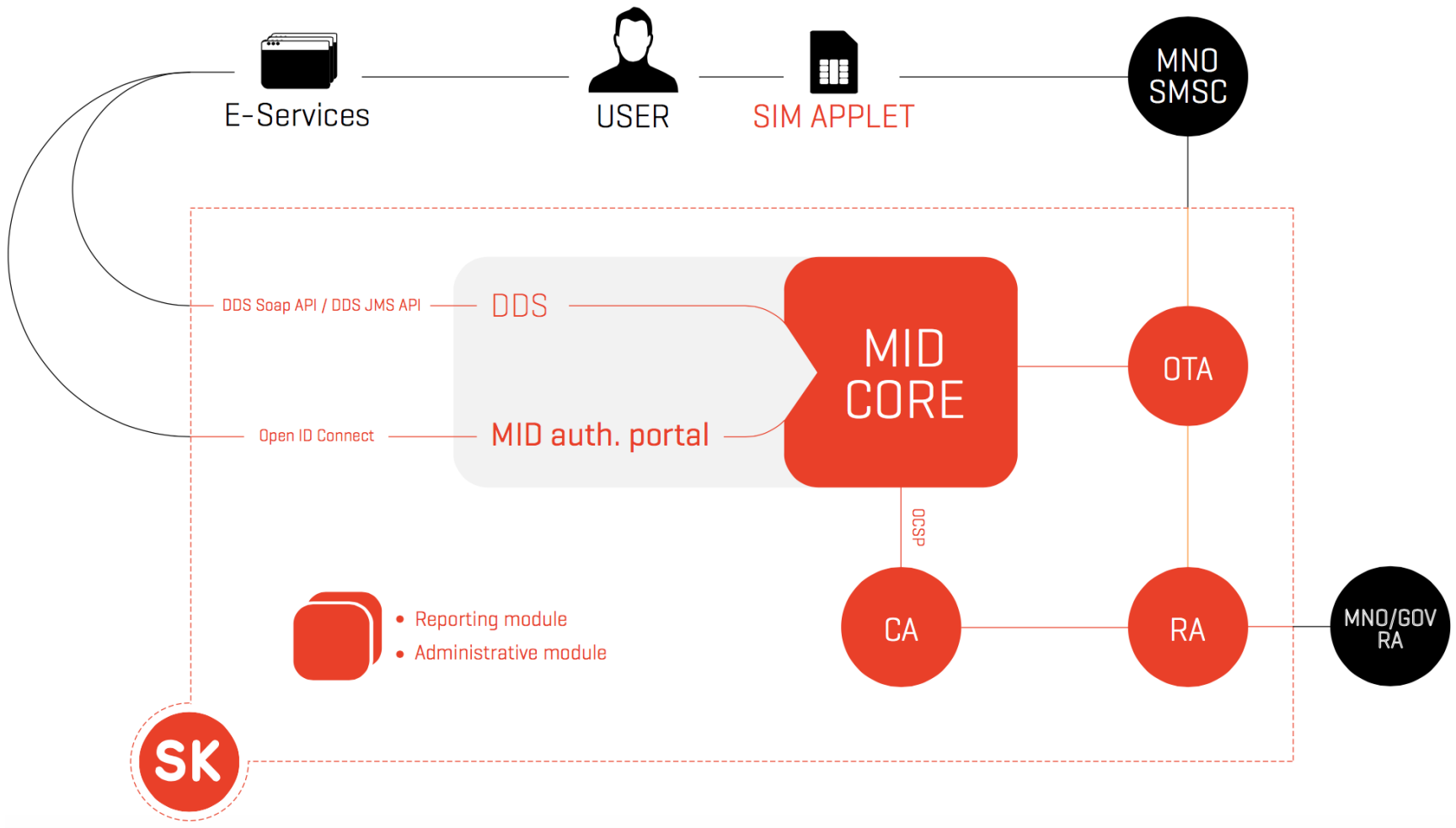
EXMID TULEMUSED

- + OpenID Connect liides
- + Juurutust kiirendav dokumentatsioon
- + Tänase Mobiil-ID alternatiivide turvaanalüüs
- + SIM kaardi ja OTA-ta Mobiil-ID lahenduse *PoC*



CYBERNETICA

BEAUTY OF THE SYSTEM



OPEN-ID CONNECT

LIIDES

- + Identiteedi kiht OAUTH 2.0 protokollil
- + REST/JSON sõnumid
- + Spec ja lisainfo: <http://openid.net/connect/>
- + Suurematest kasutavad: Google, PayPal, eBay
Microsoft, Amazon



LIHTSAM ALTERNATIIV

Spets SIM-i ei taha, kuid kuhu siis panna võtmed?

- + Telefoni
- + Telefoni riistvaralisse turvamoodulisse
- + Mälukaardile
- + Serverisse
- + *Õppida pähe*
- + Jagame mobiiltelefoni ja serveri vahel!

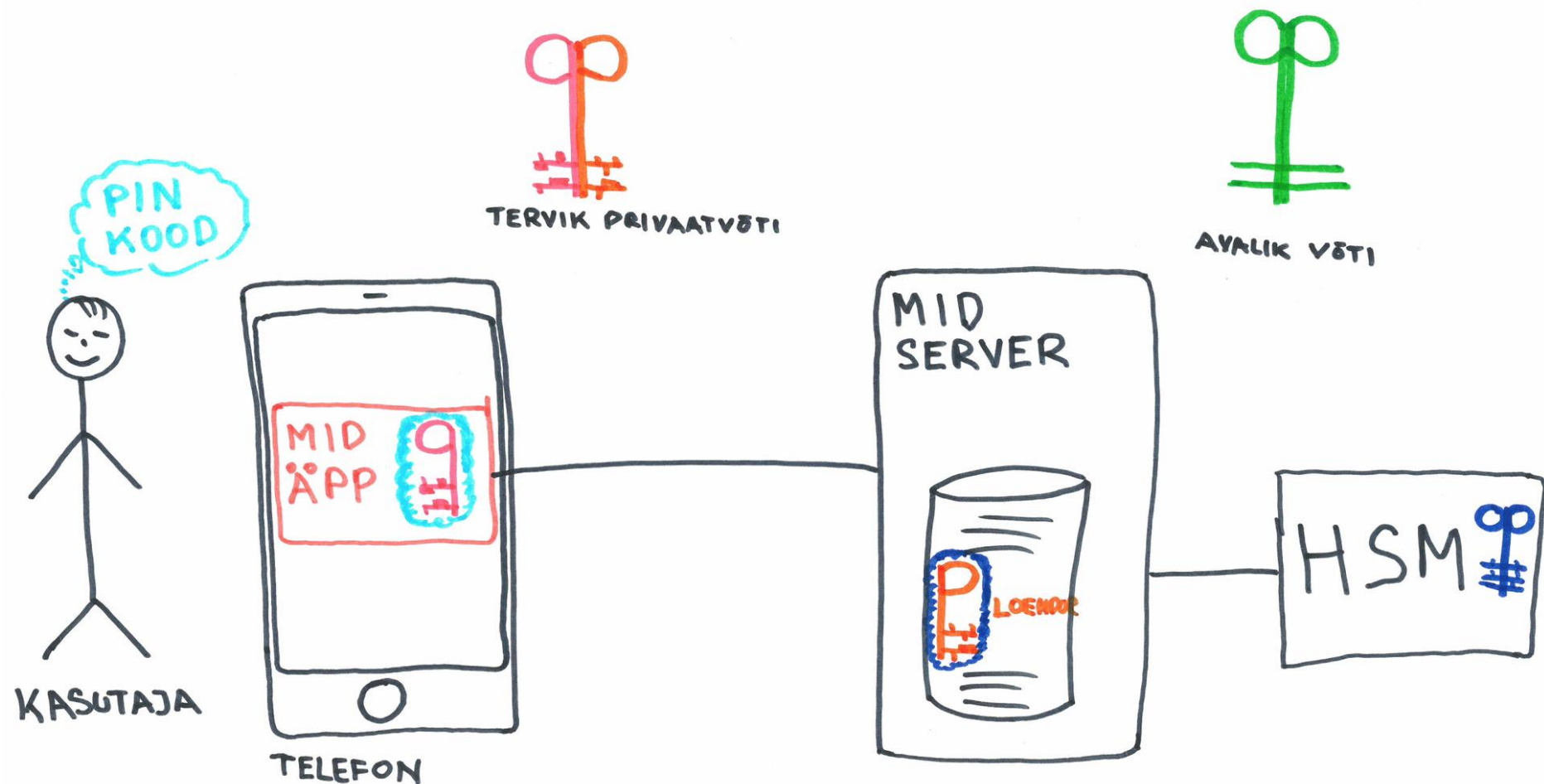
NÕUDED LAHENDUSELE

- + Kasutatav kõigis nutitelefonides
- + Telefonis olev võtmeosak kaitstud PIN koodiga
- + PIN koodi korduvsisestuse katsed tõkestatud
- + Tulemus standardne ja ühilduv EID infraga

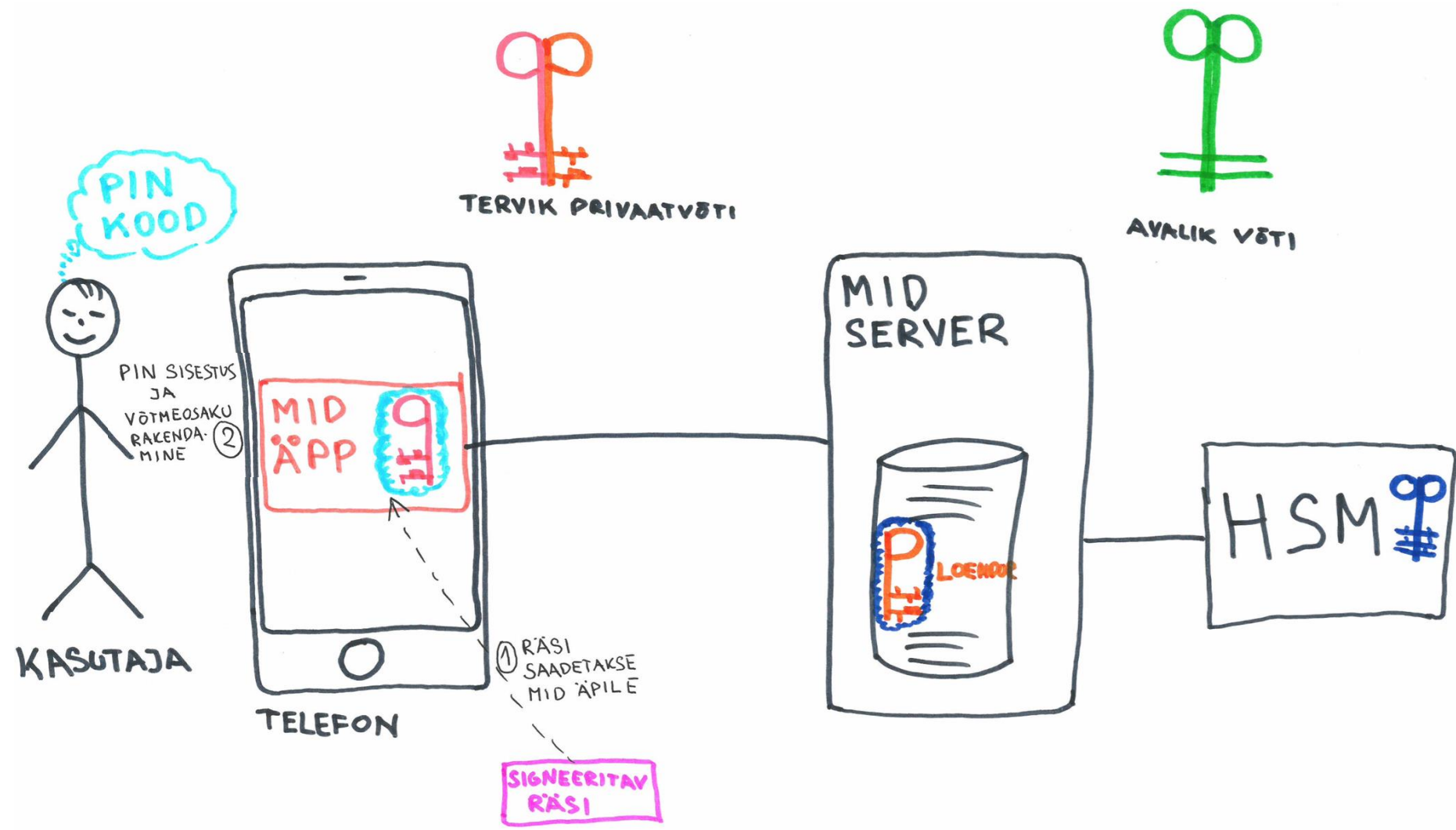
KRÜPTOGRAAFILISED ALUSED

- + Baseerub saladuse jaostamise ja lävisüsteemide mudelitel
- + Valdkonna põhjapanevad teadusartiklid:
 - Adi Shamir. „How to share a secret.“, 1979
 - Blakley, G.R. „Safeguarding cryptographic keys“, 1979
 - Shoup, V. „Practical RSA threshold signatures“, 2000

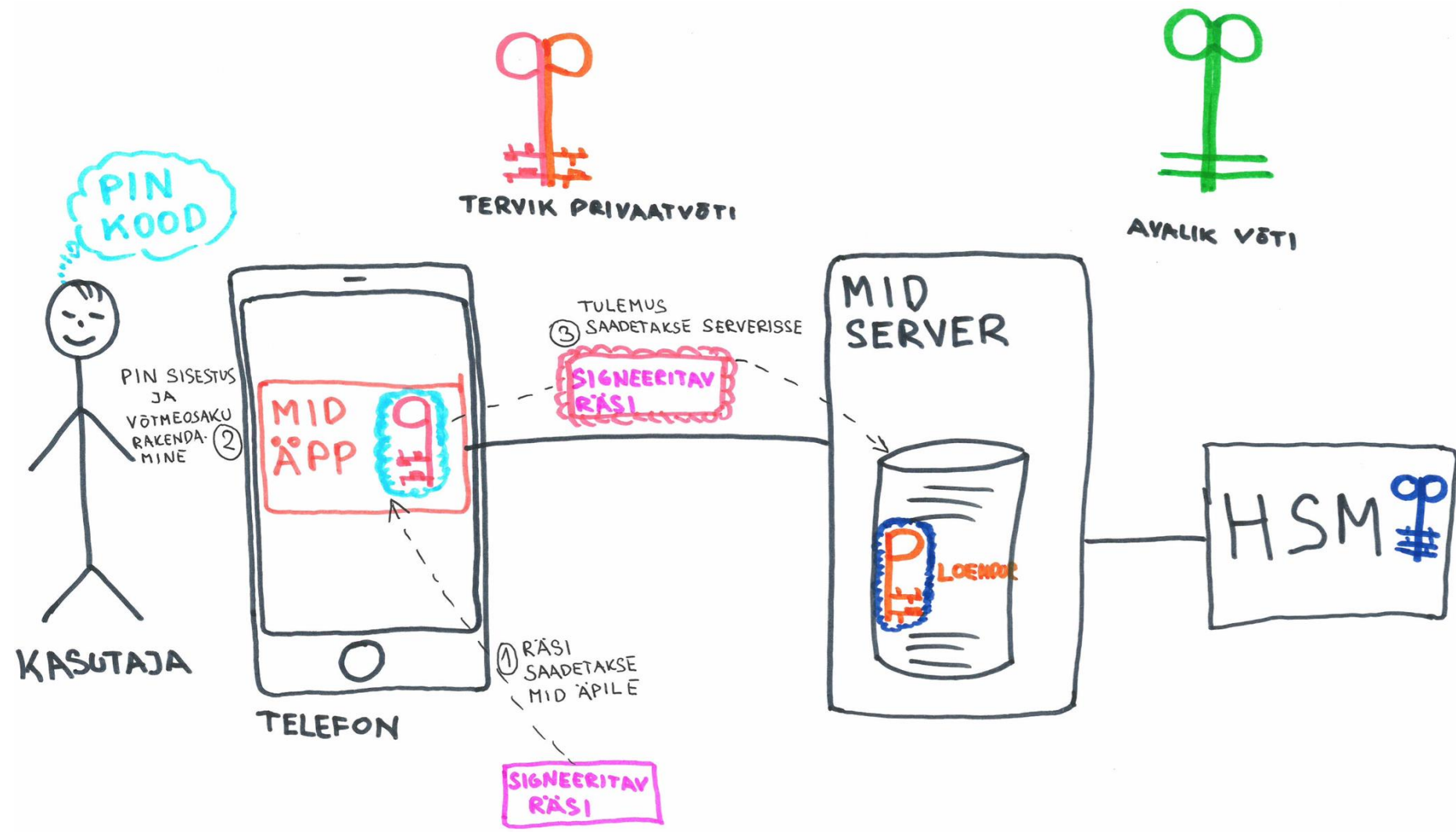
LIHTSUSTATUD SKEEM



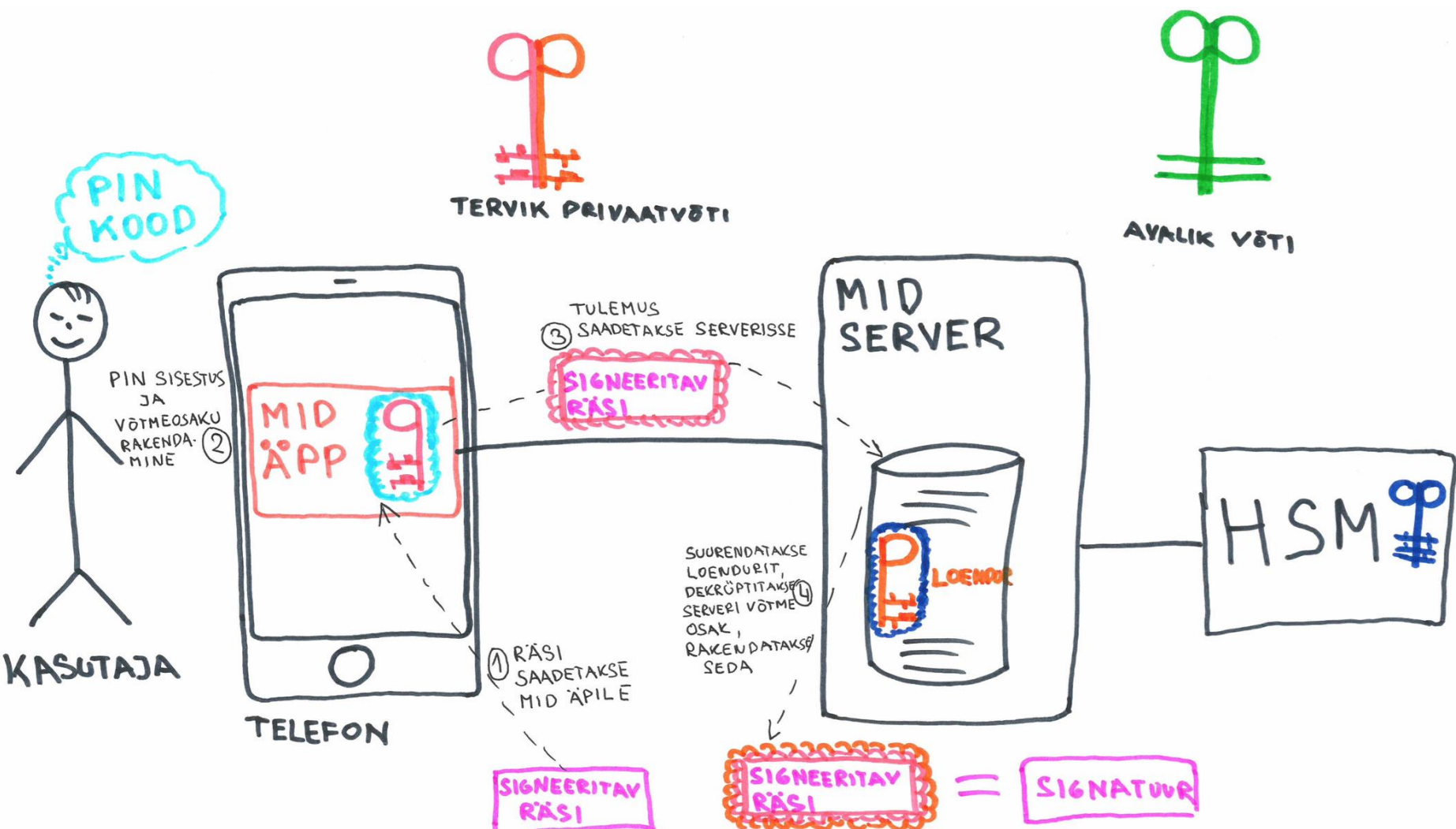
LIHTSUSTATUD SKEEM



LIHTSUSTATUD SKEEM



LIHTSUSTATUD SKEEM



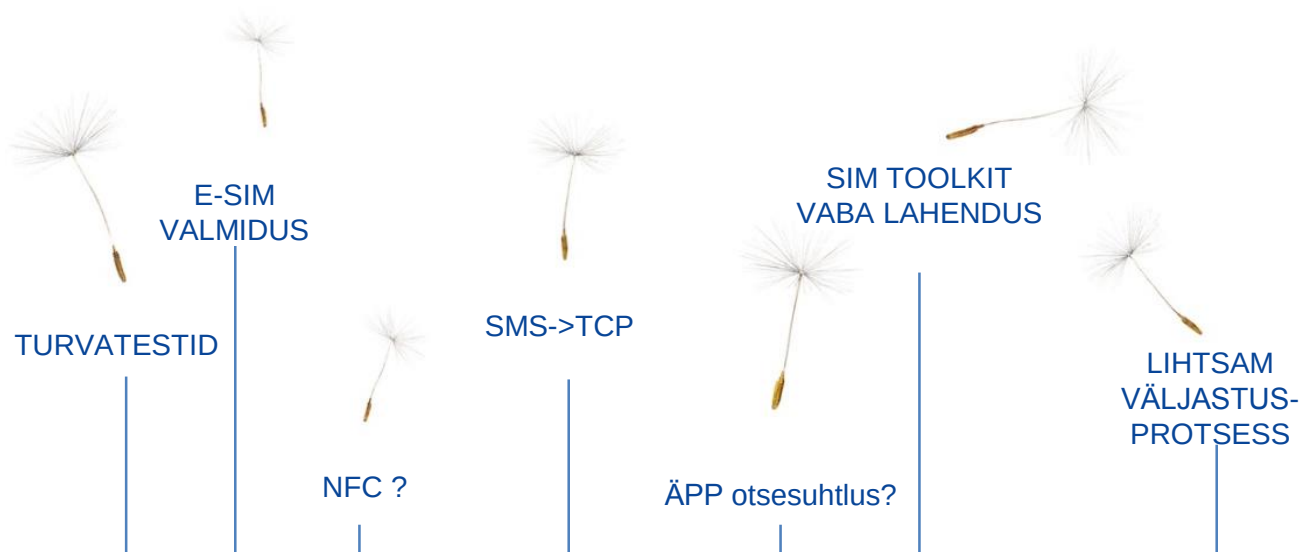
POC KOKKUVÕTE

- + Piisavalt teadusartikleid
- + Teostatav RSA puhul, tõenäoliselt ka ECC-ga
- + Operatsioonide ajad mõistlikud
- + Tulemus ühilduv DigiDoc tarkvaraga
- + Kas EIDAS'e mõttes on QSCD ?

TEINE KAUSS ON VEEL ...



SIM PÕHISE MOBIIL-ID ARENG



MOBIIL-ID APPLETI TURVATESTID

- + TÜViT valitud partneriks
- + 2015 aasta lõpuks lähtekoodi audit
- + 2016 I PA rakenduse turvatestid



LIHTSAM VÄLJASTUSPROTSESS

- + Paberivaba taotlemine
- + Kogu protsess võimalik lõptada operaatori juures
- + Riigilõivu võtmine 1 kord 5 aasta jooksul

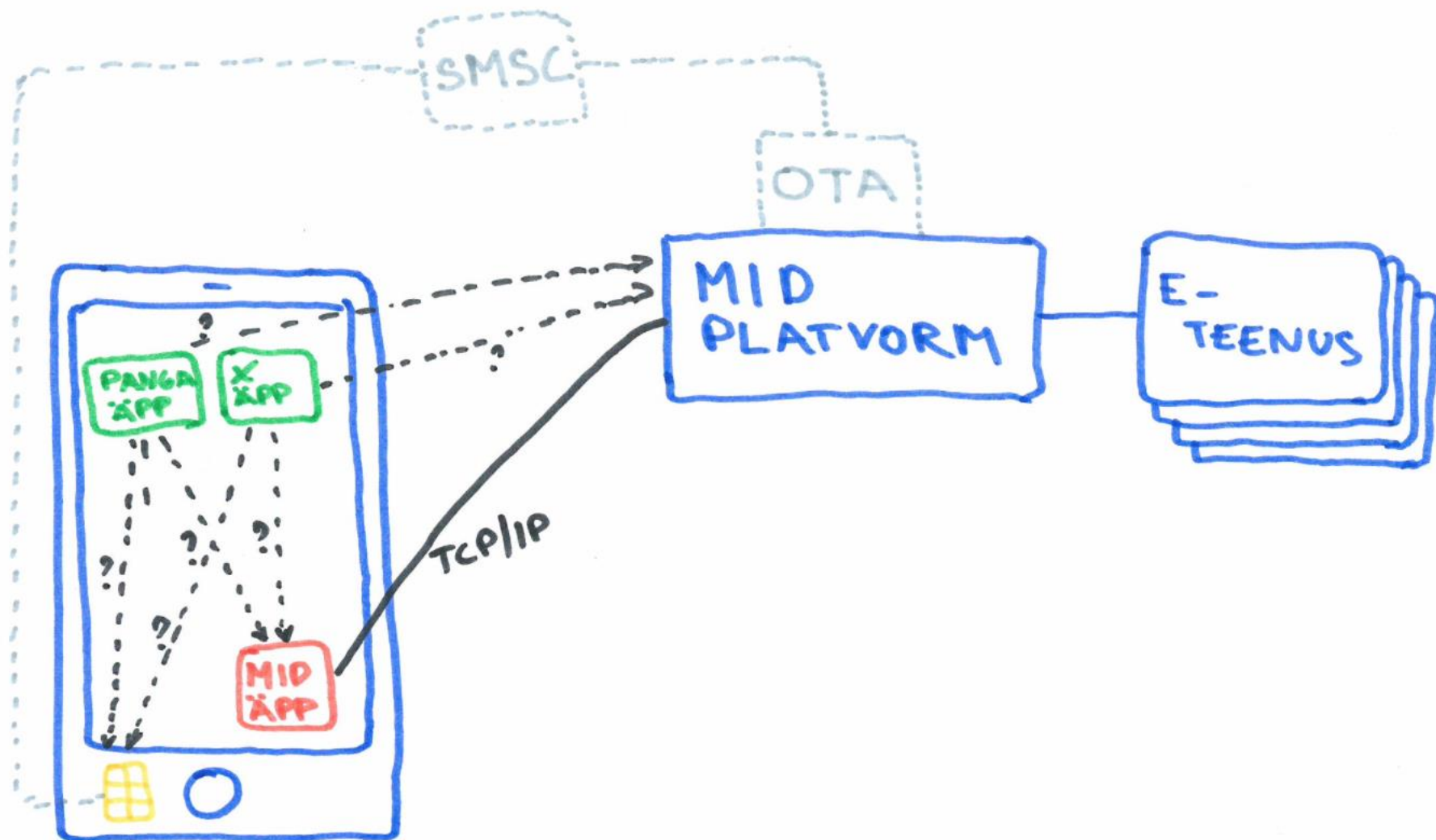


NUTIKAITSE

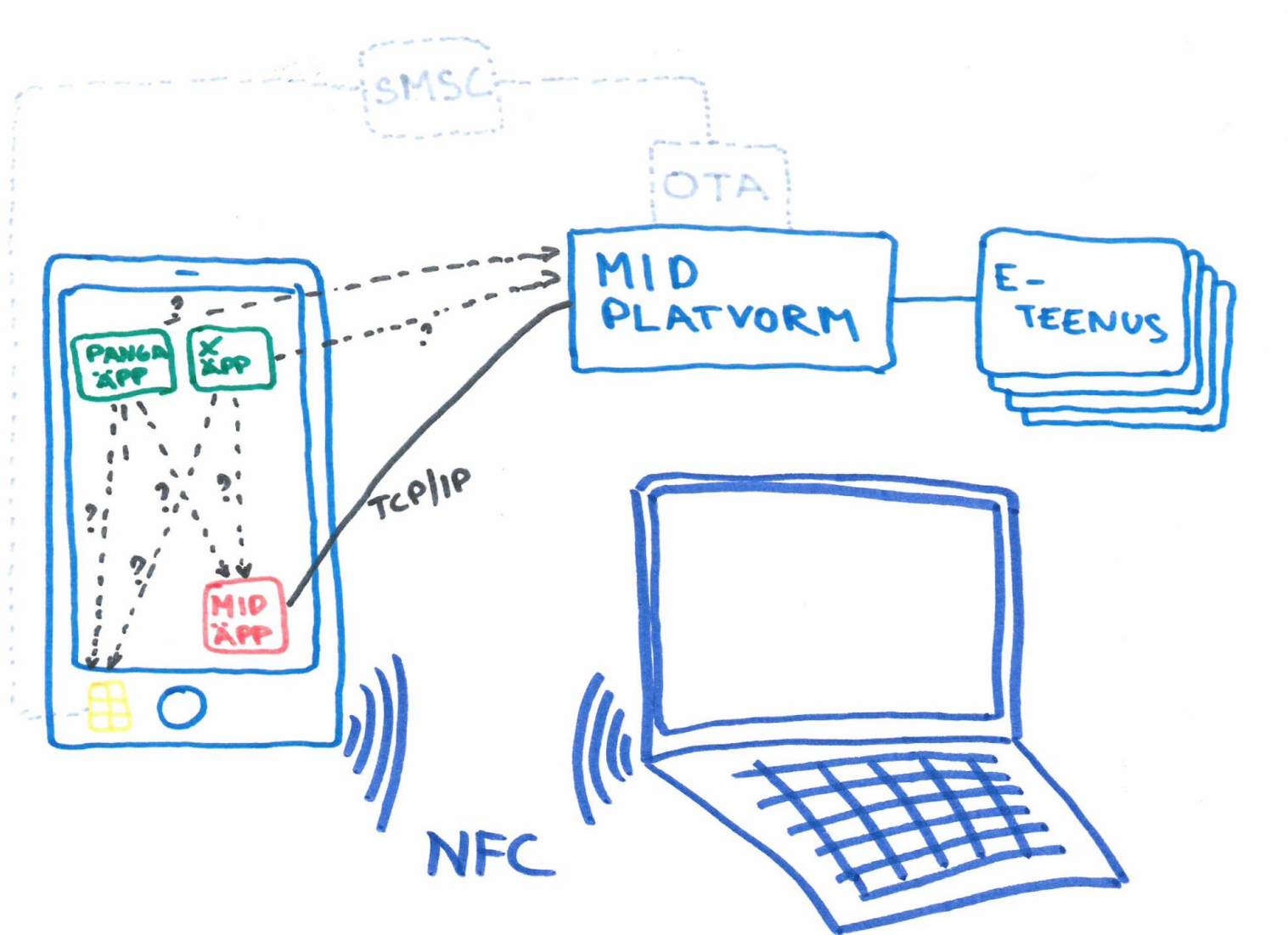
E-SIM VALMIDUS



NO STK, NO SMS

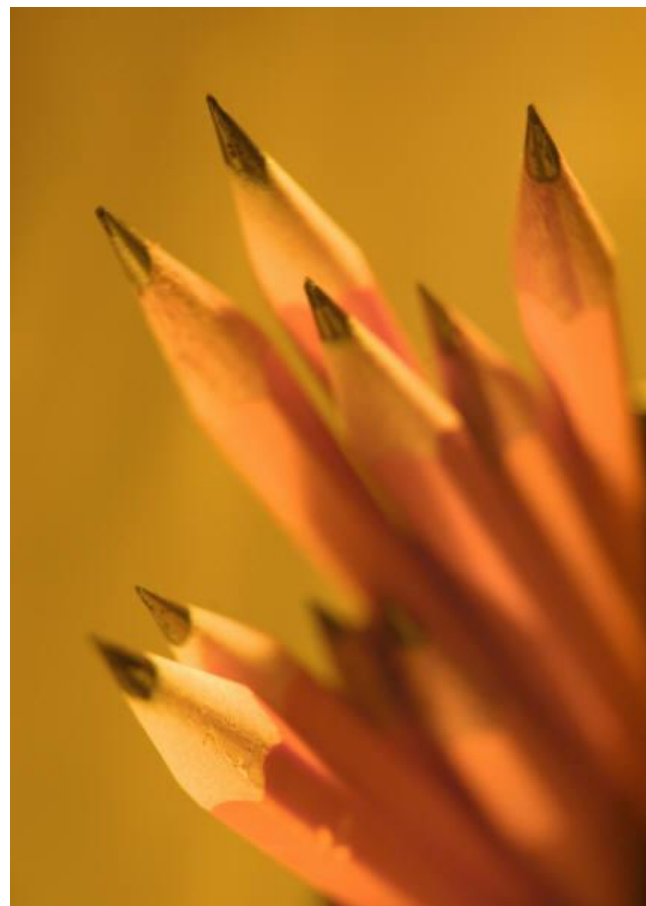


NFC ÜHILDUVUS?



KOKKUVÕTE

- + Mobiil-ID on oluline ekspordiartikkel
- + Mobiil-ID täiustamine käib mitmel rindel
- + Uuendused jõuavad ka Eesti kasutajateni



AITÄH!

