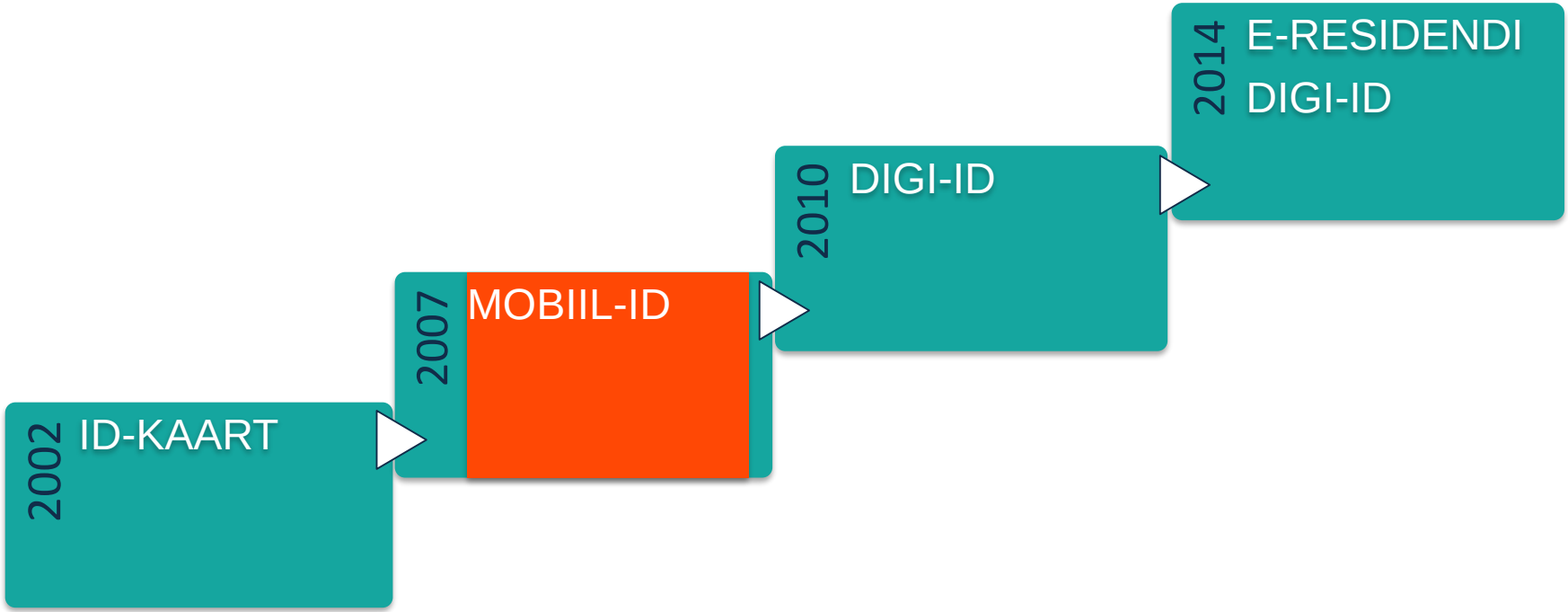
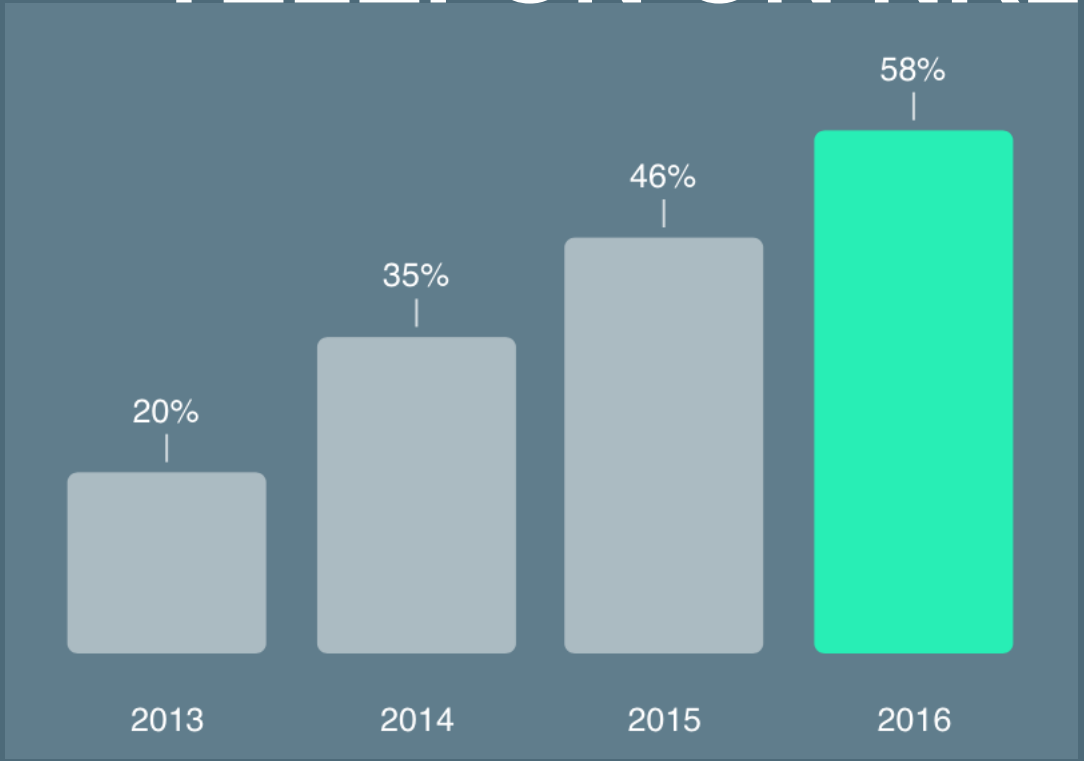
UUS EID LAHENDUS

Urmo Keskel
SK

EID ARENG EESTIS



TELEFON ON NR1!

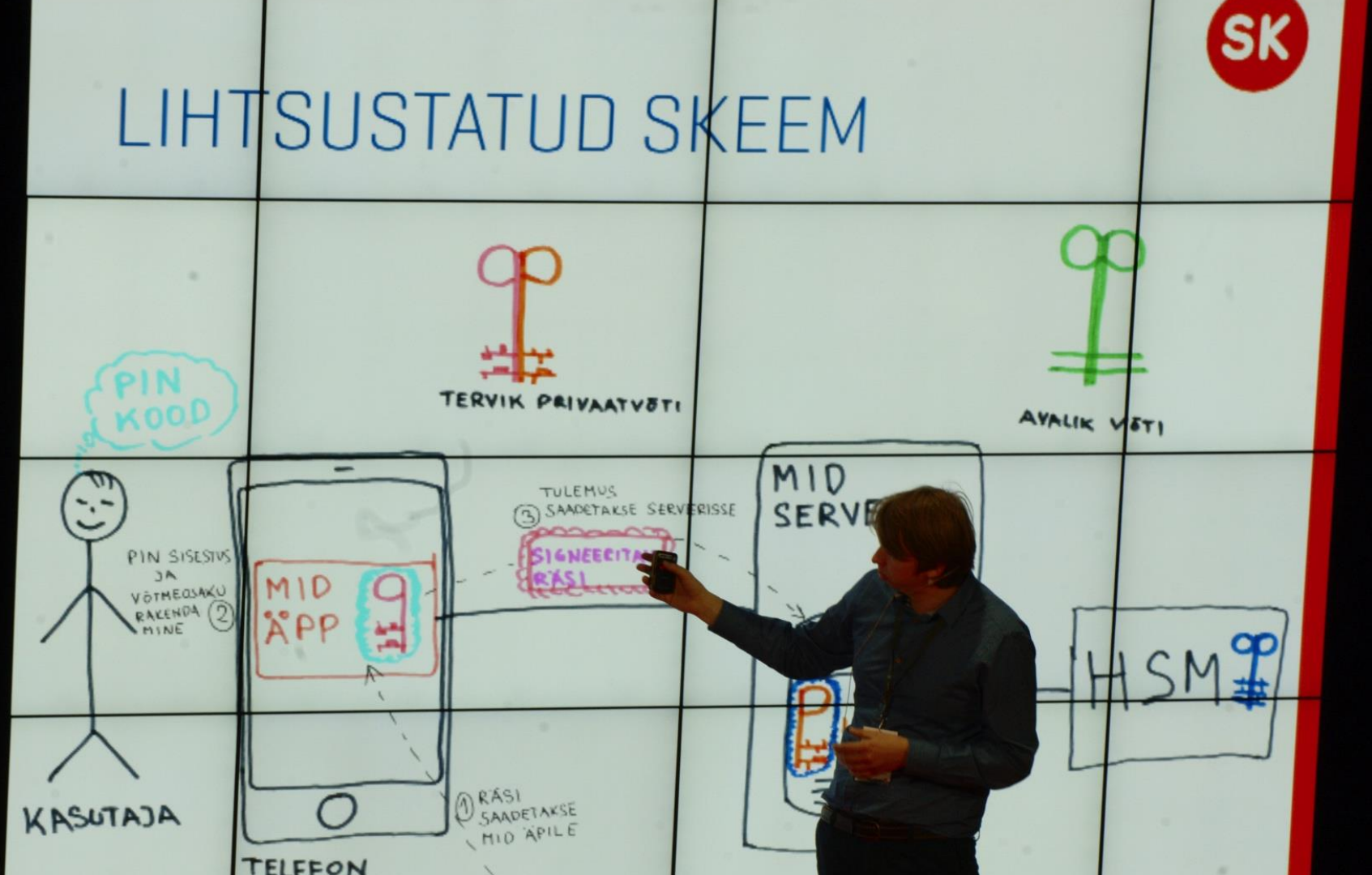


Protsent Eesti elenikest, kes kasutab interneti külastamiseks nutitelefoni vähemalt sama tihti kui arvutit

Allikas:

Google Consumer Barometer
www.consumerbarometer.com

SK Aastakonverents 2015
5. november 2015
SK Aastakonverents 2015
5. november 2015
SK
KALEV PIHL


SK
LIHTSUSTATUD SKEEM
PIN KOOD
TERVIK PRIVAATVÕTI
AVALIK VÕTI
PIN SISESTUS JA VÕTMEOSAKU RAKENDA MINE ②
KASUTAJA
MID ÄPP
TELEFON
TULEMUS ③ SAADETAKSE SERVERISSE
SIGNEERITA RÄSI
MID SERVE
HSM
① RÄSI SAADETAKSE MID ÄPILE

5

4

3

2

1

SMART-ID
Get started
Smart-ID will change
the standards of
electronic identity

TURVALINE

MUGAV

INNOVAATILINE

RISTKASUTATAV

KIIRE

RAHVUSVAHELINE

TÖÖKINDEL

ÜHILDUV

ÄPP

Funktsionaalsus:

- Konto registreerimine
- Autentimine ja allkirjastamine
- PIN koodide vahetus
- Konto sulgemine

Toetatud keeled:

eesti, läti, leedu, inglise ja vene

TOETATUD SEADMED

- Saab kasutada enamiku nutitelefonide ja tahvlitega:
  - Android 4.1 ja uuemad
  - iOS 8 ja uuemad
- Pole vaja SIM-kaarti
- Kasutamiseks vajalik internetiühendus (wifi või mobiilne andmeside)
- Ühel isikul võib olla mitu aktiivset seadet

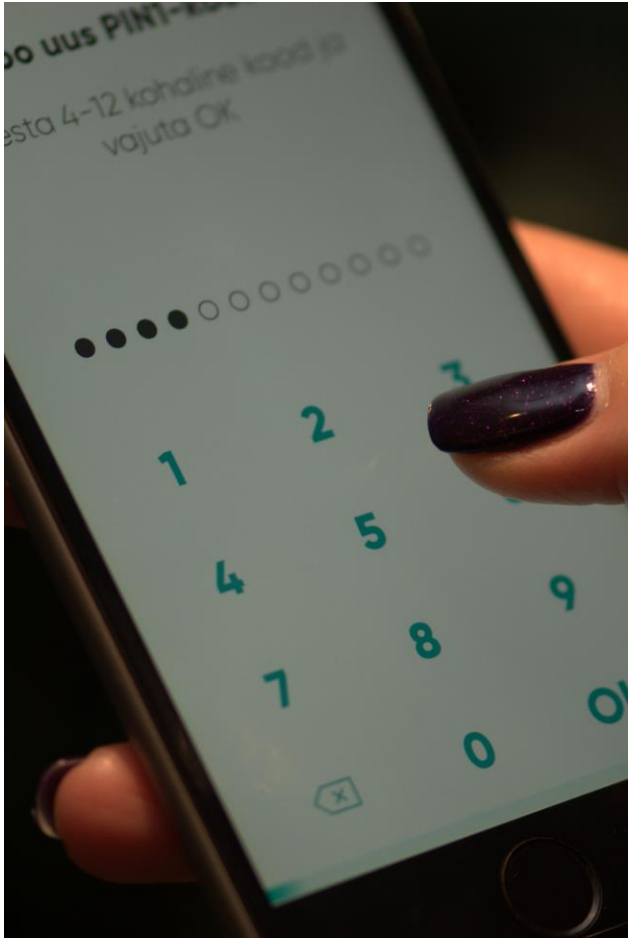
MITU SMART-ID TASET

Kvalifitseeritud

- Väljastatakse digitaalallkirjastatud avalduse alusel, st võimalik taotleda ID-kaardi, Digi-ID, Mobiil-ID, E-residendi kaardiga
- Väljastatakse ka klienditeeninduspunktides
- Kasutus kõigile avatud

Mittekvalifitseeritud

- Väjastatakse mõne identiteedipakkuja (nt pank) andmete alusel
- Kasutus piiratud



PIN KOODID

Vali ise või lase äpil pakkuda

- PIN1 isikutuvastuseks (4-12 numbrit)
- PIN2 allkirjastamiseks (5-12 numbrit)

Mitmeastmeline PIN lukustus

- 3 valesisestust lukustab PIN-i 3 tunniks
- 3 järgmist valesisestust lukustab PIN-i 24 h
- 3 järgmist valesisestust (24h pärast) lukustavad konto

Puudub PUK-kood

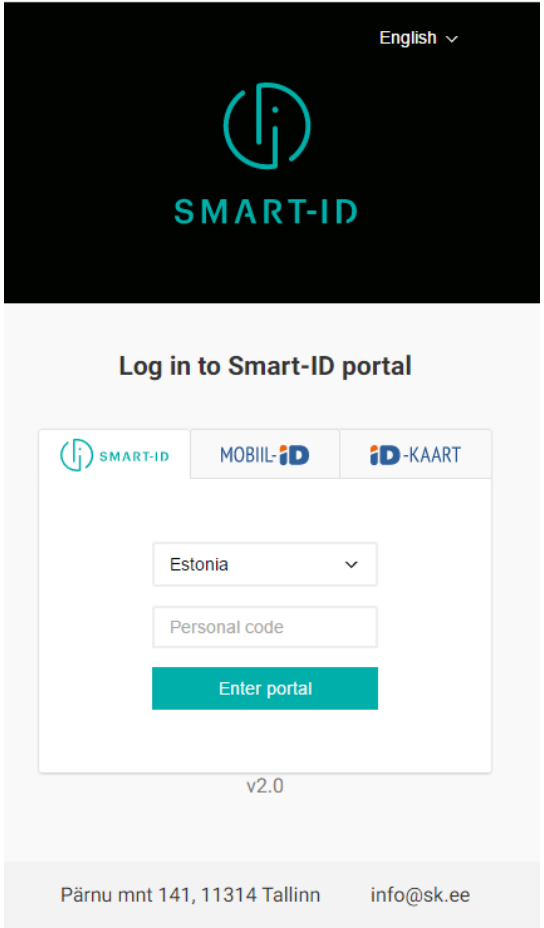
PIN-koodid serverisse ei jõua

KASUTAMINE

Mobiil-IDle sarnane kasutajakogemus

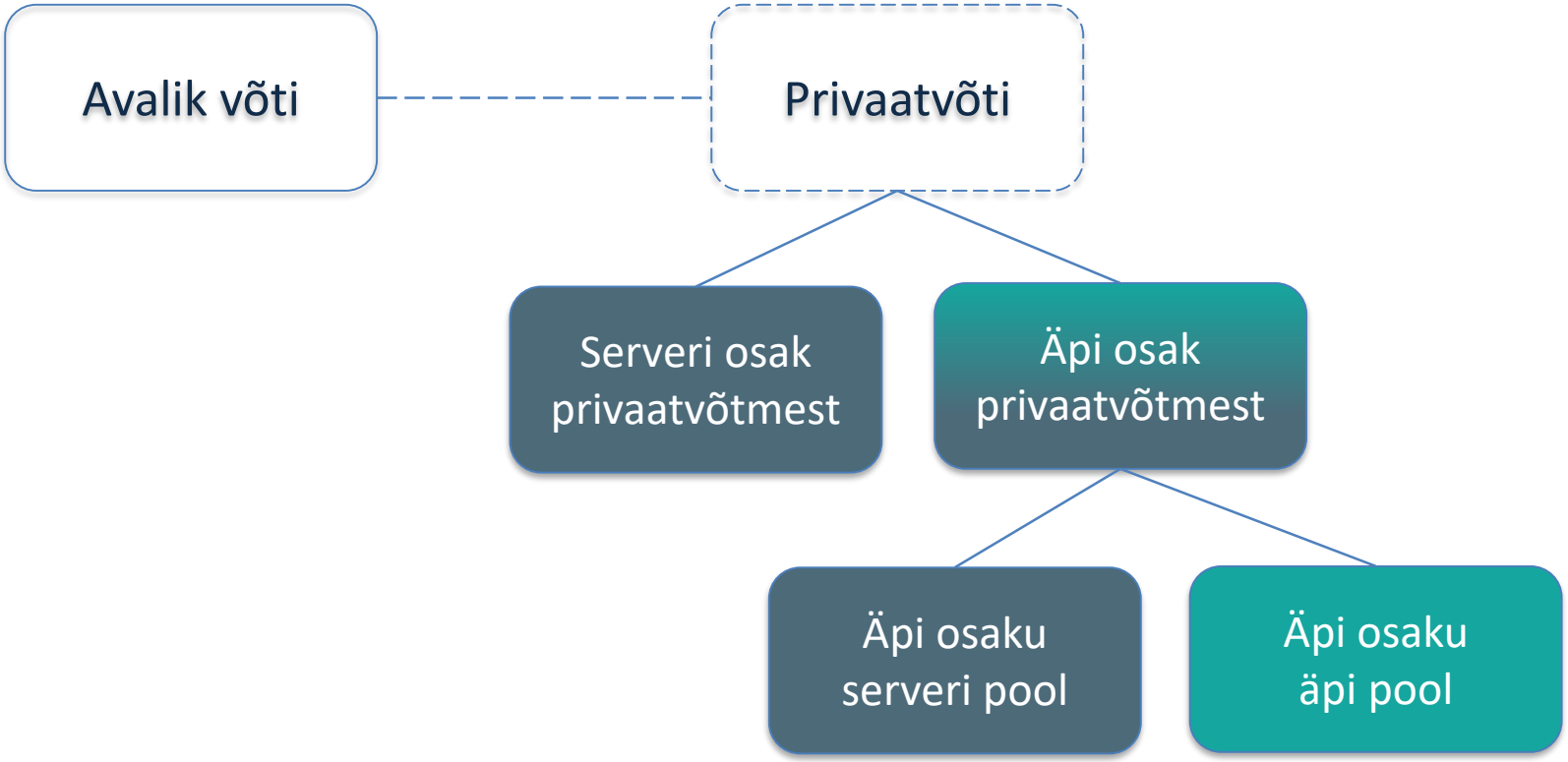
1. kasutaja algatab e-teenuses toimingu
2. e-teenus kuvab kontrollkoodi
3. telefon teavitab kasutajat toimingust, kuvab teenuse nime ja kontrollkoodi
4. Kasutaja kontrollib kontrollkoodi ja sisestab PIN-i
5. e-teenus laseb kasutaja sisse

PORTAAL



- Konto registreerimine (ID-kaardiga)
- Ülevaade:
  - Smart-ID kontodest
  - tehtud toimingutest
- Konto sulgemine

VÕTME JAGAMINE



STIILINÄIDE KRÜPTOTÕESTUSEST

Lemma 3 *If $n = pq$ and p, q are ℓ-quasi-safe primes, then if $m \leftarrow \mathbb{Z}_n^*$ is a uniform random number then* $\Pr[\mathrm{ord}(m) < \min\{\frac{p-1}{2\ell}, \frac{q-1}{2\ell}\}] = \frac{16\ell^2}{(p-1)(q-1)}$.

Proof: By assumptions, there are prime numbers p', q' such that $p-1 = 2ap'$ and $q-1 = 2a'q'$, where both a and a' belong to the interval $[1 \ldots \ell - 1]$. Hence, the size of the group $\mathbb{Z}_n^*$ is $\varphi(n) = (p-1)(q-1) = 4aa'p'q'$. As the order of an element must be a divisor of the size of the group, any element m of $\mathbb{Z}_n^*$ has order $\mathrm{ord}(m)$ divisible by $4aa'$ or $\mathrm{ord}(m) \geq \min\{p', q'\}$. As all the elements of orders divisible by $4aa'$ are roots of the polynomial $X^{4aa'} - 1$ in $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$ and any polynomial of degree d may have no more than d roots in $\mathbb{Z}_p$ and $\mathbb{Z}_q$, the number of roots in $\mathbb{Z}_n$ cannot exceed d^2. Hence, the number of elements of degree less than $\min\{p', q'\} = \min\{\frac{p-1}{2a}, \frac{q-1}{2a'}\} \geq \min\{\frac{p-1}{2\ell}, \frac{q-1}{2\ell}\}$ does not exceed $d^2 = (4aa')^2 \leq 16\ell^2$. $\square$

Autor: AS Cybernetica teadur Ahto Buldas

TURVAMEETMED

- Kontrollkood sessiooni sidumiseks
- HTTPS ühendused koos sertifikaadi *pinninguga*
- Privaatvõtme serveri osak FIPS Level-3 HSM-is
- PIN verifitseerimine võimalik vaid serveri osalusel
- Tundlike andmete transport äpist kasutades HSMi transpordivõtit
- Kloonituvastus
- Äpi taseme turvameetmed:
  - Enda PIN-dialoog
  - Ülaakende tuvastus
  - …
- …

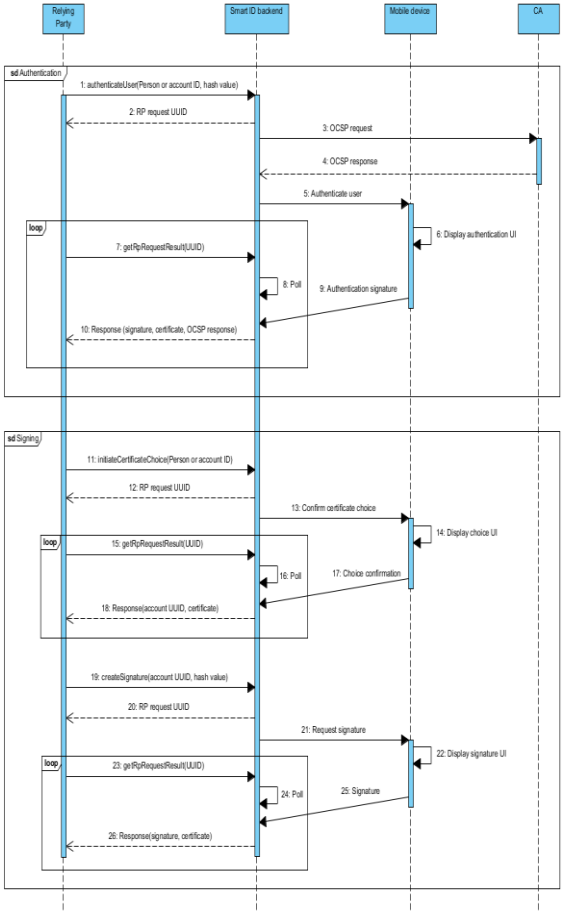
SMART-ID

DEMO

TULE PROOVI!

- Anna meile oma e-posti aadress konverentsi äpis
- Või registreeru vastavalt http://demo.sk.ee/smartidbeta/ juhtnööridele
- Anna tagasisidet!

INTEGRATSIOON



- REST API
  - Autentimine
  - Allkirjastaja sertifikaadi päring
  - Räsi signeerimine
- API allkirjastamise formaaadist sõltumatu
- Tulevikus saab sama API kaudu ka Mobiil-ID tuge integreerida

Alustage integreerimisega!

LANSEERIMISE AJAKAVA

2017 algus

- Teenus turul Eestis, Lätis, Leedus
- Ainult elektrooniline taotlemine

2017 kevad

- Väljastamine teeninduspunktides

2017 lõpp

- Smart-ID kui QSCD

SMART-ID.COM

MEESKOND

Toote väjatöötamisse kaasatud üle 100 inimese

CYBERNETICA

Stagnation Lab

mobilab.

SK

Nortal

testijad

AITÄH!

KÜSIMUSED?