REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

eID mobiilsetel platvormidel

Martin Paljak
Arendus- ja uurimistegevuse osakonna peaspetsialist
eID arhitekt

27.05.2015

Ülevaade

- **MIKS** me seda teeme ?
- **KUS** me praegu oleme ?
- **KUIDAS** korraldame ?
- **MIDA** plaanime ?

https://www.flickr.com/photos/novecentino/2339687721

https://www.flickr.com/photos/novecentino/2339687721


https://www.flickr.com/photos/garryknight/6436100219

https://www.flickr.com/photos/garryknight/6436100219

Hetkeseis

- Punkt tööplaanis
  “eID laiendamine mobiilsetele platvormidele - 31.05.2016”
- Tehniliste võimaluste analüüs
  https://open-eid.github.io/mobile
- Vahendid hankeks - 300kEUR
- Tahtmine midagi tõeliselt head ära teha!

Põhimõtted

Avatud platvorm

- Me ei loo “rakendust” vaid platvormi
- Ei tee libc vaid operatsioonisüsteemi
- Et oleks kõige lihtsam rakenduste arendajale
- Eesmärk: jätkusuutlik lahendus

Standardsed liidesed

- Seadme sees
- Seadme ja väliste süsteemide vahel
- Ühilduvus
- Nõuetele vastavus
- Mõistlik sõltumatus

Võrdsed võimalused

- Teenustele
- Ettevõtetele
- Arendajatele
- Kasutajatele

Avatud lähtekood

- “Vähemalt” LGPL litsents
- Mitte ainult lähtekood - avatud arendus
- Globaalsem haare

Eesmärk

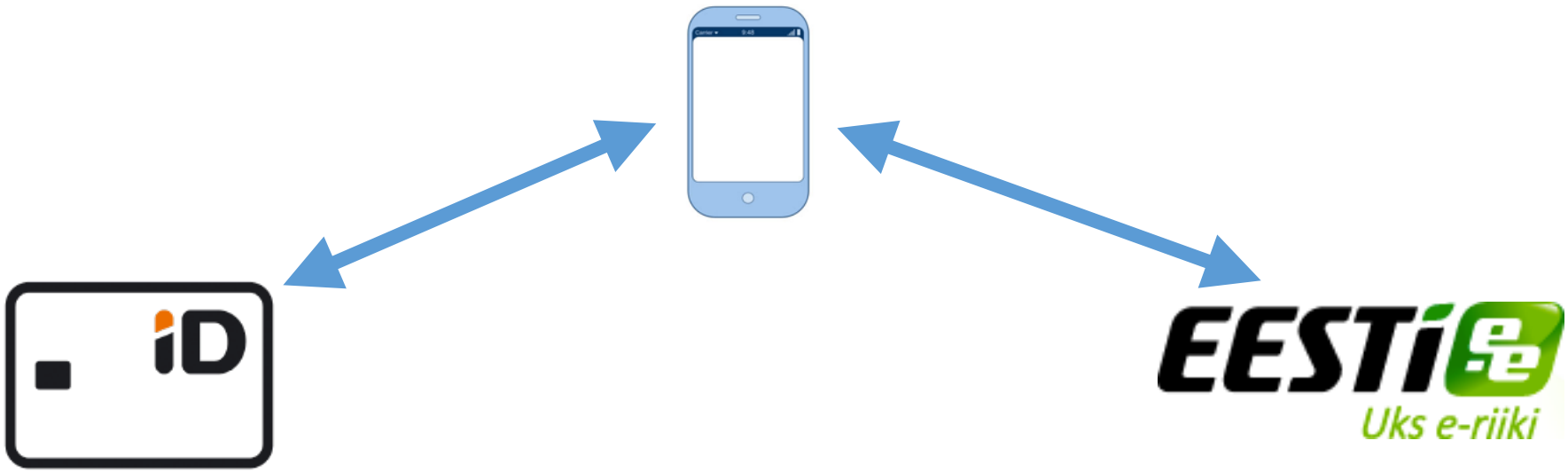
Funktsionaalne skoop

- Turvaline isikutuvastus (pilve)rakendustes
- Digiallkirja andmine (pilve)rakendustes
- Dekrüpteerimine / (krüpteerimine) rakendustes
- PIN haldus
- ƒ(kaart) mitte ƒ(eID)

Tehniline skoop

- ID-1 (ID-kaart, Digi-ID, E-resident)
- ~~Mobiil-ID ja SK DigiDocService~~
- ~~Mobiil-ID tulevikuasendajad~~
- NFC*

TODO



Probleem 1: desktop-arhitektuur

- Draiver == süsteemse API plugin / moodul
- Isikutuvastus == SSL/TLS kliendisertifikaat
- Digiallkirjastamine == in-browser plugin
- Kokkuvõtvalt: **legacy**
- Ja selle eeldamine olemasolevates veebiteenustes

Probleem 2: suhtlus kaardi(lugeja)ga

- USB/CCID (tavaline)
- Apple
- Bluetooth
- 3.5mm (audio)
- NFC*
- TCP/IP, ultrapuna, infraheli jne-misiganes

Probleem 3: rakendustevaheline suhtlus

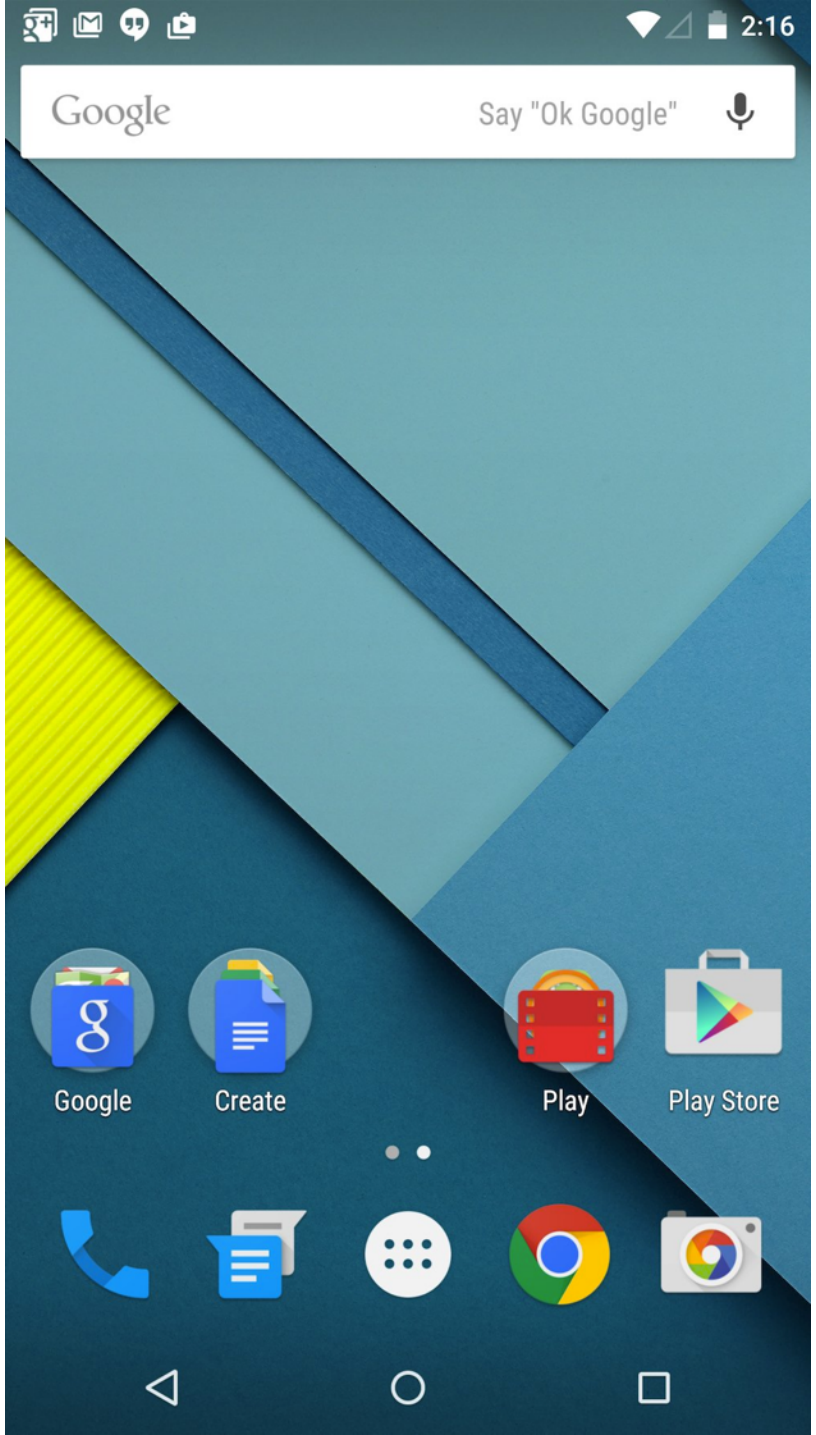
- **Sandbox**
- Veebileht
- Brauser
- DigiDoc
- Netipank
- RakendusX

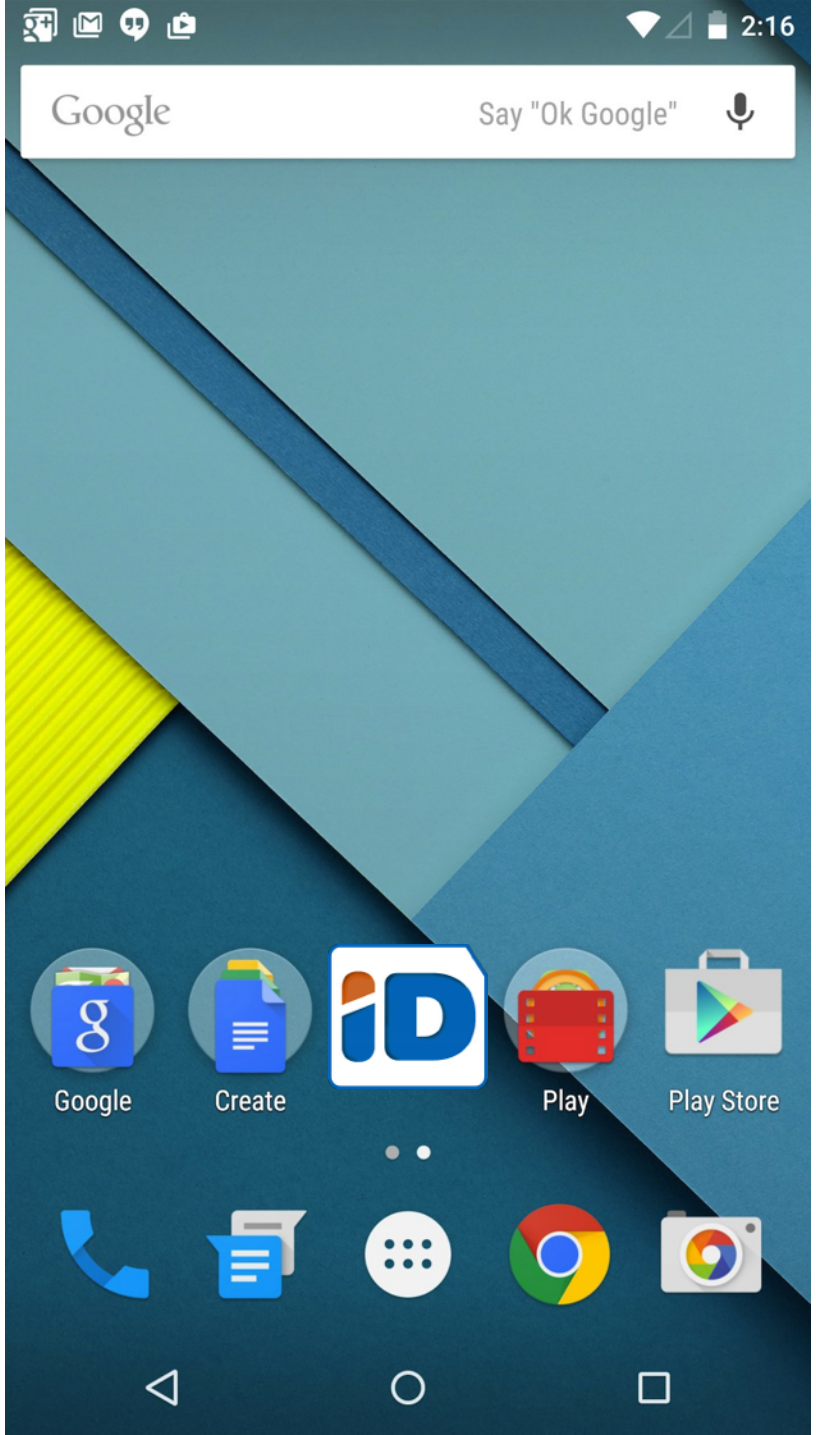
Probleem 4: kasutajakogemus

- Paigaldus
- Käivitamine
- Interaktsioon
- Integratsioon
- …

Järeldus 1: arhitektuursed muudatused

- Autentimise uuesti/ümber mõtestamine
- Digiallkiri kui platvormi teenus (hwcrypto.js)
- SDK ja API määratlemine


2:16
Google
Say "Ok Google"
Google
Create
Play
Play Store


2:16
Google
Say "Ok Google"
Google
Create
Play
Play Store

Järeldus 2: “eID rakendus"

- Tavapärane kontseptsioon mobiilidel
- Teegid on ka, aga kes uuendab?
- Parim mõistupärane integratsioon platvormiga
- Võrdne desktopi “draiveriga”

Järeldus 3: korduvkasutatavad mõistlikud moodulid

- Selgelt määratletud ja liidestega
- Võtame kasutusele või loome ise
- Maandab hanke riske, tõstab nõudeid (ja riske)

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Martin Paljak
martin.paljak@ria.ee