



www.sk.ee

2015: BDOCi ja Mobiil-ID aasta

Liisa Lukin

Lisateenuste ärijuht

Sertifitseerimiskeskus AS

AK2014 lubadused olid:



- Uus Mobiil-ID teenusplatvorm (DigiDocService)
- Mobiil-ID sertifikaatide kehtivusaja pikendamine
- Uus SIM rakendus, uus krüptoalgoritm
- Turvadomeeniga SIM kaart
- Üleminek operaatoripõhiselt lahenduselt tsentraalsele SK taristule
- BDOC 2.1 formaat kinnitatud 12.2013, olemas teegid ja lõppkasutaja tarkvara



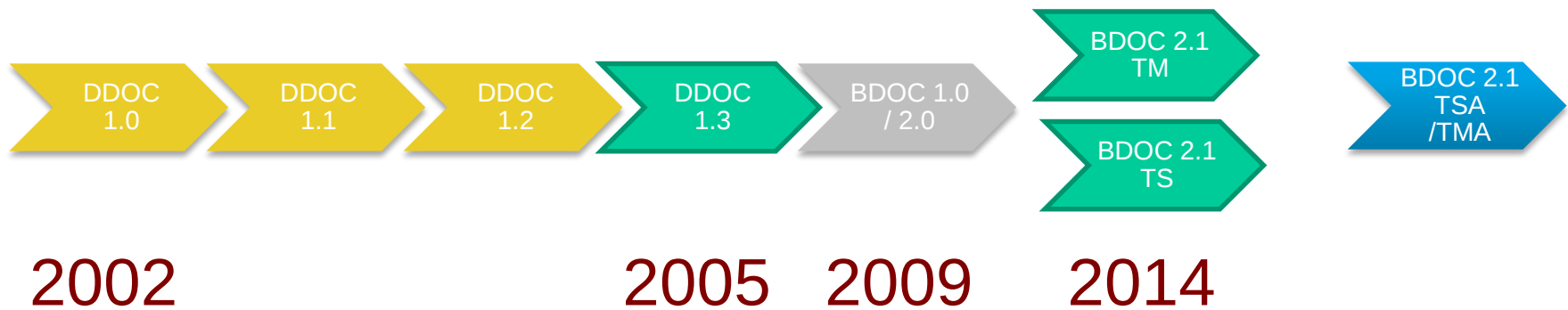
2015



- DDOC → BDOC
- Turvalisem Mobiil-ID



- Formaadi muutus on normaalne areng
- Krütograafia aegub, oluline on kaasas käia ja sellega arvestada



Miks BDOC?



- Säilinud DDOC positiivsed omadused
- Kasutusel kaasaegne krüptograafia
- Kasutusel ajakohased standardid
- Parem rahvusvaheline ühilduvus
- Formaati võimaldab lisada täiendava suurema räsiga (nt SHA-512) arhiivajatempli



Lõppkasutaja tarkvara



DigiDoc3 kliendis
BDOC tugi

2013 / 2014

DigiDoc3 kliendis
BDOC vaikimisi
formaad

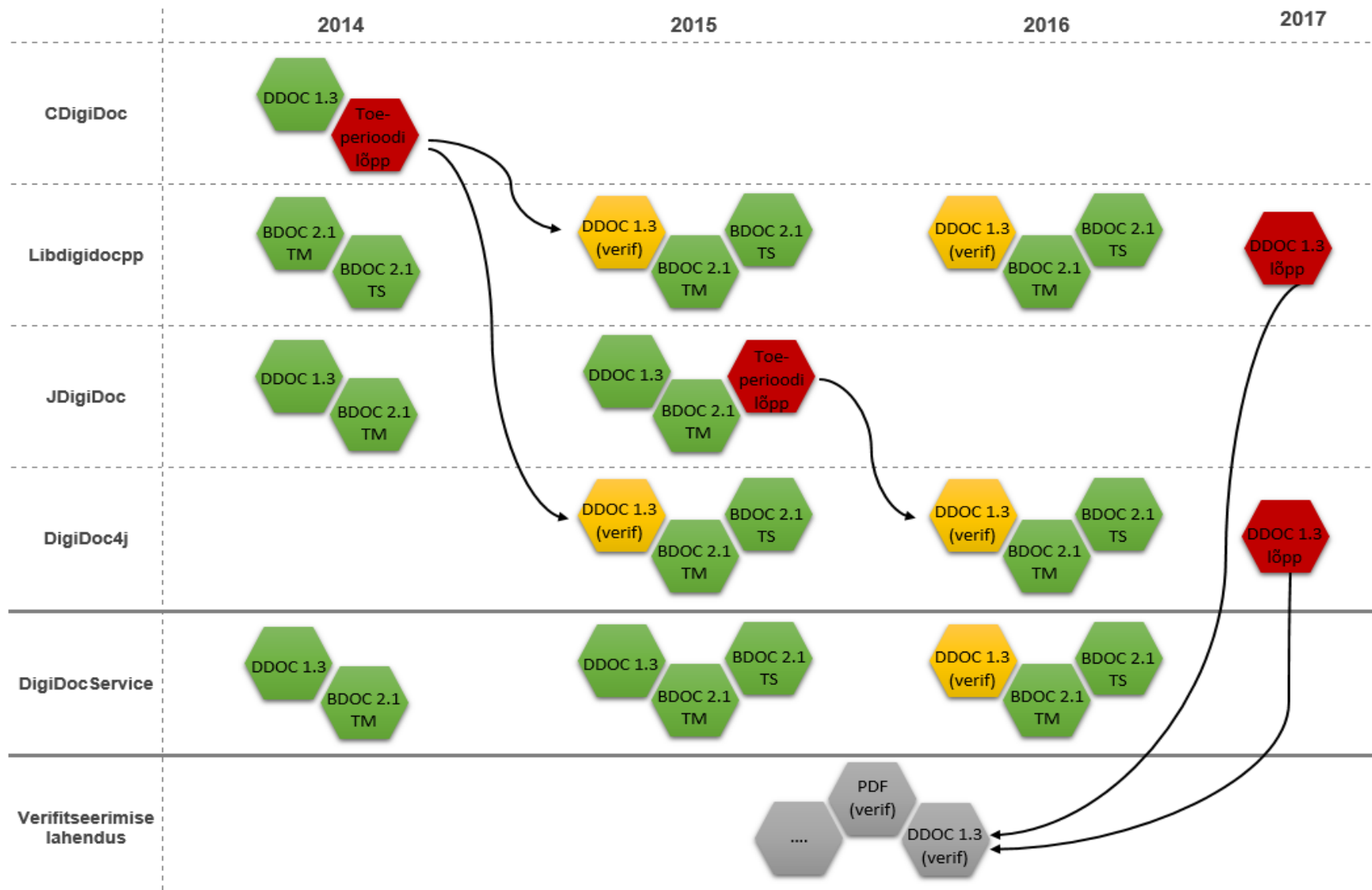
2014 / 2015

DigiDoc3 kliendis
DDOC vaid
verifitseerimiseks

2015 / 2016



DigiDoc teekide maailm



Enim mõjutatud:



- Teenused, ettevõtted, asutused, infosüsteemid, mis võtavad vastu kodanikelt digiallkirjastatud faile
- Miks kõigile oluline?
 - Turvarisk nõrgema krüptoalgoritmi kasutamisel.
 - Toodad juurde dokumente, mille pikaaegse usalduse probleemiga pead sa juba dokumendi väljastamisel tegelema hakkama.



SK aitab teid!



- Arendajate tugi
support@sk.ee
- Lõppkasutajate tugi 24/7
abiliin 1777
- Tasuta!



Turvalisem Mobiil-ID



- Eesmärk: 1K RSA sertifikaadid kehtivad kuni 31.12.2016
- Vana SIM:
 - Al 01.01.2015 saab taotleda sertifikaadid kehtivusega kuni 31.12.2016
- Uus SIM ja uus rakendus
 - 5 a. sertifikaadid
 - 2 võtmepaari: ECC (ja/või 2K RSA)



ECC tulek – mis juhtub?



- ECC sertifikaadiga ei saa DDOCI allkirjastada
 - Sinu teenuses ei saa allkirjastada uue Mobiil-ID omanik al 01.2015
 - Sinu poolt kliendile saadetud DDOC-le ei saa allkirja anda uue Mobiil-ID omanik
- Veendu, et autentimine ECC sertifikaatidega töötaks



SK ajutine tagauks



- Kui allkirjastatakse BDOCi kasutab teenus ECC sertifikaati
- Kui allkirjastatakse DDOCi kasutame teenuse poolel 2K RSA sertifikaati
- Autentimisel alati ECC sertifikaat



Astume KOOS sammu edasi ja
saavutame selle, et alates 01.01.2015
antakse enamus digitaalalkirjad BDOC
vormingus.





www.sk.ee

Liisa Lukin

Sertifitseerimiskeskus AS