www.sk.ee

Üleminek DigiDoc4J teegile

Urmo Keskel

18.05.2016

Kes teie olete?

Millest ma juttu teen

- BDOC formaadist
- JDigiDoc toe lõpust
- DigiDoc4j teegi arendusest
- Usaldusnimekirjadest
- DigiDoc4j kasutamise kogemusest

Kuningas on surnud, elagu kuningas!

- DDOC formaadi aeg on saanud ümber
  - Kasutatava SHA-1 räsialgoritmi elukaar hakkab läbi saama
  - Üha olulisem rahvusvaheline ühilduvus
- BDOC on tulnud DDOC formaati asendama
- Üle 75% loodavatest allkirjadest on BDOC formaadis
- DDOC failidele allkirjade lisamist piiratakse

Samal teemal:
https://blog.ria.ee/elagukuningas/

BDOC eelised

- Säilinud DDOC positiivsed omadused
- Kasutusel kaasaegne krüptograafia
- Kasutusel ajakohased standardid
- BDOC failid on sama sisu sisaldavast DDOC failidest väiksemad
- Parem rahvusvaheline ühilduvus
- Faili töötlus kiirem kui DDOC puhul, piirangud faili suuruse osas väiksemad

BDOC jagunemine

	BDOC TM	BDOC TS/ASiC-E
Faililaiend	.bdoc	.bdoc; .asice
Rahvusvaheline ühilduvus	Puudlik	100% ühilduv
Allkirja formaat	XAdES (ver 1.4.2)	XAdES (ver 1.4.2)
Pikaajaline tõestusväärtus tagatud	OCSP kehtivuskinnitusel baseerva ajamärgendiga	Standardsel RFC3161 ajatemplil
Toetavad teegid	DigiDoc4J CPP teek DigiDocService JDigiDoc	DigiDoc4J CPP teek DigiDocService
Toetatud DigiDoc3 versioonist	3.8 (avaldatud dets. 2013)	3.10 (avaldatud märts 2015)

Lisainfo: http://www.id.ee/index.php?id=37370

Mis saab DDOC-st?

- Dokumendi omanik peab kindlustama allkirja pikaajalise tõestusväärtuse
  - Krüptograafia aegumisest tingitud ohud
  - “kindlustada” tuleb enne kui oht realiseerub
- Riik peab tagama võimaluse DDOCi (või BDOCi) tulevikus avada ja verifitseerida
  - Pakutakse teenusena

DDOC -> BDOC

Formaadi konverteerimine ei ole võimalik!

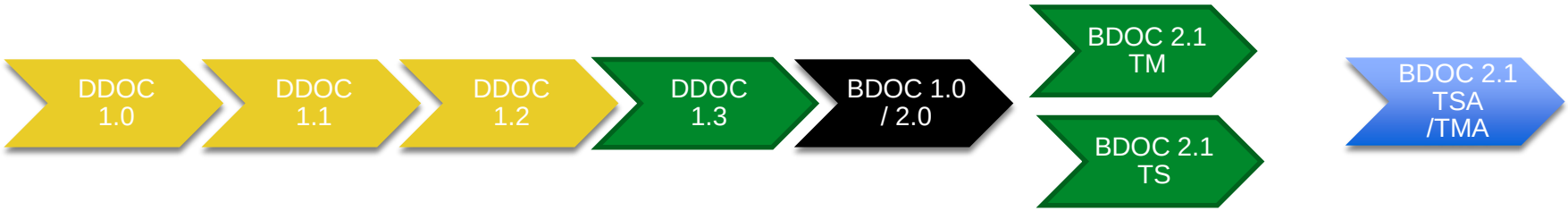
Võimalikud lahendused:

- DDOC panna BDOCi sisse ja üle tembeldada
- DDOC “laiali lammutada” ja luua BDOC, mille korrektsust kinnitada allkirja või digitempliga. Seda võiks teha usaldusteenuse pakkuja
- DDOC hoiustada digitaalarhiiviteenuse pakkuja juures
- Kas sul on üldse vaja vanu DDOCe alles hoida? Kui mitte, siis hävita ☺

Minevik -> Tulevik

Formaadi muutus on normaalne areng

Krüptograafia aegub, oluline on kaasas käia ja sellega arvestada



Muudatusi tuleb ka edaspidi ...

Lihtsam on nendega leppida ☺

- PDF allkirjad
- alusstandardite(XAdES, ASiC) uuendused
- krüptoalgoritmide uuendused
- arhiivi ajatemplid
- krüptofailiformaadi (cdoc) muutused
- uued tehnoloogiad: NFC, mobiili OS'ide tugi
- ...

Muudatused on sulle valutumad, kui kasutad ajakohaseid ja toetatud teeke:

DigiDoc4j on selleks mõistlik valik.

EIDAS määrusest tulenev vajadus

Teiste riikide e-allkirjade tunnustamine alates **01.07.2016**.

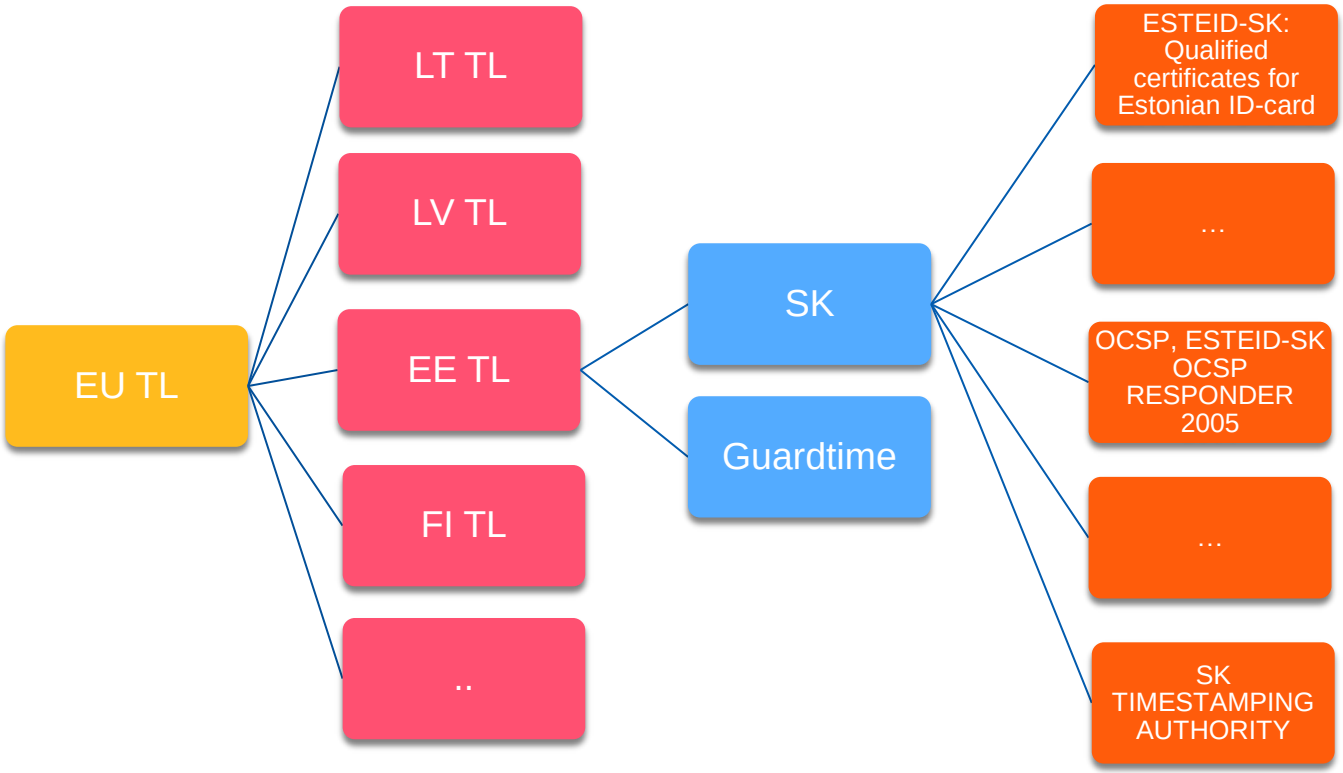
Nõuded avalikule sektorile:

- Kui kuskil aktsepteeritakse e-allkirjaga dokumente, siis **tuleb aktsepteerida** ka teistest riikidest ja teiste teenuseosutajate abil allkirjastatud samaväärse allkirja tasemega dokumente.

TL - Usaldusnimekirjad

- **T**rusted **L**ists - maakeeli usaldusnimekiri
- Kirjeldatud ETSI standarditega:
  TS 102 231 (v 3.1.2) ja TS 119 612 (v 2.2.1)
- Hierarhiline: LOTL ja riikide listid
- Kõik listid on signeeritud
- Sisaldab infot: sertifitseerimisteenuse osutajate, kehtivuskinnitusteenuse osutajate ja ajatempliteenuse osutajate kohta ning nende teenustega seotud sertifikaatide infot
- Sisu saab uudistada: http://tlbrowser.tsl.website/

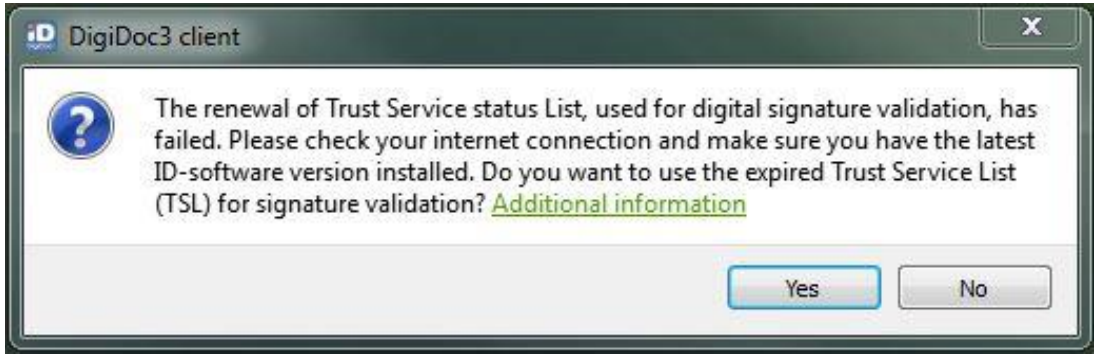
TLide hierarhia



- Euroopa Liidu keskne list
- riikide listid
- usaldusteenuse pakkujad
- usaldusteenuse pakkujate teenused

TL-ide uuendamine

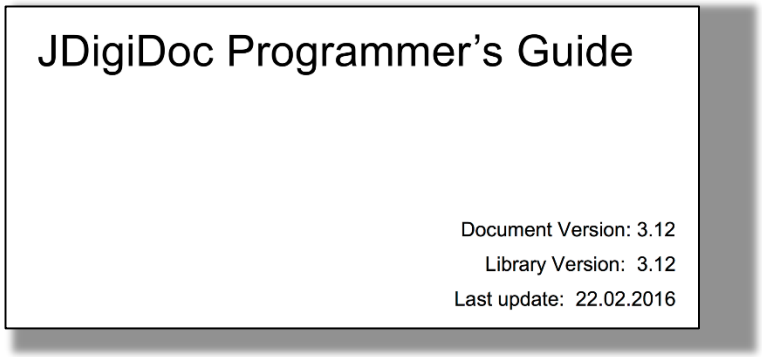
- TL-id aeguvad pidevalt (kokku 31 riiki, 1434 kirjet)
- Iga riik avaldab enda TL-i oma veebilehel (palju pöörduspunkte)
- Vajalik on TL-i kasutava rakenduse/teenuse poolt
  TL uuenduste laadimine



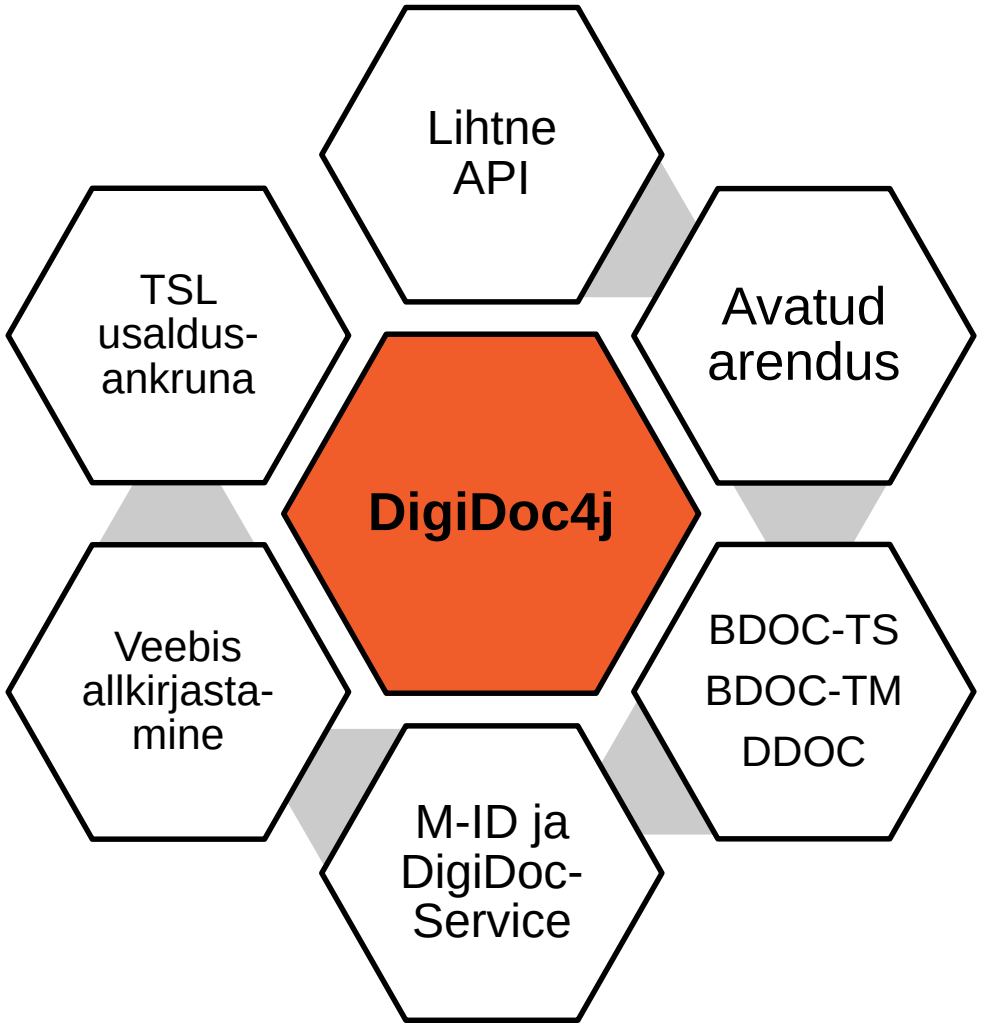
JDigiDoc teegi toeperioodi lõpp

- JDigiDoc teegi esimene versioon 2003
- Vanim seni toetatud DigiDoci teek
- On aeg puhkusele saata, DigiDoc4J on tulnud JDigiDoci asendama
- Alates juuni 2016 arendustöid enam ei teostata ja uusi versioone ei väljastata, lõpeb arendajate tugi
- Kokkuleppel võimalik osta SK-st tasulist tuge

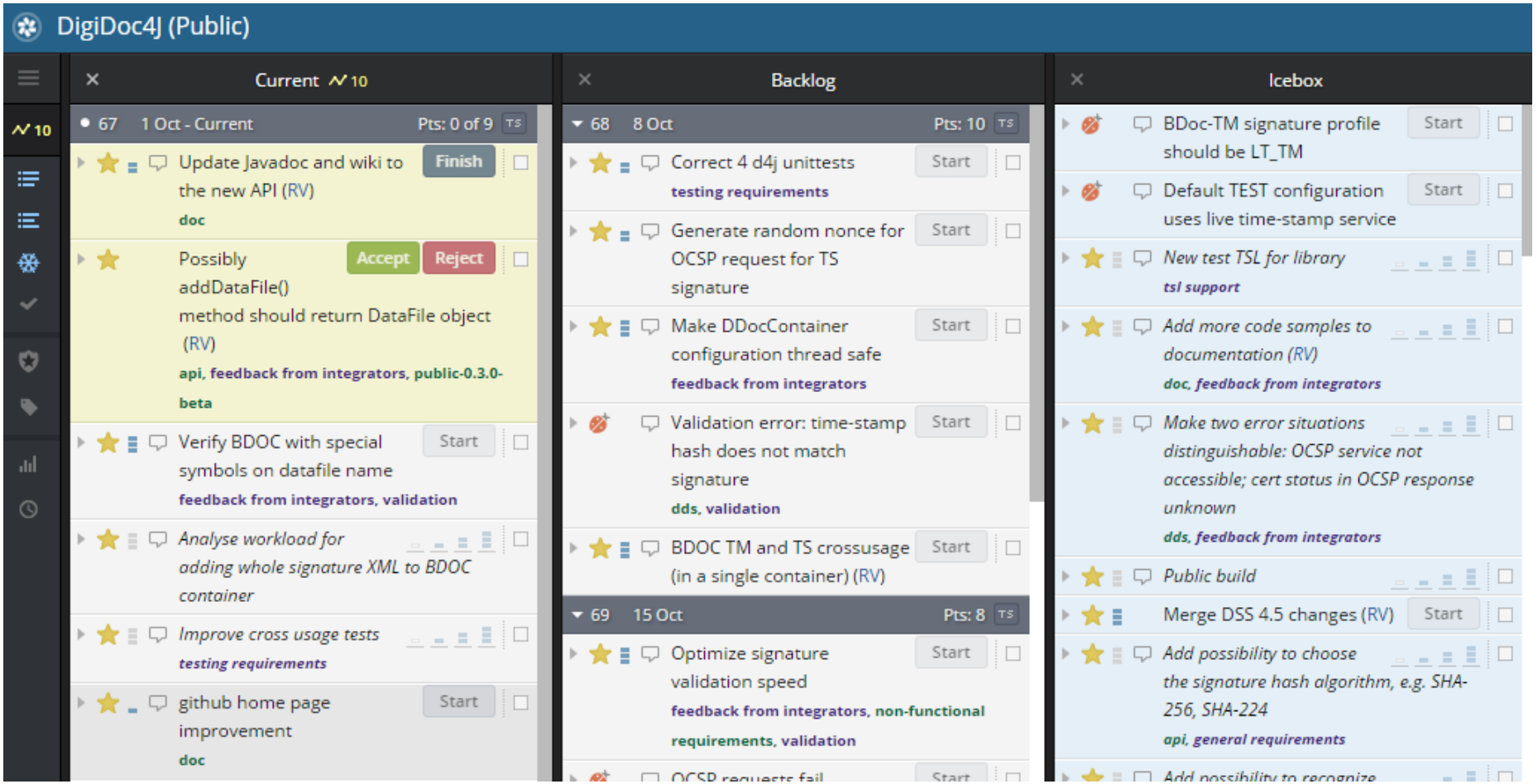
Teiste teekide toe perioodi info:
http://www.id.ee/index.php?id=30290



DigiDoc4j teegi ülevaade

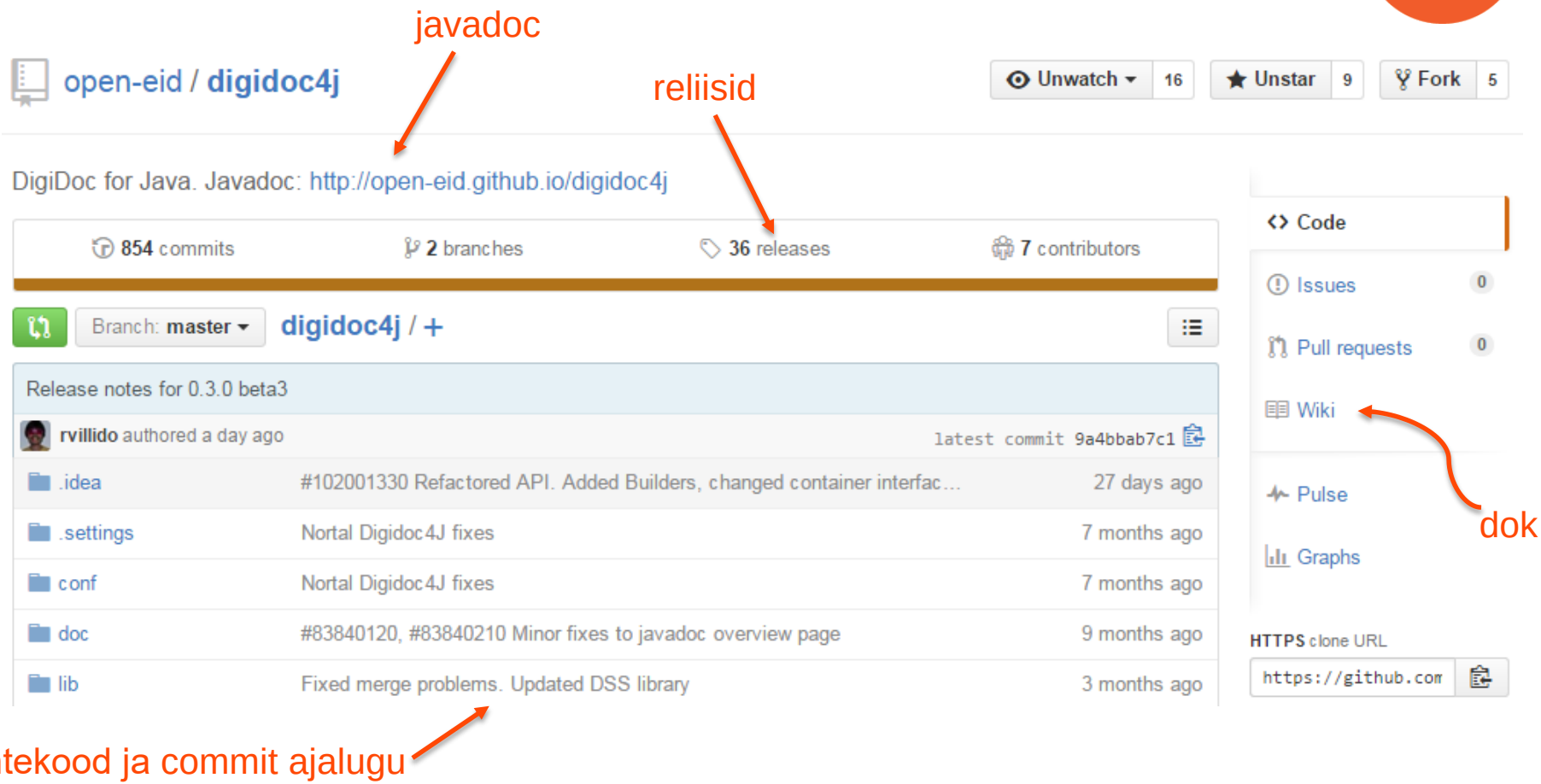


Avatud arendus - DigiDoc4j Pivotal



https://www.pivotaltracker.com/n/projects/1110130

Avatud arendus - DigiDoc4j GitHub



https://github.com/open-eid/digidoc4j

DigiDoc4j arendustsükkel

- Arendusplaane võimalik kõigil Pivotalis jälgida
- Samuti võimalus kaasa rääkida arenduste prioritiseerimises
- 2 kuu tagant stable released
- 2 nädala tagant beeta väljalasked

DigiDoc4j kasutuselevõtu kogemus

- DigiDocService oli esimene live teenus, kus DigiDoc4j kasutusel

- Kasutuselevõtt on jagatud 4 etappi:
  - 03.2015 - MobileCreateSignature allkirja loomine
  - 02.2016 - BDOC-TS allkirjade valideerimine
  - 05.2016 - BDOC-TS täis tugi
  - Q42016 - BDOC-TS ilma andmefaili edastamata

DigiDoc4j kasutuselevõtu kogemus

Hästi:

- Kood Javalikum ja paremini loetav
- Alusteegina EU DSS
- Kood testidega rohkem kaetud
- Uus lihtne builder-stiilis API
- Hoiatuste süsteem parem kui jDigiDoc’is

Mitte nii hästi:

- Varajase integreerija “rõõmud”
- Performance teemad

Abi üleminekul

Arendajatele suunatud info:

http://www.id.ee

https://open-eid.github.io/

https://github.com/open-eid/digidoc4j/

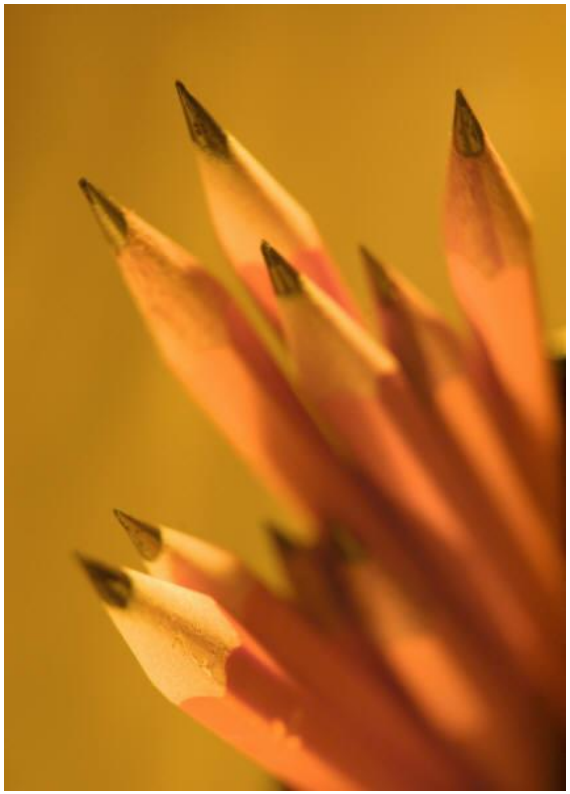
https://github.com/open-eid/digidoc4j/wiki

Arendajate tugi:

support@sk.ee

Kokkuvõtteks

- On viimane aeg võtta BDOC kasutusse
- JDigiDoc toe periood saab kohe läbi
- DigiDoc4j on küps, et sellele üle minna
- Kasutage julgelt arendajate toe abi
- Planeerige enda eelarvesse raha BDOCi ja DigiDoc4j kasutuselevõtuks



Juur-SK tipmine sertifikaat aegub

Version: 3 (0x2)

Serial Number: 999181308 (0x3b8e4bfc)

Signature Algorithm: sha1WithRSAEncryption

Issuer: emailAddress=pki@sk.ee, C=EE, O=AS Sertifitseerimiskeskus, CN=Juur-SK

Validity

Not Before: Aug 30 14:23:01 2001 GMT

Not After : Aug 26 14:23:01 2016 GMT

Subject: emailAddress=pki@sk.ee, C=EE, O=AS Sertifitseerimiskeskus, CN=Juur-SK

Peatselt tuleb SK poolt täpsem info, keda see puudutab ja mida tegema peab

www.sk.ee

Aitäh!