



[www.sk.ee](http://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 räsi algoritmi 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



	<b>BDOC TM</b>	<b>BDOC TS/ASiC-E</b>
Faililaiend	.bdoc	.bdoc; .asice
Rahvusvaheline ühilduvus	Puudlik	100% ühilduv
Allkirja formaat	XAdES (ver 1.4.2)	XAdES (ver 1.4.2)
Pikaajaline tõestusväärts tagatud	OCSP kehtivuskinnitusel baseerva ajamärgendiga	Standardisel 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 😊



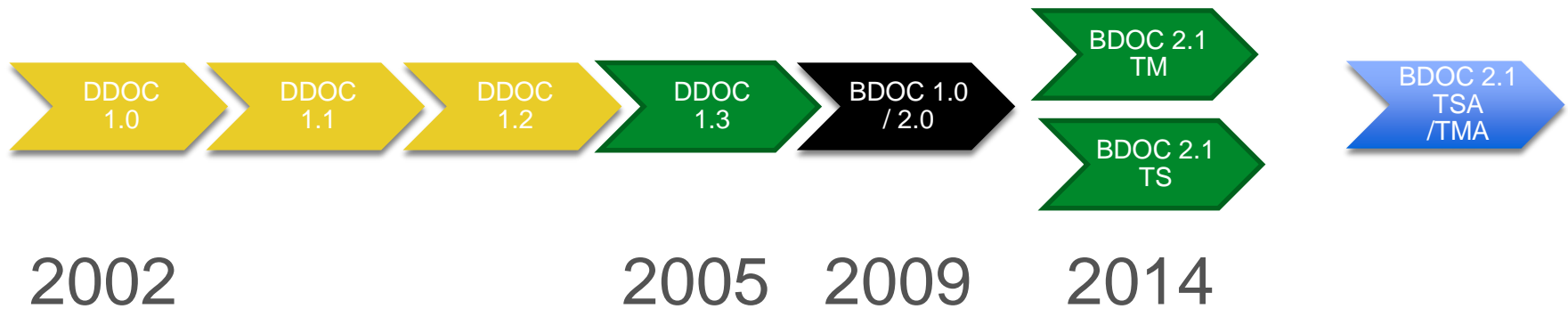




# Minevik -> Tulevik

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.

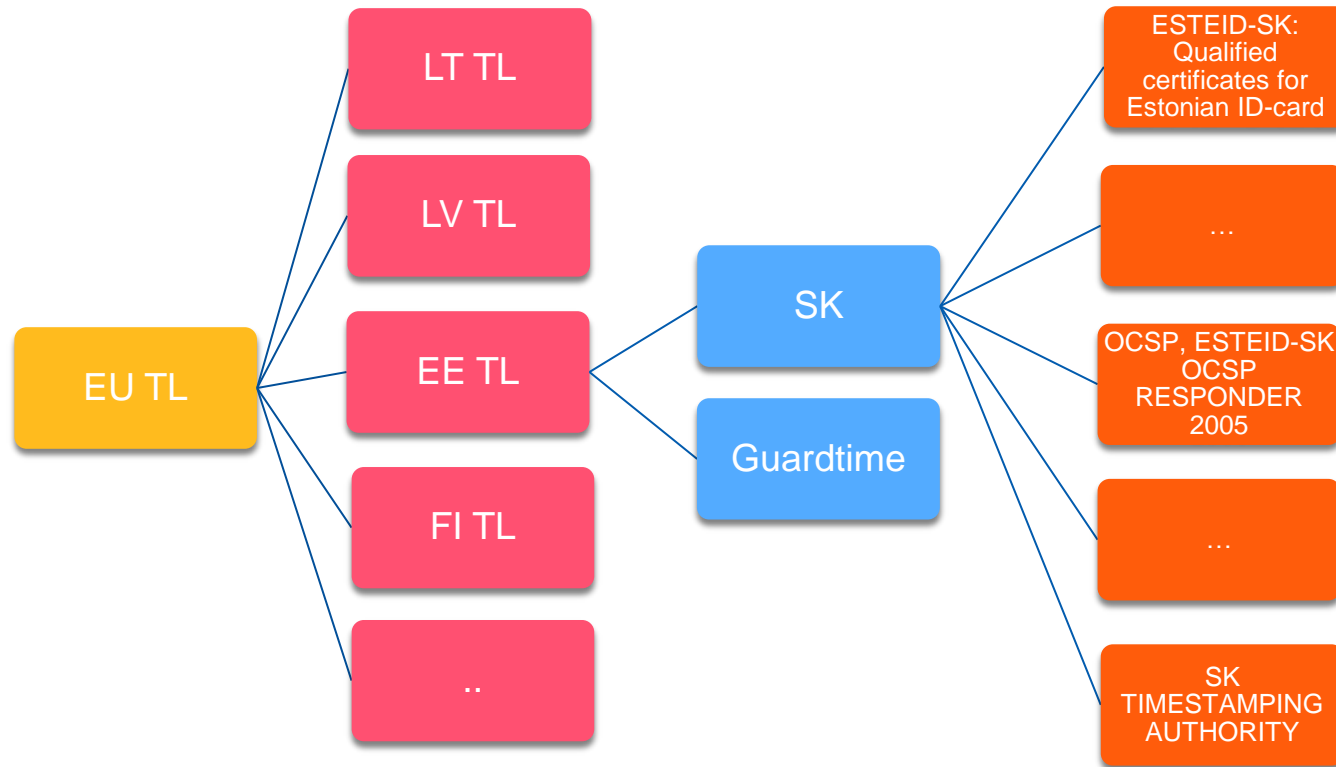








# TL - Usaldusnimekirjad

- **Trusted Lists** - 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

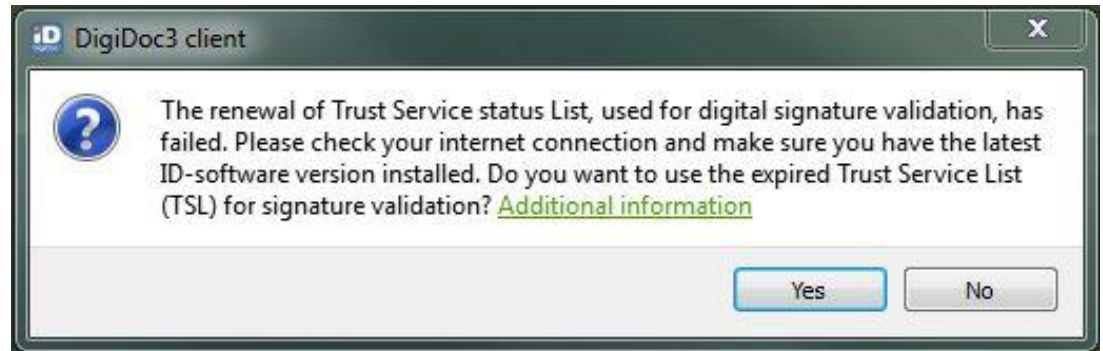


 - Euroopa Liidu keskne list  
 - riikide listid

 - 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 asendada
- 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>

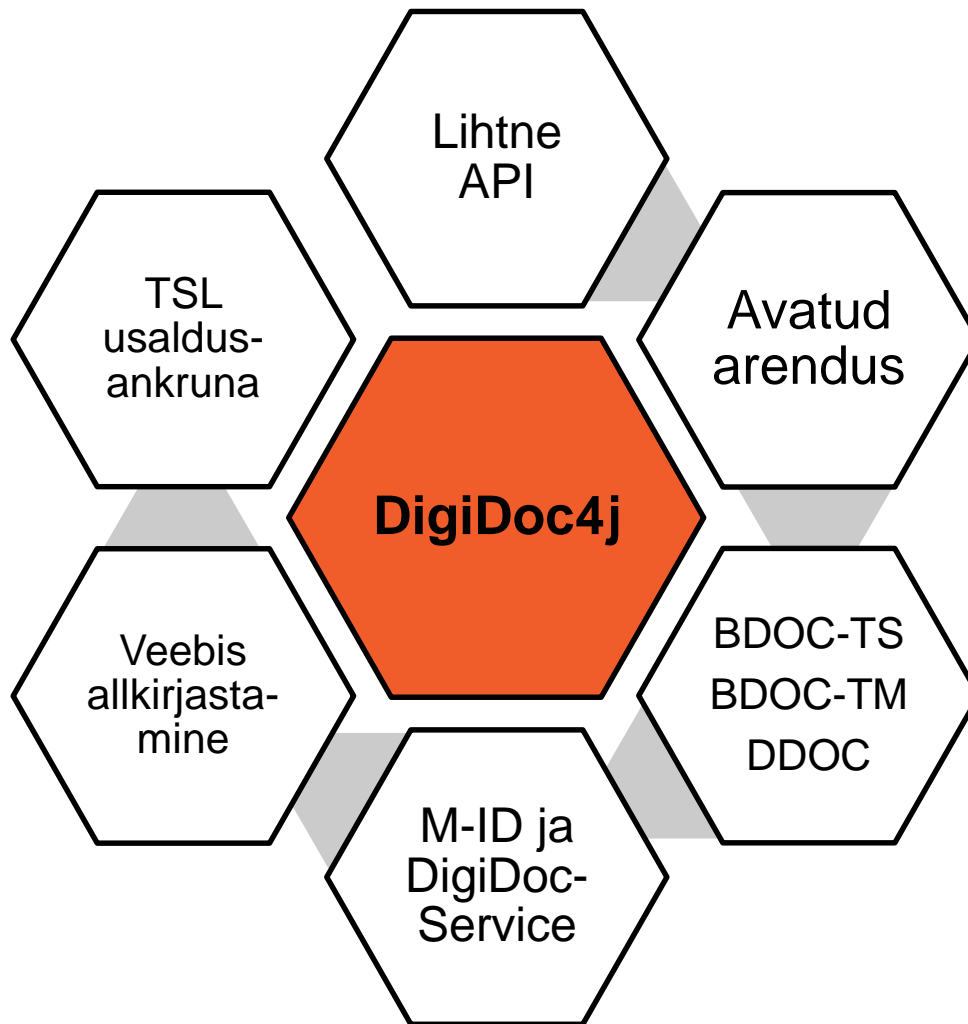
## JDigiDoc Programmer's Guide

Document Version: 3.12

Library Version: 3.12

Last update: 22.02.2016

# DigiDoc4j teegi ülevaade





# Avatud arendus - DigiDoc4j Pivotal



The screenshot displays the Pivotal Tracker interface for the project 'DigiDoc4j (Public)'. It is divided into three main columns: 'Current', 'Backlog', and 'Icebox'. Each column contains a list of tasks with their respective status, priority, and due dates.

- Current (10 points):**
  - Task 67 (1 Oct - Current, 0 of 9 pts): Update Javadoc and wiki to the new API (RV) **doc** (Status: Finish)
  - Task (Possibly addDataFile() method should return DataFile object (RV) **api, feedback from integrators, public-0.3.0-beta** (Status: Accept/Reject)
  - Task (Verify BDOC with special symbols on datafile name **feedback from integrators, validation** (Status: Start)
  - Task (Analyse workload for adding whole signature XML to BDOC container **testing requirements** (Status: Start)
  - Task (Improve cross usage tests **testing requirements** (Status: Start)
  - Task (github home page improvement **doc** (Status: Start)
- Backlog (10 points):**
  - Task 68 (8 Oct, 10 pts): Correct 4 d4j unittests **testing requirements** (Status: Start)
  - Task (Generate random nonce for OCSP request for TS signature (Status: Start)
  - Task (Make DDocContainer configuration thread safe **feedback from integrators** (Status: Start)
  - Task (Validation error: time-stamp hash does not match signature **dds, validation** (Status: Start)
  - Task (BDOC TM and TS crossusage (in a single container) (RV) (Status: Start)
  - Task 69 (15 Oct, 8 pts): Optimize signature validation speed **feedback from integrators, non-functional requirements, validation** (Status: Start)
  - Task (OCSP requests fail (Status: Start)
- Icebox:**
  - Task (BDoc-TM signature profile should be LT\_TM (Status: Start)
  - Task (Default TEST configuration uses live time-stamp service (Status: Start)
  - Task (New test TSL for library **tsl support** (Status: Start)
  - Task (Add more code samples to documentation (RV) **doc, feedback from integrators** (Status: Start)
  - Task (Make two error situations distinguishable: OCSP service not accessible; cert status in OCSP response unknown **dds, feedback from integrators** (Status: Start)
  - Task (Public build (Status: Start)
  - Task (Merge DSS 4.5 changes (RV) (Status: Start)
  - Task (Add possibility to choose the signature hash algorithm, e.g. SHA-256, SHA-224 **api, general requirements** (Status: Start)
  - Task (Add possibility to recognize (Status: Start)

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

# Avatud arendus - DigiDoc4j GitHub



open-eid / digidoc4j

Unwatch 16 Unstar 9 Fork 5

DigiDoc for Java. Javadoc: <http://open-eid.github.io/digidoc4j>

854 commits 2 branches 36 releases 7 contributors

Branch: master digidoc4j / +

Release notes for 0.3.0 beta3

rvillido authored a day ago latest commit 9a4bbab7c1

.idea	#102001330 Refactored API. Added Builders, changed container interfac...	27 days ago
.settings	Nortal Digidoc4J fixes	7 months ago
conf	Nortal Digidoc4J fixes	7 months ago
doc	#83840120, #83840210 Minor fixes to javadoc overview page	9 months ago
lib	Fixed merge problems. Updated DSS library	3 months ago

Code Issues 0 Pull requests 0 Wiki dok Pulse Graphs

HTTPS clone URL <https://github.com>

lähtekood ja commit ajalugu

<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/>

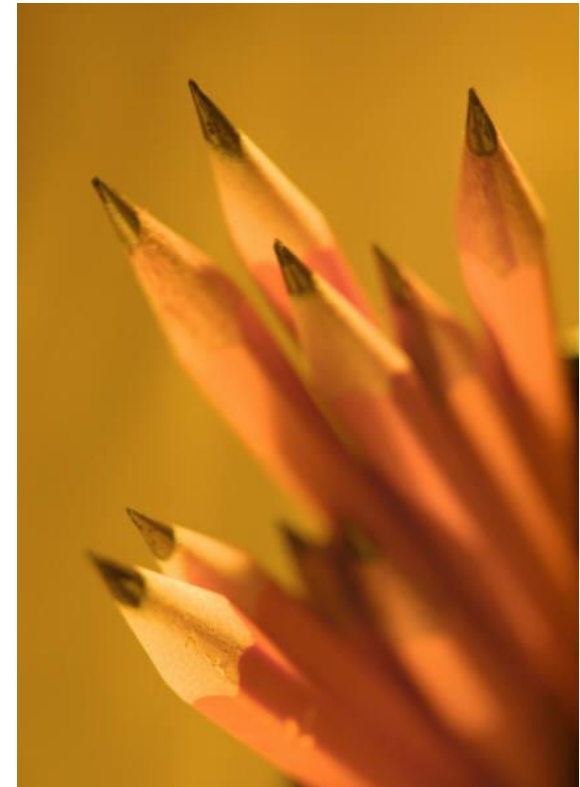
<https://github.com/open-eid/digidoc4j/wiki>

## Arendajate tugi:

[support@sk.ee](mailto: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](http://www.sk.ee)

**Aitäh!**