Nortal

nortal.com

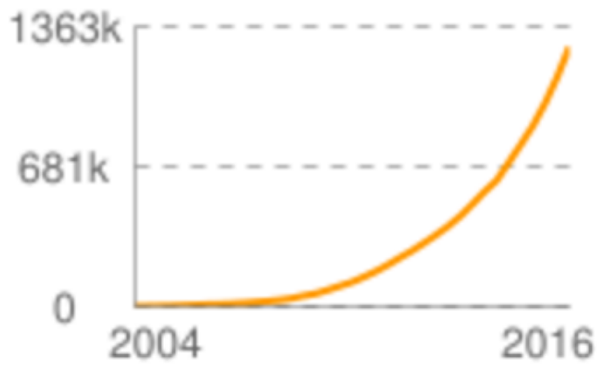
DigiDoc4j üleminek

Rainer Villido

Kavas rääkida

- Üleminek vanalt jDigidoc teegilt
- Uus teek & API
- Wiki ja Q&A dokumentatsioon
- TL Laadimine & Performance
- Korduma kippuvad küsimused

Artifacts/Year



Popular Categories

Aspect Oriented
Actor Frameworks
Application Metrics
Build Tools
Bytecode Libraries
Command Line Parsers
Cache Implementations
Cloud Computing
Code Analyzers
Collections
Configuration Libraries
Core Utilities

DigiDoc4j » 1.0.3

DigiDoc4j

org.digidoc4j » digidoc4j » 1.0.3

DigiDoc4j is a Java library for digitally signing documents and creating digital signature containers of signed documents

Artifact	Download (JAR) **(386 KB)**
POM File	View
Date	(May 03, 2016)
HomePage	https://github.com/open-eid/digidoc4j
Issue Tracker	https://www.pivotaltracker.com/n/projects/1110130

Maven | Gradle | SBT | Ivy | Grape | Leiningen | Buildr

```
<dependency>
  <groupId>org.digidoc4j</groupId>
  <artifactId>digidoc4j</artifactId>
  <version>1.0.3</version>
</dependency>
```

Uus teek: DigiDoc4j

- Maven Central Repost kättesaadav
- Uus API
- Builder Pattern
- Andmed sisse, digiallkiri välja
- Kasutajasõbralik (programmeerijale)
- Lihtsam, arusaadavam
- Tehnilised detailid on peidetud
- Laiendatav uutele formaatidele

Vanalt teegilt üleminek

- TSL (Trusted List)
  - Tulemüüri pordid lahti
- Sertifikaate pole vaja konfida
- Thread safety (paralleelsuse tugi)
- API on muutunud (lihtsamaks)
- Puudub “RAW” (valmis XAdES) allkirja lisamine
- DigiDocService (Mobiili ID) kasutamine ilma RAW allkirjata

Wiki ja Q&A

- Dokumentatsioon Githubis
- Wiki
- Palju näiteid
- Küsimused & Vastused
- Open Source kommuun (Githubi bugid jms)

Simple signing example with a signature token

This example uses a private key stored on a disk to sign two text files.

The private key is stored in the file called "signout.p12" which is protected with password "test".

```
//Create a container with two text files to be signed
Container container = ContainerBuilder.
    aContainer().
    withDataFile("testFiles/legal_contract_1.txt", "text/plain").
    withDataFile("testFiles/legal_contract_2.txt", "text/plain").
    build();

//Using the private key stored in the "signout.p12" file with password "test"
String privateKeyPath = "testFiles/signout.p12";
char[] password = "test".toCharArray();
PKCS12SignatureToken signatureToken = new PKCS12SignatureToken(privateKeyPath, password);

//Create a signature
Signature signature = SignatureBuilder.
    aSignature(container).
    withSignatureToken(signatureToken).
    invokeSigning();

//Add the signature to the container
container.addSignature(signature);
```

How to clear TSL cache

- If you discover that the trusted certificates (like root CA, Timestamp etc) are not updated, then it might help to clear TSL cache.
- TSL is cached in two locations in the temp directory set with the `java.io.tmpdir` property:
  - `java.io.tmpdir/dss-cache-tsl`
  - `java.io.tmpdir/digidoc4jTSLCache`
- Depending on your operating system, the default `java.io.tmpdir` property may point to
  - `/tmp` on **Linux** (`/tmp/dss-cache-tsl` and `/tmp/digidoc4jTSLCache`)
  - `C:\Users\_admin_\AppData\Local\Temp\` i.e. `%TEMP%` on **Windows** (`%TEMP%\dss-cache-tsl` and `%TEMP%\digidoc4jTSLCache`)
  - Somewhere obscure like `/var/folders/_4/8979h_s11kvbylb3d5p_fydm0000gn/T/` on **OSX**.
- Just delete all the files stored in the two directories

Getting an error while trying to test

- If you get an error like this `java.io.FileNotFoundException: test-tsl/trusted-test-mp.sha2` (or `trusted-test-mp.xml`)
- Then take a look at this
- We do not include test certificates in DigiDoc4j jar file so it must be configured separately.
- Great Harm may happen if someone uses test certificates in production.

TSL - Trust List

- EU digiallkirjade tugi out-of-the-box
- Keskne Euroopa TSL (Trust List)
- Usaldatud sertifikaadid
- Teek uuendab automaatselt
- Kord päevas (by default)
- Laadimine 5-15 sekundit üle interneti

Performance

- Versioonide võrdlus (Test keskkonnas)
- 0.3.0 Beta 2 ~ **342 ms** (max 2 270 ms)
- 1.0.0 ~ **544 ms** (max 5 040 ms)
- 1.0.2 ~ **44 ms** (max 388 ms)
- 1.0.3 ~ **42 ms** (max 381 ms)

Performance

- Teegi kasutamise kiirus
- Alguses suur probleem
- Läinud järjest paremaks
- jDigidoc ~**10ms**
- DigiDoc4j ~**42ms**
- Vahe **~32ms**
- Kogu EU TSL-ga **~140ms**
- Parem multithreadingu tugi

Performance

- Esimene valideerimine on aeglane
- Edasi kiire
- TSL laadimine ~5 sekundit (kuni 15)
- Esmane valideerimine ~400ms
- = Suur Ehmatus
- Edasi ~40ms
- Jätkame optimeerimist

Arendus

- Open Source, Github
- Agiilne
- Vastavalt kasutajate tagasisidele
- Paindlik arendusprotsess
- Iga nädal vaatame prioriteedid üle
- **Pull requestid oodatud**

Valideerumise vead

- Ei valideeru D4J-ga
- Põlve otsas on tehtud konteinereid
- Ei vasta standardile
- Nt kusagil on slash “/“ tagurpidi
- Kasutage ametlikke teeke

Q & A

- OCSP päringud ebaõnnestuvad
  - Vaja õigesti konfida
  - Juurdepääsutõend või IP
- Veebis allkirjastamine
  - DEMO rakendus (wikis viide)
  - hwcrypto.js

idCard.js -> hwcrypto.js

- Eelmisel kevadel
- Chrome tugi
- Asünkroonsus
- ilma page reloadita
- Uus API

Tulemas järgmisesse reliisi

- Logback rikub logimise ära
- PKCS#11 tugi
- Proxy tugi
  - Oleme prioriteeti tõstnud

Nortal

nortal.com

Tänud!

Qüsimusi?