



RIIGI INFOSÜSTEEMI AMET

PDF-allkirjade valideerimisvõimaluse st.

Tõnis Reimo
eID analüütik

Signeeritud PDF failide valideerimine

Miks?

- eIDASe rakendumine alates 01 Juuli.
- PDF vormingu laialdane kasutus.
- Tõenäoliselt on allkirjastatud PDF kõige enam Eestisse rahvusvaheliselt saadetakse vorming.

PDF'i valideerimise võimalused

- Acrobat Readeriga

Ei kontrolli allkirjastaja sertifikaadi usaldusväärset
EL usaldusnimekirja baasil.

Ei kontrolli kvalifitseertud sertifikaatide kasutamist

- Valideerimisteenusega - SiVa

Valmib 2016 lõpul

PDF ja Eesti vanemate konteineriformaatide
valideerimine

Liidestumine üle JSON ja X-Tee

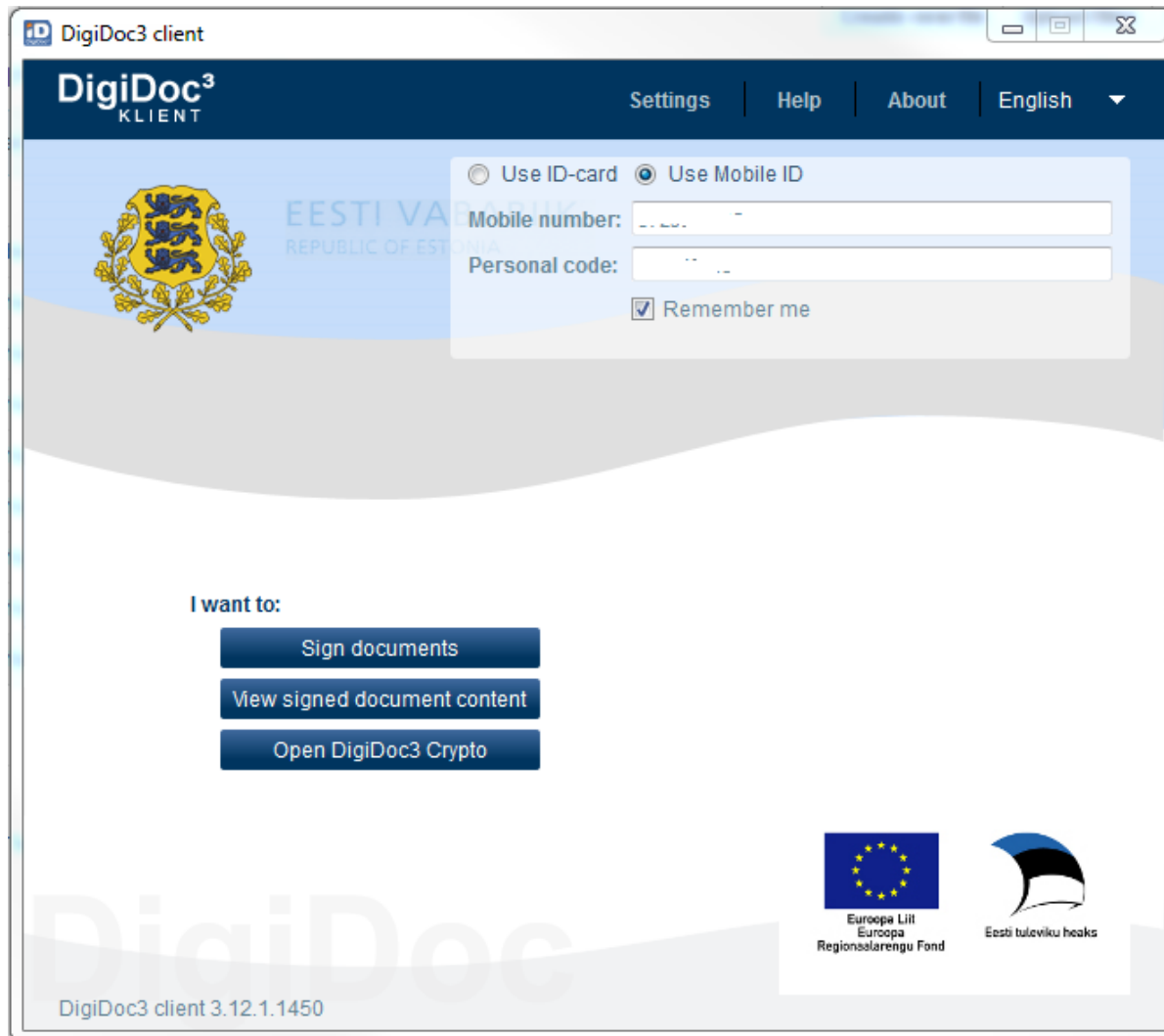
- DigiDoc Kliendiga

Testkasutuses kuni 1. Juuli 2016

PDF Valideerimispoliitika

- EL standarditest ja nõuetest valideerimisele – tunnistatakse ainult täiustatud e-allkirja millel on:
 - PADES LT või LTA vorming
 - OCSP kehtivuskinnitus ja allkirja ajatempel
- Tühistusnimekirju (CRL) ei kasutata. OCSP on kohustuslik.
- DSA algoritm ei ole lubatud.
- Allkirjastaja sertifikaat peab olema mõeldud digitaalseks allkirjastamiseks.

PDF Valideerimine DigiDoc kliendiga



PDF Valideerimine DigiDoc kliendiga

The screenshot displays the DigiDoc3 client interface for validating a PDF document. The window title is "hellopades-lt-sha512.pdf". The header includes the DigiDoc3 logo and navigation links for Settings, Help, About, and English. The main area features the Estonian coat of arms and the text "EESTI VABARIIK REPUBLIC OF ESTONIA". A login panel allows users to choose between "Use ID-card" and "Use Mobile ID", with fields for "Mobile number" and "Personal code", and a "Remember me" checkbox. Below the login panel, the "Container:" field shows the file path "hellopades-lt-sha512.pdf" with a "Save" button. The "Container content:" section lists the file "hellopades-lt-sha512.pdf" (91 KB) with a "Save files to disk" button. The "Signature" section shows a signature by "Veiko ..." signed on "07. August 2015 time 10:51", with the status "Signature is valid" and a "Show details" link. At the bottom, there are links for "Send container to email", "Browse container location", "Print summary", and "Encrypt document", along with "Add signature" and "Close" buttons. The footer indicates the version "DigiDoc3 client 3.12.1.1450".

hellopades-lt-sha512.pdf

DigiDoc³
KLIENT

Settings | Help | About | English

Use ID-card Use Mobile ID

Mobile number:

Personal code:

Remember me

Container: [Save](#)

Container content:

hellopades-lt-sha512.pdf 91 KB

[Save files to disk](#)

Signature

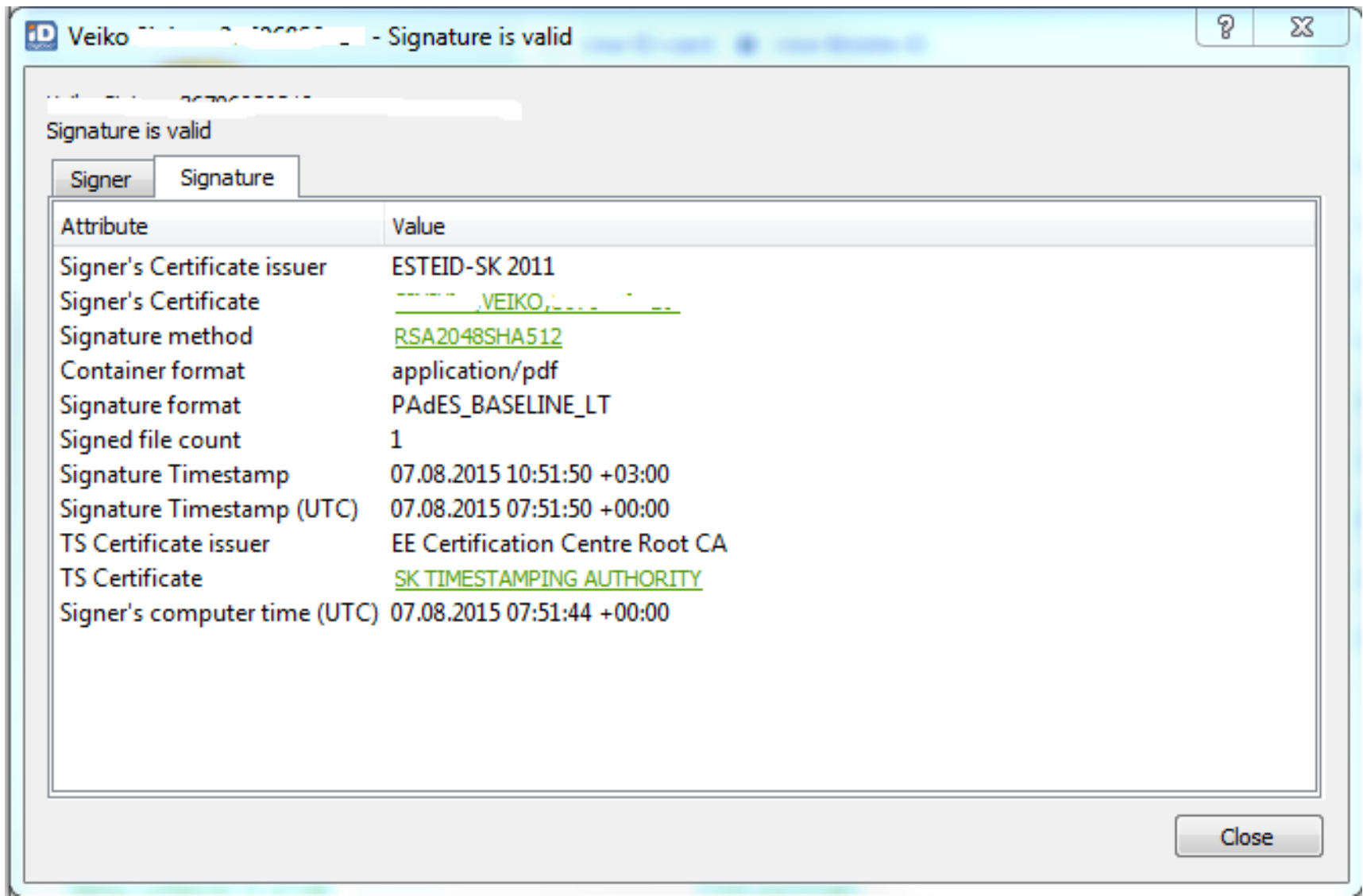
Veiko ...
Signed on 07. August 2015 time 10:51
Signature is valid [Show details](#)

[Send container to email](#) [Print summary](#)
[Browse container location](#) [Encrypt document](#)

[Add signature](#) [Close](#)

DigiDoc3 client 3.12.1.1450

PDF Valideerimine DigiDoc kliendiga



The screenshot shows a dialog box titled "Veiko [redacted] - Signature is valid". The dialog box contains a table with two columns: "Attribute" and "Value". The table lists various attributes related to the signature, such as the signer's certificate issuer, signature method, and timestamp. The "Value" column contains the corresponding values, some of which are underlined in green. A "Close" button is located at the bottom right of the dialog box.

Signature is valid

Attribute	Value
Signer's Certificate issuer	ESTEID-SK 2011
Signer's Certificate	<u>[redacted].VEIKO.[redacted]</u>
Signature method	<u>RSA2048SHA512</u>
Container format	application/pdf
Signature format	PADES_BASELINE_LT
Signed file count	1
Signature Timestamp	07.08.2015 10:51:50 +03:00
Signature Timestamp (UTC)	07.08.2015 07:51:50 +00:00
TS Certificate issuer	EE Certification Centre Root CA
TS Certificate	<u>SK TIMESTAMPING AUTHORITY</u>
Signer's computer time (UTC)	07.08.2015 07:51:44 +00:00

Close

Viited

- <http://open-eid.github.io/pdf-validator/appendix/appendix-3/>
- <https://github.com/open-eid/pdf-validator>



RIIGI INFOSÜSTEEMI AMET

Aitäh!

Tonis.reimo@ria.ee