SiGa tehniline kirjeldus

AARE NURM, NORTAL AS

21.11.2019

Tehniline ülevaade Allkirjastamisteenusega liidestumisest.

1. Allkirjastamisteenuse üldine kirjeldus
2. DigiDocSerivce-i ja Allkirjastamisteenuse funktsionaalsuse võrdlus
3. Liidestumise protsess
4. Liidese tehniline kirjeldus
5. SiGa paigaldus liidestumise katsetamiseks
6. Liidestumise dokumentatsioon
7. Demo
8. Küsimused ja vastused

1. Allkirjastamisteenuse üldine kirjeldus

Põhimõisted

- Allkirjastamisteenus – RIA poolt pakutav teenus konteinerite ja allkirjade loomiseks.
- SiGa (Signature Gateway) – tarkvara, https://github.com/open-eid/SiGa
- Konteiner – andmefailide ja allkirjade kogum (kindla formaadiga zip arhiiv).
- Allkiri – Omab erinevat tähendust. Konteineris on isiku allkirjad (signatures.xml failis). Madalal tasemel tähendab privaatvõtmega räsi krüpteerimist.
- BDOC – Eesti spetsiifiline konteineri ja allkirja formaat. Sisaldab TimeMark allkirju.
- ASICE – Euroopa Liidus standardiseeritud konteineri formaat. Sisaldab TimeStamp allkirju.
- Hashcode konteiner – SiGa spetsiifiline konteineri formaat andme edastuseks.

1. Allkirjastamisteenuse üldine kirjeldus

Põhimõisted

- TimeStamp (TS) – ajatempel, tõestus andmete eksisteerimisest antud ajahetkel.
- TimeMark (TM) – ajamärgend, tõestus andmete eksisteerimisest antud ajahetkel läbi OCSP.
- OCSP – kehtivuskinnitus. Meie kontekstis SK ID Solutionsi poolt pakutav kehtivuskinnitus (nö tasuline teenus).
- AIA OCSP – kehtivuskinnitus. Meie kontekstis SK ID Solutionsi poolt pakutav kehtivuskinnitus (nö tasuta teenus).

1. Allkirjastamisteenuse üldine kirjeldus

Allkirjastamisteenus

- Teenus avalikule sektorile konteinerite loomiseks, allkirjastamiseks ja allkirjade valideerimiseks.
- Alternatiiv järgmisel aastal (oktoober 2020) suletavale DigiDocService teenusele.
- Üks leping Riigi Infosüsteemi Ametiga, ei vaja eraldi lepinguid MIDi, TS ja OCSP jaoks.
- Ühtne liidestus konteinerite loomiseks, MIDiga allkirjastamiseks ja allkirjade valideerimiseks.
- Toetab ASICE (TS + AIA OCSP) ja BDOC (TimeMark) konteinerite formaate.
  - Soovituslik on kasutada ASICE formaati

2. DDS-i ja Allkirjastamisteenuse võrdlus

Funktsionaalsuse võrdlus

Functionality	DigiDocService	SiGa	Comment
Container creation	Yes	Yes	Creating new containers
Adding signatures	Yes	Yes	Adding signatures to signed containers
Support for BDOC and ASICE containers	Yes	Yes	Supports the hashcode form
Support for DDOC container	Yes	**No**	Not possible to use
Container hashcode form	Yes	Yes	Same hashcode format

2. DDS-i ja Allkirjastamisteenuse võrdlus

Funktsionaalsuse võrdlus

Functionality	DigiDocService	SiGa	Comment
Signing with external device	Yes	Yes	ID card, e-seal, ... (certificate must be in Estonian TSL)
Signing with Mobile-ID	Yes	Yes	SiGa supports only Estonian Mobile-ID
Authentication with Mobile-ID	Yes	**No**	SiGa is purely signing/container service, use TARA for authentication
Verification of certificate validity	Yes	**No**	Not possible to validate
Signature validation	Yes	Yes	SiGA uses Valideerimisteenus (SIVA) for validation

2. DDS-i ja Allkirjastamisteenuse võrdlus

Üldised erinevused

General differences	DigiDocService	SiGa	Comment
Protocol	SOAP/XML	REST/JSON	API is described in WADL
Hashcode container format	DigiDocService	DigiDocService	Same hahscode container format is used
Access to service	IP based	HMAC based authorization	Each request must be signed by e-service

2. DDS-i ja Allkirjastamisteenuse võrdlus

Meetodite võrdlus

- https://github.com/open-eid/SiGa/wiki/DigiDocService-comparision#method-differences

3. Liidestumise protsess

RIA Allkirjastamisteenuga liitumine

- Teenusega liitumine käib läbi help@ria.ee
- Teenuse liitumisega seotud info saab olema www.ria.ee
- Liidestumine koosneb kahest etapist:
  - Demo keskkond – liidestumise arendamiseks ja testimiseks
  - Toodangukeskkond – toodangus kasutamiseks

- Demo keskkonnas on võimalik kasutada ainult TEST allkirjastamisvahendeid (MID, ID-kaart, digitempel).

4. Liidese tehniline kirjeldus

Kasutaja autoriseerimise põhimõtted

- Igal liidestuval teenusel on unikaalne kasutajatunnus (UUID) ja saladus (signing secret).
- Kõik saadetavad päringud allkirjastatakse kasutades antud saladust.
  - Allkiri koostatakse HMAC väärtusena kasutades päiseid, meetodit, url konteksti ja päringu keha.

4. Liidese tehniline kirjeldus

Päringu päised

Header	Mandatory	Default value	Description
X-Authorization-Timestamp	+	-	Timestamp of request generation from client side. UTC timestamp of client system with precision 1 second.
X-Authorization-ServiceUUID	+	-	Unique identifier of the relying party e-service. Used to determine client and e-service making the actual request.
X-Authorization-Signature	+	-	Hex encoded value of hmac hash of the canonicalized request data (authentication headers and body contents).
X-Authorization-Hmac-Algorithm	-	HmacSHA256	Algorithm used for Hmac calculation.
Content-Type	for POST and PUT only	-	The Media type of the body of the request (used with POST and PUT requests). Only supported value is application/json; charset=UTF-8

4. Liidese tehniline kirjeldus

Päringu allkirja moodustamine

- https://github.com/open-eid/SiGa/wiki/Authorization#signature-creation-process

4. Liidese tehniline kirjeldus

Hashcode konteiner

- Hashcode konteineri kasutamise eelisteks on allkirjastatavate andmete konfidentsiaalsus ning mahupiirangute puudumine.
- Hashcode konteiner on mõeldud ainult vajalike andmete transpordiks liidestunud e-teenuse ja Allkirjastamisteenuse vahel.
- Konteineri struktuur on identne DigiDocService-s kasutatuga.
- https://github.com/open-eid/SiGa/wiki/Hashcode-container-form

4. Liidese tehniline kirjeldus

Loo uus konteiner ja allkirjasta kasutades Mobiil-ID-d

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-main-flows#create-hashcode-container-and-sign-with-mid

4. Liidese tehniline kirjeldus

Meetodid ja nende parameetrid

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#creating-container
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#start-mobile-id-signing
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#request-mobile-id-signing-status
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#request-hashcode-container
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#delete-hashcode-container

4. Liidese tehniline kirjeldus

Laadi üles allkirjastatud konteiner ja allkirjasta kasutades ID kaarti

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-main-flows#upload-signed-hashcode-container-and-sign-externally-with-id-card

4. Liidese tehniline kirjeldus

Meetodid ja nende parameetrid

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#upload-container
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#start-remote-signing
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#finalize-remote-signing

4. Liidese tehniline kirjeldus

Valideeri allkirjastatud konteinerit

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-main-flows#validate-hashcode-container

4. Liidese tehniline kirjeldus

Meetodid ja nende parameetrid

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#request-validation-of-hashcode-container-in-session
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#request-validation-of-hashcode-container-without-session

4. Liidese tehniline kirjeldus

Andmefailide käsitluse meetodid ja parameetrid

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#add-datafiles-to-unsigned-container
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#get-data-files-list
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#delete-datafile-from-unsigned-container

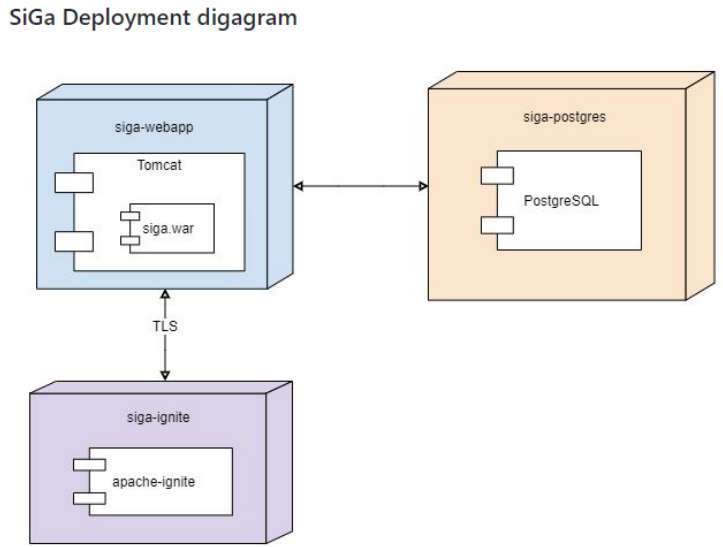
4. Liidese tehniline kirjeldus

Allkirjade käsitluse meetodid ja parameetrid

- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#request-signature-list-of-given-hashcode-container
- https://github.com/open-eid/SiGa/wiki/Hashcode-API-description#request-signer-info-on-given-signature

5. SiGa paigaldus liidestumise katsetamiseks

- Kasutada Ignite 2.7.5 versiooni
  - Vajab seadistamist!
- Testimiseks võib kasutada ka H2 sisemist andmebaasi (vaikeväärtus)
- Oluline on rakendus käivitada kasutades õigeid profiile: digidoc4jTest
- Kasutaja andmed leiab GitHubist
- Teeme dockerfile-i



6. Liidestumise dokumentatsioon

SiGa dokumentatsioon

- Liidese dokumentatsioon: https://github.com/open-eid/SiGa/wiki
- Paigalduse dokumentatsioon: https://github.com/open-eid/SiGa/blob/master/README.md
- Näidisrakenduse kood: https://github.com/open-eid/SiGa/tree/develop/siga-sample-application

7. Demo

MID ja ID kaardi allkirjastamise vood kasutades demorakendust

8. Küsimused ja vastused

- Oodatud on tagasiside nii teenusele kui tarkvarale.
- Tarkvara ning avaliku dokumentatsiooniga seotud teemad võib raporteerida läbi GitHubi: https://github.com/open-eid/SiGa/issues
- Oodatud on ka pull requestid
- Allkirjastamisteenusega seotud küsimused help@ria.ee