CYBERNETICA

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

CDOC 2.0 võtmeedastusserver

Arhitektuuridokument

Version 1.2

31.01.2023

ID D-19-13

Date	Version	Description
27.04.2022	1.0	Esialgne versioon
07.12.2022	1.1	Uuendatud versioon 2 rakendusserveriga
31.01.2023	1.2	Uuendatud versioon OSCP serveriga

Sisukord

1 Sissejuhatus

See dokument kirjeldab CDOC 2.0 võtmeedastusserveri arhitektuuri ja kasutatavaid tehnoloogiaid.

CDOC 2.0 [1] on failide salastamiseks mõeldud andmevorming. CDOC 2.0 konteinereid võib edastada üle avalike sidekanalite. Täiendava tulevikuturvalisuse saavutamiseks näeb CDOC 2.0 ette võimaluse eraldada failide dekrüpteerimiseks vajalik võtmekapsel üle avaliku võrgu liikuvast konteinerist ning edastada see vastuvõtjatele kasutades täiendavalt turvatud sidekanaleid.

Võtmeedastusserver on CDOC 2.0 süsteemi komponent, mis loob võtmekapsli edastamiseks vajaliku täiendavalt turvatud sidekanali saatja ja vastuvõtja vahel. Võtmeedastusserver pakub saatjale teenust võtmeedastuskapsli üleslaadimiseks ning vastuvõtjale teenust võtmeedastuskapsli allalaadimiseks.

Mõlemad teenused kasutavad HTTPS protokolli. Saatjale mõeldud teenus ei autendi saatjat — seda saavad kasutada kõik. Vastuvõtjale mõeldud teenus autendib vastuvõtjat TLS kliendi autentimise abil — seda saavad kasutada vaid toetatud eID vahendit (näiteks ID-kaart) omavad kasutajad.

Võtmeedastusserver talletab töökindlalt saatjate poolt edastatud võtmekapslid oma andmebaasis. Võtmeedastusserver kustutab võtmekapslid määratud aja möödumisel, et vähendada võtmeserveri võimalikul kompromiteerumisel tekkivat kahju

1.1 Viited

[1] Cybernetica AS. *CDOC 2.0 spetsifikatsioon*. D-19-12 0.7. November 2022.

2 Võtmeedastusserveri arhitektuur

CDOC 2.0 võtmeedastusserver koosneb järgnevatest komponentidest:

2.1 Server

Server koosneb kahest iseseisvast Spring Boot rakendusest:

2.1.1 Üleslaadimisrakendus

Üleslaadimisrakendus (`put-server`) pakub võtmekapslite loomise teenust ilma klienti tuvastamata.

2.1.2 Allalaadimisrakendus

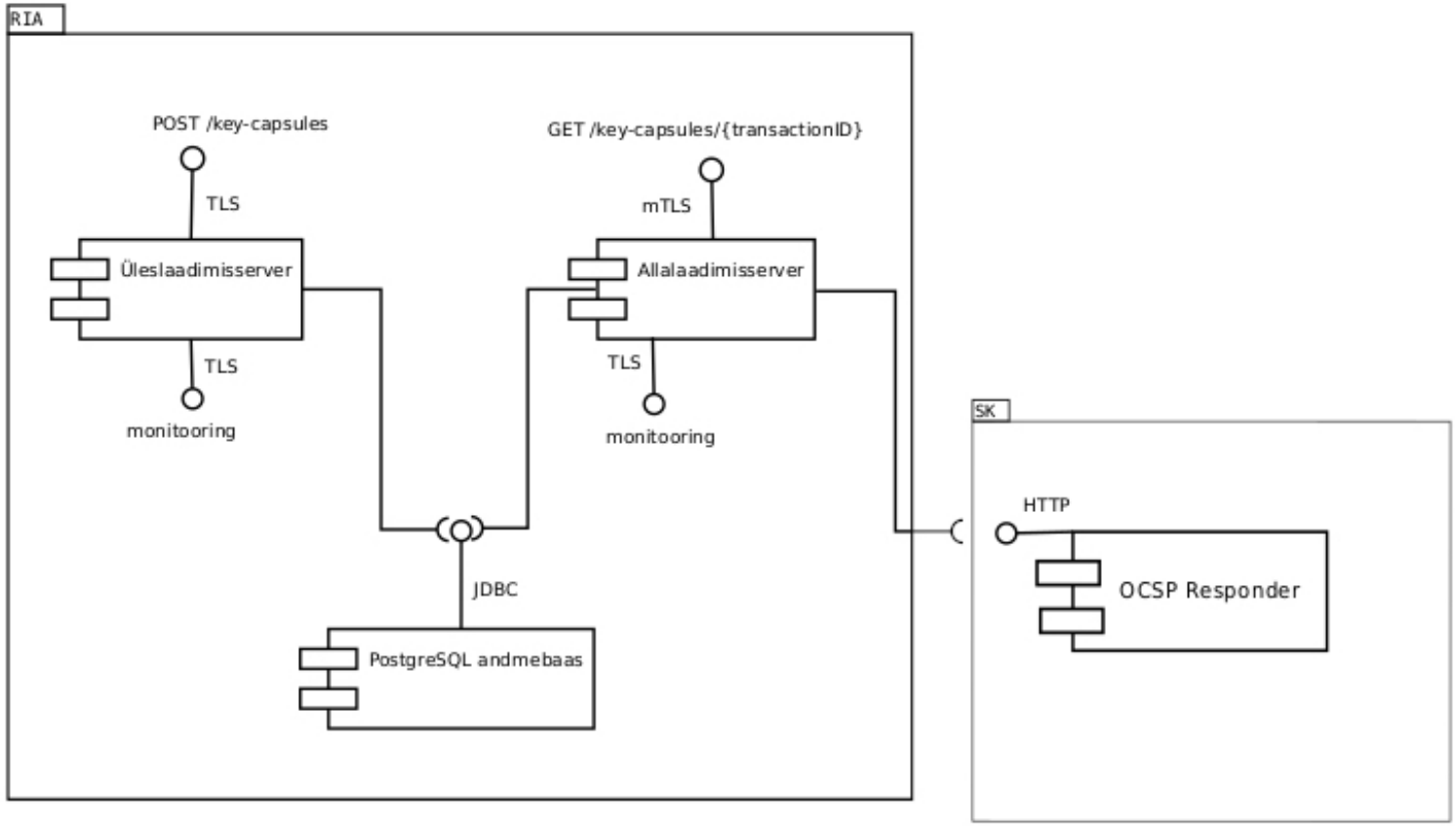
Allalaadimisrakendus (`get-server`) pakub võtmekapslite küsimise teenust, mis teostab kliendi tuvastamist (`mutual TLS`).

Võtmeedastusserveri teenuste detailne OpenAPI liides on kirjeldatud CDOC 2.0 spetsifikatsioonis [1].

2.2 Andmebaas

Võtmekaspslid salvestatakse PostgreSQL andmebaasi.

Andmebaasistuktruuride loomine ja uuendamine teostatakse `Liquibase` migratsioonide kaudu.



Joonis 1. CDOC 2.0 võtmeedastusserveri komponendid.

3 Kasutatavad tehnoloogiad

- Maven 3.8.x
- Java 17
- Spring Boot 2.0
- OpenAPI generator
  - client
  - spring
- Bouncy Castle Crypto
- FlatBuffers
- Apache Commons Compress
- PostgreSQL
- Liquibase
- SLF4J