Kõrge terviklusega andmeid talletatava andmebaasilahenduse prototüüp

Keijo Kapp

Juhendajad: Tarmo Teder
Deivis Treier

Siseministeeriumi Infotehnoloogia- ja Arenduskeskus

Siseministeeriumi Infotehnoloogia- ja Arenduskeskus

- >250 töötajat

Siseministeeriumi Infotehnoloogia- ja Arenduskeskus

- >250 töötajat
- 6 valdkonda:
  - piirivalve- ja rahvastikukorraldus
  - pääste ja hädaabi
  - politsei
  - siseturvalisus
  - tehnoloogiavaldkond
  - teenindusvaldkond

ISKE

ISKE

Kolmeastmeline etalonturbe süsteem

ISKE

Kolmeastmeline etalonturbe süsteem

- konfidentsiaalsus

ISKE

Kolmeastmeline etalonturbe süsteem

- konfidentsiaalsus
- käideldavus

ISKE

Kolmeastmeline etalonturbe süsteem

- konfidentsiaalsus
- käideldavus
- terviklus

ISKE

Kolmeastmeline etalonturbe süsteem

- konfidentsiaalsus
- käideldavus
- terviklus
  - HT.10 – Andmebaasi kirjete krüptoaheldamine

ISKE

Kolmeastmeline etalonturbe süsteem

- konfidentsiaalsus
- käideldavus
- terviklus
  - HT.10 – Andmebaasi kirjete krüptoaheldamine
  - HT.34 – Digiallkirja kasutamine

ISKE

Kolmeastmeline etalonturbe süsteem

- konfidentsiaalsus
- käideldavus
- terviklus
  - HT.10 – Andmebaasi kirjete krüptoaheldamine
  - HT.34 – Digiallkirja kasutamine
  - Kirjete revisioonide hoidmine

Krüptoaheldamine

Krüptoaheldamine

- kirjete krüptograafiline sidumine

Krüptoaheldamine

- kirjete krüptograafiline sidumine
- ridadest räside arvutamine

Krüptoaheldamine

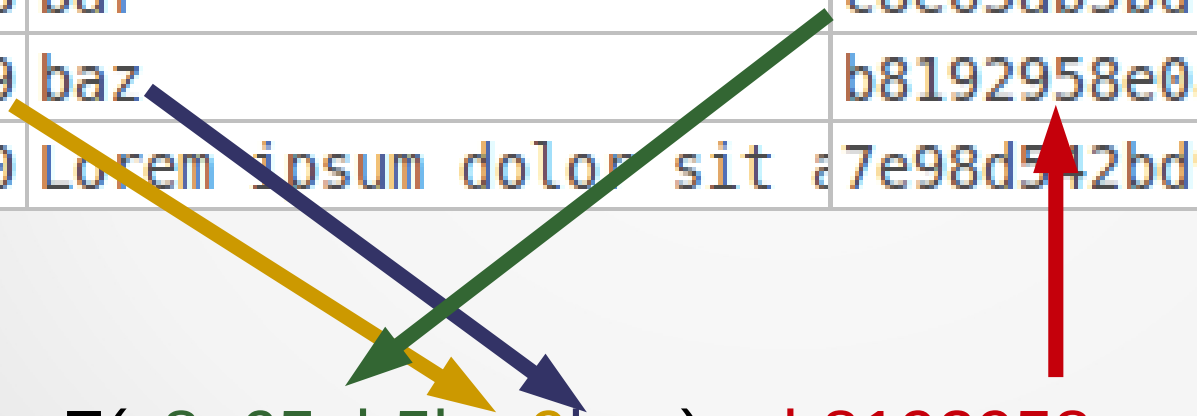
- kirjete krüptograafiline sidumine
- ridadest räside arvutamine
- päästikute (triger) kasutamine

Krüptoaheldamine

- kirjete krüptograafiline sidumine
- ridadest räside arvutamine
- päästikute (triger) kasutamine
- ahelda lülide (räside) saatmine kolmandale osapoolele

Krüptoaheldamine

id bigint	data text	hashchain character varying(255)
7	foo	c56061ec02d231cf2b08764e1c
8	bar	c8e65ab5bd727469a891dfe165
9	baz	b8192958e0a30c885cf1b84328
10	Lorem ipsum dolor sit a	7e98d542bd95cee738e59ad3ea



F(c8e65ab5b...9baz) = b8192958e...

Digiallkirjastamine

Digiallkirjastamine

- vastavalt Eesti digitaalallkirja seadusele

Digiallkirjastamine

- vastavalt Eesti digitaalallkirja seadusele
- platvorm: Java/Groovy/Grails

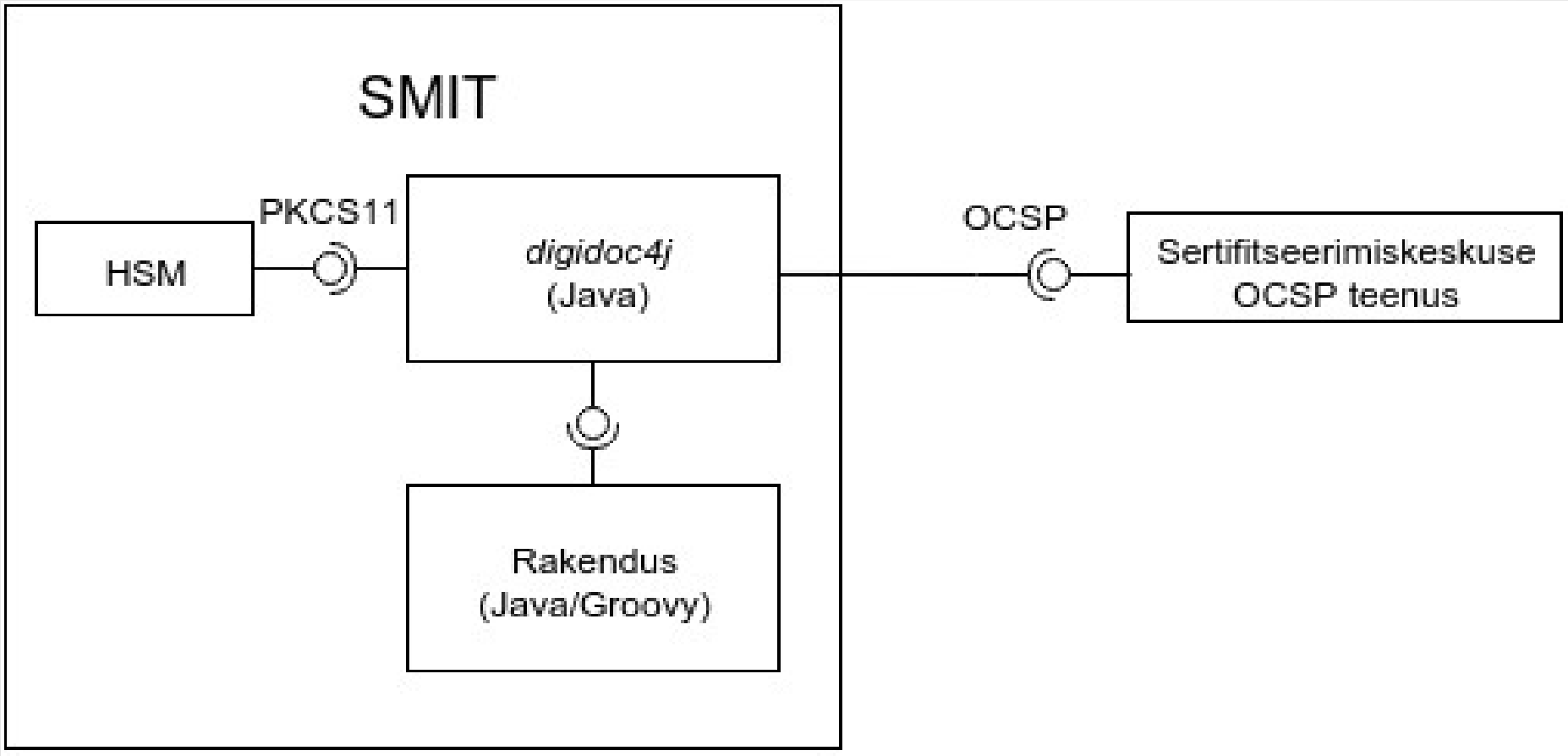
Digiallkirjastamine

- vastavalt Eesti digitaalallkirja seadusele
- platvorm: Java/Groovy/Grails
- *digidoc4j* 1.0

Digiallkirjastamine

- vastavalt Eesti digitaalallkirja seadusele
- platvorm: Java/Groovy/Grails
- *digidoc4j* 1.0
- BDOC / SHA512 / PKCS11 (HSM) / BDOC-TM

Digiallkirjastamine



Andmete revisioonide hoidmine

Andmete revisioonide hoidmine

- nn. „ajalootabelite” kasutamine välistatud

Andmete revisioonide hoidmine

- nn. „ajalootabelite” kasutamine välistatud
- kirjete muutmine välistatud

Andmete revisioonide hoidmine

- nn. „ajalootabelite” kasutamine välistatud
- kirjete muutmine välistatud
- umbes 10 revisiooni andmeobjekti kohta

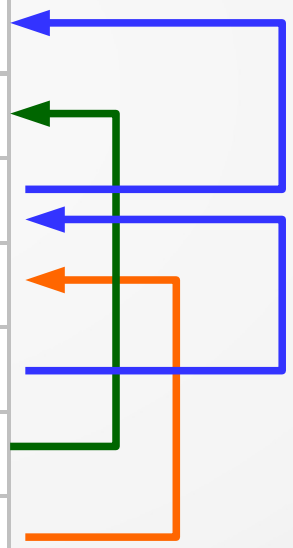
Andmete revisioonide hoidmine

- nn. „ajalootabelite” kasutamine välistatud
- kirjete muutmine välistatud
- umbes 10 revisiooni andmeobjekti kohta
- revisioonide pärimine ei ole tihe tegevus

Andmete revisioonide hoidmine

Rekursiivne viitamine eelmisele revisioonile

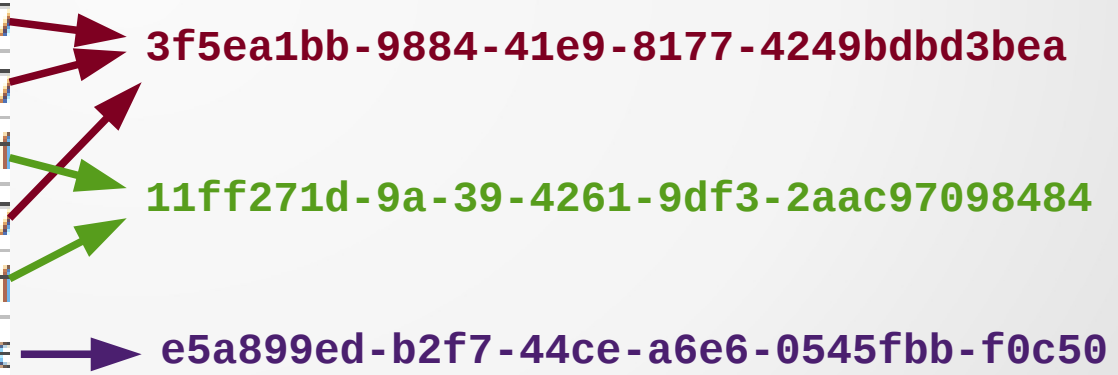
id bigint	previous_revision bigint
1	
2	
3	1
5	
6	3
7	2
8	5



Andmete revisioonide hoidmine

Revisioonide sidumine unikaalse identifikaatoriga

id bigint	object_uuid character varying(36)
1	3f5ea1bb-9884-41e9-817
2	3f5ea1bb-9884-41e9-817
3	11ff271d-9a39-4261-9df
4	3f5ea1bb-9884-41e9-817
5	11ff271d-9a39-4261-9df
6	e5a899ed-b2f7-44ce-a6e



Tänan kuulamast

Retsensendi küsimused

Retsensendi küsimused

1. Mis on räsi ja kuidas see tekitatakse?

Lühidalt: räsifunktsiooni tulemus

Retsensendi küsimused

1. Mis on räsi ja kuidas see tekitatakse?

Lühidalt: räsifunktsiooni tulemus

- Räside omadused:
  - pöördumatus

Retsensendi küsimused

1. Mis on räsi ja kuidas see tekitatakse?

Lühidalt: räsifunktsiooni tulemus

- Räside omadused:
  - pöördumatus
  - konstantne suurusjärk

Retsensendi küsimused

1. Mis on räsi ja kuidas see tekitatakse?

Lihtsaimate algoritmide näited:

F(*x*) = x mod C - 20 mod 7 = 6

F*(x)* = x & C - 00010100_2 & 0111_2 = 100_2 = 4

Turvaliseimateks peetakse SHA perekonna algoritme

Retsensendi küsimused

2. Kui suurt arvutusvõimsust see vajab, kui lahendust hakataks reaalselt kasutama?

(täpsustus: krüptoaheldamine)

- Lühidalt: mitte märkimisväärselt

Retsensendi küsimused

2. Kui suurt arvutusvõimsust see vajab, kui lahendust hakataks reaalselt kasutama?

1. Viimase kirje räsi laadimine vahemälust, andmebaasist või muust allikast
2. Sellest räsist ja sisestatava rea väärtusest uue räsi arvutamine
3. Uue räsi logimine (toimetamine teise administratiivsesse tsooni)
4. Sisestatava rea muutmine kirjutades saadud räsi vastavale väljale.

Retsensendi küsimused

2. Kui suurt arvutusvõimsust see vajab, kui lahendust hakataks reaalselt kasutama?

1. Viimase kirje räsi laadimine vahemälust, andmebaasist või muust allikast
2. Sellest räsist ja sisestatava rea väärtusest uue räsi arvutamine
3. Uue räsi logimine (toimetamine teise administratiivsesse tsooni)
4. Sisestatava rea muutmine kirjutades saadud räsi vastavale väljale.

- Testitud on ka suurte andmehulkade genereerimisel.

Retsensendi küsimused

3. Kas Sa tead kus kasutatakse sarnaseid lahendusi praktikas?

(täpsustus: krüptoaheldamine)

- Sertifitseerimiskeskus AS
- Rahvastikuregister

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Krüptoaheldamise turvariskid

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Krüptoaheldamise turvariskid
  - võimalikud veaolukorrad

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Krüptoaheldamise turvariskid
  - võimalikud veaolukorrad
  - käideldavus

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Krüptoaheldamise turvariskid
  - võimalikud veaolukorrad
  - käideldavus
  - administraatori võimalus implementatsiooni eksitada

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Krüptoaheldamise turvariskid
  - võimalikud veaolukorrad
  - käideldavus
  - administraatori võimalus implementatsiooni eksitada
  - logimismehhanismi turvalisus

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Digiallkirjastamise turvariskid

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Digiallkirjastamise turvariskid
  - digiallkirjastamise ja allkirja valideerimise kiirus

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Digiallkirjastamise turvariskid
  - digiallkirjastamise ja allkirja valideerimise kiirus
  - HSM-i PIN-koodi kasutamine

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Andmete revisioonide hoidmine

Retsensendi küsimused

4. Millised on valminud rakenduse turvariskid?

- Andmete revisioonide hoidmine
  - jõudlus

Aitäh!