



TempelPlus kasutusjuhend

Tarkvara versioon: 1.2.0

Kuupäev: 28.01.2013

Sertifitseerimiskeskus AS

2013



Sisukord

1	Sissejuhatuseks	4
2	Versiooniinfo	5
2.1	Versioon 1.2.0, jaanuar 2013	5
2.2	Versioon 1.1.1, oktoober 2012	6
2.3	Versioon 1.1.0, suvi 2012	6
2.4	Versioon 1.0.0, reliisi kuupäev 31.08.2011	7
2.5	Versioon 0.99, beeta, reliisi kuupäev 27.12.2010	8
3	Paigaldamine	8
3.1	Eeldused	8
3.2	Tempelplus'i paigaldamine windowsis	8
3.2.1	Safenet Authentication Client	8
3.2.2	Paigaldamine	8
3.2.3	PKCS11Wrapper	9
3.2.4	Seadistamine	9
3.3	Tempelplus'i paigaldamine linuxis	9
3.3.1	Alustamine	9
3.3.2	Safenet Authentication Client	10
3.3.3	Paigaldamine	11
3.3.4	Seadistamine	11
4	Eemaldamine	11
5	Kust abi saab	11
6	Seadistamine	12
6.1	JDigiDoc seaded	12



6.2	TempelPlus seaded.....	12
6.3	Seadistamine HSM-iga kasutamiseks.....	15
6.4	Seadistamine testsertifikaatide kasutamiseks.....	15
7	Tempelplus'i kasutamine test digitempliga	16
8	Kasutamine – kasutusjuhtude kaupa.....	16
8.1	Programmi abiinfo küsimine	16
8.2	Allkirjastamine	17
8.3	Allkirjade verifitseerimine	20
8.4	Allkirjade eemaldamine	21
8.5	Andmefailide konteinerist väljavõtmine	23
8.6	Konteinerite moodustamine, milles on mitu andmefaili	25
8.7	Krüpteerimine	27
8.8	Dekrüpteerimine ehk lahti krüpteerimine.....	28



1 Sissejuhatuseks

TempelPlus tarkvara on mõeldud suurema koguse failide allkirjastamiseks (ehk nõ. massallkirjastamiseks) **asutuse digitempliga** (<http://www.sk.ee/teenused/digitempli-teenus>) – näiteks arved, maksekorraldused, tunnistused jne. TempelPlus tarkvara on abiks juhtudel, kui allkirjastatavaid faile on palju ja iga allkirjastatava faili kohta peab tekkima eraldi allkirjastatud konteiner (.ddoc fail). Asutuse digitemplit saab küll kasutada ka Digidoc Client ja DigiDoc3 klient tarkvaradega, aga see võimaldab korraga vaid ühe konteineri allkirjastamist. TempelPlus tarkvara eeliseks on, et paljude allkirjade andmiseks tuleb PIN sisestada vaid ühekordselt.

Lisaks allkirjastamisele saab TempelPlus'iga ka massiliselt krüpteerida ja dekrüpteerida, verifitseerida suurt hulka ddoc faile jne.



2 Versiooniinfo

2.1 Versioon 1.2.0, jaanuar 2013

Üksikasjalik nimekiri Tempelplus'i muutustest ja uuendustest võrreldes eelmise versiooniga:

- Tempelplus kasutab uut versiooni JDigiDoc teegist (3.7.0.381)
- Täiendatud on „verify“ käsku, vt. 8.3. Lisandus parameeter „-cn“ (Subject Common Name), millega saab lisaks allkirja kehtivuse verifitseerimisele kontrollida ka selle kuulumist konkreetsele isikule/asutusele. Kasutatav kujul „-cn <cn>“
- Täiendatud on „extract“ käsku, vt. 8.5. Uuendused:
 - Lisandus valikuline parameeter „-verify“. Juhul, kui extractimisel kasutatakse „-verify“ lisaparametrit, siis andmefaili eraldamine teostatakse vaid juhul, kui allkirja verifitseerimine ka õnnestub (allkiri on sobiv ning kehtiv).
 - „-verify“ parameetrile on veel võimalik järgi kirjutada „<cn>“ väärtus (Subject Common Name). See tähendab seda, et lisaks allkirja kehtivuse verifitseerimisele kontrollitakse ka allkirja kuulumist konkreetsele isikule/asutusele.
 - Käsule lisandus „follow“ ooterežiim. Follow režiimis vea korral tekitatakse väljundkataloogi kaust "error", kuhu kopeeritakse vigased lähtefailid.
- Täiendatud on väljundfailide salvestamise loogikat seoses alamkataloogidega. Kui on määratud eraldi output_folder, siis sellesse tekitatakse samasugune alamkataloogide struktuur nagu on sisendkataloogis ja failid kirjutatakse alamkataloogidesse. Kui output_folder pole määratud, siis paigutatakse failid sisendkataloogi ja vastavatesse (olemasolevatesse) alamkataloogidesse. Funktsionaalsus lisandus järgmistele Tempelplus käskudele: **sign** – signeerimine, **extract** - andmefaili eraldamine, **remove** - allkirja eemaldamine, **crypt** – krüpteerimine, **decrypt** – dekrüpteerimine
- Täiendatud Tempelplus kolm käsku selliselt, et kui väljundkataloogis on sarnase nimega väljundfail olemas, siis uue salvestamisel lisatakse failinime lõppu „(n+1)“ järjekorranumber. Näiteks: leping.ddoc, leping(1).ddoc ja leping(2).ddoc. (Varem rakendus sellisel juhul katkestas töö, kui sihtkataloogi oldi loomas sama nimega faili, mis seal juba olemas oli). Täiendatud käsud: **extract** – andmefaili eraldamine, **remove** – allkirja eemaldamine, **crypt** - krüpteerimine



2.2 Versioon 1.1.1, oktoober 2012

Üksikasjalik nimekiri Tempelplus'i muutustest ja uuendustest võrreldes eelmise versiooniga:

- Dekrüpteerimisel saadud andmefailide salvestamise loogika on muutunud: kui varem loodi krüpteeritud faili leping.cdoci dekrüpteerimisel kataloog leping/, kuhu salvestati krüpteeritud cdoci konteineri andmefailid, siis nüüd salvestatakse failid kataloogi leping.cdoci. Juhul, kui väljundkataloogis on antud nimega fail või kataloog juba olemas, lisatakse nimele järjekorranumber kujul „<konteineri_nimi>(<jrk_nr>)“.
- Andmefailide konteinerist väljavõtmise tulemuseks saadud failide salvestamise loogika on muutunud: varem ei saanud väljundkausta faile salvestada, kui seal oli konteinerinimeline kataloog või fail juba olemas. Muudatuse tulemusena tekitatakse nüüd vajadusel uus kataloogi nimi, lisades esialgsele konteineri nimele juurde järjekorranumbri kujul „<konteineri_nimi>(<jrk_nr>)“.
- Lisatud on võimalus kasutada käsurea ja konfiguratsioonifaili parameetrit „cmn_ext_dir“, mille seadistamisel salvestatakse andmefailide konteinerist väljavõtmisel ja dekrüpteerimisel saadud failid otse väljundkausta, mitte konteinerinimelistesse alamkaustadesse (vt. 6.2, 8.5, 8.8).
- Tempelplus võimaldab nüüd kasutada kõikide kasutusjuhtude jaoks lisaks krüptopulgale ka HSM seadet. HSM-i kasutamise seadistamine on kirjeldatud peatükis 6.3 HSM-i kasutamiseks allkirjastamisel ja dekrüpteerimisel on lisatud uued käsurea parameetrid –slot ja –label (vt. 8.2, 8.8).

Märkus: HSM seadme funktsionaalsus Tempelplusis on eksperimentaalne ja nõuab kasutajalt täpset ülevaadet seadmel asuvatest sertifikaatidest ja privaativõtmetest ning nende omadustest. Tavakasutaja jaoks on soovitatav kasutada endiselt krüptopulka.

2.3 Versioon 1.1.0, suvi 2012

Üksikasjalik nimekiri Tempelplus'i muutustest ja uuendustest võrreldes eelmise versiooniga, lisaks veaparandused:

- Esmakordselt on Tempelplus tarkvarast versioon Linux platvormile
- Tempelplus võimaldab nüüd pin'i sisestust lisaks ka konfiguratsioonifailist ja käsureaparameetrina (vt. 6.2, 8.2, 8.8)
- Tempelplus kasutab uut versiooni JDigiDoc teegist (3.6.1.1)
- Tempelplusi saab kasutada uuendatud sertifikaatidega test-templitega (välja antud alates aprillist 2012, „TEST of KLASS3-SK 2010“ poolt)



-
- Tempelplus'ile on lisatud litsentsiinfo (rakenduse kataloogis `licence.txt/licence_linux.txt`), mis sisaldab ka Tempelplus poolt kasutatavate tarkvarade – JDigiDoc teegi ja IAIK PKCS#11 Wrapper'i litsentse.
 - Täiendatud on Tempelplusi tegevuste ja vigade logimist
 - Dekrüpteerimise loogika on muutunud: kui varem loodi krüpteeritud faili `leping.cdoci` dekrüpteerimisel kataloog `leping.ddoci`, kuhu pandi krüpteeritud konteineris asunud andmefailid, siis nüüd luuakse kataloog `leping/`, ilma `.ddoci` laiendita.
 - Dekrüpteerimisel –recipient võtme loogika muutus, vt. 8.8
 - Täiendatud Tempelplus'i selliselt, et kui lähtekataloogis on kolm faili, näiteks `leping.docx`, `leping.rtf` ja `leping.pdf`, siis sihtkataloogi tekib kolm tembeldatud faili, selliste failinimedega: `leping.ddoci`, `leping(1).ddoci` ja `leping(2).ddoci`. (Varem rakendus sellisel juhul katkestas töö, kui sihtkataloogi oldi loomas sama nimega faili, mis seal juba olemas oli).
 - Parandatud on Tempelplus'i töökindlust allkirjastamisel –follow režiimis. Vea korral kirjutatakse fail, mille allkirjastamisel viga ilmes, väljundkataloogi alamkataloogi `error/` ning jätkatakse tööd. Vea sisu kirjutatakse ka logifaili.
 - Parandatud on viga, kus Tempelplus ei töötanud alla 1KB suuruste lähtefailide korral korrektselt
 - Parandatud on viga, kus Tempelplus ei suutnud dekrüpteerida „DigiDoc3 krüpto“-ga krüpteeritud faili.
 - Parandatud on viga, kus Tempelplus võimaldas krüpteerimisel kasutada sobimatut sertifikaati
 - Parandatud on viga, kus Tempelplus lõpetas veateatega töö juhul, kui pin'i sisestamise dialoogiaken ilma pin'i sisestamata sulgeti.

2.4 Versioon 1.0.0, reliisi kuupäev 31.08.2011

Testitud Windows7 platvormil Safenet'i Aladdin'i eToken Pro USB pulgal oleva digitempliga (1K ja 2K võtmetega) ning kiipkaardil digitempliga (1K võtmetega). Ka see versioon tarkvarast on veel vaid käsurautiliidina ning ainult Windows operatsioonisüsteemil kasutamiseks.

- Parandatud on käsurautiliidi abiinfot
- Parandus: Tempelplus käsurautiliidiga töötamine Windowsi all ei eelda enam administraatori õigusi
- Lisandunud on –**signer_cn** parameeter allkirjastamisfunktsiooni (**tempelplus sign**) juurde, mis võimaldab allkirjastamisel valida, missuguse allkirjastamistokenil oleva



võtmega allkirjastamist sooritada. Ehk tegemist on mitme allkirjastamisvõtme toe lisandumisega TempelPlus'ile.

2.5 Versioon 0.99, beeta, reliisi kuupäev 27.12.2010

Esimene avalik beetaversioon. Realiseeritud on selles versioonis **ainult käsurea** variant tarkvarast, testitud Windows 7 platvormil. Saadaval on Windows'i msi pakina. TempelPlus'i põhifunktsioonid – allkirjastamine ja krüpteerimine/dekrüpteerimine – on testitud järgmiste token'itega:

- Kiipkaardil asutuse ID (digitempel), allkirjastamise ja autentimise/krüpteerimise sertifikaatidega, 1024 (1K) bitised võtmed
- USB pulgal (Aladdin (Safenet) eToken Pro) asutuse ID (digitempel), allkirjastamise ja krüpteerimise sertifikaatidega, 1K ja 2K võtmed, pulgal on ainult 1 PIN (ehk pulgal ei ole lisaks määratud Secondary authentication password'e pulgal olevate võtmete kasutamiseks)

3 Paigaldamine

3.1 Eeldused

Tempelplus tarkvara kasutamiseks on vajalik eelnevalt paigaldada:

- Java JDK/JRE, alates versioonist 6. Java saate lehelt <http://www.oracle.com/technetwork/java/index.html>.
- Aladdin'i eToken-i tarkvara (Safenet Authentication Client), mille saate, kui tellite SK-lt digitempli.

3.2 Tempelplus'i paigaldamine windowsis

3.2.1 Safenet Authentication Client

Veendumaks, et krüptopulk on kasutatav, tuleks käivitada Safenet Authentication Client Tools rakendus ning vaadata, kas on näha pulgal olevaid andmeid, näiteks sertifikaate.

3.2.2 Paigaldamine

Tempelplus tarkvara paigaldamine käib zip konteineri lahtipakkimise teel sobivasse kohta failisüsteemis. Pakk on allalaetav aadressilt <http://www.sk.ee/teenused/digitempli-teenus/tempelplus/>.

3.2.3 PKCS11Wrapper

Kopeerida Tempelplus'i kodukataloogis olevast alamkataloogist pkcs11wrapper\32\ või pkcs11wrapper\64\ (sõltuvalt sellest, kas tegemist on 32bitise või 64bitise masinaga) fail pkcs11wrapper.dll windowsi süsteemikataloogi (näiteks C:\windows\system32\) või mujale, kust java seda teeki näeks.

3.2.4 Seadistamine

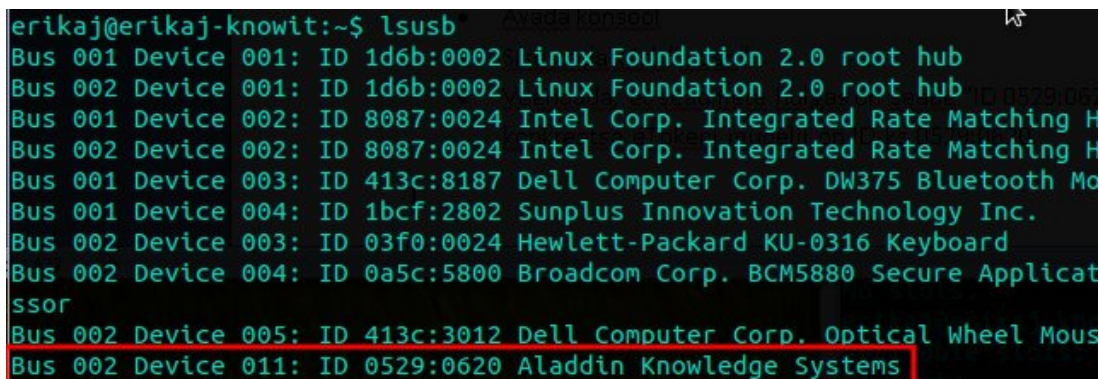
Tempelplus'i kasutamiseks tuleb teha mõningased seadistused Tempelplus rakenduse enda ja Tempelplus'i poolt kasutatava JDigiDoc teegi juures. Detailne info seadistuste kohta on peatükis 6. Seadistamise järgselt peaks Tempelplus olema kasutusvalmis. Kuidas Tempelplus'i kasutada, on kirjas peatükis 8.

3.3 Tempelplus'i paigaldamine linuxis

3.3.1 Alustamine

Enne krüptopulga kasutamist on vajalik veenduda, et USB seade on süsteemile nähtav ning kättesaadav. Selle info saab kätte terminali kaudu.

- Avada konsool
- Sisestada käsk "lsusb".)
- Veenduda, et seadmete hulgas on krüptopulga seade. Näiteks Aladdini seadmetele on iseloomulik nimetus: "ID ****.**** Aladdin Knowledge Systems".



```
erikaj@erikaj-knowit:~$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching H
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching H
Bus 001 Device 003: ID 413c:8187 Dell Computer Corp. DW375 Bluetooth Mo
Bus 001 Device 004: ID 1bcf:2802 Sunplus Innovation Technology Inc.
Bus 002 Device 003: ID 03f0:0024 Hewlett-Packard KU-0316 Keyboard
Bus 002 Device 004: ID 0a5c:5800 Broadcom Corp. BCM5800 Secure Applicat
ssor
Bus 002 Device 005: ID 413c:3012 Dell Computer Corp. Optical Wheel Mous
Bus 002 Device 011: ID 0529:0620 Aladdin Knowledge Systems
```

Figure 1 – lsusb käsk – Pildil oleva eTokeni mudeli ID-ks on 0529:0620

Juhul, kui USB seadmete nimekirjas on olemas krüptopulk, siis on see suure tõenäosusega kasutuskõlblik ning arvutiga kommunikeerimise eeldus on täidetud.

¹Fedora/Redhat keskkonnas võib olla sobiv variant: „/sbin/lsusb”. Juhul, kui antud käsud ei tööta, siis on vaja arvutisse paigaldada sobiva „usbutils” paketi. Vaikimisi on see olemas kõikides uutes linuxi distributsioonides.

3.3.2 Safenet Authentication Client

Ametlik krüptopulga seadistamise tarkvara on SafeNet Authentication Client (varasemalt tuntud kui PKI-Client). Tarkvara on ühilduv CentOS, Red Hat Enterprise, SUSE, Fedora ning Ubuntu 32/64-bitiste operatsioonisüsteemidega. Tarkvara levitatakse automaatselt paigalduvate *.rpm või *.deb pakettidena. Programmiga on kaasas põhjalik dokumentatsioon, mis koosneb kolmest osast:

- SafeNet_Authentication_Client_*_*_Linux_README.pdf – üldine taust
- SafeNet_Authentication_Client_*_*_Linux_Admin_Guide.pdf – paigaldus ning haldamine
- SafeNet_Authentication_Client_*_*_Linux_User_Guide.pdf – programmi kasutusjuhend

Tarkvara tuleb paigaldada vastavalt selle kasutusjuhendile.

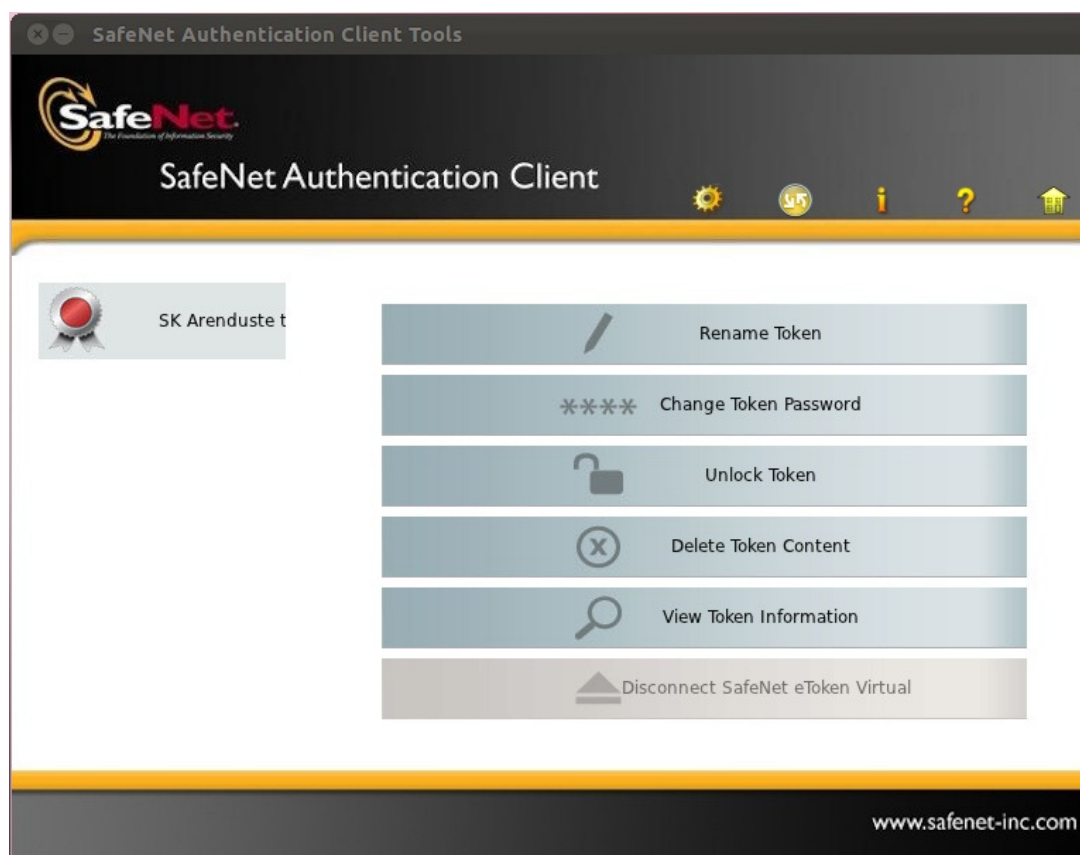


Figure 2 - SafeNet Authentication Client Tools graafilise kasutajaliides

Lisaks mugavale graafilisele kasutajaliidesele, mis võimaldab seadistada krüptopulka, paigaldatakse SafeNet Authentication Client tarkvara installeerimise käigus arvutisse lisaks sobiv PKCS#11 moodul, mille abil on võimalik ka teistel tarkvaradel suhelda krüptopulgaga, nende hulgas SK Tempelplusil.



3.3.3 Paigaldamine

Tempelplus tarkvara paigaldamine käib Linux platvormi jaoks mõeldud tar.gz konteineri lahtipakkimise teel sobivasse kohta failisüsteemis. Pakk on allalaetav aadressilt <http://www.sk.ee/teenused/digitempli-teenus/tempelplus/>.

3.3.4 Seadistamine

Tempelplus'i kasutamiseks tuleb teha mõningased seadistused Tempelplus rakenduse enda ja Tempelplus'i poolt kasutatava JDigiDoc teegi juures. Detailne info seadistuste kohta on peatükis 6. Seadistamise järgselt peaks Tempelplus olema kasutusvalmis. Kuidas Tempelplus'i kasutada, on kirjas peatükis 8.

4 Eemaldamine

TempelPlus eemaldamiseks piisab Tempelplus kodukataloogi kustutamisest.

5 Kust abi saab

TempelPlus tarkvara alaste küsimuste ja parandus- või täiendustepanekutega pöörduda SK klienditoe aadressile abi@id.ee



6 Seadistamine

TempelPlus tarkvara baseerub JDigiDoc teegi/utliidil (vt. <http://www.id.ee/index.php?id=30393>) Seega sisaldab TempelPlus nii nõ. oma seadeid kui ka JDigiDoc teegi seadeid. Tempelplus'i kasutamiseks on vajalik mõningane seadistamine, millest on juttu järgmistes alapunktides.

Märkus: seadete failides tuleks kasutada kodeeringut, mis vastab süsteemi kodeeringule, vastasel juhul võivad tekkida vead seadetes määratud väärtuste sisselugemisel.

6.1 JDigiDoc seaded

JDigiDoc teegi/utliidi olulisemad seaded asuvad järgmistes failides:

- **<TempelPlus kodukataloog>\JDigiDoc\jdidoc.bat**, olulisemad parameetrid, sätitakse TempelPlus paigalduse käigus:
- **<TempelPlus kodukataloog>\JDigiDoc\log4j.properties**
 - Parameeter **log4j.appender.file.file** – määrata väärtuseks <Tempelplus kodukataloog>\logs\tempelplus.log (linux-i puhul kasutada \ asemel / eraldajaid). NB! Siin peaks kasutama sama failiteed nagu järgmises alapunktis Tempelplus.conf parameetri **log_file** puhul. NB! logs\ kataloogi peaks olema antud kirjutamisõigus!

JDigiDoc teegi/utliidi, sh. konfigureerimise, kohta rohkem infot on JDigiDoc teegi dokumentatsioonis: **<TempelPlus kodukataloog>\JDigiDoc\doc**

6.2 TempelPlus seaded

TempelPlus olulisemad seaded asuvad järgmistes failides. NB! Allolevates seadetes asendada failiteedes eraldaja \ ise eraldajaga /, kui tegemist on linux masinaga.

- **<TempelPlus kodukataloog>\TempelPlus.bat (Windowsi puhul)**
 - Parameeter **JAVA** – täisfailitee java.exe asukohani failisüsteemis. Näiteks "C:\Program Files\Java\jre6\bin\java.exe"
- **<TempelPlus kodukataloog>\TempelPlus32.sh või Tempelplus64.sh (Linux korral)**
 - Parameeter **JAVA_HOME** – täisfailitee java binaarini failisüsteemis. Näiteks "/usr/lib/jvm/java-6-openjdk/jre/bin/java"
- **<TempelPlus kodukataloog>\TempelPlus.conf**



-
- *Allkirjastamisega, krüpteerimisega seotud parameetrid*
 - **role, country, state, city, postcode** – allkirjastaja rolli, asukohta määravad parameetrid
 - **format** – tekitatavate allkirjastatud konteinerite formaat, ainuke hetkel kehtiv variant on: ddoc
 - **crypt** – krüpteeritud konteineri faililaiend, vaikimisi väärtus: cdoc
 - **pin_enter** – PIN-i küsimise viis: kas **graafiline** (pin'i sisestuse dialoogiaken), **konsoolist** või konfiguratsioonifailist, võimalikud väärtused: graphic, console, config
 - **pin** – Juhul, kui parameetris **pin_enter** kasutatakse valikut „config“, siis selle parameetriga määratakse pin kood
 - **DIGIDOC_OCSP_RESPONDER_URL** – kehtivuskinnitusteenuse (OCSP) aadress; Live-teenuse URL: <http://ocsp.sk.ee>, Test-teenuse URL: <http://www.openxades.org/cgi-bin/ocsp.cgi>
 - **SIGN_OCSP_REQUESTS** – kas kehtivuskinnitusteenuse (OCSP) vastu tehtavad päringud allkirjatatakse (juurdepääsutõendi olemasolul) või mitte (IP põhise juurdepääsu puhul); võimalikud variandid: true, false
 - **DIGIDOC_PKCS12_CONTAINER** – juurdepääsutõendi failitee, kasutatakse koos parameetritega **SIGN_OCSP_REQUESTS=true** ja **DIGIDOC_PKCS12_PASSWD**
 - **DIGIDOC_PKCS12_PASSWD** – juurdepääsutõendi parool, kasutatakse koos parameetritega **SIGN_OCSP_REQUESTS=true** ja **DIGIDOC_PKCS12_CONTAINER**
 - *Muud seaded - failid, kataloogid*
 - **jddoc_location** – JDigiDoc teegi asukoht, <Tempelplus kodukataloog>\\JDigiDoc
 - **log_file** – logifaili asukoht, määrata väärtuseks <Tempelplus kodukataloog>\\logs\\tempelplus.log (linux-i puhul kasutada \\ asemel / eraldajaid). NB! Siin peaks kasutama sama failiteed nagu eelmises alapunktis <Tempelplus kodukataloog>\\JDigiDoc\\log4j.properties parameetri **log4j.appender.file.file** puhul. NB! logs\\ kataloogi peaks olema antud kirjutamisõigus!
-



-
- **work_directory** – TempelPlus töökataloog, ajutiste failide hoidmiseks, <Tempelplus kodukataloog>\temp, kataloogile anda kirjutamisõigus!
 - **cmn_ext_dir** –parameeter võimaldab määrata, kas .ddoc konteinerist andmefailide väljavõtmisel või .cdoc konteineri dekrüpteerimisel saadud andmefailid kirjutatakse konteinerinimelisse alamkataloogi või salvestatakse otse väljundkataloogi (-output_folder parameetriga määratud kataloogi või selle parameetri puudumisel lähtefailiga samasse kataloogi). Võimalikud väärtused on „true“ – andmefailid salvestatakse ühte kataloogi ja „false“ - salvestatakse alamkataloogidesse. Juhul, kui faili salvestamisel väljundkataloogi on sama nimega fail juba olemas, salvestatakse fail uue nimega lisades juurde järjekorranumbri kujul „<failinimi>(<jrk_nr>).<faili_laiend>“. Kui konteinerinimelise alamkataloogi loomisel on antud konteineri nimega fail või alamkataloog juba olemas, tekitatakse uus kataloogi nimi, lisades esialgsele nimele juurde järjekorranumbri kujul „<konteineri_nimi>(<jrk_nr>)“.

Märkus: antud parameetrit on võimalik määrata ka käsureal. Kui parameeter on käsureal määratud, siis konfiguratsioonifailis olevat väärtust ei arvestata.

- **DIGIDOC_LOG4J_CONFIG** – log4j.properties faili asukoht, <Tempelplus kodukataloog>\JDigiDoc\log4j.properties
 - **DIGIDOC_DF_CACHE_DIR** – JDigiDoc teegi kataloog ajutiste failide hoidmiseks, <Tempelplus kodukataloog>\JDigiDoc\temp, kataloogile anda kirjutamisõigus!
 - **bc_prov=bcprov-jdk15on-147.jar** – eelmääratud parameeter, pole vaja muuta
 - **DIGIDOC_MAX_DATAFILE_CACHED=1000** – eelmääratud parameeter, pole vaja muuta
 - **DIGIDOC_SIGN_PKCS11_DRIVER** – PKCS#11 draiveri asukoht failisüsteemis. PKCS#11 draiver paigaldatakse Aladdini eToken-i tarkvara (Safenet Authentication Client) paigalduse käigus ja asub:
 - Windowsi puhul: C:\windows\system32\TPKCS11.dll või C:\Windows\SysWOW64\TPKCS11.dll
 - Linuxi puhul: usr/lib/libeTPkcs11.so
- *Muud seaded – rakenduse käitumine*



-
- **control_question** – kas kasutajalt küsitakse toimingute kinnituseks kontrollküsimusi, variandid: yes/no
 - **date_format** – kuupäeva kuvamisel kasutatav formaat, vaikimisväärtus: dd.MM.yyyy HH:mm:ss

6.3 Seadistamine HSM-iga kasutamiseks

- **DIGIDOC_SIGN_PKCS11_DRIVER** – antud parameetri väärtuseks tuleks määrata HSM seadme PKCS#11 draiveri faili asukoht failisüsteemis. Antud asukoht tuleks lisada ka süsteemi keskkonnamuutujasse.
- HSM-i kasutamiseks allkirjastamisel ja dekrüpteerimisel on lisatud uued käsurea parameetrid `–slot` ja `–label` (vt. 8.2, 8.8)

6.4 Seadistamine testsertifikaatide kasutamiseks

Eesti testsertifikaatide kasutamiseks TempelPlus tarkvaraga tuleb sertifikaadid eelnevalt eraldi paigaldada. Testsertifikaatide paki saab alla laadida aadressilt <https://installer.id.ee/media/esteidtestcerts.jar>, saadud `esteidtestcerts.jar` fail tuleb paigaldada kataloogi `<TempelPlus kodukataloog>\JDigiDoc\lib\`.



7 Tempelplus'i kasutamine test digitempliga

Kui on soov Tempelplus tarkvara proovida (näiteks anda test-allkirju) enne LIVE-süsteemis kasutamist, siis tuleks AS Sertifitseerimiskeskusest tellida test digitempel (<http://www.sk.ee/teenused/testkaardid/>), saadud krüptopulgal olevad allkirjastamiseks mõeldud test-sertifikaadid registreerida test-OCSP teenuses (http://www.openxades.org/upload_cert.php) sobiva staatusega, ning seejärel määrata Tempelplus tarkvara konfiguratsioonifailis (Tempelplus.conf) parameetritele järgmised väärtused:

- DIGIDOC_OCSP_RESPONDER_URL=<http://www.openxades.org/cgi-bin/ocsp.cgi>
- SIGN_OCSP_REQUESTS=false
- Parameetrid DIGIDOC_PKCS12_CONTAINER ja DIGIDOC_PKCS12_PASSWD välja kommenteerida ehk lisada nende parameetrite ette märk #.

Seejärel võetakse allkirjastamisel (tembeldamisel) allkirjastaja sertifikaadi info test-OCSP teenusest ning tekkinud allkirjad (templid) on kehtivad test-allkirjad (test-templid).

8 Kasutamine – kasutusjuhtude kaupa

8.1 Programmi abiinfo küsimine

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

```
cd "c:\Program Files\TempelPlus"
```

Üldine abiinfo TempelPlus kasutamise kohta käib järgmise käsuga:

```
tempelplus -help või
```

```
tempelplus -?
```

Abiinfo küsimine konkreetse käsu, näiteks allkirjastamise kohta:

```
tempelplus sign -help või
```

```
tempelplus sign -?
```




8.2 Allkirjastamine

Allkirjastada saab korraga kas ühte faili või tervet kataloogitäit faile, allkirjastamise tulemusena tekkivad failid võib lasta salvestada lähtefailidega samasse kataloogi või määrata mõne muu (mis on soovitatavam variant). Lähtefailid, mida allkirjastatakse, saab allkirjastamise käigus ära kustutada. Samuti on võimalik rakendus panna tööle ooterežiimis, kus peale lähtefailide allkirjastamist jääb programm tööle ja ootab lähtekataloogi tekkivaid uusi faile, mida allkirjastada. Kui allkirjastatav fail on juba DigiDoc konteiner, siis allkirjastamise käigus lisatakse sellele üks allkiri. Kui allkirjastatav fail pole DigiDoc konteiner, siis tekitatakse DigiDoc konteiner ühe allkirjaga. Juhul, kui allkirjastatud faili kirjutamisel väljundkataloogi on seal sama nimega fail juba olemas, salvestatakse fail uue nimega lisades juurde järjekorranumbri kujul „<failinimi>(<jrk_nr>).ddoc“.

NB! TempelPlus'iga allkirjastamise ajaks sisesta Digitempel oma arvutisse. Kiipkaardil Digitempli korral pane kaart lugejasse, USB pulgal Digitempli korral pista pulk USB auku.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Allkirjastamiskäsu üldkuju on järgmine:

tempelplus sign <allkirjastatav fail või kataloog> <lisaparaameetrid>

Lisaparaameetrid:

- **-pin „<pin kood>“** – mittekohustuslik; pin-koodi saab rakendusele ette anda muuhulgas käsuraaparaameetrina, muud pin'i sisestuse võimalused on loetletud peatükis 6.2.
- **-output_folder <kataloog>** – mittekohustuslik paraameeter, määramaks kataloogi, kuhu kirjutatakse allkirjastatavad failid. NB! Sellesse kataloogi peaks olema Tempelplus'il õigus kirjutada.
- **-remove_input** – mittekohustuslik; kui see paraameeter on määratud, kustutatakse (allkirjastatavad) lähtefailid
- **-follow** – mittekohustuslik; paraameeter, mille kasutamisel töötab rakendus ooterežiimis. NB! Selle paraameetri puhul on kohustuslik kasutada ka – **remove_input** ja **-output_folder** paraameetreid. Vea korral kirjutatakse fail, mille allkirjastamisel viga ilmnes, väljundkataloogi alamkataloogi error/ ning jätkatakse tööd. Vea sisu kirjutatakse ka logifaili.
- **-signer_cn „<CN>“** – mittekohustuslik; paraameeter, millega saab määrata, missuguse võtmega allkirjastamist sooritatakse. Kui paraameetrit mitte kasutada, siis valitakse esimene allkirjastamisvõti. Paraameetri väärtus, kui seda paraameetrit kasutada, peaks olema allkirjastamisvõtmega seotud sertifikaadi Subject CN (Common Name) välja väärtus.



-
- **-role „<roll>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja rolli. Kui allkirjastaja roll on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparametreid
 - **-country „<riik>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **country** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparametreid
 - **-state „<osariik/maakond>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **state** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparametreid
 - **-city „<linn>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **city** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparametreid
 - **-postcode „<postiindeks>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **postcode** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparametreid

Lisaparametrid HSM seadmega kasutamiseks:

- **-slot <slot_ID>** - HSM seadme sloti ID väärtus², milles olevat sertifikaati soovitakse allkirjastamiseks kasutada. Väärtus peab olema kümnendkujul. Sloti määramisel on kohustuslik määrata ka -label parameetri väärtus.
- **-label „<labeli_nimetus>“** – allkirjastamiseks kasutatava sertifikaadi ja sellele vastava privaatvõtme label-i väärtus. Tühikute esinemisel label-i nimes tuleb väärtus panna jutumärkide vahele. Label-i määramisel peab olema määratud ka -slot parameetri väärtus.

Märkus: HSM seadme kasutamiseks peavad sertifikaat ja sellele vastav privaatvõti olema seadmel samas slotis, nende labelite väärtused peavad olema samad. Kui käsureal on määratud parameetrid -slot ja -label, siis ei arvestata parameetri -signer_cn väärtust.

Näide: Allkirjastamine lähtefailide kataloogi (näiteks C:\input\) ja sihtkataloogi (C:\output\) etteandmisega. Lähtekataloogi iga faili kohta tekib sihtkataloogi üks allkirjastatud DigiDoc konteiner:

tempelplus sign c:\input -output_folder c:\output

Programm kuvab jooksvalt, mitmendat faili parasjagu allkirjastatakse, ning edukal juhul lõpetab järgnevale analoogilise teatega:

² Kui arvutiga on ühendatud mitu HSM seadet, siis tuleks slottide ID väärtuste leidmiseks kasutada pkcs11-tool utiliiti (ID-le vastab kuueteistkümnendkujul number väljundis).



Done

7 documents signed successfully

TempelPlus v1.2.0 stopping. Time used: 18 seconds

Infoks: Juhul, kui allkirjastamise momendil sisestatakse vale krüptopulga pin kood või kommunikatsioon seadmega nurjub mingil muul põhjusel, siis krüptoseade võib muutuda selle sessiooni vältel kasutuskõlbmatuks. Selleks, et jätkata tööd, tuleb USB pulk välja võtta ning sisestada tagasi arvutisse.



8.3 Allkirjade verifitseerimine

Tempelplus tarkvara võimaldab korraga kataloogitäie allkirjastatud failide allkirjade kehtivust kontrollida. Kataloogis võib olla nii DigiDoc konteinereid kui tavalisi andmefaile.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Allkirjade verifitseerimiskäsu üldkuju on järgmine:

tempelplus verify <verifitseeritav fail või kataloog>

Näide: verifitseerime ühes kataloogis (näiteks C:\digidoc_files\) olevate allkirjastatud kontainerite allkirju:

tempelplus verify c:\digidoc_files

Lisaparametrid:

-cn <cn> - mittekohustuslik. Subject CN väärtus. Verifitseeritakse, kas konkreetne asutus/isik on allkirja autor.

Näide: **tempelplus verify c:\digidoc_files\ -cn „MÄNNIK,MARI-LIIS,47101010033“**

Programm kuvab jooksvalt, mitmendat faili parasjagu töödeldakse ning näitab leitud allkirjade puhul allkirja infot – allkirjastaja, kuupäev, kehtivus -, ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 documents verified successfully

TempelPlus found 14 valid (or matching) signatures and 0 invalid (or not matching) signatures

TempelPlus v1.2.0 stopping. Time used: 2 seconds



8.4 Allkirjade eemaldamine

TempelPlus võimaldab korraga paljudelt failidelt allkirju eemaldada ja seda kahte moodi: eemaldatakse kas kõigilt etteantud kataloogis sisalduvatelt allkirjastatud failidelt kõik allkirjad või kõigilt allkirjastatud failidelt ühe konkreetse isiku allkirjad. Tulemuseks on DigiDoc failid, millest on üks või kõik allkirjad eemaldatud.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Allkirjade eemaldamiskäsu üldkuju on järgmine:

tempelplus remove <allkirja tunnus> <lähtefail või lähtekataloog> -output_folder <sihtkataloog>

Allkirja tunnused võivad olla järgmisel kujul:

- **ALL** – eemaldatakse allkirjastatud faili kõik allkirjad
- **„<CN>“** – allkirjastatud failist eemaldatakse konkreetse isiku/asutuse antud allkiri. Isik on määratud tema ID-kaardi või Digitempli allkirjastamise sertifikaadis oleva Subject CN (Common Name) välja väärtusega. ID-kaardi omanikel on see näiteks kujul „Perekonnanimi,Eesnimi,Isikukood“

Näide 1: eemaldame ühes kataloogis (näiteks C:\digidoc_files\) olevate kõigi allkirjastatud konteinerite kõik allkirjad ning kirjutame ilma allkirjadeta DigiDoc konteinerid teise kataloogi (näiteks C:\digidoc_files2\):

tempelplus remove ALL c:\digidoc_files\ -output_folder c:\digidoc_files2

Programm kuvab jooksvalt, mitmendat faili parasjagu töödeldakse, näitab leitud allkirjade puhul allkirjastajate infot ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 documents were handled successfully. 14 signatures removed

TempelPlus v1.2.0 stopping. Time used: 4 seconds

Näide 2: eemaldame ühes kataloogis (näiteks C:\digidoc_files\) olevate kõigi allkirjastatud konteinerite puhul konkreetse isiku (MARI-LIIS MÄNNIK, 47101010033) allkirjad ning kirjutame eemaldatud allkirjadega DigiDoc konteinerid teise kataloogi (näiteks C:\digidoc_files2\):

tempelplus remove „MÄNNIK,MARI-LIIS,47101010033“ c:\digidoc_files\ -output_folder c:\digidoc_files2



Programm kuvab jooksvalt, mitmendat faili parasjagu töödeldakse, näitab leitud allkirjade puhul allkirjastajate infot ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done**7 documents were handled successfully. 2 signatures removed****TempelPlus v1.2.0 stopping. Time used: 2 seconds**

8.5 Andmefailide konteinerist väljavõtmine

TempelPlus võimaldab kataloogitäiest allkirjastatud konteineritest välja võtta neis konteinerites sisalduvad andmefailid. Konteinerist (olgu näiteks fail1.ddoc) välja võetud andmefailide jaoks tehakse fail1.ddoc nimeline kataloog ja andmefailid salvestatakse sinna. Juhul, kui väljundkataloogis on antud konteineri nimega fail või alamkataloog juba olemas, tekitatakse uus kataloogi nimi, lisades esialgsele nimele juurde järjekorranumbri kujul „fail1.ddoc(<jrk_nr>)“.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Andmefailide konteinerist väljavõtmiskäsu üldkuju on järgmine:

tempelplus extract <lähtefail või lähtekataloog> -output_folder <sihtkataloog>

- **-output_folder <sihtkataloog>** – mittekohustuslik parameeter, määramaks kataloogi, kuhu salvestatakse konteinerist väljavõetavad failid. NB! Sellesse kataloogi peaks olema Tempelplus'il õigus kirjutada.

Lisaparaameetrid:

- **-cmn_ext_dir** – antud parameetri määramisel ei kirjutata konteinerist väljavõetud andmefailide konteinerinimelisse alamkataloogi, vaid salvestatakse otse väljundkataloogi (-output_folder parameetriga määratud kataloogi või selle parameetri puudumisel lähtefailiga samasse kataloogi). Juhul, kui kataloogis on sama nimega fail juba olemas, salvestatakse fail uue nimega lisades juurde järjekorranumbri kujul „<failinimi>(<jrk_nr>).<faili_laiend>“. Märkus: antud parameetrit on võimalik määrata ka konfiguratsioonifailis (vt. ptk 6.2). Kui parameeter on käsureal määratud, siis konfiguratsioonifailis olevat väärtust ei arvestata.
- **-verify (<cn>)** – juhul, kui extractimisel kasutatakse „-verify“ lisaparaameetrit, siis andmefaili eraldamine teostatakse vaid juhul, kui allkirja verifitseerimine ka õnnestub (allkiri on sobiv ning kehtiv). Antud parameetrile on veel võimalik järgi kirjutada „<cn>“ väärtus (Subject Common Name). See tähendab seda, et lisaks allkirja kehtivuse verifitseerimisele kontrollitakse ka allkirja kuulumist konkreetsele isikule/asutusele.
- **-remove_input** – mittekohustuslik; kui see parameeter on määratud, kustutatakse lähtefailid, millest faile välja võetakse.
- **-follow** – mittekohustuslik; parameeter, mille kasutamisel töötab rakendus ooterežiimis. **NB!** Selle parameetri puhul on kohustuslik kasutada ka – **remove_input** ja **-output_folder** parameetreid. Vea korral kirjutatakse fail, mille konteinerist väljavõtmisel viga ilmnes, väljundkataloogi alamkataloogi error/ ning jätkatakse tööd. Vea sisu kirjutatakse ka logifaili.



Näide 1: võtame ühes kataloogis (näiteks C:\digidoc_files\) olevate kõigi allkirjastatud konteinerite seest välja kõik neis sisalduvad andmefailid ning tekitame teise kataloogi (näiteks C:\digidoc_files2\) iga lähtekataloogi DigiDoc konteineri nimelise kataloogi, mis sisaldab vastavas konteineris sisalduvaid andmefaile:

tempelplus extract c:\digidoc_files\ -output_folder c:\digidoc_files2

Programm kuvab jooksvalt, mitmendat faili parasjagu töödeldakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

2 documents where handled successfully. 3 files extracted

TempelPlus v1.2.0 stopping. Time used: 2 seconds



8.6 Konteinerite moodustamine, milles on mitu andmefaili

TempelPlus võimaldab moodustada korraga palju (ilma allkirjadeta) DigiDoc konteinereid, kus on üks või mitu andmefaili.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Konteinerite moodustamise käsu üldkuju on järgmine:

tempelplus container <lähtefail või lähtekataloog> <lisaparaameetrid>

Kui ette antakse lähtefail, moodustatakse üks konteiner, kui aga lähtefaili sisaldav kataloog, siis moodustatakse niipalju konteinereid, kui palju on lähtekataloogis faile – iga faili kohta üks DigiDoc konteiner.

Lisaparaameetrid:

- **-output_folder <kataloog>** – mittekohustuslik; loodavad konteinerid tekitatakse selle paraameetriga määratud kataloogi
- **-add_file <kataloog või tühikuga eraldatud failide list>** - mittekohustuslik; selle paraameetriga määratud failid lisatakse igasse loodavas konteinerisse

Näide 1: olgu meil lähtekataloogis (näiteks C:\datafiles\) hulk andmefaile. Tekitame teise kataloogi (näiteks C:\digidoc_files) iga lähtekataloogi andmefaili kohta ühe DigiDoc konteineri, milles on lähtekataloogi vastav andmefail:

tempelplus container c:\datafiles\ -output_folder c:\digidoc_files

Programm kuvab jooksvalt, mitmendat faili parasjagu tekitatakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 documents created successfully.

TempelPlus v1.2.0 stopping. Time used: 1 seconds

Näide 2: olgu meil lähtekataloogis (näiteks C:\datafiles\) hulk andmefaile. Tekitame teise kataloogi (näiteks C:\digidoc_files) iga lähtekataloogi andmefaili kohta ühe DigiDoc konteineri, milles on lähtekataloogi vastav andmefail ning veel 2 faili:

tempelplus container c:\datafiles\ -output_folder c:\digidoc_files\ -add_file c:\file1.txt c:\file2.dat



Programm kuvab jooksvalt, mitmendat faili parasjagu tekitatakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 documents created successfully.

TempelPlus v1.2.0 stopping. Time used: 1 seconds

Näide 3: olgu meil lähtekataloogis (näiteks C:\datafiles\) hulk andmefaili. Tekitame teise kataloogi (näiteks C:\digidoc_files) iga lähtekataloogi andmefaili kohta ühe DigiDoc konteineri, milles on lähtekataloogi vastav andmefail ning veel kõik failid, mis sisalduvad kataloogis C:\datafiles2:

tempelplus container c:\datafiles\ -output_folder c:\digidoc_files\ -add_file c:\datafiles2

Programm kuvab jooksvalt, mitmendat faili parasjagu tekitatakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 documents created successfully.

TempelPlus v1.2.0 stopping. Time used: 1 seconds



8.7 Krüpteerimine

TempelPlus'i abil saab korraga terve kataloogitäie faile krüpteerida, ühele või mitmele adressaadile ehk isikule või asutusele, kes oma ID-kaardiga või Digitempliga krüpteeritud failid lahti krüpteerida (ehk dekrüpteerida) saavad.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Krüpteerimiskäsu üldkuju on järgmine:

tempelplus encrypt <lähtefail või lähtekataloog> -cert <sertifikaadifail(id)> -output_folder <sihtkataloog>

Kui krüpteeritakse mitmele adressaadile, siis sertifikaadifailid tuleks üksteisest tühikuga eraldada. **-output_folder** on mittekohustuslik parameeter.

Näide: olgu meil lähtekataloogis (näiteks C:\datafiles\) hulk andmefaile. Krüpteerime failid kahele isikule/asutusele (eeldusel, et meil on nende isikute/asutuste ID-kaardi/Digitempli autentimise (krüpteerimise) sertifikaadifailid olemas) ning salvestame krüpteeritud konteinerid sihtkataloogi (näiteks C:\encrypted_files\):

**tempelplus encrypt c:\datafiles\ -cert c:\certs\isik1_auth.cer
c:\certs\asutus2_crypt.cer -output_folder c:\encrypted_files**

Programm kuvab jooksvalt, mitmendat faili parasjagu tekitatakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 files encrypted successfully!

TempelPlus v1.2.0 stopping. Time used: 5 seconds



8.8 Dekrüpteerimine ehk lahti krüpteerimine

TempelPlus'i abil saab korraga terve kataloogitäie krüpteeritud faile lahti krüpteerida (ehk dekrüpteerida), eeldusel, et krüpteeritud failide adressaadiks on sellesama Digitempli omanik, kelle Digitempliga dekrüpteerima hakatakse. Ehk – et kasutatava Digitempliga saaks dekrüpteerida, peavad failid olema krüpteeritud, kasutades sellesama Digitempli autentimise (krüpteerimise) sertifikaati.

Iga krüpteeritud konteineri kohta tekitatakse dekrüpteerimisel krüpteeritud faili nimeline kataloog, kuhu kirjutatakse krüpteeritud konteineris olevad andmefailid. Juhul, kui väljundkataloogis on krüpteeritud faili nimega fail või alamkataloog juba olemas, tekitatakse uus kataloogi nimi, lisades esialgsele nimele juurde järjekorranumbri kujul „<failinimi>.cdoc(<jrk_nr>)“.

NB! TempelPlus'iga dekrüpteerimise ajaks sisesta Digitempel oma arvutisse. Kiipkaardil Digitempli korral pane kaart lugejasse, USB pulgal Digitempli korral pista pulk USB auku.

Avada käsurida ja navigeerida TempelPlus'i kodukataloogi (vajadusel asenda sobiva kataloogiga):

cd "c:\Program Files\TempelPlus"

Dekrüpteerimiskäsu üldkuju on järgmine:

tempelplus decrypt <lähtefail või lähtekataloog> -recipient <CN> <lisaparaameetrid>

- **-recipient „<CN>“** – mittekohustuslik; selle parameetriga saab määrata krüpteeringu adressaati. Adressaat on määratud tema ID-kaardi või Digitempli autentimise (krüpteerimise) sertifikaadis oleva Subject CN (Common Name) välja väärtusega. Kui parameeter on määramata, siis leitakse krüpteeritud konteineris olevale adressaadile vastav võti krüptopulgalt, millega dekrüpteerida, kui selline leidub.

Lisaparaameetrid:

- **-pin „<pin kood>“** – mittekohustuslik; pin-koodi saab rakendusele ette anda muuhulgas käsureaparaameetrina, muud pin'i sisestuse võimalused on loetletud peatükis 6.2.
- **-output_folder <kataloog>** - mittekohustuslik; selle parameetriga määratakse kataloog, kuhu lahtikrüpteerimise tulemus kirjutatakse
- **-remove_input** – mittekohustuslik; kui see parameeter on määratud, kustutatakse (dekrüpteeritavad) lähtefailid
- **-follow** – mittekohustuslik; parameeter, mille kasutamisel töötab rakendus ooterežiimis. **NB!** Selle parameetri puhul on kohustuslik kasutada ka – **remove_input** ja **-output_folder** parameetreid



- **-cmn_ext_dir** – antud parameetri määramisel ei kirjutata dekrüpteeritud andmefaile krüpteeritud faili nimelisse alamkataloogi, vaid salvestatakse otse väljundkataloogi (-output_folder parameetriga määratud kataloogi või selle parameetri puudumisel lähtefailiga samasse kataloogi). Juhul, kui kataloogis on sama nimega fail juba olemas, salvestatakse fail uue nimega lisades juurde järjekorranumbri kujul „<failinimi>(<jrk_nr>).<faili_laiend>“. Märkus: antud parameetrit on võimalik määrata ka konfiguratsioonifailis (vt. ptk 6.2). Kui parameeter on käsureal määratud, siis konfiguratsioonifailis olevat väärtust ei arvestata.

Lisaparameetrid HSM seadmega kasutamiseks:

- **-slot <slot_ID>** - HSM seadme sloti ID väärtus³, milles olevat sertifikaati soovitakse dekrüpteerimisel kasutada. Väärtus peab olema kümnendkujul. Sloti määramisel on kohustuslik määrata ka -label parameetri väärtus.
- **-label „<labeli_nimetus>“** – dekrüpteerimiseks kasutatava sertifikaadi ja sellele vastava privaatvõtme label-i väärtus. Tühikute esinemisel label-i nimes tuleb väärtus panna jutumärkide vahele. Label-i määramisel peab olema määratud ka -slot parameetri väärtus.

Märkus: HSM seadme kasutamiseks peavad sertifikaat ja sellele vastav privaatvõti olema seadmel samas slotis, nende labelite väärtused peavad olema samad. Kui käsureal on määratud parameetrid -slot ja -label, siis ei arvestata parameetri -recipient väärtust.

Näide: olgu meil lähtekataloogis (näiteks C:\encrypted_files\) hulk krüpteeritud faile. Dekrüpteerime Digitempliga, mille autentimise (krüpteerimise) sertifikaadis on Subject CN välja väärtus „AsutusX: lepingute kinnitus“. Lahtikrüpteerimisel tekkinud kataloogid (koos andmefailidega) kirjutame sihtkataloogi (näiteks C:\decrypted_files):

tempelplus decrypt c:\encrypted_files\ -output_folder c:\decrypted_files\ -recipient „AsutusX: lepingute kinnitus“

Programm kuvab jooksvalt, mitmendat faili parasjagu töödeldakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done

7 files decrypted successfully! 7 files created.

TempelPlus v1.2.0 stopping. Time used: 19 seconds

Infoks: Juhul, kui dekrüpteerimise momendil sisestatakse vale krüptopulga pin kood või kommunikatsioon seadmega nurjub mingil muul põhjusel, siis krüptopulk võib muutuda selle

³ Kui arvutiga on ühendatud mitu HSM seadet, siis tuleks slottide ID väärtuste leidmiseks kasutada pkcs11-tool utiliiti (ID-le vastab kuueteistkümnendkujul number väljundis).



sessiooni vältel kasutuskõlbmatuks. Selleks, et jätkata tööd, tuleb USB pulk välja võtta ning sisestada tagasi arvutisse.