TempelPlus kasutusjuhend

Tarkvara versioon: 1.0.0
Kuupäev: 31.08.2011

Sertifitseerimiskeskus AS

2011

Sisukord

1 Sissejuhatuseks

TempelPlus tarkvara on mõeldud suurema koguse failide allkirjastamiseks (ehk nö. 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 tarkvaraga, 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 1.0.0, 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 käsureautiliidina ning ainult Windows operatsioonisüsteemil kasutamiseks.

- Parandatud on käsurea utiliidi abiinfot
- Parandus: Tempelplus käsurea utiliidiga 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.

2.2 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 (Aladdini (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

Tarkvara paigaldamine käib Windows msi paki abil, pakk on saadaval aadressilt http://www.sk.ee/tempelplus. Paigalduspakett tekitab All Programs alla TempelPlus programmigrupi, kus on vajalikud viited TempelPlus'ga töötamiseks.

4 Eemaldamine

TempelPlus eemaldamiseks Windows'i all valida All Programs → TempelPlus → uninstall

5 Kust abi saab

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

6 Seadistamine

TempelPlus tarkvara baseerub JDigiDoc teegil/utiliidil (vt. http://www.id.ee/28729?id=28733) Seega sisaldab TempelPlus nii nö. oma seadeid kui ka JDigiDoc teegi seadeid. Vaikimisi sätted TempelPlus'i kasutamiseks määratakse tarkvara paigalduse ajal, nii et TempelPlus peaks kohe peale paigaldamist olema kasutamisvalmis, aga seaded on ka käsitsi vastavalt vajadusele muudetavad.

6.1 JDigiDoc seaded

JDigiDoc teegi/utiliidi olulisemad seaded asuvad järgmistes failides:

- **<TempelPlus kodukataloog>\JDigiDoc\jdigidoc.bat**, olulisemad parameetrid, sätitakse TempelPlus paigalduse käigus:
    - **JDIGIDOC_HOME** – JDigiDoc teegi asukoht failisüsteemis
    - **JAVA_PATH** – java.exe asukoht failisüsteemis, vaja muuta vaid juhul, kui paigalduspakett java't ei leia.
- **<TempelPlus kodukataloog>\JDigiDoc\jdigidoc-win.cfg**, JDigiDoc teegi seaded, TempelPlus'i kasutamiseks vaja muuta pole.

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

6.2 TempelPlus seaded

TempelPlus olulisemad seaded asuvad järgmistes failides:

- **<TempelPlus kodukataloog>\TempelPlus.bat**
    - Parameeter **JAVA_PATH** – java.exe asukoht failisüsteemis, vaja muuta vaid juhul, kui paigalduspakett java't ei leia.
- **<TempelPlus kodukataloog>\SignatureLogging.properties**
    - Parameeter **log4j.appender.file.file** – TempelPlus'i logifaili asukoht failisüsteemis, määratakse paigalduspaketi poolt
- **<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 või käsurealt, võimalikud variandid: graphic, console
- **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**

o *Muud seaded - failid, kataloogid*

- **jddoc_location** – JDigiDoc teegi asukoht, määratakse paigalduspaketi poolt
- **log_file** – logifaili asukoht, määratakse paigalduspaketi poolt
- **work_directory** – TempelPlus töökataloog, ajutiste failide hoidmiseks jms, määratakse paigalduspaketi poolt
- **DIGIDOC_LOG4J_CONFIG** - SignatureLogging.properties faili asukoht, määratakse paigalduspaketi poolt
- **DIGIDOC_DF_CACHE_DIR** – JDigiDoc teegi kataloog ajutiste failide hoidmiseks, määratakse paigalduspaketi poolt
- **bc_prov=bcprov-jdk15-125.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. Määratakse paigalduspaketi poolt, kui mõni leitakse, järgmises prioriteetsuse järjekorras:
    - Aladdini eToken-i draiver (C:\\windows\\system32\\eTPKCS11.dll)
    - ID-kaardi tarkvaraga kaasa tulev OpenSC PKCS#11 draiver (C:\\Windows\\System32\\opensc-pkcs11.dll)

- *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

7 Kasutamine – kasutusjuhtude kaupa

7.1 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 -?

7.2 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 ootereziimis, kus peale lähtefailide allkirjastamist jääb programm tööle ja ootab lähtekataloogi tekkivaid uusi faile, mida allkirjastada. Üldine põhimõte on, et kui allkirjastamise käigus peaks sihtkataloogi, kuhu allkirjastatud faile salvestatakse, tekkima sellise nimega fail, mis on sihtkataloogis juba olemas, siis sama nimega faile üle ei kirjutata ja programm lõpetab veateatega töö. 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. **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> <lisaparameetrid>

Lisaparameetrid:

- **-output_folder <kataloog>** – mittekohustuslik parameeter, määramaks kataloogi, kuhu kirjutatakse allkirjastatavad failid
- **-remove_input** – mittekohustuslik; kui see parameeter on määratud, kustutatakse (allkirjastatavad) lähtefailid
- **-follow** – mittekohustuslik; parameeter, mille kasutamisel töötab rakendus ootereziimis. **NB!** Selle parameetri puhul on kohustuslik kasutada ka **–remove_input** ja **–output_folder** parameetreid
- **-signer_cn „<CN>"** – mittekohustuslik; parameeter, millega saab määrata, missuguse võtmega allkirjastamist sooritatakse. Kui parameetrit mitte kasutada, siis valitakse esimene allkirjastamisvõti. Parameetri väärtus, kui seda parameetrit 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 käsureaparameetrit
- **-country „<riik>"** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **country** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparameetrit

- **-state „<osariik/maakond>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **state** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparameetrit

- **-city „<linn>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **city** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparameetrit

- **-postcode „<postiindeks>“** – mittekohustuslik; võimaldab allkirjastatavale konteinerile lisada allkirjastaja asukoha infot. Kui **postcode** parameeter on määratud ka TempelPlus.conf konfiguratsioonifailis, siis eelistatakse käsureaparameetrit

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 küsib terve kataloogitäie failide allkirjastamise jaoks 1 korra PIN’i, kuvab jooksvalt, mitmendat faili parasjagu allkirjastatakse, ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done
7 documents signed successfully
TempelPlus v0.99 stopping. Time used: 18 seconds

7.3 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 konteinerite allkirju:

tempelplus verify c:\digidoc_files

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 signatures and 0 invalid signatures
TempelPlus v0.99 stopping. Time used: 2 seconds

7.4 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 v0.99 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 v0.99 stopping. Time used: 2 seconds

7.5 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.

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>

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 v0.99 stopping. Time used: 2 seconds

7.6 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> <lisaparameetrid>

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

Lisaparameetrid:

- **-output_folder <kataloog>** – mittekohustuslik; loodavad konteinerid tekitatakse selle parameetriga määratud kataloogi
- **-add_file <kataloog või tühikuga eraldatud failide list>** - mittekohustuslik; selle parameetriga määratud failid lisatakse igasse loodavasse 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 v0.99 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 v0.99 stopping. Time used: 1 seconds

Näide 3: 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 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 v0.99 stopping. Time used: 1 seconds

7.7 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 v0.99 stopping. Time used: 5 seconds

7.8 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. **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> <lisaparameetrid>

- **-recipient „<CN>"** – kohustuslik; selle parameetriga saab määrata krüpteeringu adressaati. Adressaat on määratud tema ID-kaardi või Digitempli autentimise (krüpteerimise) sertifikaadis oleva Subject CN (Common Name) välja väärtusega.

Lisaparameetrid:

- **-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 ootereziimis. **NB!** Selle parameetri puhul on kohustuslik kasutada ka **–remove_input** ja **–output_folder** parameetreid

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 küsib PIN'i (kiipkaardil Digitempli korral PIN2'te, USB pulgal Aladdini eToken'i peal Digitempli korral pulga PIN'i) ja seejärel kuvab jooksvalt, mitmendat faili parasjagu töödeldakse ning edukal juhul lõpetab järgnevale analoogilise teatega:

Done
7 files decrypted successfully! 7 files created.
TempelPlus v0.99 stopping. Time used: 19 seconds