Att koppla TDialog till PhenixID Signing

Innehållsförteckning

1. Inledning

Detta dokument syftar till att ge all nödvändig information om hur TDialog konfigureras tillsammans med PhenixID Signing. Notera att själva installationen av TDialog beskrivs i installationsdokumentationen och installationen av PhenixID Signing beskrivs i Phenix ID:s dokumentation. Dokumentet fokuserar på TDialogs dokumentation, men nämner även vissa förutsättningar i konfiguration på Signing-sidan.

2. Förutsättningar

Installerad TDialog

Installerad PhenixID Signing.

Verifiera att PhenixID signing är installerad enligt följande konfiguration:

- Ingen Basic Authentication på REST-anropet från TD (vilket i praktiken innebär att man bör skydda relevanta PhenixID-URL:er från att bli anropad från andra).
- När PhenixID skickar tillbaka dokument till TD ska de vara base64-encodade.

För mer information hänvisas till PhenixID (https://support.phenixid.se/sbs/trusteddialog-pdf-sign/).

Brandväggsöppning

TDialog måste kunna kommunicera med PhenixID på porten som ska användas för REST (porten i <PhenixURL> nedan). Verifiera detta med telnet <PhenixURL> från TD-servern.

3. Startinformation

- URL till PhenixID-signing, i dokumentet kallat <PhenixURL>, inklusive port.
- Path till TDialog, i dokumentet kallat <TDPath>.

4. Konfiguration

4.1. Skapa nyckelpar för att signera requests

- Skapa 2048-bitars privat RSA-nyckel
  ```
  $ openssl genrsa -out private_key.pem 2048
  ```
- Konvertera till PKCS#8 (så att Java kan läsa den)
  ```
  $ openssl pkcs8 -topk8 -inform PEM -outform DER -in
  private_key.pem -out private_key.der -nocrypt
  ```
- Skapa ett certifikat av den privata nyckeln
  ```
  $ openssl req -x509 -sha256 -nodes -days 1095 -new -key
  private_key.pem -out certificate.crt
  Ingen certifikatsinformation behövs.
  ```
- trusteddialog.crt ska skickas till PhenixID, det används för att verifiera att information från TDialog är korrekt (mer specifikt den JSON Web Token som skickas med REST-anropet, om PhenixID behöver mer information).
- private_key.der ska läggas i /config i TDialog-installationen och pekas ut med parametern .

4.2. Ta PhenixID TLS-certet och skapa jks

- Surfa till <PhenixURL>.
- Ladda ner certifikatet för sidan, döp till phenixidsigningrestcert.cer
- Kör: `keytool -importcert -file "phenixidsigningrestcert.cer" -keystore phenixidsigningrestcert.jks -alias "phenixidsigningrestcert"` Om Windows: Kör i vanlig gammaldags Windows-prompt (CMD) istället för PowerShell, och keytool är en del av Java-installationen.
- Ange ett lösenord. Notera att det enda denna jks innehåller är att den litar på PhenixID-certifikatet, den innehåller i sig inga privata nycklar. Därför är säkerhetskraven inte så höga. Lösenordet kallas nedan för <TD_REST_PASSWORD>.
- Lägg phenixidsigningrestcert.jks i /config i TDialog-installationen

4.3. Lägg till i application-prod.properties

- Lägg till följande i application-prod.properties och ersätt <TDPath> etc med värdena för installationen (observera att pathar skrivs med framåtslashar i Java):

```
server.signing.phenixid.new-style-key=true
server.signing.phenixid.private-key-
file=<TDPath>/config/private_key.der
server.signing.phenixid.enabled=true
# Domain below excludes https:// but includes port number
# e.g. signing.grevlinge.se:8443
server.signing.phenixid.signing-domain=<PhenixURL>
server.signing.phenixid.jwt-recipient-path=/td
server.signing.phenixid.rest-signing-path=/files/integration
server.signing.phenixid.web-signing-path=/sign
server.signing.phenixid.certjkslocation=<TDPath>/config/pheni
xidsigningrestcert.jks
server.signing.phenixid.certjkspwd=<TD_REST_PASSWORD>
```