TARGET – Instant Payment Settlement

FAQs v2.0

GoSignDesktop installation

1. NRO

The Ascertia solution is the NRO solution designed for all Target services. In TIPS it was introduced with release 4.0 and in T2S with release 6.0.

Hereunder you can find the frequently asked questions which were raised by most of the participants during the installation of Go-Sign application both in single or multi user configuration. They have been divided in three sections:

- *General*: questions that are independent from the type of configuration implemented (single or multi user configuration)
- *Single-user configuration*: questions that are referred to the installation of Go-Sign application in single user mode
- *Multi-user configuration*: questions that are referred to the installation of Go-Sign application in multi user mode

1.1 General

1. *How do you get the GSD software?*

   The links are provided in ESMIG Qualified Configuration document and they work only if you are already logged into the ESMIG Portal. The software is the same for each environment, only access urls are different.

   updated GSD SU and MU download URLs for T2S are currently reported in the T2S_NRO_Technical_Document (1.8.5 latest version).

2. *Is the using of the GSD free of charge or the license fee is applicable? Does every Commercial Bank need a contract / licence with Ascertia on its own? Or is this included, as provided by ECB inside the Eurosystem?*

   4CB entered into a license agreement with Ascertia and costs will be managed accordingly by 4CB.

3. *Which browsers are supported by NRO?*

   The qualified browsers are Chrome 88.0+ and Firefox 78.0+. Edge will be qualified within a specific change request even though it is supposed to be already working.

4. *How the gosign certificate installed by the software is managed? It currently has expiry date 2 years after installation. What happens when expired? Will we receive notification of 4CB? Will new certificate be included in new software releases?*

   We will check with Ascertia possibility to include new certificates in new software releases; in any case the final certificate renewal procedure will be reviewed and shared after the new release. At the moment, following steps could be performed for certificate renewal:

   a) Stop Go>Sign Desktop (application/service)

   b) Go to Go>Sign Desktop installation directory i.e “C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf“ and remove the file 'gosign.keystore'

   c) Restart Go>Sign Desktop and it will add the new self-signed certificate and remove the previous one from windows keystore.

   d) Repeat the actions performed for single user / multiuser installations

4CB will not be in position to send expiral notification to each customer as the certificate is different for each installation and is generated at installation time.

5. *Is there any plan to include Go-Sign on ESMIG U2A?*

   Single user client download URL are alredy included in the ESMIG portal. The one for multi user will be added. The planning is to be agreed internally.

6. *Why cannot the certificate be imported in the local server trust store instead of in each user's trust store? What happens if we run the import more than once?*

   The GSD client currently checks the user's trust store, therefore the gosign certificate has to be imported in each user's trust store. Importing the same certificate more than once should actually have no impact on the user's trust store.

7. *Can users change the default password for cacerts? **new***

   No, users are not supposed to change it.

8. *Can users change the default location of* gosign_app.properties*? If so, how? **new***

   The possibility to change the default location is currently not envisaged. The Service Provider will investigate if it's possible to make it configurable in a future minor release.

   The current location of gosign_app.properties is:
   C:\Users\USERNAME\

1.2 *Single-User configuration*

1. *Which are the Windows 10 versions that are supported?*

   Windows 10 Enterprise is qualified by 4CB. Different Windows 10 versions may be working; best effort support will be provided in this latter case.

2. *What is the correct software version?*

   The correct software version for GSD Single-user is:
   ADSS-Go-Sign-Desktop-v.6.6.0.14-win64.msi

3. *Is there a need to check the certificate of gosign desktop against any CRL?*

   No need to check the certificate of the go sign desktop against any CRL as it is a self-signed one.

4. *In case of proxy.pac file being used on a workstation/desktop, the following rule should be included in order to add the appropriate exception: **updated ***

```
if (dnsDomainIs(host, "client.go-sign-desktop.com")){
return "DIRECT";
}
```

1.3 Multi-user configuration

1. *Which Windows Server versions are supported?*

   Windows 2016 Server Enterprise is qualified. Different Windows Server versions may be working; best effort support will be provided in the latter case.

2. *What is the correct software version?*

   The correct software version for GSD Multi-user is:

   a) ADSS-Go-Sign-Desktop-v.6.6.0.14-win64.msi
   b) gsdmu_1.2.zip (GSD Multi user code add-on)*****
   c) NSSM service wrapper 2.24 2014-08-3

   The **gsdmu_1.2.zip** (GSD Multi user code add-on) has been released to fix the issue faced within INC000000312070 . All customers are requested to download it and replace the appropriate file Go-Sign-Desktop.jar on terminal server side restarting the service to make the new file active.

3. *Service is only required for Multi User?*

   This is correct, the Single User desktop version does not require setup for service

4. *How GSD.exe manage the multi-users?*

   The service/parent instance will run at port 8782; user/child processes will start during user NRO tasks and will listen on higher ports (i.e. 8784, 8786 ecc). Ports used by Go-Sign-Desktop.exe user / child instances are freed once the customer disconnect / log-off from the terminal server instance.

5. *How to import client.gosign certificate into java <cacerts> keystore?*

   Command is reported in the Esmig 1.3.1 guide; default java password is to be used. With next release this step will not be required anymore.

6. *What account NETWORK SERVICE windows need to be used on the windows service?*

   The account is <nt authority\networkservice>

7. *The Service Wrapper is mentioned to Start the "Go-Sign-Desktop.exe" is this correct or should it link to the GSD.exe? Will the new release of the Ascertia GSD client, also include the step for wrapping the service?*

   Correct service wrapper command to be used is reported in the 1.3.1 guide and also below:
   "*C:\Program Files\Ascertia\Go-Sign-Desktop\nssmServiceWrapper\win64\nssm.exe" install "Go Sign Service" "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-Sign-Desktop.exe"*
   This is the solution available at the moment; alternate solutions being checked by Ascertia to automate service creation.

8. *Should the citrix end user launch the Go-Sign-Desktop.exe? Or only GSD.exe ? **updated***

From user point of view, NRO interaction is expected to prompt the user to start ascertiaGSD application (via GSD.exe), which will start Go-Sign-Desktop.exe application in turn.
Specifically, the GSD.exe performs the following operation:

- First time when executed by the user: it adds a registry entry for Go>Sign Desktop to run via custom URL i.e 'ascertia:appId=<UUID>'. The following registry keys will need to be added to user profiles in case not persistent:
  - Create .reg file
  - insert the following lines

  - Execute this reg file to actually insert the registry keys. (GPO can be used as alternate method to directly insert the keys)

- Second time, during NRO task (after user presses ok to start ascertiaGSD application) it creates/updates 'gosign_app.properties' file under userProfile and starts the Go-Sign-Desktop.exe application

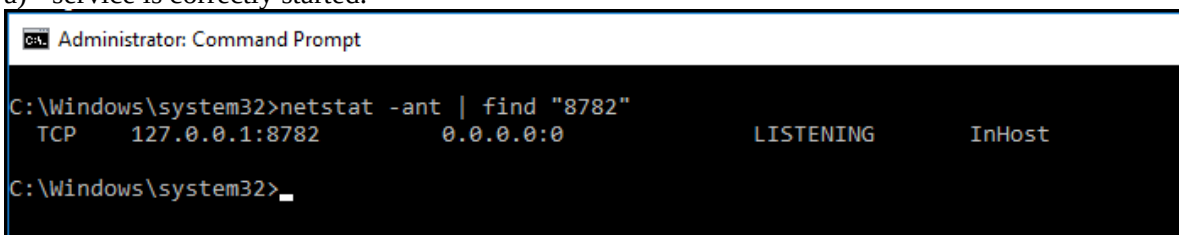
9. *Is it possible to use another port other than the default port 8782?*

   8782 port should be used for the moment.

10. *Which are the GSD MU checks to be done before the user starts an NRO task? How is it possible to test if the service is running?*

1) GSD parent instance/service checks to be done by IT Admin:

a) service is correctly started:



b) Using the test URL "https://client.go-sign.desktop:8782/gosign-desktop" in GSD MU context will currently generate the "Port is not configured" message. This basically means that the latest jar is correctly being used. It is not an error message and it will be modified in the next release to provide more meaningful information.

If the service is correctly running, GSD service/parent instance log should be found at C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs

2) Certificate checks to be done by IT Admin: ****updated****

a) « gosign » certificate for Network Service user
   i) start command prompt for "Network Service" user environment (*psexec -i -u "nt authority\network service" cmd.exe*)
   ii) run certmgr.msc tool
   iii) check and note down certificate thumbprint / serial number

iv) check that friendly name = « **gosign** » is correctly present in the certmgr initial display panel *(check valid for all the import activities required).*

b) gosign » certificate for business user
   i) check and note down certificate thumbprint / serial number and compare it with the one in point a.iii) above
   ii) check that friendly name = « **gosign** » is correctly present in the certmgr initial display panel. If not present the following can be added in the user logon(/logoff) scripts in order to automatically perform this step :

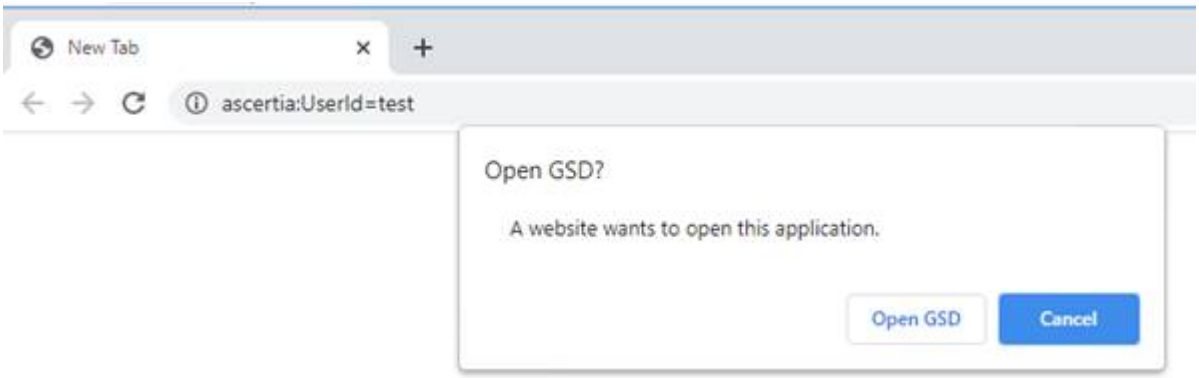
$cert = Get-ChildItem -path "Cert:\CurrentUser\ROOT\" | where{$_.Subject -eq "CN=client.go-sign-desktop.com"}
$cert.FriendlyName = "gosign"

Alternatively, the following powershell commands can be used:

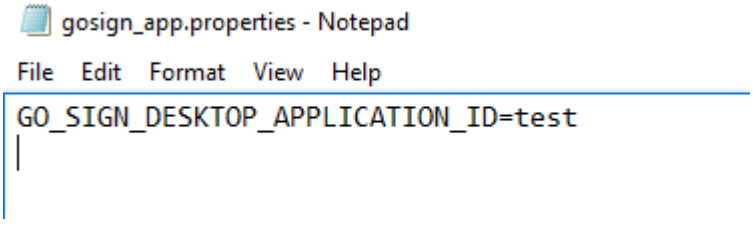
$cert = Get-ChildItem -path "Cert:\CurrentUser\ROOT\" | where{$_.Subject -eq "CN=client.go-sign-desktop.com"}
$cert.FriendlyName = "gosign"

If above checks (1 and 2) are ok:

3) Business user could optionally perform the following actions/checks:
   i) Open Chrome and type the following URL:

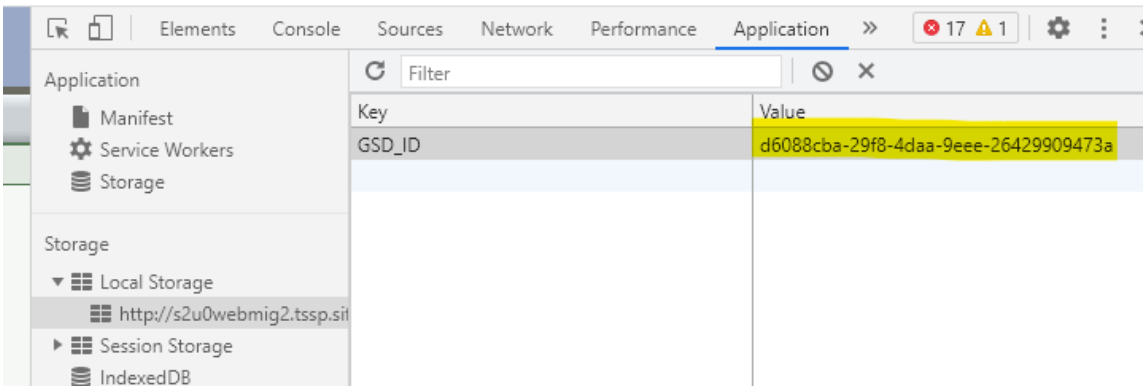


   ii) Click Open GSD
   iii) Check c:\users\%username%\gosign_app.properties is populated as follows



   iv) If ok, being this action above only a test, please check/cleanup userinfo.properties file and proceed with NRO task. If NOK, please investigate any GPO or UAC possibly preventing the user to update the gosign_app.properties file and evaluate the following workaround in the meanwhile. NRO will not work properly in case GSD application launched by the user during NRO task cannot create and/or update the gosign_app.properties file.

v) Workaround:
   (1) gosign_app.properties may be populated manually with the following string: GO_SIGN_DESKTOP_APPLICATION_ID=<GSD_ID>.
   (2) The <GSD_ID> value will be printed out in the following browser tool once user has started the NRO process (and will change after log off / log on from Citrix session):



*11. Where are the GSD operations logged on the server? **new***

GSD operations are logged at two different levels:

a) At main application level (parent/service instance): C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs
b) At user's level (user/child instance): C:\Users\USERNAME\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs

*12. Does the "Open GSD application" pop-up open for each NRO session or only once per day? **new***

The pop up appears only the first time. As long as the user session (i.e. user/child instance) remains alive, the pop-up will not appear again.

*13. What is the function of userinfo.properties file? **new***

This file contains the mapping between the GSD session id and the port used by each child/user instance. It is populated by the service/parent instance using information provided by user/child instances.

*14. Can we import the certificate generated during the single installation for import on java cacert and on all user windows trust store? **new***

The certificate generated during the single user client installation (sec. 2.1.1) have to be imported both in "cacerts" java keystore and in each user trust-store. Please also see point 10 (par. 2).