ESMIG U2A

Qualified Configurations

V1.3

Author	4CB
Version	1.3.4
Date	07/10/2022
Status	Final
Classification	Unclassified
Accessible	
Classified until	

History of releases

RELEASE	DATE	ISSUES	STATUS[1]
1.0	01/03/2021	First version. Applicable for TIPS	Draft
1.0.1	06/04/2021	Second version, clarifications on support for terminal servers	Draft
1.1	05/05/2021	Third version. Extension to CLM and RTGS GUIs	Final
1.2	26/07/2021	Added terminal server support for Ascertia client. Extension to ECMS. Ascertia client URLs changed. Minor clarifications on U2A configurations. Added section in the annex concerning the GSD multi-user solution	Final
1.3	20/08/2021	Minor integrations to GSD multi-user solution installations Notes and typos amended	Final
1.3.1	15/10/2021	Added notes about HSM based certificate usage. Added clarifications in the "GSD multi-user solution installation" Annex.	Final
1.3.2	01/12/2021	GSD MU installation procedure revised according to 6.9 client delivery	Final
1.3.3	03/12/2021	Minor editorial changes; amended download URLs for T2S SU and MU; amended MU install procedure (Sec. 2.1.4 and 2.1.5)	Final
1.3.4	07/10/2022	SU and MU install procedure amended to reflect last changes introduced with GSD 6.9.0.9 client. Replies provided in the FAQ 2.0 (DEC21) have been included as well.	

[1] Status value : Draft, Open, Final, Dismiss

Table of contents

1 INTRODUCTION

1 Introduction

1.1 Purpose and Objectives

This document describes the general configuration that ESMIG users shall be complaint with in order to access TIPS, T2S, ECMS, RTGS, CLM and CRDM GUI via the ESMIG web portal.

A specific section is devoted to describe the technical framework needed to fully implement the non-repudiation of origin functionality (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.

1.2 Background remarks

The aim of the ESMIG qualified configurations is to provide ESMIG users with a specific configuration that is proved to be fully working.

As already mentioned, the NRO solution, based on the Ascertia Go>Sign Desktop application, will be the unique U2A NRO solution to be adopted for TARGET services, therefore only one version of the Go>Sign Desktop client will be used and distributed across the different services.

Important also to hightlight that Go>Sign Desktop client applications are already in use in TARGET2 for Internet Access and Contingency Network and 4CBs will guarantee that no different versions are needed by the relevant services using the client, before the go-live of CSLD project.

2 Ascertia GSD Single User Client (SU)

2.1 Qualified configuration

As already mentioned, the 4CB has qualified a specific subset of the NSPs compatibility matrix. These configurations have been extensively tested and support on them is guaranteed.

NSP	SWIFT	SIA-COLT
OS	Windows 10 Enterprise	
Browser	Google Chrome 88+ Firefox 78.9+	
Go>Sign Desktop SU	> = 6.9.0.1	

These cryptographic key stores, used to access the signing keys, are supported:

- PKCS#11 for hardware-based tokens
- HSM based certificates (as per NSP specifications)

The 4CB will ask customers running a software version lower than that qualified to upgrade to a qualified version in order to proceed with problem investigation.

The 4CB will investigate issues experienced by customers while running a software version higher than that qualified: if the root cause is linked to the specific software version, then the 4CB will attempt to find a workaround (which may involve customers downgrading their software to a qualified version). The 4CB will evaluate whether a fix for the issue can be included in a future relevant TARGET Service GUI release.

Customers using totally or partially different system components or versions than those mentioned are then responsible to verify the full compatibility with the relevant TARGET Service GUI in the test environments and the system. The 4CB will in any case, provide support to the maximum extent possible for checking / testing alternative configurations in order to support troubleshooting process.

The local customer system set-up, i.e. adaption of the local firewall and security policies in order to enable the client installation, HTTPS transfer communication, access to the certificates on the USB tokens/HSM from the client machines (either physical or remote workstations) is under the sole responsibility of the end users (that may also need to involve their internal IT Dept. as well as external providers, in case of product specific issues).

2.2 Technical requirements and recommendations

2.2.1 Single user download URLs

The client is available for download on the ESMIG portal (after log-in) at the following URLs. The software is the same for each environment, only access urls are different.

EAC PORTAL

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_SU

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_SU

UTEST PORTAL

https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_SU

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_SU

PROD PORTAL

https://esmig-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_SU

https://esmig-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_SU

The full installation guide provided by Ascertia can be upon request and it can be used as reference for specific needs (e.g. automated installations). Downloading and installing the Go>Sign Desktop client is a mandatory step to sign/verify U2A requests. Installation requires administrative privileges; local IT support must be involved to make sure the installation correctly ends.

4CB entered into a license agreement with Ascertia and costs will be managed accordingly by 4CB ; disclaimer accepted by the user at installation phase should not be taken into consideration. Customer should open support request to 4CB only and NOT to Ascertia directly. 4CB will involve Ascertia as appropriate.

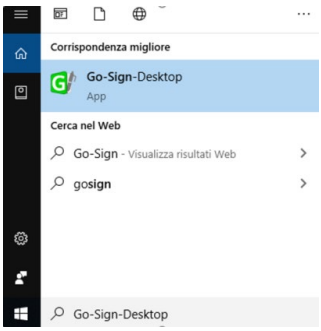
2.2.2 Removing previous Go>Sign Desktop client

In case a previous version of the Go>Sign Desktop client is already installed on a workstation, users or IT Admin should uninstall ths version first (e.g. 6.9.0.1) and then install the new one.

Users / IT Admin are also required to explicitily delete the existing gosign user certificate before installing the updated client version. This will ensure that one and only one "gosign" certificate will be installed for a user.

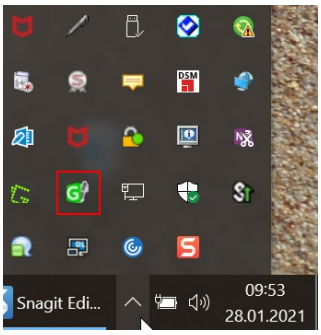
2.2.3 Go>Sign Desktop Client Requirements and post-installation remarks

After installation, ADSS Go>Sign Desktop will start automatically at the user logon therefore user is not expected to manually start the client. Due to specific security settings, this might not happen, resulting signature attempts to end with a similar error "Go>Sign desktop not running/installed". In this case, it is necessary to start the client manually before initiating a browsing session. It is possible to lookup for the Go>Sign via the Windows Search bar:



- If the icon is not found, this can be probably linked to problems occurred during the installation. The local IT support needs to be involved in this case.

- Ensure that the Go>Sign icon is featured in the system tray:



If the icon is not found, this can be probably linked to problems occurred during the installation. The local IT support needs to be involved in this case.

ADSS Go>Sign Desktop relies on TLS communication with the web application (on port 8782). This communication is secured using a TLS server certificate having hostname:

client.go-sign-desktop.com.

Therefore, the local client machine must be able to resolve this FQDN (Fully Qualified Domain Name complete domain name for a specific computer, or host, on the internet) to itself. In order to achieve

this, the standard installation procedure foresees that the Go>Sign Desktop Installer automatically adds the entry :

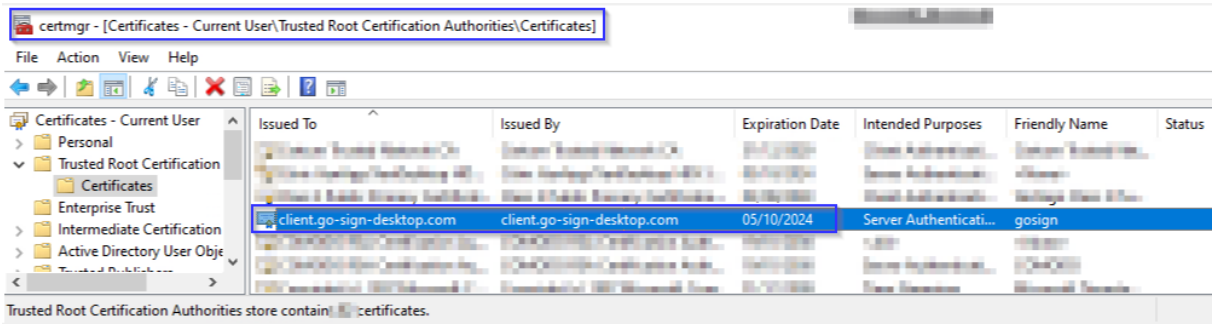
127.0.0.1 client.go-sign-desktop.com

in the Operating System host file in order to register the client.go-sign-desktop.com as a local domain (Windows OS: C:\Windows\System32\Drivers\etc\hosts). This will add the FQDN client.go-sign-desktop.com to resolve to IP address 127.0.0.1.

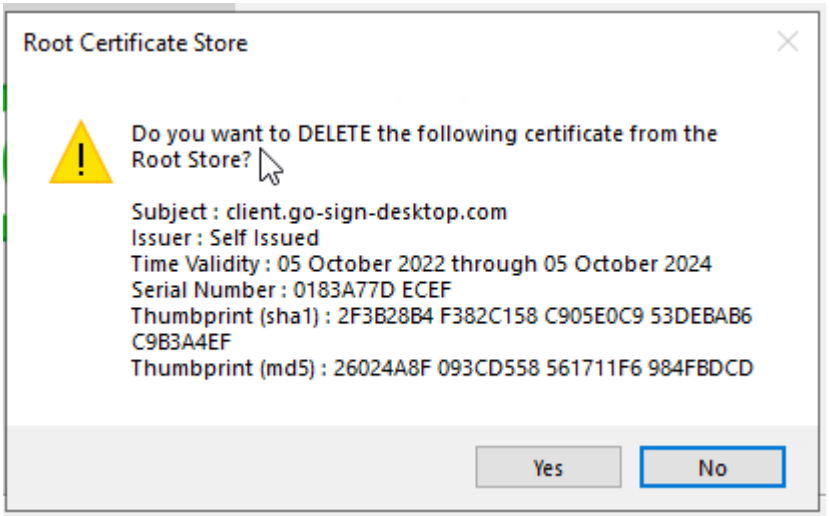
The default value client.go-sign-desktop.com must not be changed.

The TLS server certificate will be self-signed and different for each workstation where the client will be installed.

Open Command prompt and use "certmgr.msc"

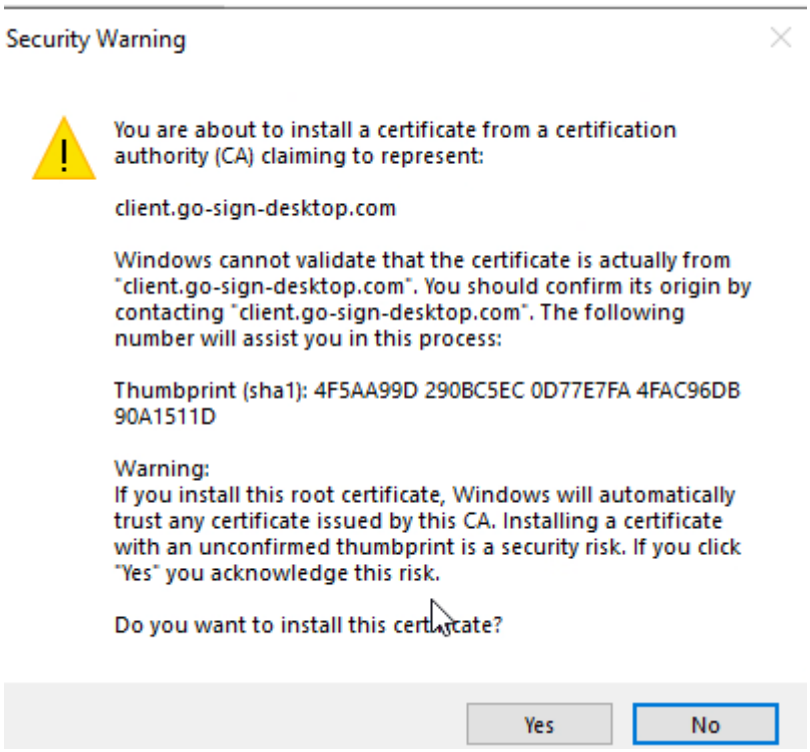


If user are asked during the single user GoSign installation: "Do you want to DELETE the following certificate from the Root Store?"



please confirm with "YES"

and afterwards next dialogue "You are about to install a certificate from a certification authority (CA) claiming to represent: …"



please confirm again with "YES".

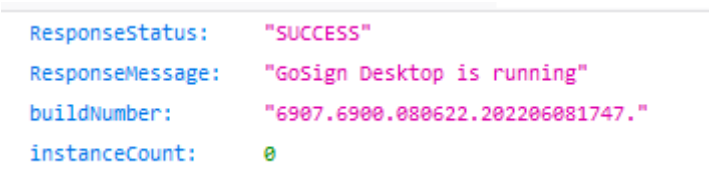
Please note hat this dialogue may also appear when the GoSign application will start for the first time, e.g. in case workstation is shared by multiple users .

The end users have to ensure that the security settings of their institutions, i.e. firewalls, allow for installation of the desktop client as well as for code signing certificate revocation check, if not generally disabled. By default, User Account Control Settings (UAC) are enabled in windows. ADSS Go>Sign Desktop needs user permissions to make changes on the installing device. Windows always prompt a dialog to get the user permissions if user granted the permissions then ADSS Go>Sign Desktop would be installed on the device.

In order to check the correct version Go>Sign desktop is installed, users can right click on the go sign icon and choose "about". After that the following window appears:

or

In order to check that ADSS Go>Sign Desktop is running properly, user should access the test URL https://client.go-sign-desktop.com:8782/gosign-desktop ; the following message is expected to be displayed (FF and Chrome browser, respectively):



{"ResponseStatus":"SUCCESS","ResponseMessage":"GoSign Desktop is running","buildNumber":"6907.6900.080622.202206081747.","instanceCount":0}

Port 8782 must not be changed into gosign-desktop.properties file otherwise the overall NRO setup will not work.

2.2.4 Additional requirements

Here following a list of items to be checked before starting the test sessions or in case of exceptions that may block the testing. Internal IT support may be needed to perform these checks because of security restrictions that may be in place preventing the end users to complete them autonomously:

- As a general remark, please make sure that the configurations listed in the relevant NSPs documentation are applied (as a not exhaustive example, the mandatory changes on the pac file). For further details please refer to the "SWIFT's Solution for ESMIG U2A Setup Guide Step-by-Step" document and the " SIAnet.XS Connectivity Services for ESMIG U2A User Guide"

- In case of local network exceptions in the browser (i.e. **TUNNEL CONNECTION FAILED, NAME NOT RESOLVED**) during first interaction with Ascertia backend infrastructure: add DSS host certificates in browsers keyring (e.g Chrome and Firefox). Host names following for information:

SIA TST	esmig-tst-dss.u2a.sianet.sia.eu
SIA CRT	esmig-cert-dss.u2a.sianet.sia.eu
SIA PRD	esmig-dss.u2a.sianet.sia.eu
SWIFT TST	esmig-tst-dss.emip.swiftnet.sipn.swift.com
SWIFT CRT	esmig-cert-dss.emip.swiftnet.sipn.swift.com
SWIFT PRD	esmig-dss.emip.swiftnet.sipn.swift.com

The same above URL may need to be added to the browsers trusted sites.

- In case of Cross-Origin Resource Sharing (CORS) issue during first interaction with new Ascertia infrastructure, please temporarily disable CORS checks both in Chrome and/or FF

a. FF --> https://addons.mozilla.org/es/firefox/addon/access-control-allow-origin/ + Toggle ON

b. Chrome --> "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-web-security --user data-dir="C:\.....\Chrome" (for single user environment)

c. Chrome --> "C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --disable-web-security (for multi user environment)

- 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";
}
```

- Check installation / install "client.go-sign-desktop.com" certificate in Chrome and Firefox explicitly (or check first if it is in all browsers keyring after GSD client installation). Without this exception error code 404 may be displayed. Also ensure that Firefox is allowed to check / read certificates from Windows keystore. As already stated above, one and only one gosign certificate has to be present in user trust store; in case two or more gosign certificates present, client may not start or may start with exceptions.
    - No need to check the certificate of the go sign desktop against any CRL as it is self-signed.

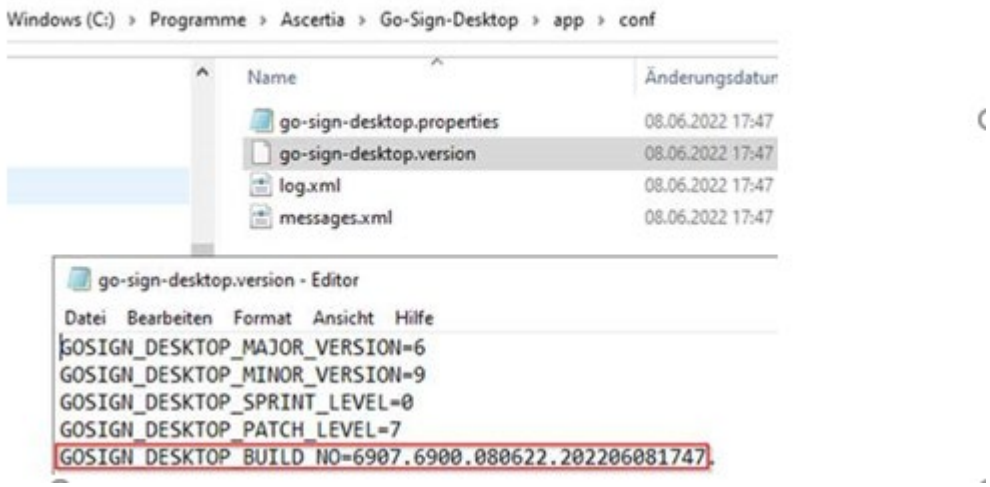
- It is finally suggested to ensure that one token at time is connected to a workstation during signing operation.

2.3 Mandatory troubleshooting information

When opening the incident to 4CB Service Desk, users must provide the following:

- OS and browser in use plus type of installation (SU) and its version ("About" panel or information from the following file):

C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\gosign-desktop.version



- "go-sign-desktop.log" (DEBUG level, see next section)
- Copy of %userprofile%\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs\go-sign-desktop.properties (if any changes applied from default values)
- Browser console log file (F12 button)
- Browers network trace file (F12 button) – *only in case of network-related issue and if explicility required*
- Relevant screenshots reporting any useful exception

It is higly suggested to check any expcetion first with the internal IT/Network support for a preliminary analysis and then with 4CB. NSP may be involved as well in case of network-related issues.

2.3.1 Client logging information and changing log level

ADSS Go>Sign Desktop application has two log levels. First informational, which is for normal use, and second, debug, which should only be used when investigating performance issues, functionality problems, etc. For Windows OS and go>sign client configuration, users can view ADSS Go>Sign Desktop application logs at:

C:\Users\[User_Name]\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs\

By default, ADSS Go>Sign Desktop logging level is set to INFO. To enable detailed debug logging, follow these instructions:

1. Go to ADSS Go>Sign Desktop installation path
   C:\Users\[User_Name]\AppData\Roaming\Ascertia\Go-Sign-Desktop
2. Edit the go-sign-desktop.properties file using a suitable text editor.
3. Change the value of the property GOSIGN_DESKTOP_LOG_MODE from INFO to DEBUG and save the file.
4. Stop ADSS Go>Sign Desktop application → right click ADSS Go>Sign Desktop application icon and select the option Quit.
5. Start ADSS Go>Sign Desktop application → Start Menu

Please note that go-sign-desktop.log and go-sign-desktop.properties have been moved to new location compared to old GoSign 6.9.0.1.

3 Ascertia GSD Multi User Client (MU)

3.1 Qualified configuration

As already mentioned, the 4CB has qualified a specific subset of the NSPs compatibility matrix. These configurations have been extensively tested and support on them is guaranteed.

NSP	SWIFT	SIA-COLT
OS	Windows 2016 Server Enterprise	
Browser	Google Chrome 88+ Firefox 78.9+	
Go>Sign Desktop MU	> = 6.9.0.1	

3.2 Technical requirements and recommendations

3.2.1 Multi user download URLs

ESMIG customers can download the client from the following URLs (after log-in to ESMIG portal):

EAC PORTAL

https://esmig-eac-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_MU

https://esmig-eac-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_MU

UTEST PORTAL

https://esmig-cert-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_MU

https://esmig-cert-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_MU

PROD PORTAL

https://esmig-portal.u2a.sianet.sia.eu/gosign/download/64bit_client_MU

https://esmig-portal.emip.swiftnet.sipn.swift.com/gosign/download/64bit_client_MU

Downloading and installing the Go>Sign Desktop client is a mandatory step to sign/verify U2A requests. Installation requires administrative privileges; local IT support must be involved to make sure the installation correctly ends.

4CB entered into a license agreement with Ascertia and costs will be managed accordingly by 4CB ; disclaimer accepted by the admin at installation phase should not be taken into consideration. Customer should open support request to 4CB only and NOT to Ascertia directly. 4CB will involve Ascertia as appropriate.

3.2.2 Suggested upgrade procedure

If a previous MU client installation is present on server environment, please follow the below checklist in order to correctly upgrade to the new release:

1. Stop the parent/service instance and any other child/user instance (mandatory to ensure proper clean up of all folders)

2. Client de-installation from control panel

3. Clean up the "gosign" certificate from the Trusted Root CA stores of both the Current User (certmgr.msc) AND the local Computer (certlm.msc)

4. Check service deleted + check all Ascertia folders/subfolders deleted

5. New client installation (as per section 3.2.3) + additional steps:

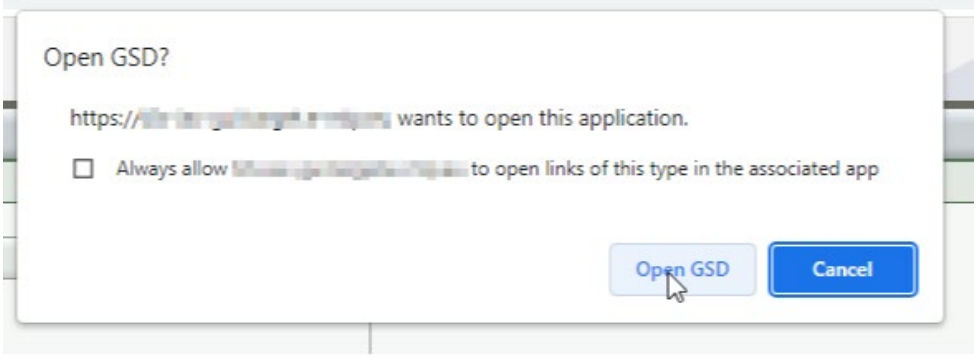
   a. Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe" (or account that performed installation). This command will add the new gosign certificate into server admin trust store.

   b. Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe" (or account that performed installation). This command will add the new gosign certificate into LM trust store.

   c. Change service start type to AUTO

   d. Re-start the service (than it will be managed as "AUTO")

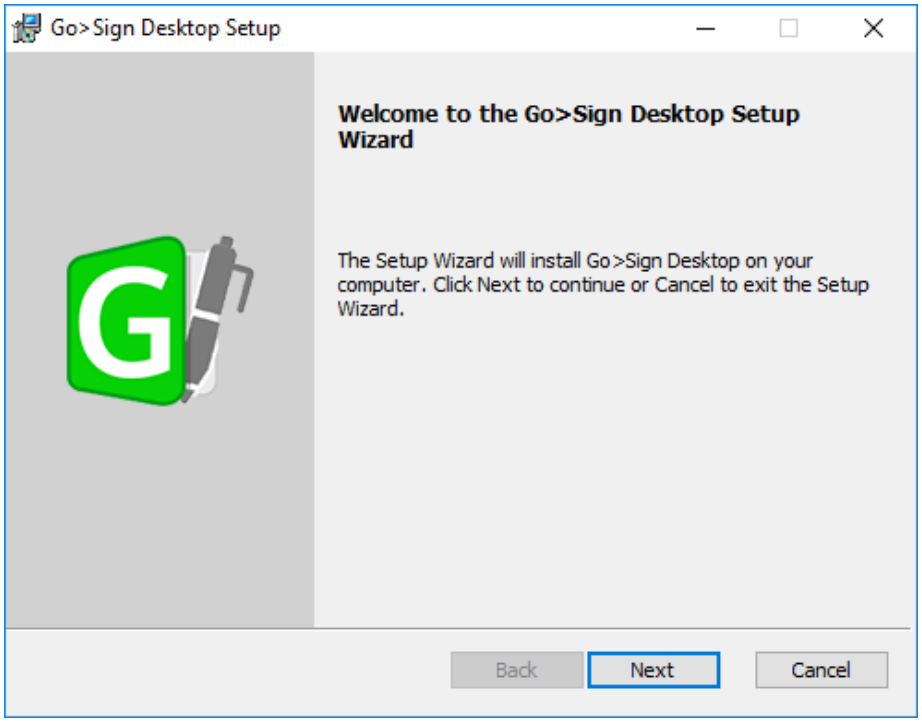
The client invocation on user side will be triggered by the web application (via Javascript) with the first attempt to sign an instruction (and each time the user needs to sign one) and is transparent to users.



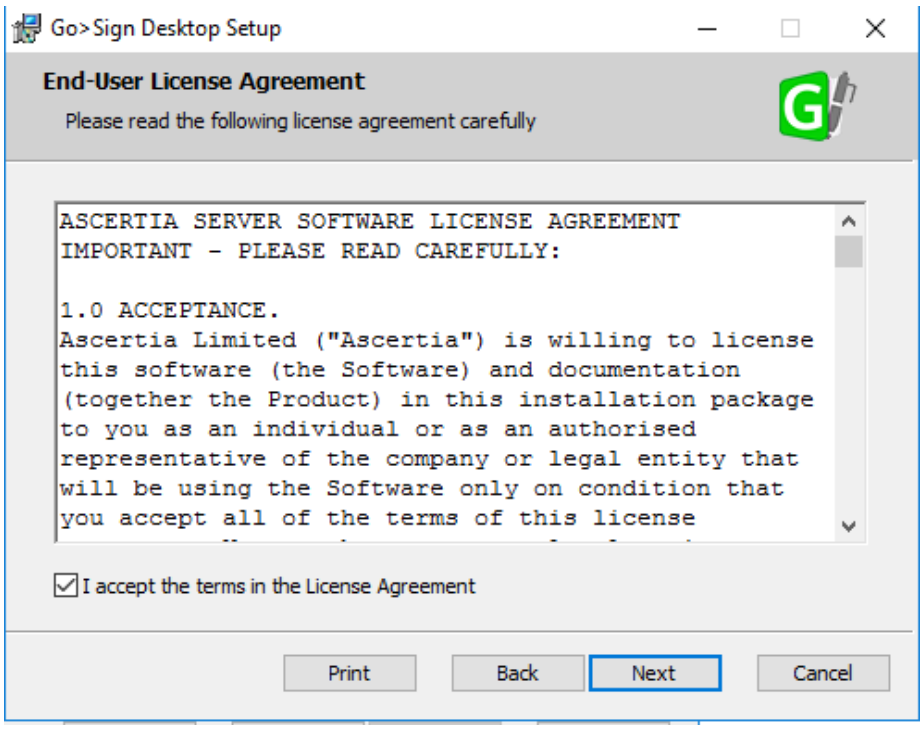
(Attention: please note that there may be individual company settings that do not allow the user to launch an application. If this is the case, please check with your local IT support/IT security! This function must be enabled.)

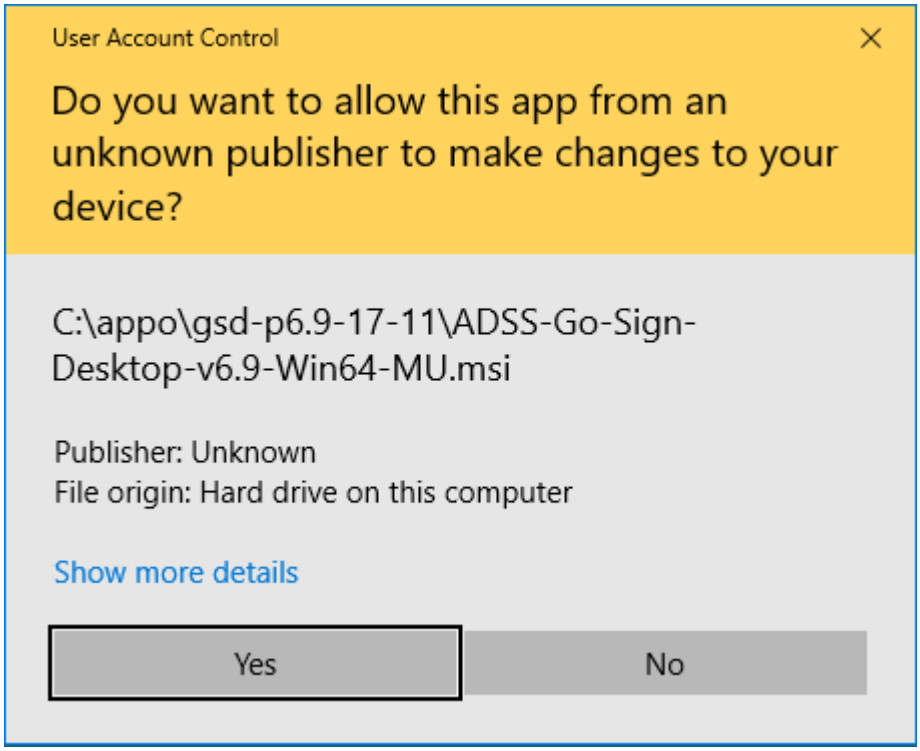
3.2.3 First installation of GSD multi user client

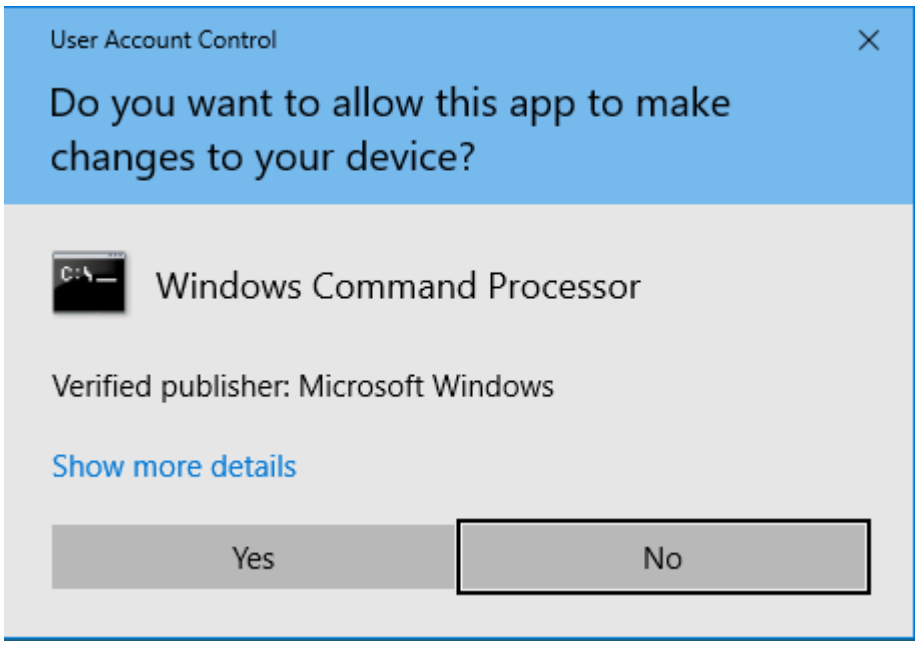
- Open Command prompt as Administrator
- Execute command: chgusr /install
- then run ADSS-Go-Sign-Desktop-v6.9.0.9-Win64-MU.msi installation package

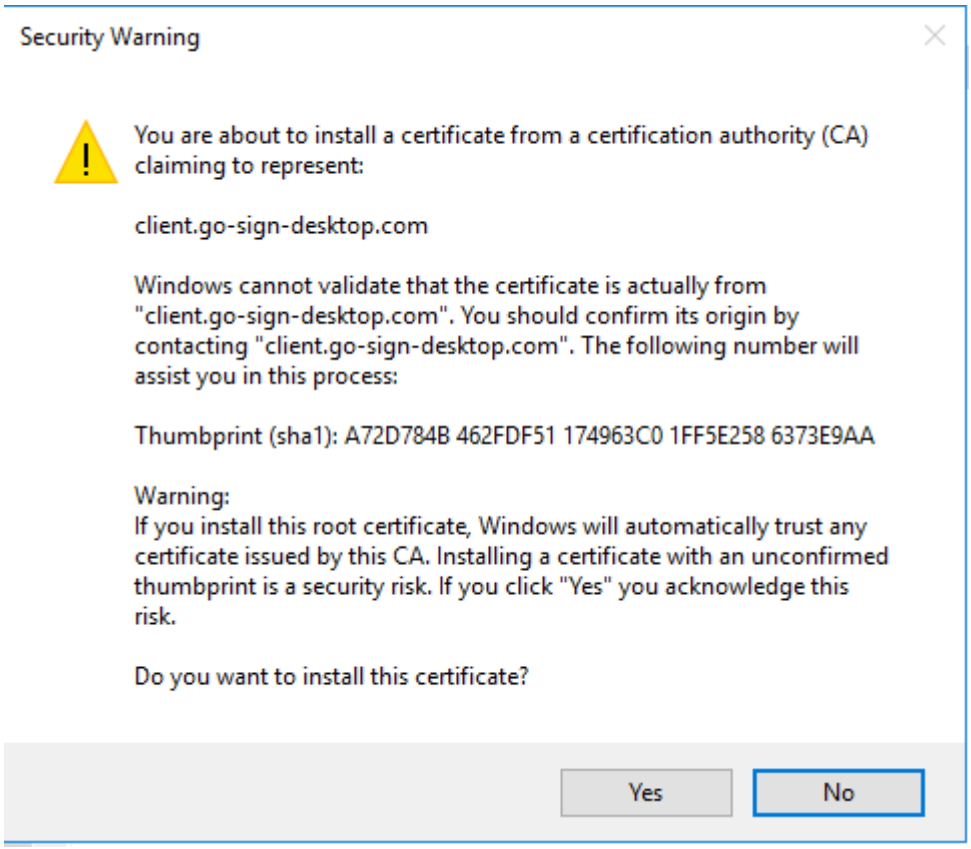


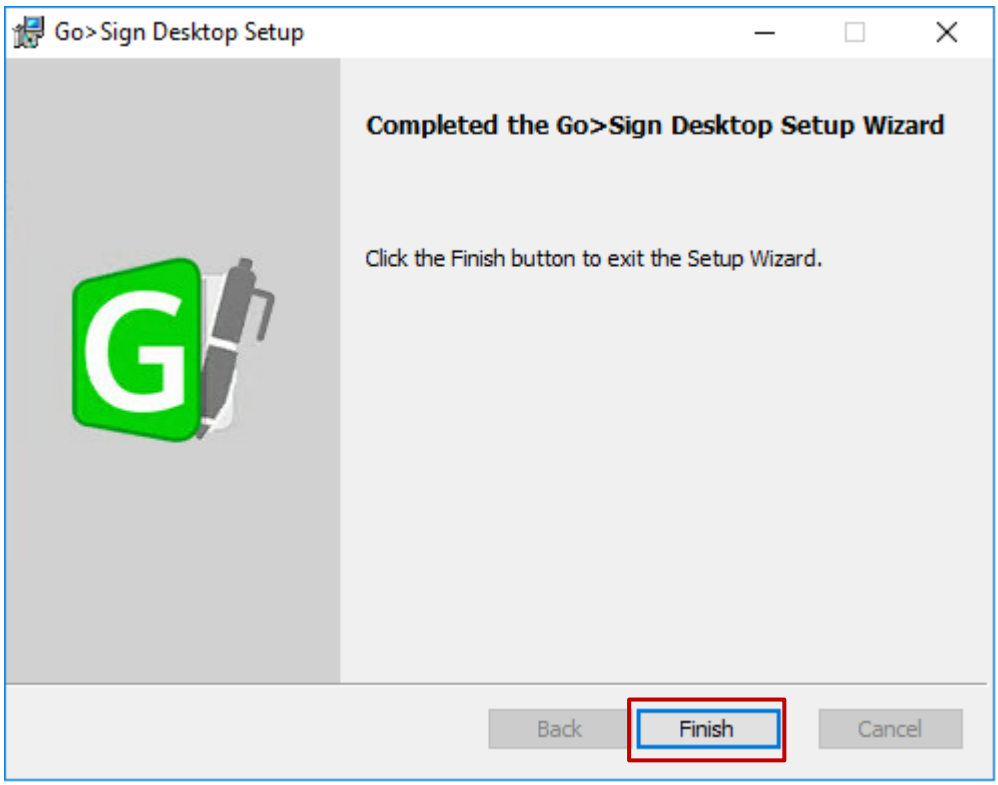
Click Next and accept End User License Agreement


Go>Sign Desktop Setup
End-User License Agreement
Please read the following license agreement carefully
ASCERTIA SERVER SOFTWARE LICENSE AGREEMENT
IMPORTANT - PLEASE READ CAREFULLY:
1.0 ACCEPTANCE.
Ascertia Limited ("Ascertia") is willing to license this software (the Software) and documentation (together the Product) in this installation package to you as an individual or as an authorised representative of the company or legal entity that will be using the Software only on condition that you accept all of the terms of this license
I accept the terms in the License Agreement
Print
Back
Next
Cancel


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
C:\appo\gsd-p6.9-17-11\ADSS-Go-Sign-Desktop-v6.9-Win64-MU.msi
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
No


User Account Control
Do you want to allow this app to make changes to your device?
Windows Command Processor
Verified publisher: Microsoft Windows
Show more details
Yes
No

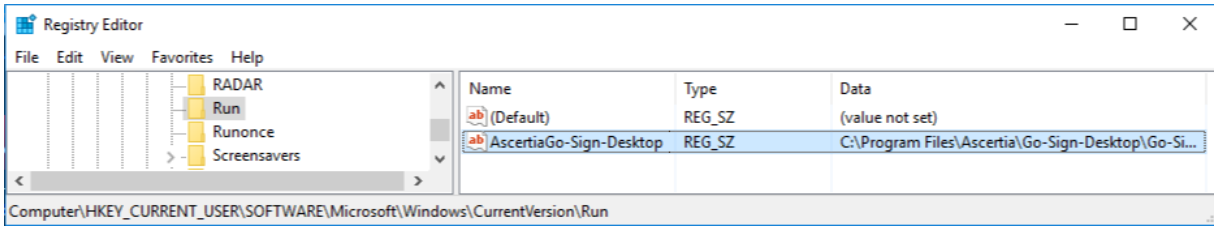

Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
client.go-sign-desktop.com
Windows cannot validate that the certificate is actually from "client.go-sign-desktop.com". You should confirm its origin by contacting "client.go-sign-desktop.com". The following number will assist you in this process:
Thumbprint (sha1): A72D784B 462FDF51 174963C0 1FF5E258 6373E9AA
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No



3.2.4 Additional installation steps

Following tasks need to be executed by IT Admin only once before starting the service other service will NOT start at all !

1. The registry key for automatic start of GSD client on administrator login should be removed to avoid unexpected / undesired behaviour of the NRO MU solution (will be fixed in the next release).



2. Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe" (or account that performed installation). This command will add the new gosign certificate into server admin trust store.

3. Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe" (or account that performed installation). This command will add the new gosign certificate into LM trust store.

4. Change service start type to AUTO (will be fixed in the next release) and start the service

GSD.exe applies following changes to local machine registry (HKLM) and adss "gosign" certificate local computer trust store:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia]
"URL Protocol"="GSD"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia\shell]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia\shell\open]
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Ascertia\shell\open\command]
@="C:\\Program Files\\Ascertia\\Go-Sign-Desktop\\GSD.exe %1
```

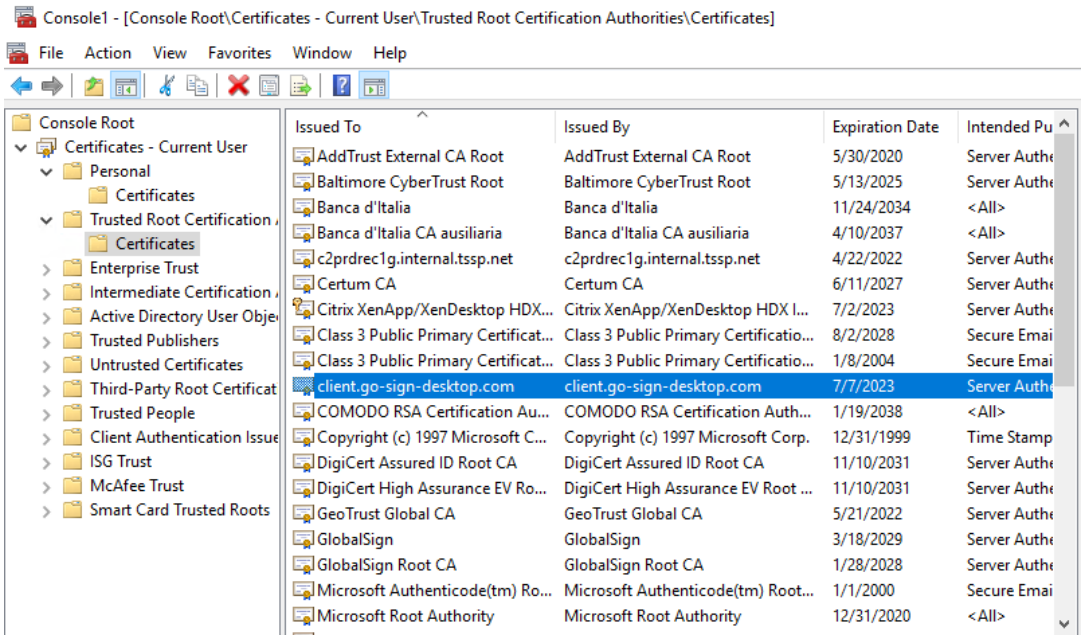
The above registry changes may need to be applied to all users at user logon in case non-persistent profiles. They will allow browsers to correctly trigger the start of GSD user/child instances, when user will be prompted to do so during an NRO task.

3.3 Post installation checks

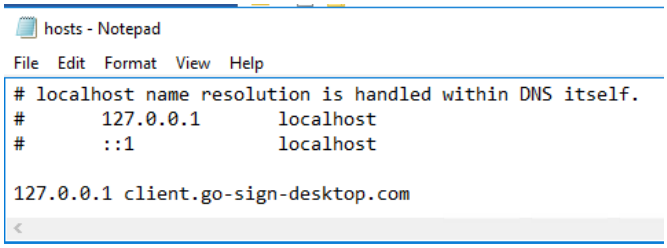
3.3.1 Post installation checks – IT ADMIN

1. "gosign" certificate present in Admin and LM trust store + host file correctly updated
2. GSD service has to be started FIRST and will be listening on 8782 port
   - https://client.go-sign-desktop.com:8782/gosign-desktop (confirms service running)
3. Child instances will start during NRO task and will listen on higher ports e.g. 8784, 8786 ecc
   - Business users have NOT to start manually the Go-sign-desktop.exe tray application!
4. In case of need, please check and share
   - Service log file "C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\logs"
   - User log file (%userprofile%/Documents/ Ascertia/Go-Sign-Desktop/logs/go-sign-desktop.log)

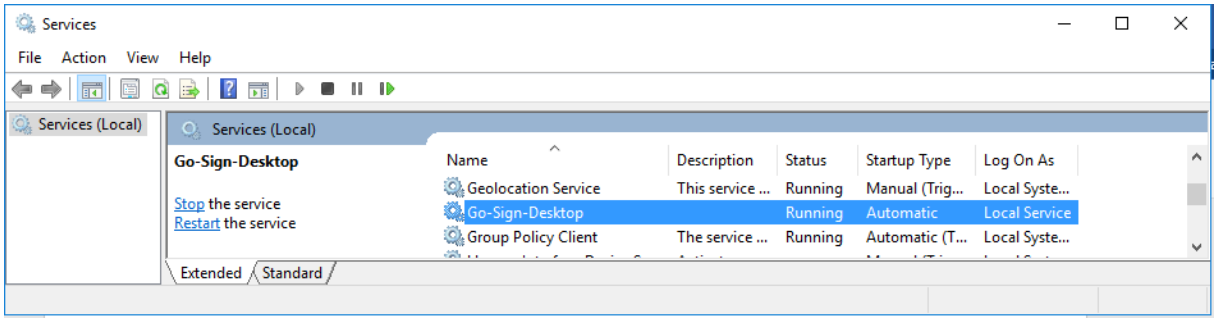
1 Check that certificate client.go-sign-desktop.com is imported in the (Administrator) User Certificate store by running *certmgr.msc* tool:

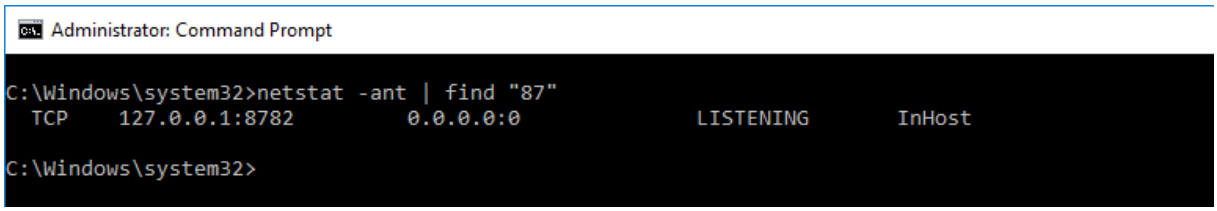


1 Check for the following definition in the host file:



2 Check service running and listening on 8782 (with Local Service account)

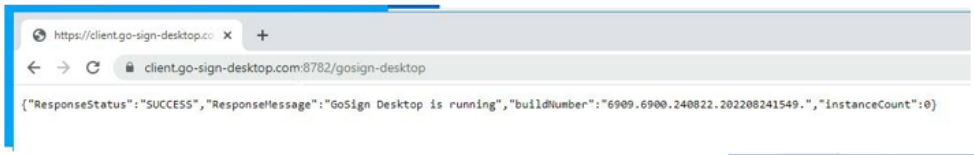




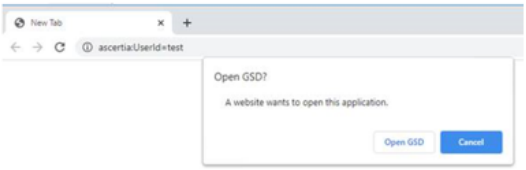
Port 8782 must not be changed into gosign-desktop.properties file otherwise the overall NRO setup will not work.

3.3.2 Post installation checks – BUSINESS USER / IT ADMIN

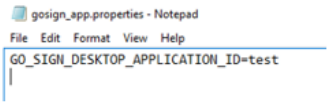
– GSD service running: https://client.go-sign-desktop.com:8782/gosign-desktop



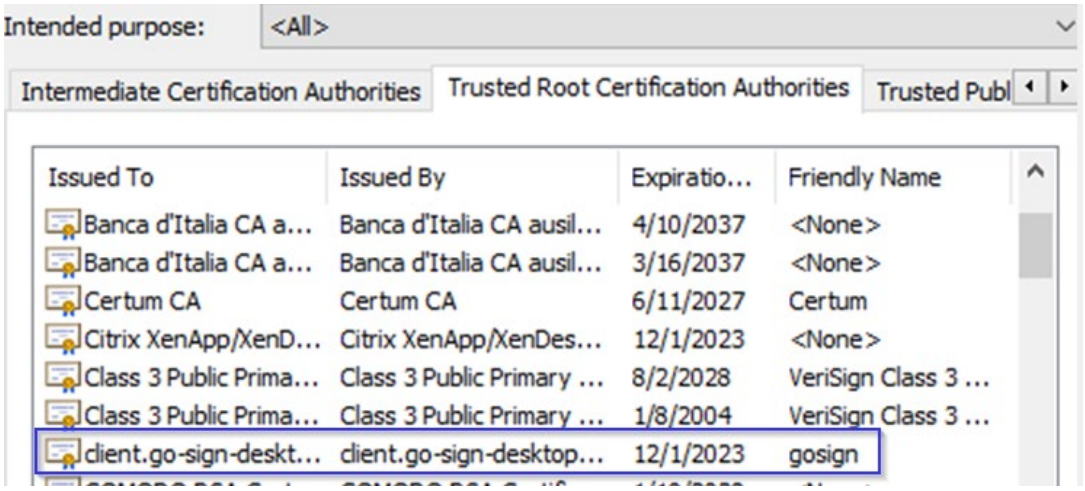
– Check if user is able to start "manually" a GSD client instance



- Open Chrome and type the following URL "ascertia:UserId=test"
- Click Open GSD
- Check c:\users\%username%\gosign_app.properties is populated as follows



User can also check the gosign certificate is visible at computer level in the browser keystore:



Once logged in, the below URLs can be used by customers to check both:

- the communication path from customer premises to Ascertia backend infrastructure
- the availability of the Ascertia backend infrastructure itself

CERT stage URLs:

SWIFT: https://esmig-cert-dss.emip.swiftnet.sipn.swift.com/adss/gosign/applet/lib/adss_gosign.js

SIA: https://esmig-cert-dss.u2a.sianet.sia.eu/adss/gosign/applet/lib/adss_gosign.js

PROD stage URLs:

SWIFT: https://esmig-cert-dss.emip.swiftnet.sipn.swift.com/adss/gosign/applet/lib/adss_gosign.js

SIA: https://esmig-dss.u2a.sianet.sia.eu/adss/gosign/applet/lib/adss_gosign.js

Actually, the above URLs are being contacted by the application in order to trigger the NRO sign/verify flow. For this reason, the user or IT Admin is not expected to perform any action with the JS file.

In order to properly perform NRO task, users are expected to allow execution of GSD user instance (before actual signature) in order to trigger start of a child GSD application that will then communicate with the GSD service/parent instance.

GSD child instances will listen on greater ports than the GSD service/parent one (8782) and will start dedicated Go-Sign-Desktop.exe application for each different web origin.

3.4 Additional features

3.4.1 GSD child instance housekeeping

6.9.0.9 MU release introduce dynamic house-keeping of GSD child instances in order to optimize load on the server environment. This feature is disabled by default and can be by applying the following changes in the go-sign-desktop.properties (and restarting the service):

Parameter	Description	Please take into account the following information when activating HouseKeeping
GOSIGN_DESKTOP_ENABLE_HEART_BEAT **Default = FALSE**	housekeeping is not active (all three of the following parameters are then ignored)	Please set the value to **TRUE** if you want to enable house keeping
GOSIGN_DESKTOP_MAX_IDLE_TIME **Default = 2**	time interval of user session inactivity in minutes until GoSign instance is automatically ended	Please do not exceed WEB session Timeout. Proposal, as starting value = **15** minutes
GOSIGN_DESKTOP_MAX_IDLE_INTERVAL **Default = 1**	the value controls (also in minutes) in which time interval the process runs to check if the house keeping is required for active GoSign instances (Please be aware that the maximum time a GoSign client session lives is the **sum of the two values**: GOSIGN_DESKTOP_MAX_IDLE_TIME + GOSIGN_DESKTOP_MAX_IDLE_INTERVAL)	Proposal, as starting value = **3** minutes
GOSIGN_DESKTOP_MAX_INSTANCES_PER_USER **Default = 2**	Maximum number of parallel GoSign instances per user. Please notice for each different ORIGIN a new GoSign instances must be started (i.e. different browsers or different business applications or different stages)	Maximum **3** or **4** should be enough for standard user

Some additional technical remarks can be considered in order to manage GSD child instances in a Citrix terminal server environment, specifically:

- Two parameters at terminal server level with regards to user session limits policy settings

Session idle timer

The duration after which the Citrix terminates an idle session if there is no user activity (i.e. such as from the mouse, keyboard, or touch for the specified interval.

This setting enables or disables a timer that specifies how long an uninterrupted user device connection to a desktop is maintained if the user supplies no input. When this timer expires, the session is placed in the disconnected state and the Disconnected session timer applies.

Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop can remain locked before the session is logged off.

- Please also activate or check if the following setting is active on your TS infrastructure **https://support.citrix.com/article/CTX891671**

This registry key allows to terminate executables that have been started by / from a published application (only valid for Citrix TS enviroment). Exe to be added in the key would be **javaw.exe**, in this specific case.

3.4.2 Log files rolling mechanism

6.9.0.9 client also implements rolling mechanism for log files which can be controlled via the following parameters (go-sign-desktop.properties):

```
GOSIGN_DESKTOP_LOG_FILE_PATH = default

GOSIGN_DESKTOP_CONF_FILE_PATH = default

GOSIGN_DESKTOP_LOG_FILE_MAX_SIZE = 1 MB

GOSIGN_DESKTOP_LOG_FILE_MAX_COUNTER = 10
```

'GOSIGN_DESKTOP_LOG_FILE_PATH' its default value is 'default':

|AppData|Roaming|Ascertia|Go-Sign-Desktop|logs|go-sign-desktop.log.

Another path can be entered e.g. '\\\\<file server IP>\\Shared\\gosign' and Go>Sign Desktop will append the username and the file name and start logging at the shared network location. Child instance should have access to the network location!

go-sign-desktop.properties file moved into new (default) path:

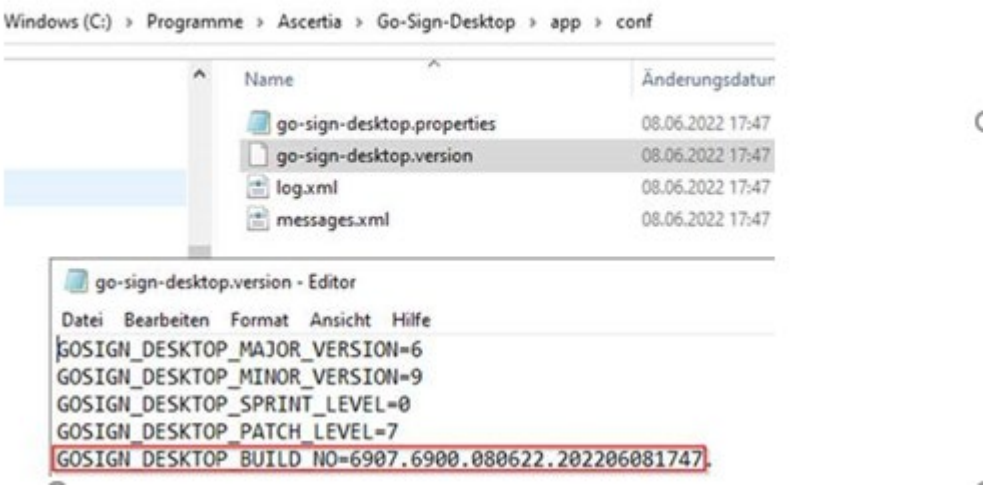
%userprofile%|AppData|Roaming|Ascertia|Go-Sign-Desktop

3.5 Mandatory troubleshooting information

When opening the incident to 4CB Service Desk, users must provide the following:

- OS and browser in use plus type of installation (MU) and client version

C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\gosign-desktop.version



- GSD log files:
  - Service log "C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\logs"
  - Child instance log (%userprofile%/Documents/Ascertia/Go-Sign-Desktop/logs/go-sign-desktop.log)
- Copy of %userprofile%\AppData\Roaming\Ascertia\Go-Sign-Desktop\logs\go-sign-desktop.properties (if any changes applied from default values)
- Copy of C:\Windows\ServiceProfiles\LocalService\Documents\Ascertia\Go-Sign-Desktop\GSD.db file – *if explicitily asked by Service Desk*
- Browser console log file (F12 button)
- Browers network trace file (F12 button) – *only in case of network-related issue and if explicility asked by Service Desk*
- Relevant screenshots reporting any useful exception

It is higly suggested to check any expcetion first with the internal IT/Network support for a preliminary analysis and then with 4CB. NSP may be involved as well in case of network-related issues.

3.5.1 Client logging information and changing log level

ADSS Go>Sign Desktop application has two log levels. First informational, which is for normal use, and second, debug, which should only be used when investigating performance issues, functionality problems, etc. IT ADmin can view ADSS Go>Sign Desktop application logs at:

%userprofile%\AppData\Roaming\Ascertia\Go-Sign-Desktop\go-sign-desktop.properties

File. To enable detailed debug logging, follow these instructions:

6. Go to the above path
7. Edit the go-sign-desktop.properties file using a suitable text editor.
8. Change the value of the property GOSIGN_DESKTOP_LOG_MODE from INFO to DEBUG and save the file.
9. Stop ADSS Go>Sign Desktop service and start it again
10. Retry the web failing web transaction to collect relevant trace files

4 Annex

4.1 SU client - Gosign certificate renewal procedure

Once the Gosign certificate will need to be renewed, please execute the following steps in order to proceed with renewal process:

1) Stop Go>Sign Desktop

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

4) Remove the existing gosign certificate from local machine trust store

4) Restart Go>Sign Desktop and it will prompt to install the new self-signed certificate.

Procedure may be verified in advance and possibly adapted, in case specific tools for installation / sw distribution have been adopted on customer side.

4.2 MU client - Gosign certificate renewal procedure

Once the Gosign certificate will need to be renewed, please execute the following steps in order to proceed with renewal process:

1) Stop Go>Sign Desktop service

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

3) remove gosign certificate from local machine trust store

4) remove gosign certificate from admin user trust store

5) Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe" (or account that performed installation). This command will add the gosign certificate into admin trust store

6) Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe" (or account that performed installation). This command will add the gosign certificate into LM trust store

7) Re-start the service

Procedure may be verified in advance and possibly adapted, in case specific tools for installation / sw distribution have been adopted on customer side.

In case of terminal server cluster, the renewal procedure to follow for server >1 is described in the next section and has to start from step #2.

4.3 Distributing MU client on Terminal server cluster – suggested procedure

The following procedure has been correctly tested and implemented in order to distribute the MU client in a terminal server cluster:

1 install GSD MU 6.9.0.9 as described in this guide (on server > 1)

2 stop of any Go-Sign-Desktop instance possibly opened

4 remove gosign certificate (generated by installation) from local machine trust store

5 remove gosign certificate (generated by installation) from admin user trust store

6 copy/replace gosign.cer file in server >1 (from server 1)

7 copy/replace cacerts java keystore file in server >1 (from server 1)

8 copy/replace gosign.keystore file in server >1 (from server 1)

9 Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\Go-sign-desktop.exe" (or account that performed installation). This command will add the gosign certificate into admin trust store

10 Execute once from admin the command "C:\Program Files\Ascertia\Go-Sign-Desktop\GSD.exe" (or account that performed installation). This command will add the gosign certificate into LM trust store

11 Re-start the service

4.4 Useful log files

The three files attached contain logs of successful signing test cases, done with 6.9.0.9 client (MU: service and child instance; SU: client application). They are meant to be checked by customer IT support in order to confirm the Ascertia local setup is working correctly, in a terminal server environment or in a desktop one.


single User GoSign LOG PKCS#11 INFO


multi user GoSign localService LOG PK


multi user GoSign child LOG PKCS#11 I