ESMIG U2A

Qualified Configurations

(Applicable for TIPS)

V1.0

Author	
Version	1.0
Date	01/03/2021
Status	Draft
Classification	Unclassified
Accessible	
Classified until	

Table of content

1 INTRODUCTION

1.2. Purpose and Objectives

This document describes the general configuration that TIPS users shall be complaint with in order to access TIPS and CRDM GUI via the ESMIG web portal. A specific section is devoted to describe the technical framework needed to fully implement the new non-repudiation of origin functionality (NRO) as described in the TIPS-0034-SYS. With the implementation of this Change Request, applet technology will be decommissioned in favour of a java independent solution.

1.2.1. 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. Currently the only TARGET Service already running on ESMIG is TIPS. The document will be regularly updated as soon as the other TARGET Services will approach the user testing phases to enlarge the relevant scope.

Against this background, the Ascertia solution, which is going to be implemented for TIPS, will be the unique U2A NRO solution also to be adopted for T2 –T2S services and ECMS, therefore only one Go>Sign Desktop application version will be used and distributed across the different services.

Important also to hightlight that Go>Sign Client applications are already in use in TARGET2 for Internet Access and Contingency Network and 4CBs will guarantee that no different client versions are needed by T2, T2S and TIPS, before the go-live of CSLD project.

1.2.2. Qualified configurations

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.

Go>Sign DESKTOP CLIENT (version will be regularly updated by the 4CB)		
NSP	SWIFT	SIA-COLT
OS	Windows 10	
Browser	Google Chrome 88.0+, Firefox 68.0+	

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

- MS CAPI/CNG (Windows)

- PKCS#11 for hardware-based tokens

The Ascertia solution based on the Go Sign Desktop client is not compatible with the Citrix Terminal Server solution. The Citrix Virtual Desktop solution is, on the other hand, fully supported by Ascertia, allowing the implementation of a jump host to be used to connect to the relevant TARGET Service (i.e. not directly from the operator workstations).

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 TIPS 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 TIPS 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 from the client machines (either physical or remote workstations) is under the sole responsibility of the TIPS participants (that may also need to involve their internal IT Dept. as well as external providers, in case of product specific issues).

1.3. Technical requirements and recommendations

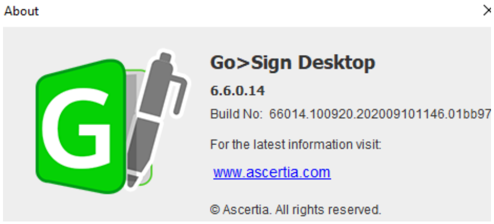
1.3.1. Download mechanism

The client is available for download at the following URLs on the ESMIG portal: (links yet to be provided).

The following URL will also provide the full installation guide provided by Ascertia that can be used as reference: (link yet to be provided).

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

Please make sure the correct version Go>Sign desktop is installed (at the time this document has been drafted the relevant version is 6.6.0.14, however it will be regularly updated by the 4CB). To check this please right click on the go sign icon and choose “about”. After that the following window appears:



About

Go>Sign Desktop
6.6.0.14
Build No: 66014.100920.202009101146.01bb97
For the latest information visit:
www.ascertia.com
© Ascertia. All rights reserved.

1.3.2. Go>Sign Desktop Client Requirements

The client invocation on TIPS user side will be triggered by TIPS 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.

ADSS Go>Sign Desktop relies on TLS communication only with the TIPS application (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 procedure foresees that the Go>Sign Desktop Installer automatically adds the entry :

127.0.0.1 client.go-signdesktop.com

in the Operating System host file 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 TLS server certificate will be self-signed and different for each workstation where the client will be installed. Once loaded into Windows OS, it is expected to be found in the Root CA keyring (i.e. and not in the personal certificate keyring).

The TIPS users have to ensure that the security settings of their institutions, i.e. firewalls, allow for installation of the applet/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.

1.3.3. Other technical 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.

- In case of certificate exceptions in the browser during first interaction with new Ascertia infrastructure: add DSS host certificates (possibly sent by the TIPS/NSP infrastructure) in browsers keyring (Chrome, Firefox ecc). 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"

- Check windows host file for the definition 127.0.0.1 client.go-sign-desktop.com

- 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 is displayed.

https://client.go-sign-desktop.com:8782

Additional useful contents may also be found in the Ascertia FAQs site. This URL can be consulted in advance before opening a ticket to the TIPS Service Desk:

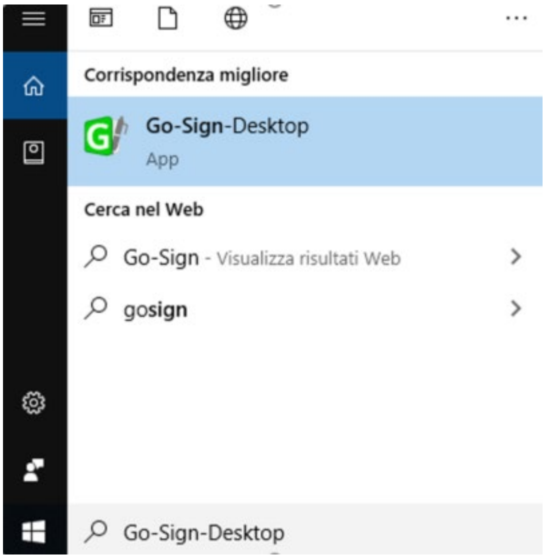
https://faqs.ascertia.com/display/ADSS/ADSS+Go%3ESign+Service#ADSSGo%3ESignService-HowtoaddresstheADSSCORSpolicyissueforadss_gosign.jsfile

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

1.4. Running the Application Go-Sign-Desktop

Once the application is installed, it is usually configured to run automatically when a Windows session is started. However, due to specific security settings, this might not happen, resulting signature attempts to end with a similar error "Go>Sign desktop not running/installed".

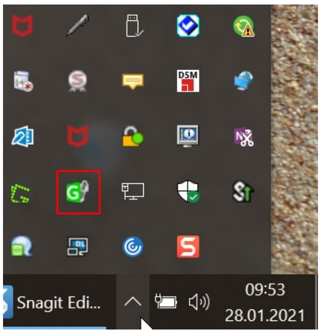
In this case, it is necessary to run it manually before initiating a browsing session in ICM. It is possible to lookup for the Go>Sign via the Windows Search bar:



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.

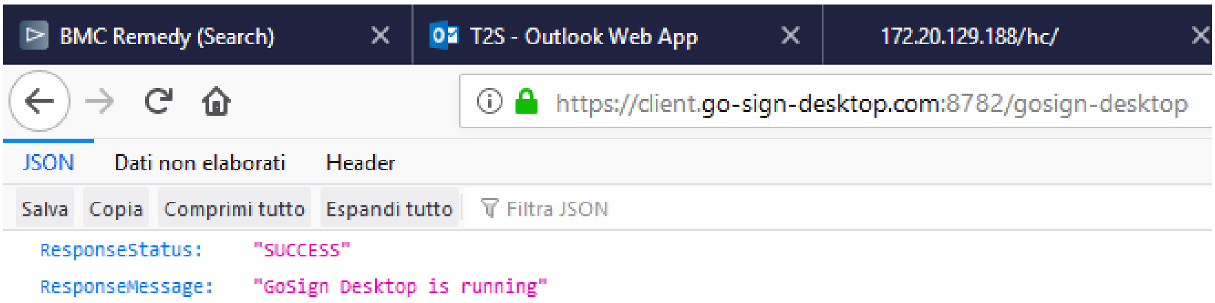
1.4.1. Verifying Go>Sign application running

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



In addition, it is requested to verify that Go>Sign is running properly, by accessing the URL https://client.go-sign-desktop.com:8782/gosign-desktop

The screenshot below is the expected result with Mozilla Firefox:



```
ResponseStatus:     "SUCCESS"
ResponseMessage:    "GoSign Desktop is running"
```

1.5. Troubleshooting information

1.5.1. Logging information

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\

and should send the send the “GoSignDesktopLog.txt” when opening the incident to 4CB HelpDesk.

1.5.2. Changing logging level

1. Go to ADSS Go>Sign Desktop installation path → C:\Program Files\Ascertia\Go-Sign-Desktop\app\conf\
2. Edit the gosign_desktop.properties file using a suitable text editor.
3. Change the value of the property GOSIGN_DESKTOP_LOG_LEVEL 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