TARGET2 internet access using TOKEN
(Aruba Key)

Installation instructions

Responsible authority: Deutsche Bundesbank

Author: National Service Desk
TARGET Services

Version: 7.0

As at 02.09.2019
List of versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>09/12/2014</td>
<td>National Service Desk</td>
<td>First version</td>
</tr>
<tr>
<td>1.1</td>
<td>01/07/2015</td>
<td>National Service Desk</td>
<td>New ECB requirements</td>
</tr>
<tr>
<td>2.0</td>
<td>01/03/2016</td>
<td>National Service Desk</td>
<td>Revision, bit4xpki added, Gemalto uninstalled</td>
</tr>
<tr>
<td>2.1</td>
<td>05/05/2016</td>
<td>National Service Desk</td>
<td>Comment on Google Chrome browser added regarding Java compatiblity</td>
</tr>
<tr>
<td>2.11</td>
<td>08/09/2016</td>
<td>National Service Desk</td>
<td>Editorial revision – no change to content</td>
</tr>
<tr>
<td>3.0</td>
<td>05/01/2017</td>
<td>National Service Desk</td>
<td>New ECB requirements and implementation of requirements from the 10.0 release</td>
</tr>
<tr>
<td>4.0</td>
<td>09/01/2018</td>
<td>National Service Desk</td>
<td>Editorial revisions and implementation of requirements from the 11.0 release</td>
</tr>
<tr>
<td>4.1</td>
<td>16/04/2018</td>
<td>National Service Desk</td>
<td>Changes to Go&gt;Sign Desktop 5.5 entered</td>
</tr>
<tr>
<td>4.11</td>
<td>25/04/2018</td>
<td>National Service Desk</td>
<td>Comment on Go&gt;Sign Desktop 5.5 entered</td>
</tr>
<tr>
<td>5.0</td>
<td>01/12/2018</td>
<td>National Service Desk</td>
<td>Complete revision</td>
</tr>
<tr>
<td>6.0</td>
<td>01/05/2019</td>
<td>National Service Desk</td>
<td>Editorial revisions and implementation of requirements from the 12.1 release</td>
</tr>
<tr>
<td>7.0</td>
<td>02/09/2019</td>
<td>National Service Desk</td>
<td>Editorial revisions and implementation of requirements from the 13.0 release</td>
</tr>
</tbody>
</table>
Contents

1 CONFIGURATIONS TESTED BY IA SUPPORT (LAST UPDATED: 16/08/2019) ..................... 4
  1.1 WINDOWS 7 32-BIT AND 64-BIT ................................................................. 4
  1.2 WINDOWS 8 32-BIT AND 64-BIT ................................................................. 4
  1.3 WINDOWS 10 32-BIT AND 64-BIT ............................................................... 5
  1.4 FIREFOX ESR .............................................................................................. 5
  1.5 INTERNET EXPLORER 11 ................................................................. 6

2 UPDATE TOKEN (CURRENT VERSION: 1.8.3) .................................................. 7
  2.1 CERTIFICATE IMPORT (BIT4XPKI.DLL) VIA BIT4ID ........................................ 9

3 FIREFOX ESR CONFIGURATION ........................................................................... 16

4 ASCERTIA GO>SIGN DESKTOP INSTALLATION ..................................................... 21
  4.1 CHECKING THE GOSIGN INSTALLATION .................................................... 24

5 INTERNET EXPLORER 11 ..................................................................................... 25

6 FREQUENT ERRORS ............................................................................................. 30
  6.1 THE RED INDICATOR LIGHT FLASHES WHEN THE TOKEN IS INSERTED .......... 30
  6.2 ERROR MESSAGE “SSL-HANDSHAKE-ERROR” ........................................... 30
  6.3 ERROR CODE “I86” .................................................................................. 31
  6.4 CHANGING OR RESETTING/UNBLOCKING YOUR PIN IN THE BIT4ID SMART CARD MANAGER .................................................................................. 32
  6.5 SCANNING AND FIXING THE TOKEN ....................................................... 33

7 CONTACT AND SUPPORT .................................................................................. 34
1 Configurations tested by IA support
(last updated: 16/08/2019)

1.1 Windows 7 32-bit and 64-bit

<table>
<thead>
<tr>
<th>System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Klassifikation:</td>
<td>3.7 Windows-Leistungindex</td>
</tr>
<tr>
<td>Prozessor:</td>
<td>AMD Athlon(tm) II X2 215 Processor 2.70 GHz</td>
</tr>
<tr>
<td>Installierter Arbeitsspeicher (RAM):</td>
<td>3,00 GB (2,50 GB verwendbar)</td>
</tr>
<tr>
<td>Systemtyp:</td>
<td>32 Bit-Betriebssystem</td>
</tr>
<tr>
<td>Stift- und fingereingabe:</td>
<td>Für diesen Bildschirm ist keine Stift- oder fingereingabe verfügbar.</td>
</tr>
</tbody>
</table>

1.2 Windows 8 32-bit and 64-bit

<table>
<thead>
<tr>
<th>System</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Rating:</td>
<td>4.5 Windows Experience Index</td>
</tr>
<tr>
<td>Prozessor:</td>
<td>Intel(R) Pentium(R) CPU G640 @ 2.80GHz 2.79 GHz</td>
</tr>
<tr>
<td>Installed memory (RAM):</td>
<td>1.00 GB</td>
</tr>
<tr>
<td>System type:</td>
<td>32-bit Operating System, x64-based processor</td>
</tr>
<tr>
<td>Pen and Touch:</td>
<td>Limited Touch Support with 8 Touch Points</td>
</tr>
</tbody>
</table>
1.3 Windows 10 32-bit and 64-bit

<table>
<thead>
<tr>
<th>Edition</th>
<th>Windows 10 Pro</th>
</tr>
</thead>
<tbody>
<tr>
<td>Produkt-ID</td>
<td>00331-20020-00000-AA705</td>
</tr>
<tr>
<td>Prozessor</td>
<td>Intel(R) Core(TM) i5-4310U CPU @ 2.00GHz 2.60 GHz</td>
</tr>
<tr>
<td>Installierter RAM</td>
<td>4,00 GB</td>
</tr>
<tr>
<td>Systemtyp</td>
<td>64-Bit-Betriebssystem, x64-basierter Prozessor</td>
</tr>
<tr>
<td>Stift- und Toucheingabe</td>
<td>Für diese Anzeige ist keine Stift- oder Toucheingabe verfügbar.</td>
</tr>
</tbody>
</table>

1.4 Firefox ESR

Please note that if you use Mozilla Firefox you will also need to download and install the “Go>Sign Desktop” in TARGET2.

It is possible to use the log-in and information functions in TARGET2 without the “Go>Sign Desktop”; however, it is essential for recording and approving payments.
1.5  Internet Explorer 11

Please note that as of the TARGET2 Release 13, you will also need to download and install the “Go>Sign Desktop” in TARGET2 when using Internet Explorer 11.
It is possible to use the log-in and information functions in TARGET2 without the “Go>Sign Desktop”; however, it is essential for recording and approving payments.
2 Update token (current version: 1.8.3)

When using the token for the first time, an update window will appear at the bottom right of the screen, where an Aruba Key update is loaded in several steps (steps 1 to 6 only appear for a few seconds).
Double-click on the symbol in the bottom right-hand corner of the taskbar to open an installation window and view the installation.

Please note: We recommend that you download the update.
If the download is blocked by the local security settings (e.g. network computers, firewall, etc.), it will not be possible to use the token.

Solution: Adjust the local security settings or connect the token to a stand-alone computer (without any security restrictions) with an active internet connection.
Once the update has been downloaded, the token can be run on any computer.
Once the download is completed, click “Yes” to start the installation. This may take several minutes.
2.1 Certificate import (bit4xpki.dll) via Bit4id

When installing the token on a new PC for the first time, the certificate is imported via the toolbar. Only then will all the necessary drivers and files be installed automatically.

Click on the Windows Start button and open Windows Explorer.
Select the “Aruba Key” drive.
Now launch the “Autorun.exe” file in the “utility” folder.

After opening the toolbar, select the “Utilities” subcategory by clicking on this icon.

Having opened this subcategory, select the “Import Certificate” icon.
This installs AK910Switch Service, amongst other things.

Next, select a language.
The available languages are German, English, Spanish, Italian and Portuguese.

Confirm the welcome window that appears by clicking on “Weiter” (Next) and the installation will begin.
Place a tick in the box “Ich akzeptiere das Lizenzabkommen” (I accept the licence agreement) to accept the terms and conditions. The process is started by clicking “Instal-lieren” (Install).

The installation will start and should be completed within a short period of time.

After successful installation, the PC must be restarted.
The “Bit4id - Smart Card Manager” file can be found in the Windows Start menu by going to “Alle Programme” (All programs) and clicking on the “Bit4id” folder, followed by the “Universal Middleware for Incard” subfolder.

The following window will appear when the “Bit4id - Smart Card Manager” file is opened.

General information on the token and certificate is listed on the “Chipkarte” (Chip card) tab.

You can change the PIN on the “PIN ändern” (Change PIN) tab.
On the “Chipkarte entsperren” (Unblock chip card) tab, it is possible to unblock a blocked PIN (PUK required; see also chapter 6.3).

Clicking “Ausführen” (Run) on the “Erweitert” (Advanced) tab ...

... opens the certificate installed on the smart card, which can be selected by double-clicking on the user name.
A window will appear with information on the certificate. You can install the certificate by clicking the “Zertifikat installieren” (Install certificate) button.

Then confirm again by clicking on “Weiter” (Next).

Confirm once more by clicking “Weiter” (Next) in the import assistant window.
In this window you click on the “Fertig stellen” (Complete) button.

The installation is now completed and confirmed by clicking “OK”.

More information on the software version is listed on the last tab (“Über” (About)).
3 Firefox ESR configuration

Enter “about:config” in the address bar of your Firefox browser to check the TLS settings.

Confirm the “This might void your warranty” warning. On the next screen, enter “security.tls.version.max” in the search field.
This item should be set to 4. “security.tls.version.min” should be set to 1, however.

Under “Extras” (Tools) and “Einstellungen” (Settings), you can open “Datenschutz und Sicherheit” (Data protection and security). In this submenu, you can disable pop-up windows or set “Ausnahmen” (Exceptions) for the URL
https://trgt-papss.target2ssp.eu (live environment) and
https://trgt-papss-cust.target2ssp.eu (test environment).
Datenerhebung durch Firefox und deren Verwendung

Berechtigte Websites - Pop-ups

Sie können festlegen, welchen Websites Sie erlauben möchten. Pop-up-Fenster zu öffnen. Geben Sie bitte die exakte Adresse der Website ein, der Sie das erlauben möchten, und klicken Sie dann auf Erlauben.

Adresse der Website

Website | Status
-------|-------
https://login-papss-cust.target2sp.eu | Erlauben
https://login.papsc.target2sp.eu | Erlauben

Website entfernen | Alle Websites entfernen

Abbrechen | Änderungen speichern
You can view certificate information by clicking on “Erweitert” (Advanced), “Zertifikate” (Certificates), and then “Zertifikate anzeigen” (View certificates).

Before reinstalling, first click “Kryptographie-Module” (Security devices) and unload the “Neues PKCS#11 Modul” by selecting the module and clicking “Entladen” (Unload).

Once the module is unloaded, you can then load it again (using the “Laden” button). Now select “Durchsuchen” (Browse).

When installing for the first time, this step is not necessary, you can go straight to “Laden” (Load).
On the C:/ drive in the Windows directory, you will find the “System32” folder.

The “System32” folder contains the “bit4xpki.dll” file (if the “bit4ipki.dll” file is also still in the folder, it can be deleted and the “bit4id_xpki.exe” file installed from the token under “utility”).

Close this window by clicking “OK”.

You will find “Neues PKCS#11 Modul” on the left.

After checking you have the right module, close the window by clicking “OK”.
Relaunch the browser and enter the following URL into the address bar:

For the test environment:  https://trgt-papss-cust.target2ssp.eu
For the live environment:  https://trgt-papss.target2ssp.eu

You will be asked for the PIN (eight-character PIN was sent).

The TARGET2 start screen is launched.
4 Ascertia Go>Sign Desktop installation

To download the Go>Sign Desktop file, navigate to “Services > Administration > Download Ascertia Go>Sign Desktop”.

Here you will find both “Ascertia Go>Sign Desktop 32 bit” as well as “Ascertia Go>Sign Desktop 64 bit” versions ready for download and installation.

If the download is carried out using Mozilla Firefox, the file extension will be “.msi”, if Internet Explorer is used, it will be “.man”.

Start the download by double-clicking on the version number.

Now you can decide whether to open or save the file.

Choose where to save the file (the specified path should be kept).
The installation assistant opens. Click “Next”.

Complete the short installation by clicking “OK”.

As a final step, you should restart the PC.
4.1 Checking the GoSign installation

To check whether the GoSign Desktop has been installed properly and is running correctly, you can call up the following URL in the Firefox address bar to query the status:

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

Response Status: "SUCCESS"
Response Message: "GoSign Desktop is running"
5 Internet Explorer 11

In Windows 10, Internet Explorer will continue to run. The Edge browser is not supported by TARGET2 and/or “Ascertia Go>Sign Desktop” and can therefore not be used.

To find IE11, click on the Windows Start button, and then “Alle Apps” (All Apps).

Under “W” you will find the option “Windows-Zubehör” (Windows accessories), which is where Internet Explorer 11 is located.
Once you open Internet Explorer 11, you will see the menu bar. If the menu bar is hidden, go to the top of the screen, click the right mouse button and place a tick next to the option “Menüleiste” (Menu bar).

Go to “Extras” (Tools) and select the option “Popupblocker” (Pop-up blocker). The pop-up blocker should be set to “Popupblocker ausschalten” (Turn off pop-up blocker).

If the pop-up blocker is enabled, the following pages must be entered in the “Popupblocker Einstellungen” (Pop-up blocker settings): 

- [https://trgt-papss-cust.target2ssp.eu](https://trgt-papss-cust.target2ssp.eu) for the test environment
- [https://trgt-papss.target2ssp.eu](https://trgt-papss.target2ssp.eu) for the live environment.
Navigate to the “Extras” tab and then go to “Einstellungen der Kompatibilitätsansicht” (Compatibility view settings), where you should add the entry “Target2ssp.eu” by clicking “Hinzufügen” (Add).

You can view and confirm the security certificate by navigating to “Internetoptionen” (Internet options). To do this, click on the cog symbol in the upper right-hand corner and then select “Internetoptionen” (Internet options) and go to the “Inhalte” (Content) tab.

On the “Eigene Zertifikate” (Personal) tab, you will find the certificate belonging to the inserted token (used to check the correct installation).
Now you can test your access to the system:

Call up one of the two TARGET2 pages:
https://trgt-papss-cust.target2ssp.eu
https://trgt-papss.target2ssp.eu
and …

... confirm the security certificate by clicking “OK”.

Enter your PIN ...

... and the TARGET2 application will be launched.
In the “Extras” (Tools) menu, you can either turn off the pop-up blocker or manually add the sites [https://trgt-papss.target2ssp.eu](https://trgt-papss.target2ssp.eu) and [https://trgt-papss-cust.target2ssp.eu](https://trgt-papss-cust.target2ssp.eu) in the “Popupblocker Einstellungen” (Pop-up blocker settings).

In order to avoid saving any incorrect settings or links, we recommend that you always delete your browser history. You can do this by going to “Internetoptionen” (Internet options) and selecting the option “Sicherheit” (Security).
6 Frequent errors

6.1 The red indicator light flashes when the token is inserted.

One possible reason for this could be that the SIM card is not correctly inserted in the token. Check that the SIM card is correctly inserted in the SIM card slot and secure it with adhesive tape if necessary.

6.2 Error message “ssl-handshake-error”

Should this error message occur, it is possible that the token is not/incorrectly inserted in the USB port of the PC or that the SIM card has not been inserted correctly.

Should this error message continue to occur, you will be required to install/reinstall the security device (see p. 18).
6.3 Error code “I86”

Error code I86

Cause
The previous session was not terminated using the “Log Out” button, which means that the session is still active on the server.

Solution
- Terminate the current session by clicking on the “Log Out” button.
- Close the browser.
- Restart the browser.
- Log on to TARGET2 again.
6.4 Changing or resetting/unblocking your PIN in the Bit4id Smart Card Manager

Alternatively, you can also change/unblock your PIN in the Bit4id Smart Card Manager:

In the Windows Start menu, go to “Alle Programme” (All Programs) and open the “Bit4id - Smart Card Manager” file located in the “Bit4id” folder in the “Universal Middleware for Incard” subfolder.

You can change the PIN on the “PIN ändern” (Change PIN) tab.

On the “Chipkarte Entsperren” (Unblock chip card) tab, you have the option of unblocking a blocked PIN (in both cases you will be required to enter the PUK).
6.5 Scanning and fixing the token

If the following window appears once you have inserted the token, click on “Überprüfen und reparieren (empfohlen)” (Scan and fix (recommended)).

Then place a tick next to the two options for the data carrier check and confirm these by clicking on “Starten” (Start).

After a few moments, an information window will appear, which can be closed by clicking on “Schließen” (Close).
7 Contact and support

Should you have any further questions, you can contact the TARGET2 internet support team between the hours of 8:00 and 16:00.

Telephone hotline: +49 (0)69 9566 4044
Email: ia_support@bundesbank.de

For all general questions relating to TARGET2, please contact your competent customer service team (see the table below for contact details) or the National Service Desk.

The TARGET National Service Desk can be contacted as follows.

Telephone hotline (live environment): +49 (0)69 9566 8870
Email: t2servicedesk@bundesbank.de
Fax: +49 (0)69 9566 508870

The customer service teams can be contacted as follows.

<table>
<thead>
<tr>
<th>Customer service team in</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Berlin</td>
<td>+49 (0)30 3475 2929</td>
<td><a href="mailto:KBS-BBB@bundesbank.de">KBS-BBB@bundesbank.de</a></td>
</tr>
<tr>
<td>Düsseldorf</td>
<td>+49 (0)211 874 2929</td>
<td><a href="mailto:KBS-NRW@bundesbank.de">KBS-NRW@bundesbank.de</a></td>
</tr>
<tr>
<td>Frankfurt</td>
<td>+49 (0)69 9566 2929</td>
<td><a href="mailto:KBS-H@bundesbank.de">KBS-H@bundesbank.de</a></td>
</tr>
<tr>
<td>Hamburg</td>
<td>+49 (0)40 3707 2929</td>
<td><a href="mailto:KBS-HMS@bundesbank.de">KBS-HMS@bundesbank.de</a></td>
</tr>
<tr>
<td>Hanover</td>
<td>+49 (0)511 3033 2929</td>
<td><a href="mailto:KBS-BNS@bundesbank.de">KBS-BNS@bundesbank.de</a></td>
</tr>
<tr>
<td>Leipzig</td>
<td>+49 (0)341 860 2929</td>
<td><a href="mailto:KBS-STM@bundesbank.de">KBS-STM@bundesbank.de</a></td>
</tr>
<tr>
<td>Mainz</td>
<td>+49 (0)6131 377 2929</td>
<td><a href="mailto:KBS-RS@bundesbank.de">KBS-RS@bundesbank.de</a></td>
</tr>
<tr>
<td>Munich</td>
<td>+49 (0)89 2889 2929</td>
<td><a href="mailto:KBS-BY@bundesbank.de">KBS-BY@bundesbank.de</a></td>
</tr>
<tr>
<td>Stuttgart</td>
<td>+49 (0)711 944 2929</td>
<td><a href="mailto:KBS-BW@bundesbank.de">KBS-BW@bundesbank.de</a></td>
</tr>
</tbody>
</table>