
	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

TARGET2 Internet Zugang mit TOKEN (Firma Certa)



Installationsanleitung

Verantwortlich Deutsche Bundesbank

Autor: National Service Desk
TARGET Services



Version: 8.2

Stand: 15.06.2022

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	



Versionsführung

Version	Datum	Autor	Beschreibung der Änderung
1.0	09.12.2014	National Service Desk	Erstmalige Erstellung
1.1	01.07.2015	National Service Desk	Neue EZB Vorgaben
2.0	01.03.2016	National Service Desk	Neue Überarbeitung, Bit4xpki neu, Gemalto Deinstallation
2.1	05.05.2016	National Service Desk	Bemerkung zu Google Chrome Browser bzgl. Java-Kompatibilität eingefügt
2.11	08.09.2016	National Service Desk	Redaktionelle Überarbeitung – ohne inhaltliche Änderung
3.0	05.01.2017	National Service Desk	Neue EZB Vorgaben und Umsetzung der Anforderungen aus dem Release 10.0
4.0	09.01.2018	National Service Desk	Redaktionelle Überarbeitung und Anforderungen aus dem Release 11.0
4.1	16.04.2018	National Service Desk	Änderungen zum Go - Sign Desktop 5.5 eingefügt
4.11	25.04.2018	National Service Desk	Anmerkung zum Go - Sign Desktop 5.5 eingefügt
5.0	01.12.2018	National Service Desk	Vollständige Überarbeitung
6.0	01.05.2019	National Service Desk	Redaktionelle Überarbeitung und Anforderungen aus dem Release 12.1
7.0	02.09.2019	National Service Desk	Redaktionelle Überarbeitung und Anforderungen aus dem Release 13.0
7.1	02.12.2019	National Service Desk	Ergänzende Informationen zum Go - Sign Desktop
7.2	01.09.2020	National Service Desk	Änderungen zum Mozilla Firefox eingefügt
8.0	26.10.2020	National Service Desk	Änderung aufgrund Softwareänderung von ARUBA-Key auf Firma Certa
8.1	09.02.2022	National Service Desk	Änderung der Qualified Configurations SSP V15
8.2	15.06.2022	National Service Desk	Wegfall Internet Explorer 11

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

Inhaltsverzeichnis

1	Vom Internetsupport getestete Konfigurationen (Stand: 26.10.2020)	4
1.1	Windows 10 (32 und 64 Bit)	
1.2	Firefox ESR	
2	Einrichtung des Token	5
2.1	Einstecken des Tokens in einen freien USB-Port	
2.2	Installation der Anwendung „Bit4id – PKI Manager“	6
3	Firefox ESR Konfiguration	7
4	Installation Ascertia Go-Sign Desktop	12
4.1	Überprüfung der GoSign Desktop Installation	15
5	Entsperren oder Ändern der PIN	17
6.1	Bit4id – Smart Card Manager	
6.2	Bit4id – PKI Manager	18
6	Häufig auftretende Fehler	20
7.1	Fehlercode „ssl_error_handshake_failure_alert“	
7.2	Error-Code 404 – Go-Sign Desktop not running/installed	21
7.3	Error-Code I86: User session conflict detected	22
7	Systemkonfigurationen für den internetbasierten TARGET2-Zugang	23
8	Kontakt und Support	24

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

1 Vom Internetsupport getestete Konfigurationen (Stand: 26.10.2020)



1.1 Windows 10 32 Bit und 64 Bit

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

1.2 Firefox ESR



Bitte beachten Sie, dass bei Verwendung des Mozilla Firefox zusätzlich die Software „Go-Sign Desktop“ in TARGET2 heruntergeladen und installiert werden muss. Der Login und die Auskunftsfunktionen in TARGET2 sind zwar auch ohne „Go-Sign Desktop“ möglich. Zur Erfassung und Freigabe von Zahlungen wird dieser jedoch zwingend benötigt.

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

2 Einrichtung des Tokens

ACHTUNG:

Vor Einrichtung des/der Token muss die Freischaltung des Zertifikats erfolgen!
 Hierzu müssen die beiden Empfangsbestätigungen (List of SMARTCARD to deliver.../
 List of Phrase to deliver...) an die auf dem Begleitschreiben des/der Token aufgeführte Adresse
 der Deutschen Bundesbank unterschrieben zurückgesandt werden.
 Erst danach ist der Login auf TARGET2-ICM möglich!

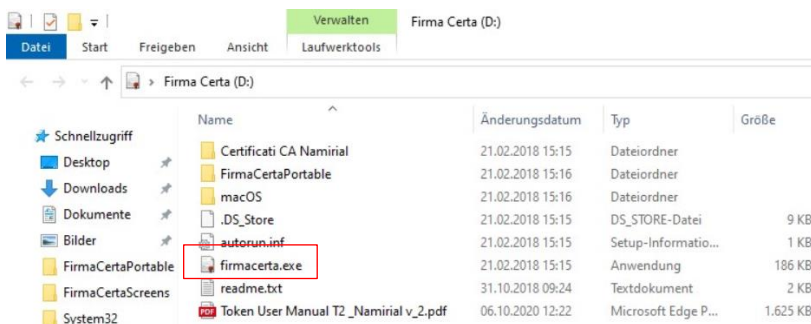
2.1 Einstecken des Tokens in einen freien USB-Port:



Verbinden Sie den Token durch Einstecken in einen freien USB-Port mit dem Rechner. Nach erfolgreicher Verbindung erfolgt automatisch der Zertifikatsimport. Hierzu erscheint folgendes Fenster:

Nach wenigen Sekunden erfolgt die Information durch Erscheinen eines weiteren Fensters, dass die Smartcard erfolgreich eingerichtet ist.



Falls diese beiden Fenster nach Einstecken in den USB-Port und Erkennung durch den Rechner nicht erscheinen, starten Sie bitte die Anwendung „firmacerta.exe“, die auf dem Token gespeichert ist (die beiden Fenster sollten nun erscheinen):



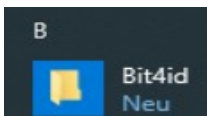
	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

Hinweis:

Es kann sein, dass bei Öffnen der Anwendung „firmacerta.exe“ eine Softwareaktualisierung angeboten wird. Diese ist für die Ersteinrichtung jedoch nicht zwingend notwendig und kann gegebenenfalls später durchgeführt zu werden.

Sofern auf dem lokalen Rechner bereits weitere Banca d'Italia Token genutzt werden, ist die Einrichtung an dieser Stelle bereits abgeschlossen und der Token einsatzbereit.

Dies sehen Sie auch, wenn im Windows-Startmenü der Ordner „bit4id“ vorhanden ist:



Ist BIT4ID nicht vorhanden, führen Sie bitte die Schritte in Kapitel 2.2 durch.

2.2 Installation der Anwendung „Bit4id – PKI Manager“:

!!!(Diese Installation ist nur dann erforderlich, wenn nicht bereits Banca d'Italia Token auf diesem Rechner eingerichtet sind und parallel genutzt werden (egal ob ARUBA-key oder Firma Certa), siehe Hinweis auf vorheriger Seite 7 (unten))!!!



Mit Öffnen der Anwendung „SwitchService.exe“ wird die Installation durchgeführt. Diese Installationsdatei ist unter folgendem Pfad im Ordner „Driver“ auf dem Token bereitgestellt:

Firma Certa (D:) > FirmaCertaPortable > Driver

» Dieser PC > Firma Certa (D:) > FirmaCertaPortable > Driver

phan	Name	Änderungsdatum	Typ	Größe
	Key4SwitchService_installer.exe	21.02.2018 16:15	Anwendung	775 KB
cte	Namirial_OberthurKit.exe	21.02.2018 16:16	Anwendung	74.659 KB
	SwitchService.exe	21.02.2018 16:16	Anwendung	19.614 KB
	SwitchService_old.exe	21.02.2018 16:16	Anwendung	4.822 KB
ite	Wacom-STU-Driver-5.2.1.exe	21.02.2018 16:16	Anwendung	6.409 KB

Folgen Sie den Installationsschritten und schließen die Installation damit ab. Anschließend ist ein Neustart des Rechners erforderlich.

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

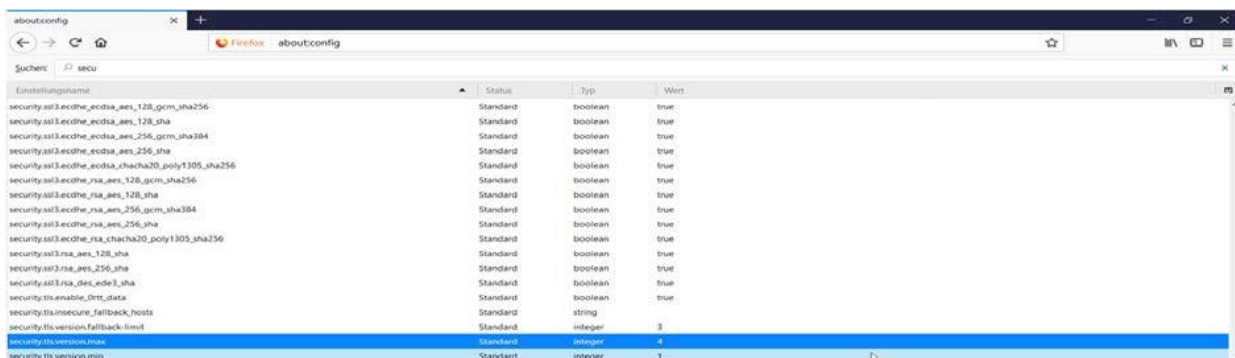
3 Firefox ESR Konfiguration



Geben Sie in der Eingabezeile ihres Firefox Browsers „About: Config“ ein um die TLS Einstellung zu kontrollieren.



Bestätigen Sie die Meldung zur Gewährleistung. Im nächsten Screen geben Sie in das Suchen Feld: „security.tls.version.max“ ein.

Diese Einstellung sollte auf 4 eingestellt sein. „Security.tls.version.min“ sollte dagegen auf 1 stehen.

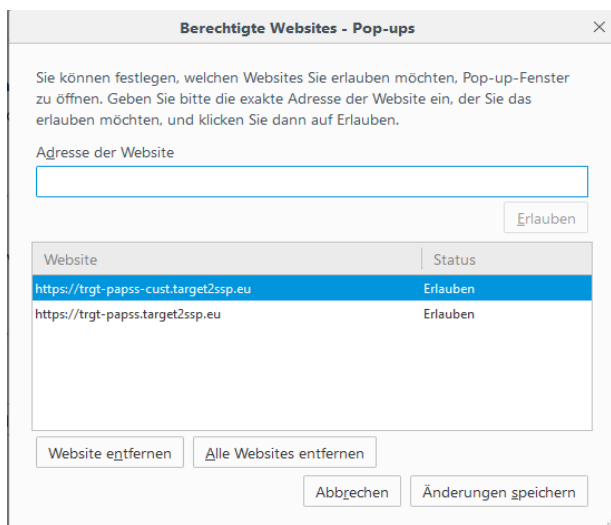
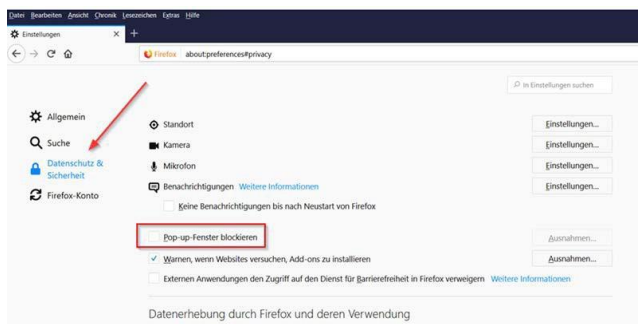


	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

Über „Extras“ und „Einstellungen“ gelangen Sie in das Untermenü „Datenschutz und Sicherheit“. Hier können Sie die „Pop-up Fenster“ deaktivieren bzw. über die Ausnahmen die Seiten

<https://trgt-papss.target2ssp.eu/ICM/>. (Produktion)

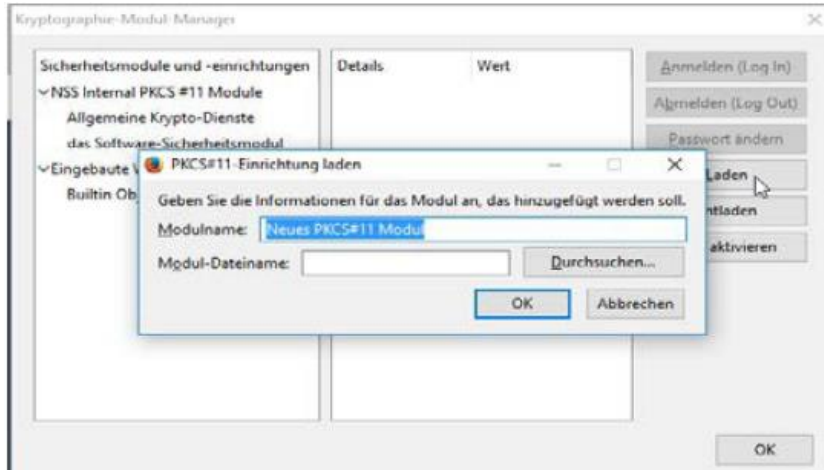
<https://trgt-papss-cust.target2ssp.eu/ICM/>. (Test) hinzufügen.



Ebenfalls in der Rubrik „Datenschutz & Sicherheit“ scrollen Sie ganz bis nach unten auf der Seite. Dort lässt sich das Zertifikat anzeigen und die Auswahl der Kryptographie-Module konfigurieren (für den Import der „bit4xpki.dll“-Datei):

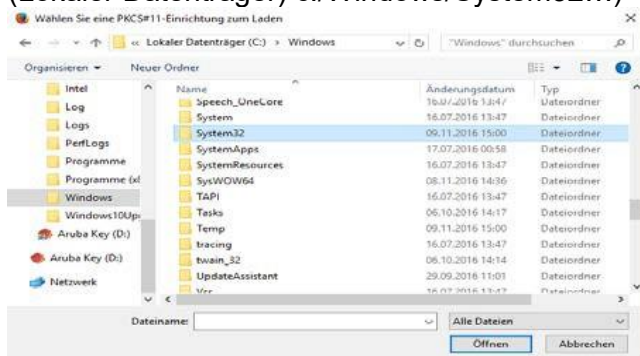


Hierzu öffnen Sie den „Kryptographiemodul Manager“ durch Betätigung des Buttons „Kryptographie Module“

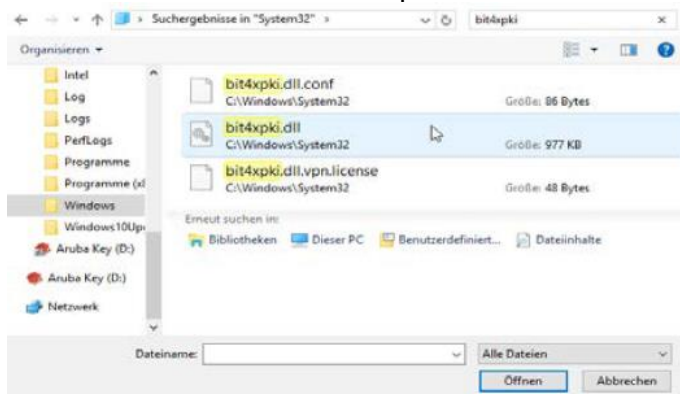


Hier wählen Sie zunächst die Option „Laden“ aus. Den vorgeschlagenen Modulnamen (‘Neues PKCS#11 Modul’) bitte so stehen lassen. Unter „Durchsuchen...“ wählen Sie den Pfad aus, von wo die erforderliche dll-Datei importiert werden soll, nämlich:



(Lokaler Datenträger) c:/Windows/System32...)

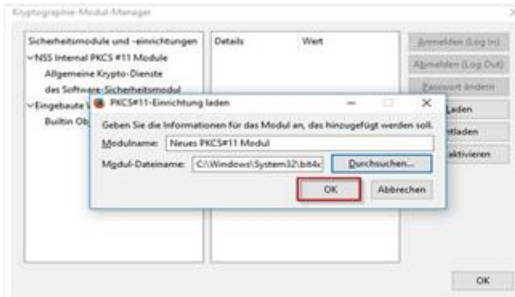


... und dort die Zieldatei „bit4xpki.dll“ markieren und mit „Öffnen“ auswählen:

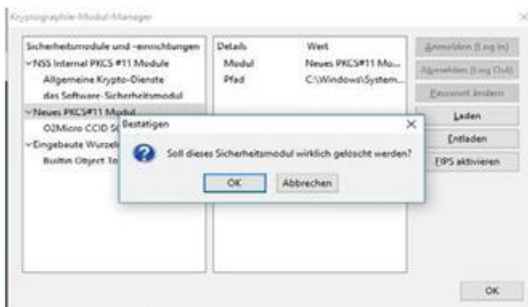


Mit Bestätigung des Buttons „OK“ ist der Import-Vorgang abgeschlossen:

	<h2>National Service Desk Deutsche Bundesbank</h2>	
	<p>TARGET2 Internet Zugang mit TOKEN (Firma Certa)</p>	



Falls der Import-Vorgang wiederholt werden muss (z.B. aufgrund einer Neuinstallation) muss das vorhandene PKCS#11 Modul zunächst entladen werden. Markieren Sie das zu entladende Modul aus, betätigen den Button „Entladen“ und bestätigen mit „OK“:





Anschließend kann die dll-Datei wie weiter oben beschrieben als Neues PKCS#11 Modul erneut geladen werden.

Nach Neustart des Mozilla Firefox Browsers sollte nun der Login möglich sein.

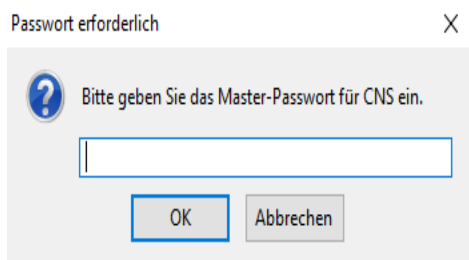
Für den Login rufen Sie bitte eine der beiden URL´s auf:

Testumgebung: <https://trgt-papss-cust.target2ssp.eu/ICM/>

Produktionsumgebung: <https://trgt-papss.target2ssp.eu/ICM/>

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	



Unmittelbar nach Aufruf der URL werden Sie zur Eingabe der PIN (Master-Passwort) aufgefordert:



Nach erfolgreicher Eingabe und Bestätigung mit „OK“ gelangen Sie auf den Startbildschirm von TARGET2-ICM:



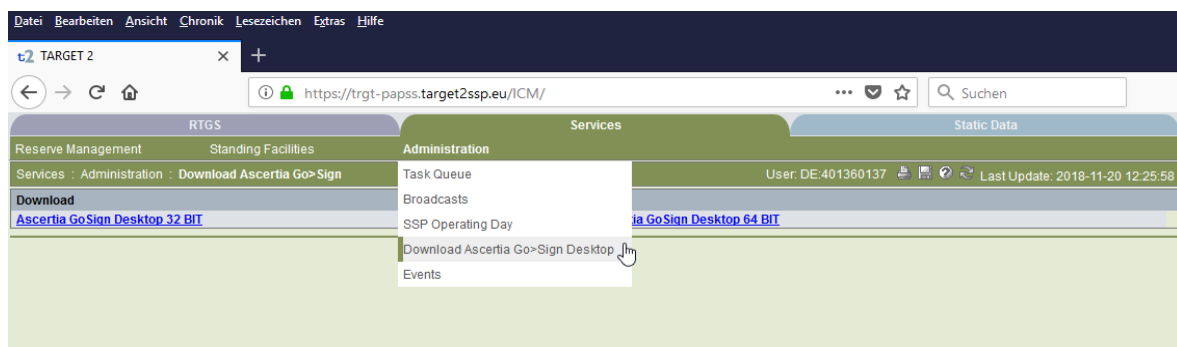
Sollte der Login-Versuch fehlschlagen mit der Fehlermeldung „ssl-Handshake-Error-Alert...“ überprüfen Sie den erfolgreichen Import der „bit4xpki.dll“-Datei, wie auf den beiden Seiten zuvor beschrieben. Weiter prüfen Sie, ob der Token richtig eingesteckt ist und die eingebaute Leuchtdiode dauerhaft leuchtet (nicht blinkt).

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

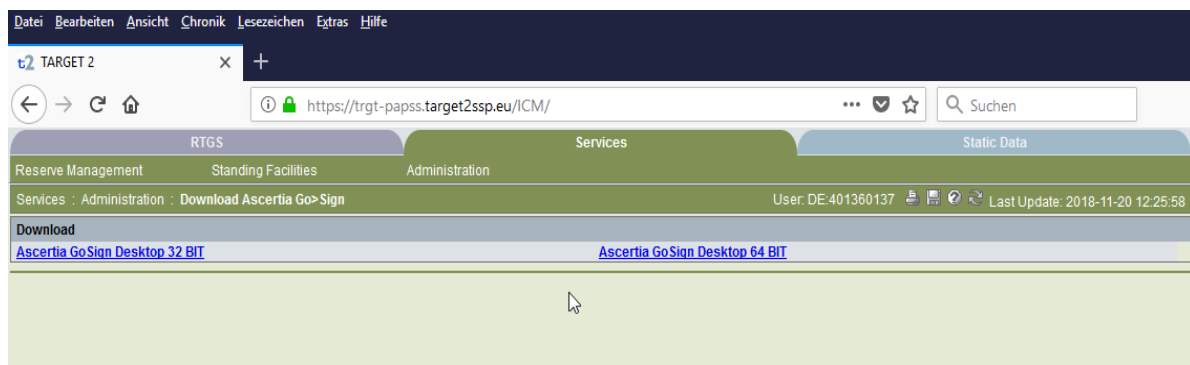
4 Installation Ascertia Go-Sign Desktop

ACHTUNG:
Download und Einrichtung sollte mit dem Mozilla Firefox Browser durchgeführt werden.

Zum Download der Go>Sign Desktop Datei wählen Sie das Register „Services > Administration > Download Ascertia Go>Sign Desktop“





In diesem Bereich steht Ihnen die Versionen „Ascertia Go>Sign Desktop 32 Bit“ sowie „Ascertia Go>Sign Desktop 64 Bit“ zum Download und zur Installation bereit.

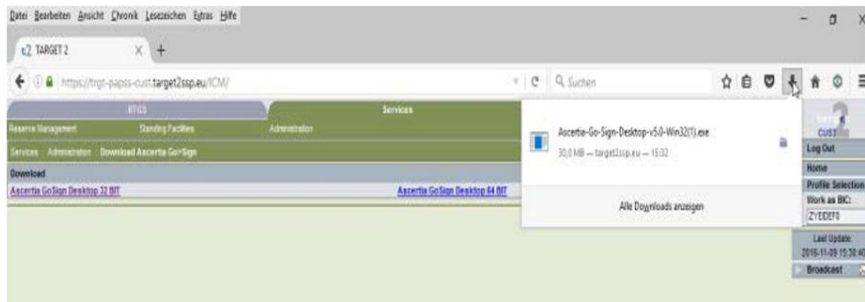


Erfolgt der Download mit dem Mozilla Firefox, lautet die Dateieindung ".msi", bei Verwendung des Internet Explorers ".man".

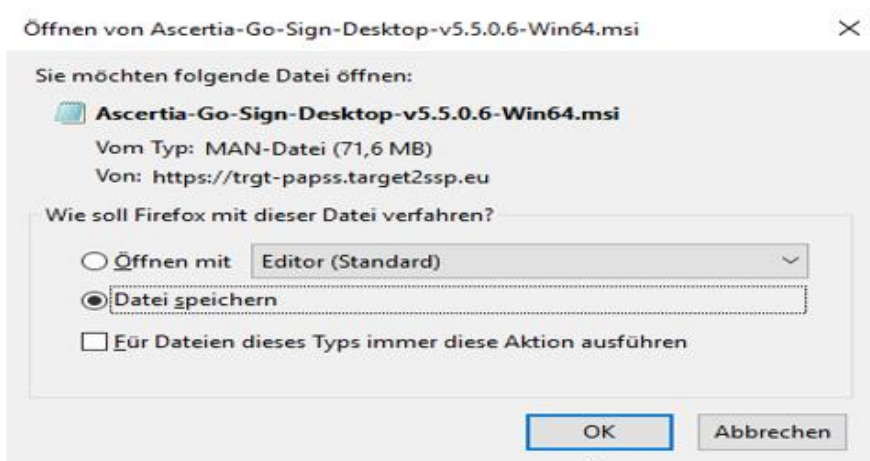
Zur Installation der „.man“ – Datei muss die Dateieindung manuell in „.msi“ geändert werden.

	<h2>National Service Desk Deutsche Bundesbank</h2>	
	<p>TARGET2 Internet Zugang mit TOKEN (Firma Certa)</p>	

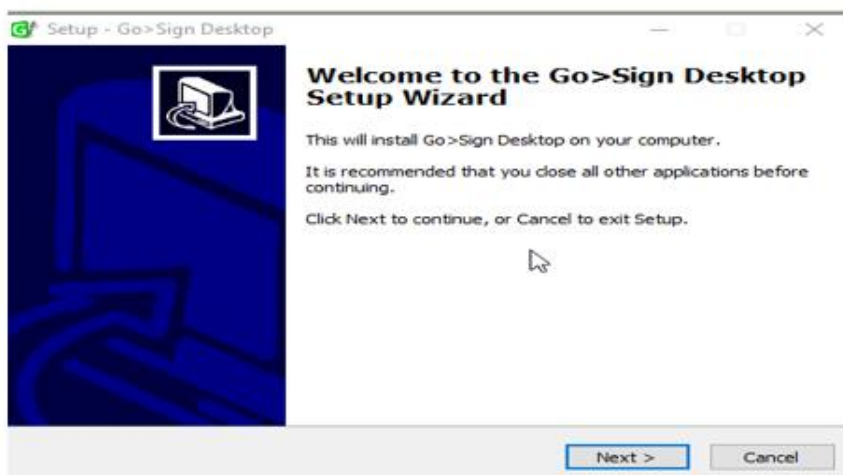
Mit einem Doppelklick auf der Versionsnummer starten Sie den Download.





Nun kann man sich entscheiden, ob man die Datei öffnen oder speichern möchte.

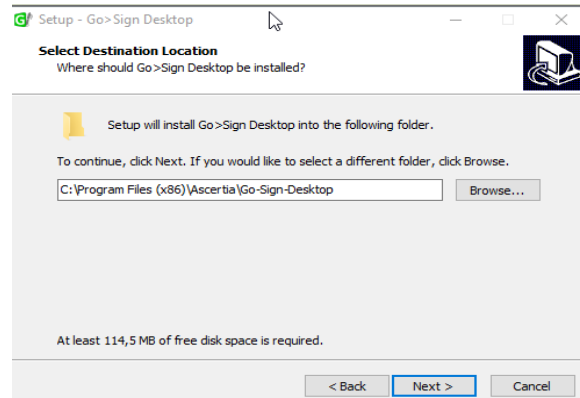


Anschließend legen Sie den Ablageort fest (der vorgegebene Pfad sollte beibehalten werden).

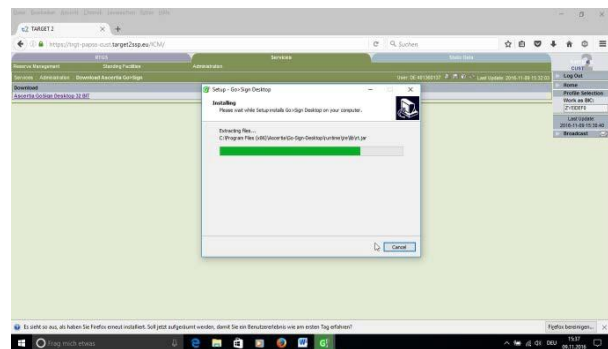


	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

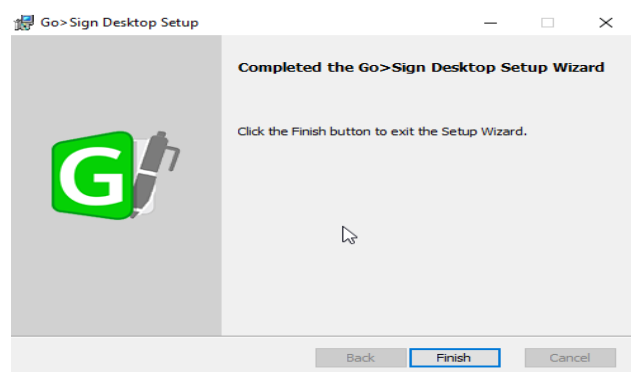
Der Installations – Assistent öffnet sich.
Wählen Sie „Next“.





Die kurze Installation schließen Sie mit
„OK“ ab.



Zuletzt ist ein Neustart des Rechners
notwendig.

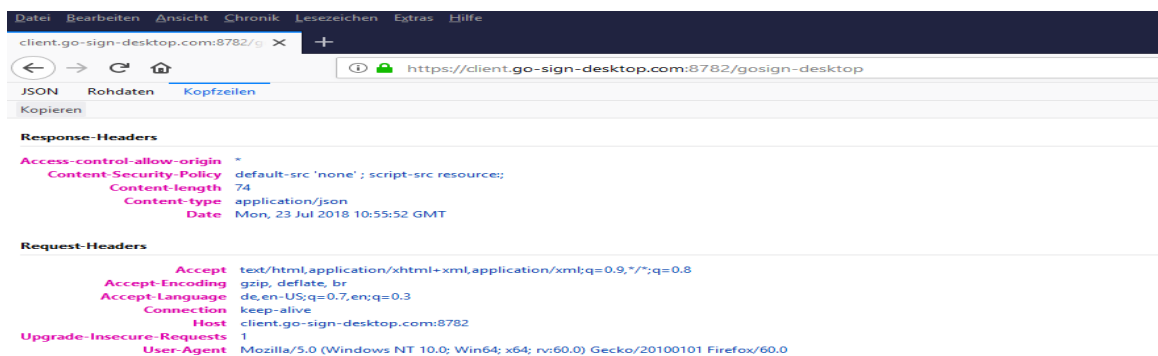
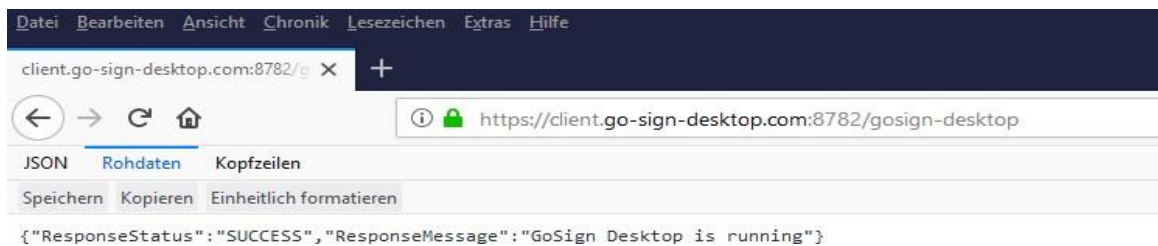
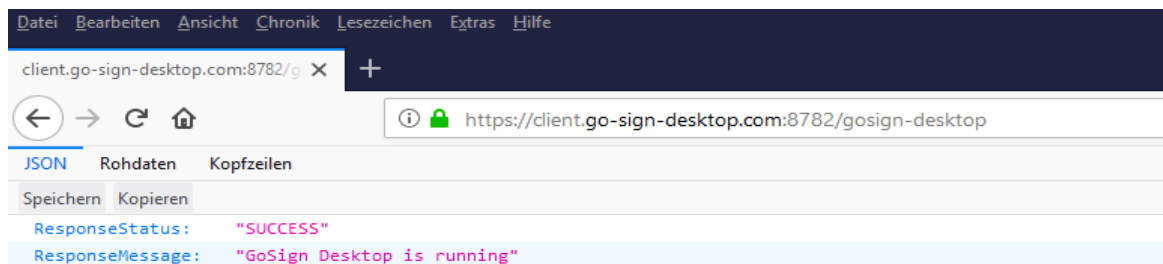


Starten Sie nun den Go>Sign Desktop über das Windows Fenster im Ordner „Ascertia“. Da-
mit der Go>Sign automatisch mit dem Betriebssystem startet, kann er auch in das
Autostart Menü eingetragen werden.

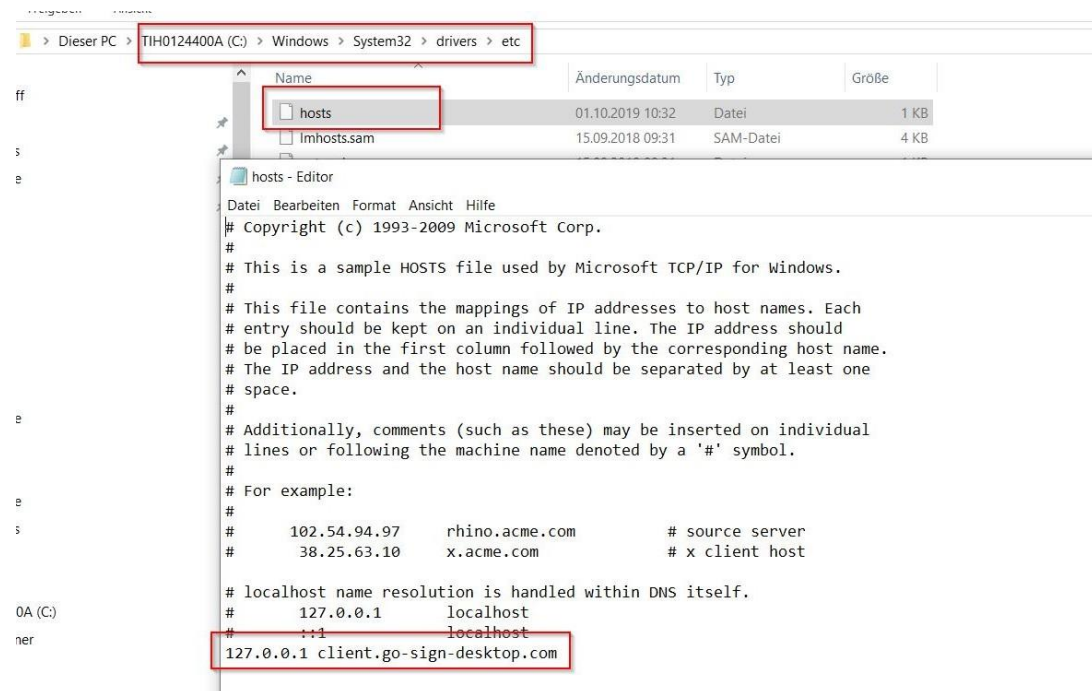
	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

4.1 Überprüfung der GoSign Desktop Installation



Um zu überprüfen, ob der „GoSign Desktop“ richtig installiert wurde und korrekt läuft, können Sie in der Adresszeile des Firefox die folgende URL aufrufen und den Status abfragen: <https://client.go-sign-desktop.com:8782/gosign-desktop>



Bitte prüfen Sie bei auftretenden Problemen in der Host – Datei den korrekten Eintrag der Go>Sign Adresse 127.0.0.1 „client.go-sign-desktop.com“



Damit der Browser fehlerfrei mit dem Go>Sign Desktop kommunizieren kann, ist es in Einzelfällen notwendig das PAC – File entsprechend anzupassen.

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

5 Entsperrten oder Ändern der PIN


Falls der Zugang mit dem Token aufgrund mehrmaliger Falscheingabe der PIN gesperrt wurde oder die PIN geändert werden soll, gehen Sie bitte wie folgt bei der Entsperrung/Änderung vor. Die Vorgehensweise ist sowohl für den Bit4id – Smart Card Manager (vom ARUBA Key Token installiert) oder Bit4id – PKI Manager (vom Firma Certa Token installiert). beschrieben.

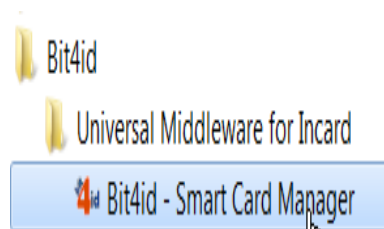
Wichtig:

Der Token muss mit einem USB-Port am Rechner verbunden sein.

Zur Entsperrung benötigen Sie den PIN/PUK-Brief, der Ihnen bei Auslieferung des Tokens mit zugesandt wurde.

5.1 Bit4id – Smart Card Manager

Zunächst öffnen Sie im Windows-Start-Menü  unter „Alle Programme“, im Ordner „Bit4id“, Unterordner „Universal Middleware for Incard“ die Anwendung „Bit4id – Smart Card Manager“





Nach Öffnen der Anwendung und kurzer Auslesung der Smartcard erscheint der angezeigte Start-Bildschirm. Dort ist das entsprechende Register zu wählen, welche Aktion durchgeführt werden soll:

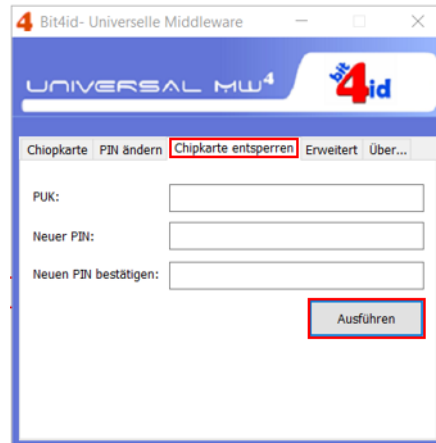


Im Register „PIN ändern“ muss der alte PIN (einfach) und der neue PIN (zweifach) eingegeben werden. Bestätigen Sie die Eingabe durch Betätigung des Buttons „Ausführen“.



	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

Im Register „Chipkarte entsperren“ muss die PUK (einfach) und der neue PIN (zweifach) eingegeben werden.
(Statt neuer kann auch die alte PIN eingegeben werden).
Bestätigen Sie die Eingabe durch Aktivierung des Buttons „Ausführen“.




Damit ist die Entsperrung/Änderung der PIN abgeschlossen und der Login auf TARGET2-ICM sollte mit der neuen oder entsperrten PIN möglich sein.

5.2 Bit4id – PKI Manager

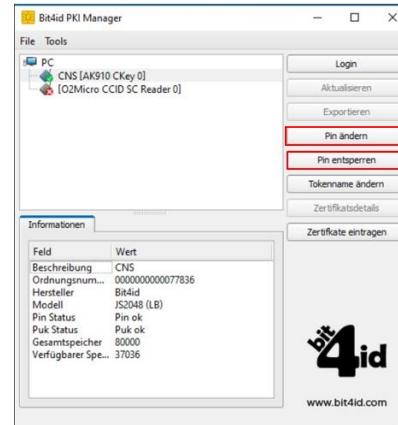
Falls auf dem Desktop aufgeführtes Link-Symbol vorhanden ist, kann der „Bit4id – PKI Manager“ durch Doppelklick direkt geöffnet werden.



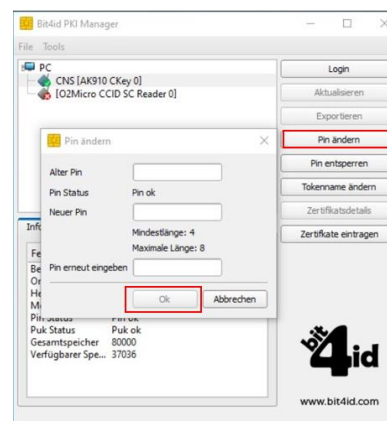
Sonst finden Sie die Anwendung im Windows-Start-Menü  unter „Alle Programme“, im Ordner „Bit4id“.



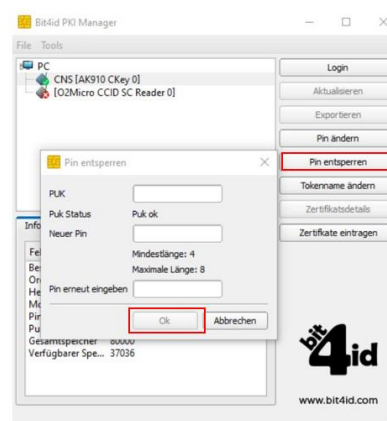
Nach Öffnen der Anwendung und kurzer Auslesung der Smartcard erscheint der angezeigte Start-Bildschirm. Dort ist das entsprechende Register zu wählen, welche Aktion durchgeführt werden soll:





Im Register „PIN ändern“ muss der alte PIN (einfach) und der neue PIN (zweifach) eingegeben werden. Bestätigen Sie die Eingabe durch Betätigung des Buttons „Ok“.



Im Register „Chipkarte entsperren“ muss die PUK (einfach) und der neue PIN (zweifach) eingegeben werden. (Statt neuer kann auch die alte PIN eingegeben werden). Bestätigen Sie die Eingabe durch Aktivierung des Buttons „Ok“.

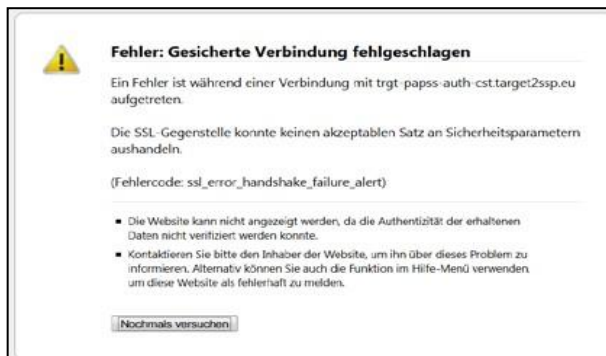


Damit ist die Entsperrung/Änderung der PIN abgeschlossen und der Login auf TARGET2-ICM sollte mit der neuen oder entsperrten PIN möglich sein.

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

6 Häufig auftretende Fehler

6.1 Fehlercode „ssl_error_handshake_failure_alert“ (fehlgeschlagener Login-Versuch bei Nutzung Mozilla Firefox)





Die Fehlermeldung "SSL_ERROR_HANDSHAKE_FAILURE_ALERT" erscheint, wenn der **Token nicht** in den Rechner **eingesteckt ist**, bei Aufruf der TARGET2-ICM-URL mit dem Mozilla Firefox Browser. Oder der Token kann **keine Verbindung zum Rechner** herstellen (Blinken der Leuchtdiode im Token).

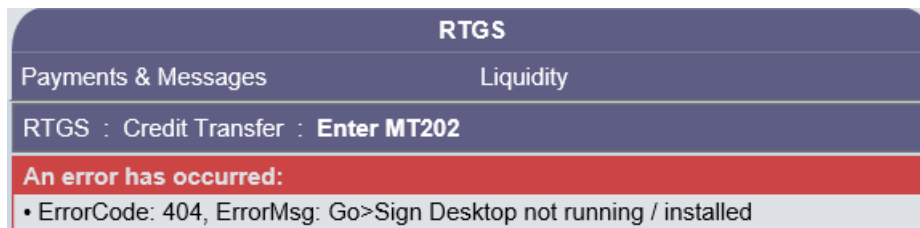
Daher rufen Sie erst dann die URL auf wenn die Diode im Token gleichmäßig leuchtet und nicht mehr blinkt.

Weiter kann es sein, dass die im Token eingelegte **SIM-Karte** etwas **verrutscht** ist und sie daher keinen Kontakt mehr hat. Daher öffnen Sie das SIM-Kartenfach und überprüfen ob die SIM-Karte richtig eingelegt ist.

Erscheint die Fehlermeldung danach immer noch ist der (erneute) Import der Datei "bit4xpki.dll" erforderlich. Die Vorgehensweise ist in dieser Installationsanleitung im Kapitel 3 beschrieben.

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

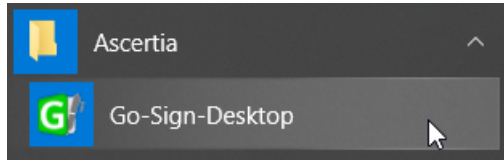
6.2 Error-Code 404 – Go-Sign-Desktop not running/ installed (erscheint bei Erfassung oder Freigabe einer MT103/202-Zahlung)



Bei Auftreten dieser Fehlermeldung überprüfen Sie, ob Ascertia Go-Sign Desktop Datei, wie in Kapitel 4 beschrieben, heruntergeladen und installiert wurde. Weiter prüfen Sie, ob die Go-Sign Desktop Datei gestartet und im Hintergrund aktiv ist. Dies erkennen Sie, wenn in der Windows-Taskleiste folgendes Symbol vorhanden ist:



Falls die Go-Sign Desktop Datei manuell gestartet werden muss finden Sie diese unter folgendem Pfad im Windows-Startmenü, unter „Alle Programme“, Buchstabe „A“:





Erscheint die Fehlermeldung bei der Zahlungserfassung oder –freigabe führen Sie unbedingt die in Kapitel 4.1 beschriebenen Überprüfungsschritte aus, durch Aufruf der dort angegebenen URL und Prüfung des korrekten „Hosts-Eintrags“.

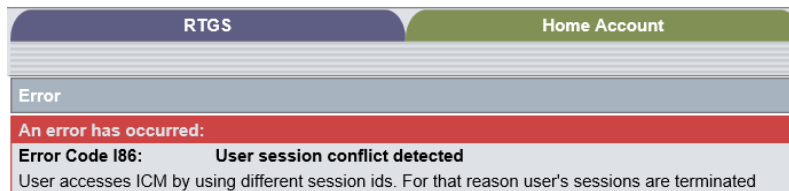
Merke:

Die Go-Sign Desktop Datei **MUSS** unbedingt die Möglichkeit haben eine Verbindung zur URL: <https://client.go-sign-desktop.com:8782/gosign-desktop> aufzubauen.

Daher auch die lokalen Firewall-Einstellungen, Windows-Defender, etc. dahingehend überprüfen!

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

6.3 Error Code I86: User session conflict detected





Ursache:

Die vorhergehende Session wurde nicht mit „Log Out“ beendet.
Daher ist die Session ist auf dem Server noch aktiv.

Lösung:

- aktuelle Session mit „Log Out“ beenden
- Browser schließen
- Browser neu starten
- neu auf TARGET2 einloggen

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

7 Systemkonfigurationen für den internetbasierten TARGET2-Zugang (Herausgeber: Europäische Zentralbank, Stand: Juni 2022)



page 2 of 3

In the tables below you can find the system components qualified by the 3CB and valid for SSP release V15.0.

Customers using totally or partially different system components or versions than the ones mentioned here are responsible to verify the compatibility between their components and the ones listed in the table below in the test environment. In such case the 3CB can provide no technical support in case of problems.

These lists will be updated at every TARGET2 release.

Internet Explorer users will rely on the same configuration (based on the local installation of the Go>Sign Desktop Client) that has proved to be stable over the previous releases for Firefox users.

Windows 10 represents the main supported Operating System.



1. ICM

1.1. Internet Access

	System components and relevant versions for Internet Access^b
Operating System - Microsoft	Microsoft Windows 10 64-bit Release 2009
Mozilla Firefox	Enterprise Support Release (ESR) v 91
Microsoft Edge	Edge v100 in Compatibility Mode (limited support only)
Ascertia Go>Sign Desktop client	Version available ICM: Services – Administration - Download Ascertia Go>Sign Desktop Minimum requirement is version 6.9.0.1

^a In case of emergency fixes due to security reasons the list might be updated in between.

^b Although not being qualified any longer, participants may still technically make use of IE11 to access the ICM. Participants are however invited to consider the risks that are associated to using this browser, given that it will not be supported by Microsoft from June 2022 onwards.

	National Service Desk Deutsche Bundesbank	
	TARGET2 Internet Zugang mit TOKEN (Firma Certa)	

8 Kontakt und Support

Bei weiteren Fragen steht Ihnen in der Zeit von 8:00 Uhr bis 16:00 Uhr das Team vom TARGET2 Internetsupport gerne zur Verfügung:

Telefon-Hotline: 069 9566 8870 (Option 3, Internetsupport)

Email: ia_support@bundesbank.de

Für allgemeine Fragen zu TARGET2 wenden Sie sich bitte an ihren zuständigen Kundenbetreuungsservice (siehe Kontakttabelle unten) bzw. an den National Service Desk TARGET-Services.

Telefon-Hotline: 069 9566-8870 (Option 1 Produktion, Option 2 Test)

Email: targetservices@bundesbank.de

Kontakt zum KBS (Kundenbetreuungsservice):

KBS-Stelle	Telefon	Email
Berlin	030 3475-2929	KBS-BBB@bundesbank.de
Düsseldorf	0211 874-2929	KBS-NRW@bundesbank.de
Frankfurt	069 9566-2929	KBS-H@bundesbank.de
Hamburg	040 3707-2929	KBS-HMS@bundesbank.de
Hannover	0511 3033-2929	KBS-BNS@bundesbank.de
Leipzig	0341 860-2929	KBS-STH@bundesbank.de
Mainz	06131 377-2929	KBS-RS@bundesbank.de
München	089 2889-2929	KBS-BY@bundesbank.de
Stuttgart	0711 944-2929	KBS-BW@bundesbank.de