

[T2G] GLOBALTRUST Trust2Go

[public - Trust2Go-Benutzerdokumentation]

Trust2Go-Benutzerdokumentation komplett siehe:
<https://service.globaltrust.eu/static/trust2go-benutzer.pdf>

Autor: Hans G. Zeger

Version 1.1 / 5. Dezember 2022

OID-Nummer: 1.2.40.0.36.1.2.7.1

Gültigkeitshistorie OID-Nummer: 1.2.40.0.36.1.2.7.99

© e-commerce monitoring GmbH 2022

Redaktioneller Hinweis: Das vorliegende Dokument ist mit einer Signatur versehen. Das Datum der Signatur kann aus verschiedenen rechtlichen und organisatorischen Gründen vom Datum des Gültigkeitsbeginns des Dokuments abweichen. Die Signatur gibt keine Auskunft über den Gültigkeitsbeginn des Dokuments, sondern bestätigt nur Herkunft und Unversehrtheit des Inhalts.

Urheberrechtshinweis: Das Dokument unterliegt dem Urheberrecht und wird nur im Rahmen der Zertifizierungsdienste zur Verfügung gestellt. Eine darüber hinausgehende Verwendung, eine vollständige oder auszugsweise Übermittlung an Dritte oder die Veröffentlichung des Dokuments durch Dritte bedarf der vorherigen Zustimmung des Autors/der Autoren und des Zertifizierungsdiensteanbieters.

3 [T2G-DOK3] SIGNATOR-DOKUMENTATION TRUST2GO

Online-Version dieser Dokumentation:

<https://service.globaltrust.eu/static/trust2go-benutzer.pdf>

Inhalt

1	[InfoDEF] Definitionen	3
2	[InfoSECRET] Geheimhaltungs- und Aktivierungsmanagement.....	5
3	[InfoTrust2Go] Informationen zu den Betriebsgrundlagen	6
4	[InfoService] Technische Voraussetzungen Nutzung von Trust2Go	6
	a) Produktion	6
	(1) SMS-User - Produktion - StandAlone-Signatur	6
	(2) App-User - Produktion - StandAlone-Signatur	7
	(3) SMS-User - Produktion - Prozess-Integration	7
	(4) App-User - Produktion - Prozess-Integration.....	7
	b) Test	8
	(1) SMS-User - Test - StandAlone-Signatur	8
	(2) App-User - Test - StandAlone-Signatur.....	8
	(3) SMS-User - Test - Prozess-Integration.....	8
	(4) App-User - Test - Prozess-Integration	8
5	[InfoWeb] Information Vertragsdetails des Signator mittels 'Trust2GoWeb' ..	10
6	[KompAppAndr] Installation (Erst/Neu) Produktionsversion	
	'Trust2GoAuthApp' - Version Android	11
7	[KompAppIos] Installation (Erst/Neu) Produktionsversion	
	'Trust2GoAuthApp' - Version IOS	12
8	[KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent)...	17
	a) Installation	17
	(1) Systemvoraussetzungen	
	(2) Vorbereitung: Feststellen Windows-Version	17
	(3) Start Installation eSign Agent.....	19
	(4) Installation .NET Framework 4.8	21
	(5) Installation e-Sign Agent	25
	(6) Deinstallation bestehende Version e-Sign Agent	31
	b) Konfiguration e-Sign Agent	33
	(1) Konfiguration 'Trust2GoServer'	33
	(2) Konfiguration Logging	33
	c) Anzeige Version e-Sign Agent.....	35
9	[ErstRegAuthApp] (Erst)Registrierung 'Trust2GoAuthApp' - inklusive	
	Aktivierung QRSCD Private Key	36
10	[ErstRegAuthWeb] (Erst)Registrierung 'Trust2GoWeb' - inklusive	
	Aktivierung QRSCD Private Key	39
11	[UpdateAuthApp] Update 'Trust2GoAuthApp'	43
12	[AendAktPINApp] Änderung AktivierungsPIN mit 'Trust2GoAuthApp'	44
13	[AendAktPINWeb] Änderung AktivierungsPIN mittels 'Trust2GoWeb'.....	47
14	[AktWeitPrivKeyApp] Aktivierung weiteres Zertifikat(Private Key) mittels	
	'Trust2GoAuthApp'.....	50
15	[AktWeitPrivKeyWeb] Aktivierung weiteren Private Key mittels	
	'Trust2GoWeb'.....	52

16	[ErstQualSig] Erstellen qualifizierte Signatur	55
a)	Erstellen qualifizierte Signatur in PDF mittels 'Trust2GoClient' (e-Sign Agent) + 'Trust2GoAuthApp'.....	55
b)	Erstellen qualifizierte Signatur in PDF mit 'Trust2GoClient' + SMS.....	62
c)	Erstellen qualifizierte Signatur in PDF mit 'Trust2GoAPI' + 'Trust2GoAuthApp' ...	67
d)	Erstellen qualifizierte Signatur in PDF mit 'Trust2GoAPI' + 'Trust2GoWeb'.....	67
e)	Erstellen qualifizierte Signatur in XML mit 'Trust2GoAPI' + 'Trust2GoAuthApp' ...	67
f)	Erstellen qualifizierte Signatur in XML mit 'Trust2GoAPI' + 'Trust2GoWeb'.....	67
17	[DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp'.....	68
18	[DeRegAuthWeb] DeRegistrierung mittels 'Trust2GoWeb'	71
19	[DeInstAuthApp] Deinstallation 'Trust2GoAuthApp'.....	74
20	[NeuRegAuthApp] NeuRegistrierung 'Trust2GoAuthApp'	75
21	[SperreSignator] Sperre durch den Signator.....	79
a)	Sperre Signator mittels 'Trust2GoWeb'.....	79
b)	Sperre Signator mittels 'Trust2GoAuthApp'.....	82
22	[SperreVDA] Sperre durch den VDA	83
23	[AktAccount] Freigabe / Aufhebung Sperre.....	84
a)	Aufhebung Sperre ohne Verlust des AktivierungsPIN (keine Neuausstellung Zertifikate)	84
b)	Aufhebung Sperre nach Verlust des AktivierungsPIN und Neuausstellung Zertifikate	84
(1)	Aktivierung neues Zertifikat mittels 'Trust2GoAuthApp'	85
(2)	Aktivierung neues Zertifikat mittels 'Trust2GoWeb'	85
24	[LogApp] Übermittlung Logdaten aus 'Trust2GoAuthApp'.....	86
25	[SignCheckAdobe] Signaturcheck in Adobe Acrobat DC.....	88
26	[SignCheckEU] Test-Tools der Europäischen Kommission	91
27	[ChangeServ] Wechsel 'Trust2GoAuthApp' Server.....	92
28	[ChangeEnv] Wechsel 'Trust2GoAuthApp' zwischen Test- und Produktions-Umgebung.....	94

Diese Dokumentation wendet sich an den ⇨ Signator und beschreibt alle bereitgestellten Komponenten, Informationen, Prozesse und Use-Cases zur Nutzung von Trust2Go.

Hinweis!

Die in dieser Dokumentation gezeigten Screenshots sollen die Nutzung erleichtern. Abhängig vom verwendeten Smartphone, verwendeter Workstation oder verwendetem Browser können die Screenshots Abweichungen aufweisen. Sie unterstützen uns in der Verbesserung der Usability, wenn Sie uns Abweichungen dokumentieren. Abhängig vom Nutzungsverhalten können auch einzelne - nicht dokumentierte - zusätzliche Schritte (Screens) erforderlich sein oder übersprungen werden.

1 [INFODEF] DEFINITIONEN

3

VDA

Kurzbezeichnung des Vertrauensdiensteanbieters GLOBALTRUST (Firmenwortlaut: "e-commerce monitoring gmbh")

In dieser Dokumentation verwendete Begriffe. Verweise auf die Definition erfolgen mit ⇒.

2. Auth-Faktor ("2FA")

Zweiter Mechanismus zur Authorisierung einer qualifizierten ⇒ Signatur, kann durch ⇒ AuthenticationApp oder SMS erfolgen. Dient zur Bestätigung, dass der ⇒ AktivierungsPIN tatsächlich vom ⇒ Signator stammt.

AktivierungsPIN

Das für die Verwendung der ⇒ Signer's Interaction Component (SIC) und zur Aktivierung des ⇒ QRSCD Private Key vom ⇒ Signator vergebene Kennung.

AuthenticationApp 'Trust2GoAuthApp'

Smartphone-App zur Nutzung des ⇒ 2. Auth-Faktors zur Authorisierung einer qualifizierten ⇒ Signatur.

Hash-Wert

Hash-Wert einer Datei die signiert werden soll, wobei nur zulässige Dokumenten-Hash-Verfahren erlaubt sind

Massensignatur

Versehen mehrerer ⇒ Hash-Werte mit je einer individuellen ⇒ Signatur, wobei bei qualifizierten ⇒ Signaturen die Liste der ⇒ Hash-Werte vor Start des Signaturvorgangs vorliegen muss.

Private Key

Privater Schlüssel der einem bestimmten ⇒ Signator zugeordnet ist und der mit diesem Schlüssel ⇒ Signaturen durchführt.

QRSCD Private Key

⇒ Private Key des ⇒ Signators der nur innerhalb der vorab definierten ⇒ Qualified Remote Signature Creation Device (QRSCD) genutzt werden kann.

Qualified Remote Signature Creation Device (QRSCD)

Signaturerstellungseinheit (⇒ QSCD) die im Trustcenter des VDA positioniert ist und qualifizierte ⇒ Signaturen nach Anforderung des ⇒ Signators erstellt.

Qualified Signature Creation Device (QSCD)

Signaturerstellungseinheit zur Ausstellung qualifizierter ⇒ Signaturen nach Anforderung des ⇒ Signators.

Signator (auch Benutzer)

Person, die unter Zuhilfenahme eines ⇒ Signer Interface (SI) eine ⇒ Signatur erstellt.

Signatur

Verschlüsselung eines ⇒ Hash-Wertes mit dem ⇒ QRSCD Private Key des ⇒ Signators und verbinden mit dem Zertifikat des ⇒ Signators gemäß ⇒ [eIDAS-VO], [SVG] und [SVV].

Signaturvorgang

Gesamtheit aller Schritte zur Erstellung einer einzelnen ⇒ Signatur oder mehrerer, zusammengefasster Signaturen (⇒ Massensignatur).

Signer's Interaction Component (SIC)

Lokale Programmkomponente unter Kontrolle des ⇒ Signators, die den ⇒ Signaturvorgang auslöst.

TransportPIN

Bei der Ausstellung eines Zertifikates vergebenes Passwort, dass den zugeordneten ⇒ QRSCD Private Key gegen unauthorisierte Nutzung absichert. Vor Nutzung des ⇒ QRSCD Private Key zur ⇒ Signatur MUSS der ⇒ Signator einen vom TransportPIN abweichenden ⇒ AktivierungPIN vergeben.

Vorgangs-ID

Zufällig generierte 5-8-stellige Zahlen-/Buchstabenkombination die durch das ⇒ Signer Interface (SI) generiert wird und einem einzelnen ⇒ Signaturvorgang zugeordnet wird. Die Vorgangs-ID dient dem ⇒ Signator bei der Freigabe durch den ⇒ 2. Auth-Faktor als zusätzliches Hilfsmerkmal zur Zuordnung einer ⇒ Signatur zu einem bestimmten ⇒ Signaturvorgang.

2 [INFOSECRET] GEHEIMHALTUNGS- UND AKTIVIERUNGSMANAGEMENT

5

Das Trust2Go-Service verwendet folgende Secrets:

- den ⇒ **TransportPIN**: gesetzt bei der erstmaligen Auslieferung eines Zertifikates
- den **erstmals** vergebenen ⇒ **AktivierungsPIN**: gesetzt vom ⇒ Signator
- einen **neu** vergebenen ⇒ **AktivierungsPIN**: gesetzt vom ⇒ Signator auf Grund des Wunsches den ⇒ AktivierungsPIN zu ändern
- einen ⇒ **FreigabeTAN**: mittels SMS übermittelt, zur Bestätigung einer ⇒ Transaktion
- einen ⇒ **PINCode**: lokal am Smartphone des ⇒ Signators vergeben, zur Bestätigung einer Signaturanforderung durch die ⇒ AuthenticationApp
- ⇒ **FaceID** oder ⇒ **Fingerprint**: lokal am Smartphone verfügbarer Sicherheitsmechanismus zur Bestätigung einer Signaturanforderung durch die ⇒ AuthenticationApp

Timeouts, die zu beachten sind

- Automatisches Logout bei 'Trust2GoWeb' nach 15 Minuten
- Registrierung der ⇒ AuthenticationApp des ⇒ Signators oder der SMS-Freigabe bis zur Bestätigung der SMS Nachricht: 600 Sekunden
- Signaturanfrage bis zur Authentifizierung durch die ⇒ AuthenticationApp, per SMS Nachricht oder per TAN Generator: 600 Sekunden

Hinweis

Die 'Trust2GoAuthApp' hat nach Start am Smartphone kein Timeout. Sie läuft solange, bis sie vom Benutzer aktiv abgeschaltet wird. Die Abschaltung einer App ist abhängig vom Betriebssystem und (teilweise) von der Hardware des Smartphones.

3 [INFOTRUST2Go] INFORMATIONEN ZU DEN BETRIEBSGRUNDLAGEN 6

Use-Cases im Überblick

- Ein ⇒ Signator kann im Rahmen einer Trust2Go-Anwendung mehrere Zertifikate mit unterschiedlichen ⇒ QRSCD Private Keys einsetzen.
- Zur ⇒ Signatur wird für alle Zertifikate eines Benutzernames derselbe ⇒ AktivierungsPIN verwendet.
- Im Falle des nachträglichen Bezugs eines neuen Zertifikates mit einem eigenen ⇒ QRSCD Private Key MUSS der zu diesem ⇒ QRSCD Private Key zugeordnete ⇒ TransportPIN durch den ⇒ AktivierungsPIN ersetzt werden.
- Der ⇒ Signator hat jederzeit Möglichkeit den bestehenden ⇒ AktivierungsPIN durch einen neuen ⇒ AktivierungsPIN zu ersetzen.

Policies zur Erbringung der Zertifizierungsdienste ([GCP] + [GCPS])

DE: <https://globaltrust.eu/certificate-policy/>

EN: <https://globaltrust.eu/en/certificate-policy-2/>

Wichtige Informationen zu Trust2Go

DE-TEXT: <https://service.globaltrust.eu/static/qualified-info-de.txt>

EN-TEXT: <https://service.globaltrust.eu/static/qualified-info-en.txt>

DE-PDF: <https://service.globaltrust.eu/static/general-de.pdf>

[knowhow.text.](#)

Impressum

DE-TEXT: <https://service.e-monitoring.at/static/impressum.txt>

EN-TEXT: <https://service.e-monitoring.at/static/imprint.txt>

DE-HTML: <https://globaltrust.eu/impressum/>

EN-HTML: <https://globaltrust.eu/en/imprint/>

AGB

DE-TEXT: <https://service.e-monitoring.at/static/agb.txt>

EN-TEXT: <https://service.e-monitoring.at/static/terms.txt>

DE-PDF: <https://www.e-monitoring.at/static/agb.pdf>

EN-PDF: <https://www.e-monitoring.at/static/terms.pdf>

4 [INFOSERVICE] TECHNISCHE VORAUSSETZUNGEN NUTZUNG VON TRUST2Go 6

Hinweis

Innerhalb betrieblicher Netze kann es erforderlich sein die Zugriffe in den lokalen Firewall-Konfigurationen freizuschalten.

Um Trust2Go verwenden zu können muss eine der folgenden Voraussetzungen gegeben sein.

A) PRODUKTION 6

(1) SMS-User - Produktion - StandAlone-Signatur 6

- aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten

II	Dienst	3	A	DIENST-12 - "Trust2Go"
				[T2G-DOK3] Signator-Dokumentation
				Trust2Go

- Mobiltelefon mit SMS-Funktion (Betriebssystem egal)
- Zugang zu <https://t2g.globaltrust.eu> (Port 443)
- Windows Workstation ab Windows 10
- Installation e-Sign Agent (⇒ 8 [KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent))

(2) *App-User - Produktion - StandAlone-Signatur*

7

- aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten
- Smartphone mit Betriebssystem
Android (ab 8.0.0, empfohlen ab 10.0) oder
iOS (ab 10, empfohlen ab 11)
- Installation 'Trust2GoAuthApp'
⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android oder
⇒ 7 [KompApplos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS
- Zugang zu <https://t2g.globaltrust.eu> (Port 443)
- Windows Workstation ab Windows 10
- Installation e-Sign Agent (⇒ 8 [KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent))

(3) *SMS-User - Produktion - Prozess-Integration*

7

- aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten
- Mobiltelefon mit SMS-Funktion (Betriebssystem egal)
- Zugang zu <https://t2g.globaltrust.eu> (Port 443)
- Integration der API-Funktionen
⇒ (1) Abruf Zertifikate des Signators
⇒ (2) Signatur eines oder mehrerer Hashwerte

(4) *App-User - Produktion - Prozess-Integration*

7

- aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten
- Smartphone mit Betriebssystem
Android (ab 8.0.0, empfohlen ab 10.0) oder
iOS (ab 10, empfohlen ab 11)
- Installation 'Trust2GoAuthApp'
⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android oder
⇒ 7 [KompApplos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS
- Integration der API-Funktionen
⇒ (1) Abruf Zertifikate des Signators
⇒ (2) Signatur eines oder mehrerer Hashwerte

B) TEST	8
(1) SMS-User - Test - StandAlone-Signatur	8
<ul style="list-style-type: none"> - aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten - Mobiltelefon mit SMS-Funktion (Betriebssystem egal) - Zugang zu https://t2gtest.globaltrust.eu (Port 443) - Windows Workstation ab Windows 10 - Installation e-Sign Agent (⇒ 8 [KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent), p125) 	
(2) App-User - Test - StandAlone-Signatur	8
<ul style="list-style-type: none"> - aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten - Smartphone mit Betriebssystem Android (ab 8.0.0, empfohlen ab 10.0) oder iOS (ab 10, empfohlen ab 11) - Installation 'Trust2GoAuthApp' <ul style="list-style-type: none"> ⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android, p119 oder ⇒ 7 [KompAppIos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS, p120 - Zugang zu https://t2gtest.globaltrust.eu (Port 443) - Windows Workstation ab Windows 10 - Installation e-Sign Agent (⇒ 8 [KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent), p125) 	
(3) SMS-User - Test - Prozess-Integration	8
<ul style="list-style-type: none"> - aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten - Mobiltelefon mit SMS-Funktion (Betriebssystem egal) - Zugang zu https://t2gtest.globaltrust.eu (Port 443) - Integration der API-Funktionen <ul style="list-style-type: none"> ⇒ (1) Abruf Zertifikate des Signators (p58) ⇒ (2) Signatur eines oder mehrerer Hashwerte (p59) 	
(4) App-User - Test - Prozess-Integration	8
<ul style="list-style-type: none"> - aufrechter Vertrag für mindestens ein Trust2Go-Zertifikat: qualifiziert oder fortgeschritten - Smartphone mit Betriebssystem Android (ab 8.0.0, empfohlen ab 10.0) oder iOS (ab 10, empfohlen ab 11) - Installation 'Trust2GoAuthApp' <ul style="list-style-type: none"> ⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android, p119 oder 	

II	Dienst		A	DIENST-12 - "Trust2Go"
		3	[T2G-DOK3] Signator-Dokumentation	Trust2Go

- ⇒ 7 [KompApplos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS, p120
- Integration der API-Funktionen
 - ⇒ (1) Abruf Zertifikate des Signators (p58)
 - ⇒ (2) Signatur eines oder mehrerer Hashwerte (p59)

5 [INFOWEB] INFORMATION VERTRAGSDetails DES SIGNATOR MITTELS
'TRUST2GOWEB'

10

<https://t2g²⁰.globaltrust.eu/trust2go/public/index.html>

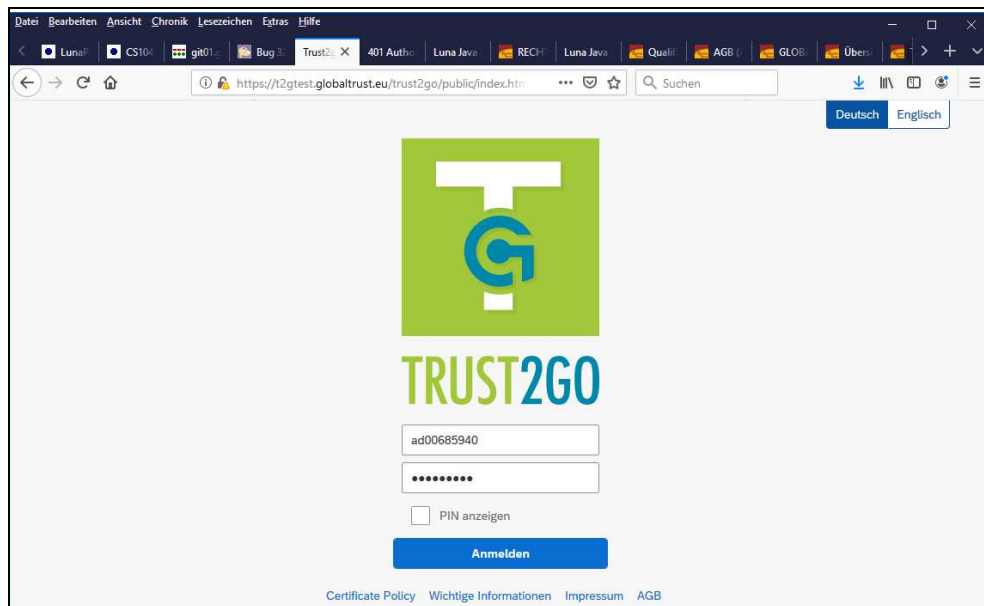


Abbildung 16: Anmeldung Signator Web

Anmelden ⇒

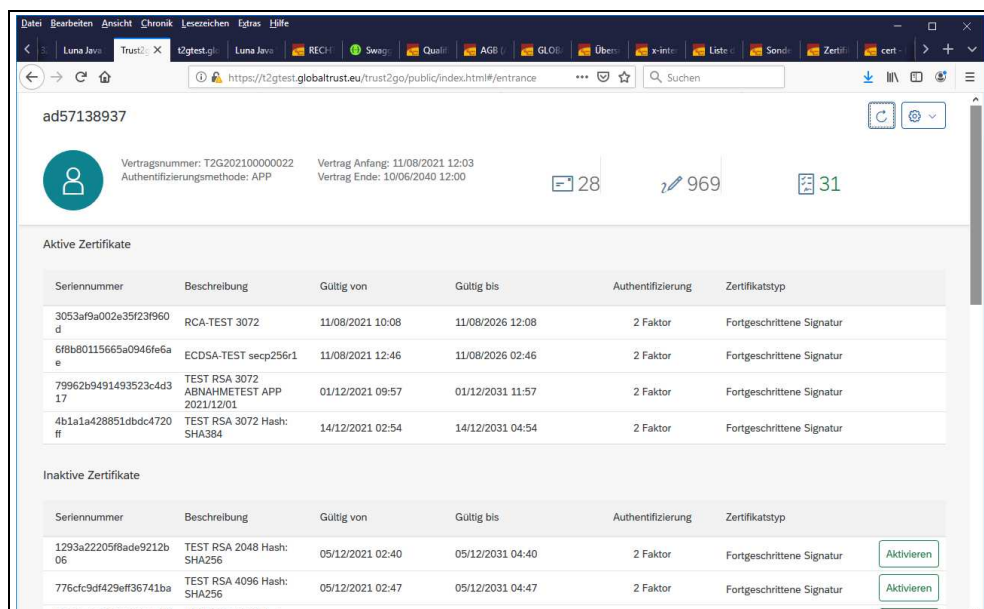


Abbildung 17: Vertragsübersicht Signator Web

²⁰ im Testbetrieb ist statt **t2g** ⇒ **t2gtest** zu verwenden

6 [KOMPAPPANDR] INSTALLATION (ERST/NEU) PRODUKTIONSVERSION
'TRUST2GOAUTHAPP' - VERSION ANDROID

11

Hinweis

- Dieser Abschnitt beschreibt die Erstinstallation der 'Trust2GoAuthApp'. Je nach Art der Änderung der App sind bei neuerlicher Installation unterschiedliche Schritte zu beachten. Beachten Sie dazu die Informationen des VDA sorgfältig. Ein Abweichen kann zur Sperre oder zum Verlust aller ihrer Zertifikate führen.
- Vorgangsweise bei einfachem Update (es werden einige Features von Trust2Go verbessert, es findet jedoch kein Systemwechsel statt)
⇒ 11 [UpdateAuthApp] Update 'Trust2GoAuthApp' (p151)
- Vorgangsweise bei Wechsel von Testsystem ⇒ Produktionssystem
STEP 1 ⇒ 17 [DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp' (p176)
STEP 2 ⇒ 19 [DeInstAuthApp] Deinstallation 'Trust2GoAuthApp' (p182)
STEP 3 ⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion
'Trust2GoAuthApp' - Version Android (p119) (dieser Abschnitt)

Systemvoraussetzung:

Android ab Version 9.0.0 (empfohlen wird ab Version 10)

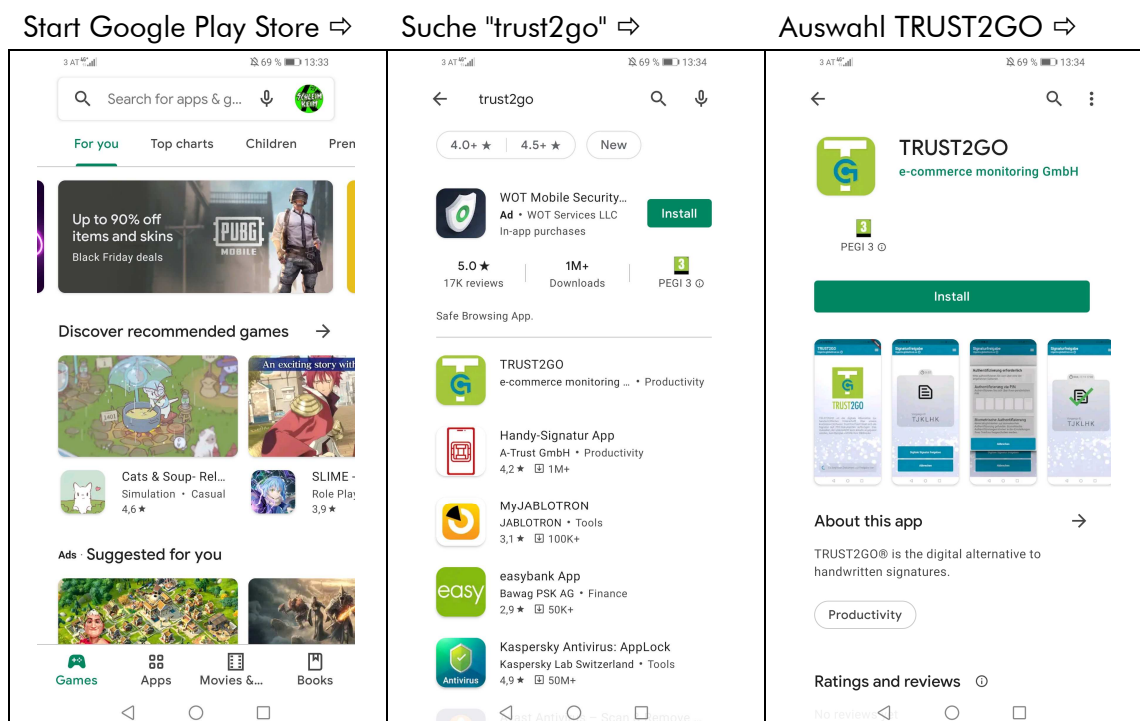


Abbildung 18: Installation Trust2Go-App Android Prod I

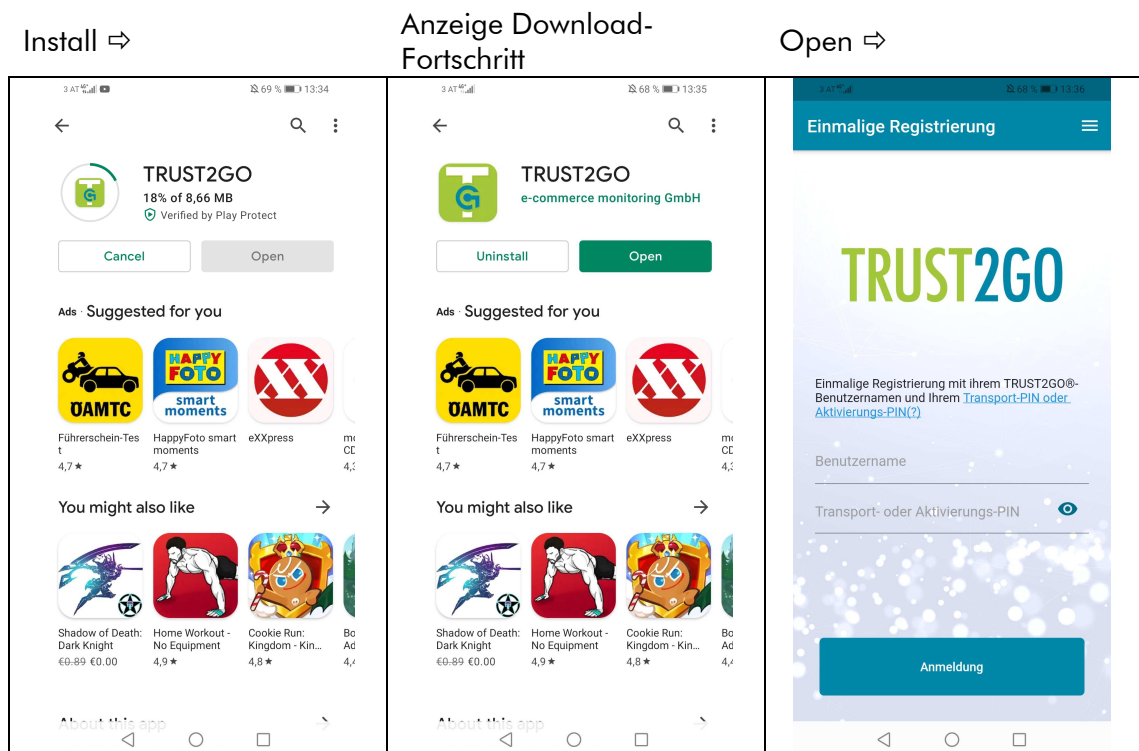


Abbildung 19: Installation Trust2Go-App Android Prod II

Weiter mit ⇒ 9 [ErstRegAuthApp] (Erst)Registrierung 'Trust2GoAuthApp' - inklusive Aktivierung QRSCD Private Key (p144)

7 [KOMPAPPLOS] INSTALLATION (ERST/NEU) PRODUKTIONSVERSION 'TRUST2GOAUTHAPP' - VERSION IOS

12

Hinweis

- Dieser Abschnitt beschreibt die Erstinstallation der 'Trust2GoAuthApp'. Je nach Art der Änderung der App sind bei neuerlicher Installation unterschiedliche Schritte zu beachten. Beachten Sie dazu die Informationen des VDA sorgfältig. Ein Abweichen kann zur Sperre oder zum Verlust aller ihrer Zertifikate führen.
- Vorgangsweise bei einfachem Update (es werden einige Features von Trust2Go verbessert, es findet jedoch kein Systemwechsel statt)
⇒ 11 [UpdateAuthApp] Update 'Trust2GoAuthApp' (p151)
- Vorgangsweise bei Wechsel von Testsystem ⇒ Produktionssystem
STEP 1 ⇒ 17 [DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp' (p176)
STEP 2 ⇒ 19 [DeInstAuthApp] Deinstallation 'Trust2GoAuthApp' (p182)
STEP 3 ⇒ 7 [KompApplos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS (p120) (dieser Abschnitt)

Systemvoraussetzung

Gerät: ab iPhone 5S

Betriebssystem: iOS ab Version 10.0 (empfohlen wird Version ab 12.4.8)



Start Apple Store ➞

Suchen ➞

Trust2Go ➞

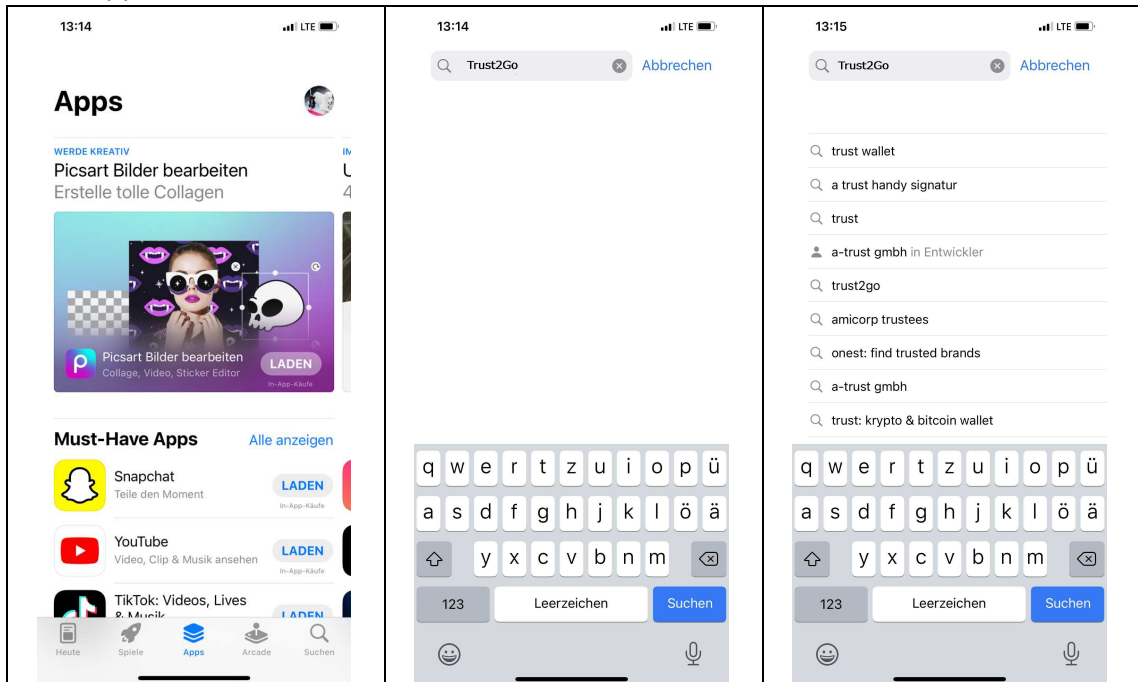


Abbildung 20: Installation Trust2Go-App IOS Prod I

App trust2go ⇒

LADEN (Doppelclick) ⇒

Installationsstatus

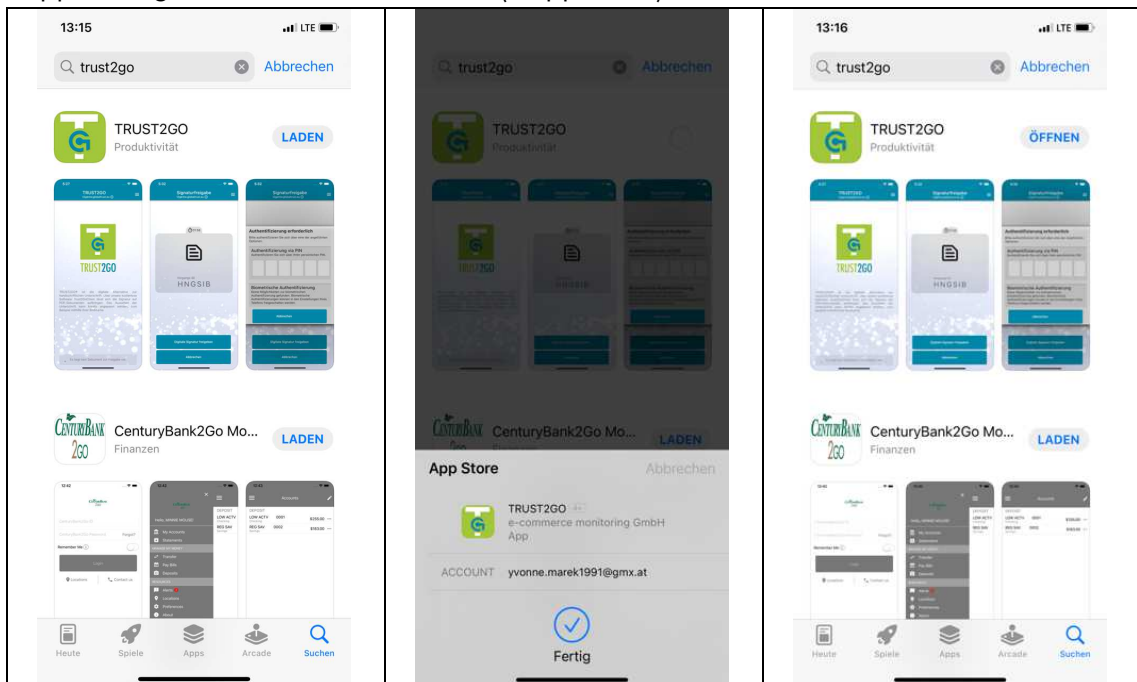


Abbildung 21: Installation Trust2Go-App IOS Prod II

ÖFFNEN ⇒

Nicht erlauben ⇒

ans Ende gehen ⇒

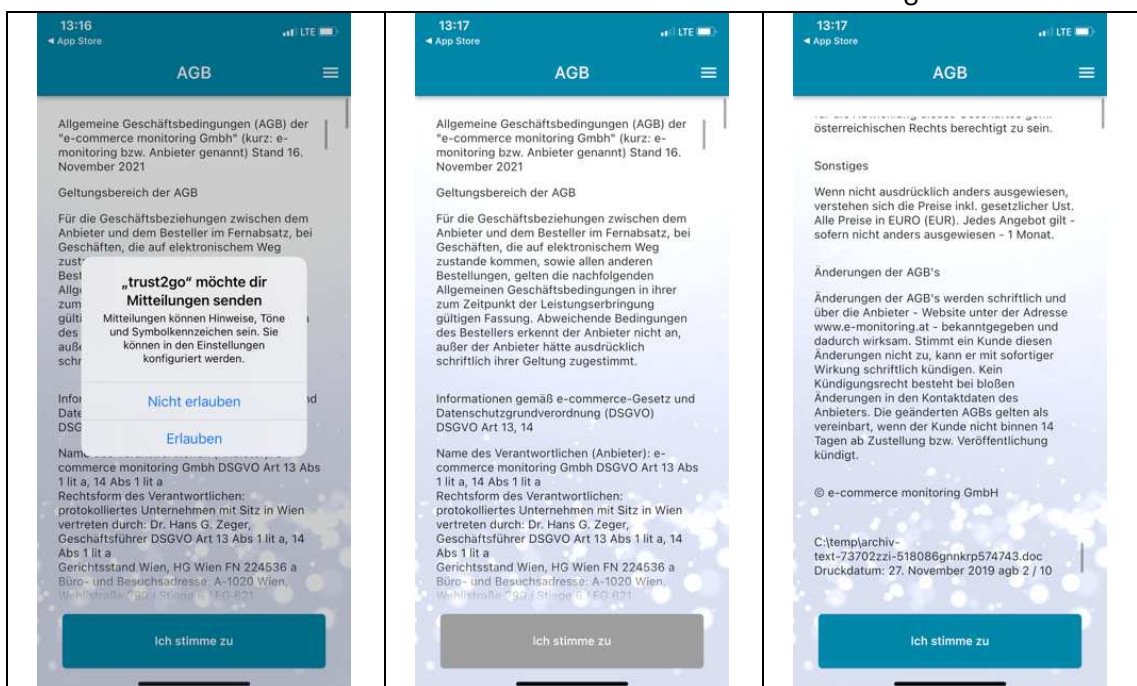


Abbildung 22: Installation Trust2Go-App IOS Prod III

Ich stimme zu ⇒

Signatordaten eingeben

Anmeldung ⇒

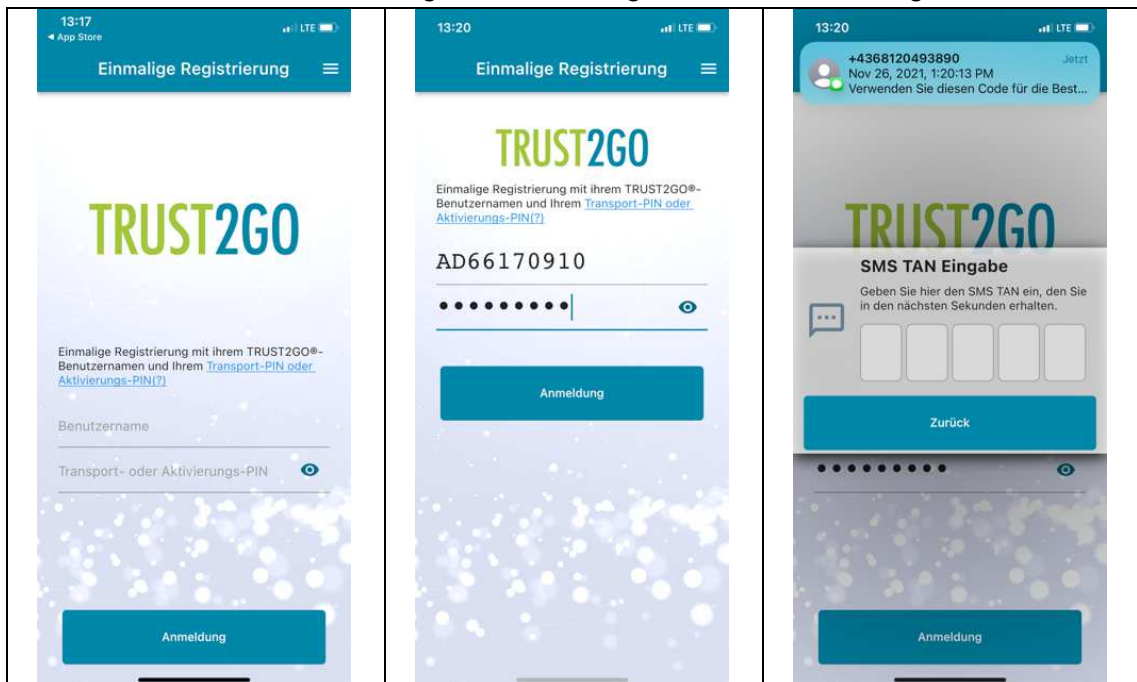


Abbildung 23: Installation Trust2Go-App IOS Prod IV

zugesendeter SMS
eingeben ⇒persönlichen PINCode
festlegen und eingeben ⇒

ans Ende gehen ⇒

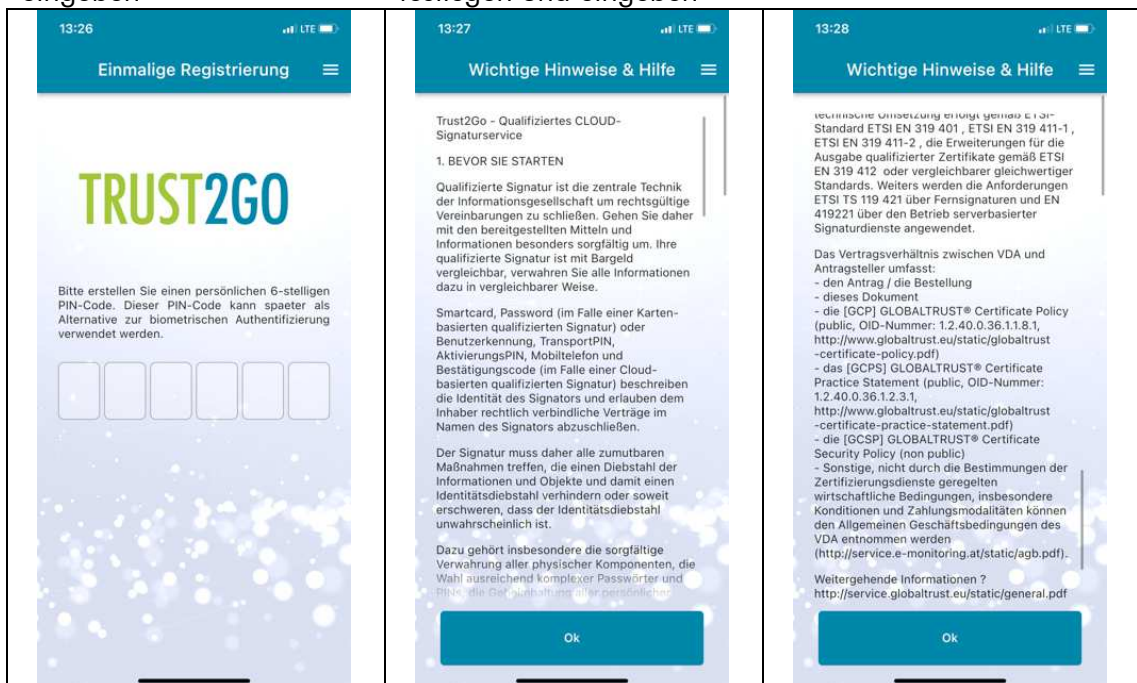


Abbildung 24: Installation Trust2Go-App IOS Prod V

OK ⇨



Abbildung 25: Installation Trust2Go-App IOS Prod VI

II	Dienst	3	A	DIENST-12 - "Trust2Go"
				[T2G-DOK3] Signator-Dokumentation
				Trust2Go

8 [KOMPEsign] INSTALLATION + KONFIGURATION 'TRUST2GOCLIENT' (E-SIGN AGENT) 17

A) INSTALLATION 17

Download des e-Sign Agent in ein geeignetes Verzeichnis (zB C:\download)
<https://service.globaltrust.eu/static/eSignAgent.msi>

(1) Systemvoraussetzungen

.NET Framework 4.8, verfügbar unter:

- Windows 10 ab 1607 (getestet, 1511 wird NICHT unterstützt)
- Windows 8.1 ab v 6.3 B9600
- weitere Windows-Versionen wurden nicht getestet

Hinweis

Die Installation des e-Sign Agent bzw. des .net-Frameworks erfordert Administratorrechte.

Hinweis

In seltenen Einzelfällen haben uns Benutzer berichtet, dass die Installation nicht möglich war, weil es Inkompatibilitäten mit anderen - installierten - Programmen gab. Wir empfehlen in derartigen Fällen die Installation auf einer Workstation zu versuchen, die nicht Teil eines Corporate Networks ist. Aktuell wurde uns eine Inkompatibilität mit "baramundi Management Agent" kommuniziert.

(2) Vorbereitung: Feststellen Windows-Version 17

Versionsanzeige für Windows 10

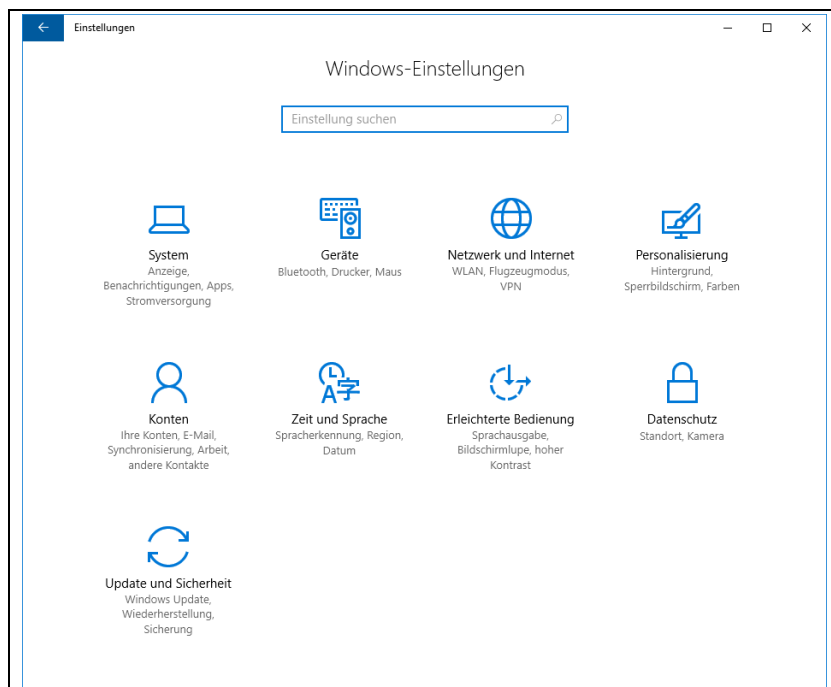


Abbildung 26: Windows 10: Windows-Einstellungen I

System ⇒ Info ⇒

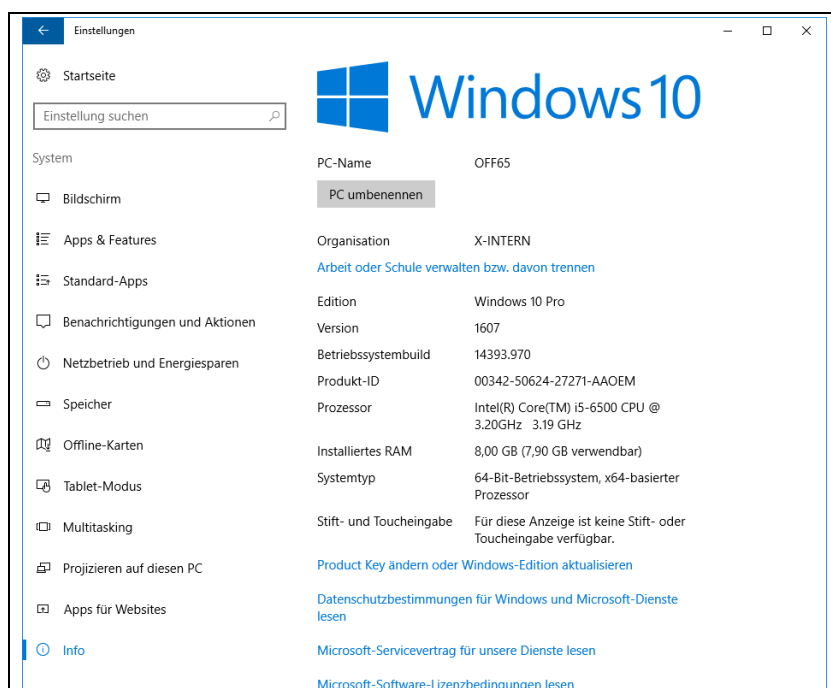


Abbildung 27: Windows 10: Windows-Einstellungen II

Versionsanzeige für Windows 8.1


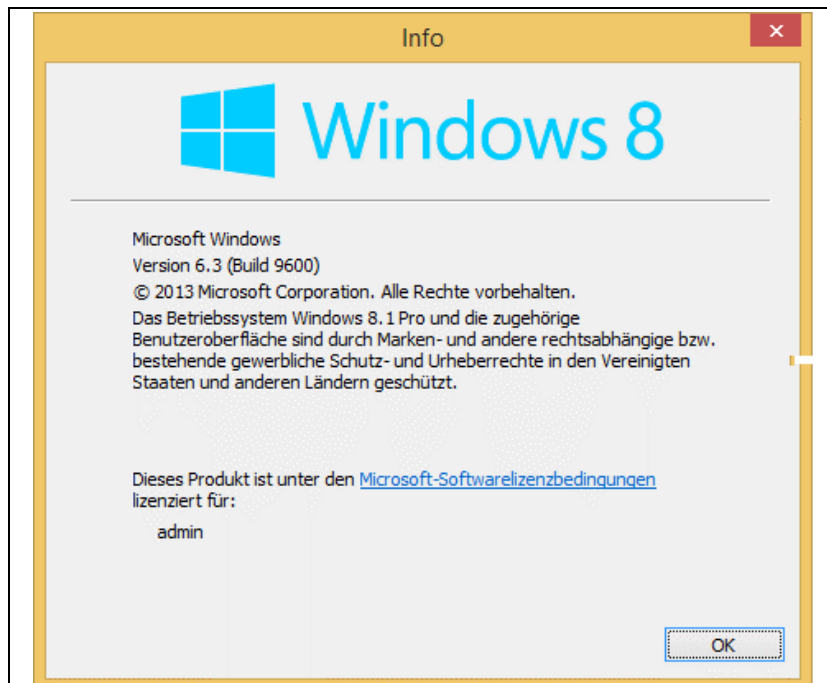
 + "R" ⇨

Abbildung 28: Windows 8.1: Windows-Einstellungen III

(3) Start Installation eSign Agent

19

Hinweis!

Falls das Programm schon installiert ist und eine neue Version installiert werden soll, dann muss die bisherige Version deinstalliert werden (⇒ (6) Deinstallation bestehende Version e-Sign Agent, p139).

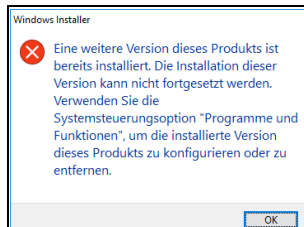


Abbildung 29: Hinweis e-Sign Agent schon installiert

C:\download\eSignAgent.msi ⇒ (Doppelclick) ⇒

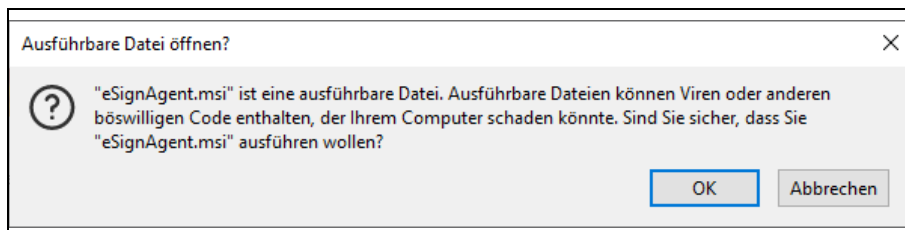


Abbildung 30: Start Installation e-Sign Agent

OK ⇒

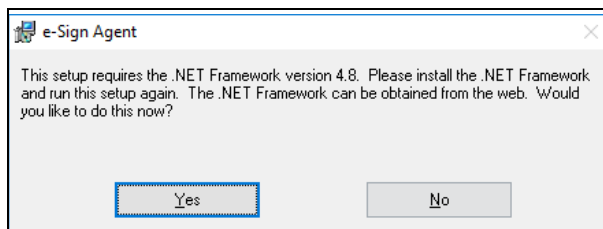


Abbildung 31: Hinweis auf notwendiges .net-Framework I

Hinweis

Fehlt die erforderliche .net-Version ⇒ (4) Installation .NET Framework 4.8 (p129)
ansonsten weiter mit ⇒ (5) Installation e-Sign Agent (p133)

(4) *Installation .NET Framework 4.8*

21

Dieser Abschnitt kann übersprungen werden, wenn eine .NET-Version gleich oder höher als 4.8 installiert ist.

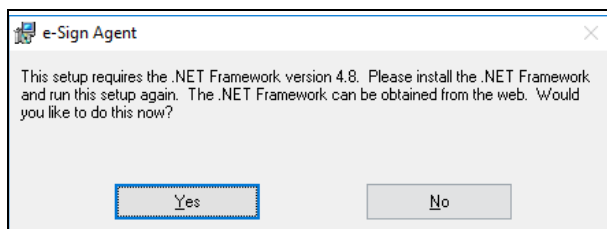


Abbildung 32: Hinweis auf notwendiges .net-Framework II

Yes →

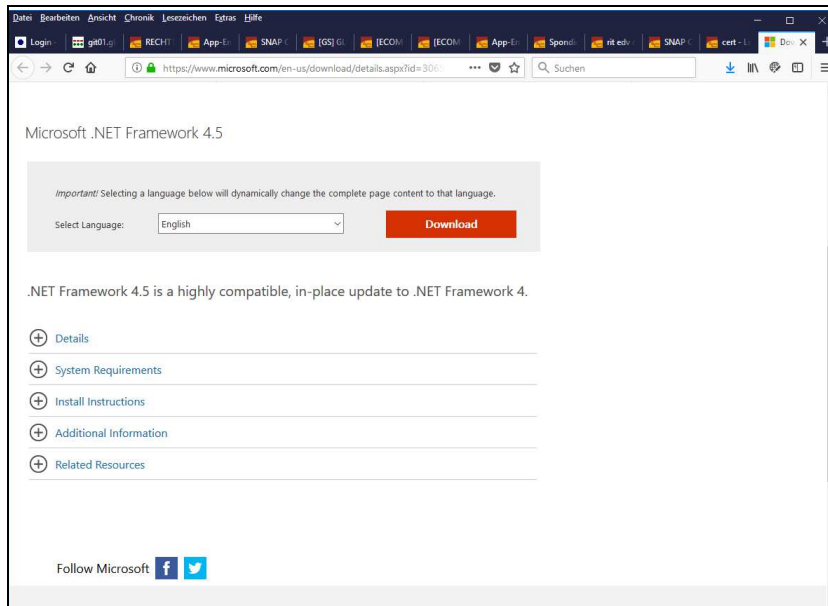
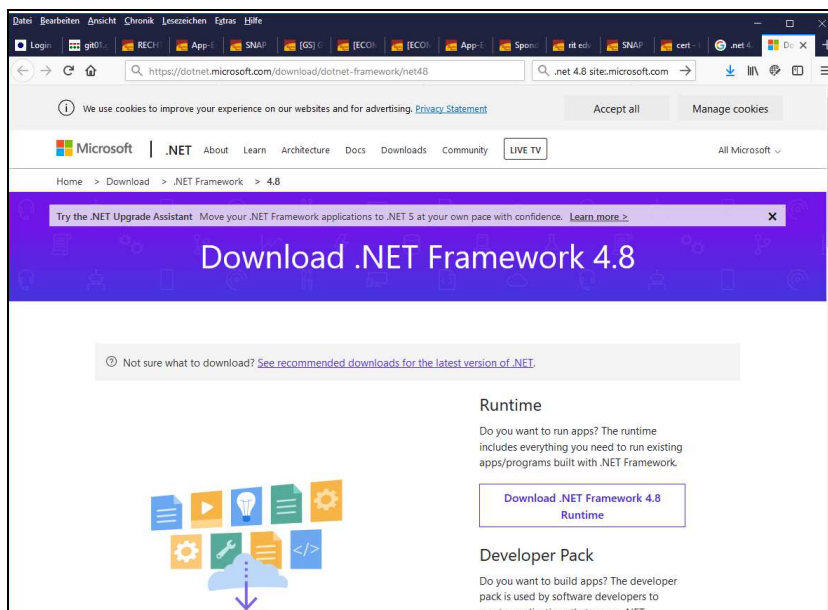
**Link auf .NET 4.8**<https://dotnet.microsoft.com/download/dotnet-framework/net48>

Abbildung 34: .net Framework 4.8

Web-Installer<https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-web-installer>**Offline-Installer (empfohlene Variante)**<https://dotnet.microsoft.com/download/dotnet-framework/thank-you/net48-offline-installer>

C:\download\ndp48-x86-x64-allos-enu-offline-runtime.exe ⇒ (Doppelclick) ⇒ Ja ⇒

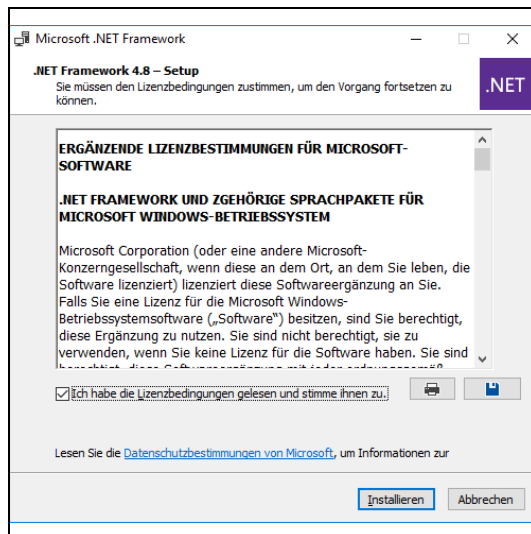


Abbildung 35: Lizenzbestimmungen Microsoft-Software

Ich habe die Lizenbedingungen gelesen und stimme ihnen zu: Anhaken

Installieren ⇒

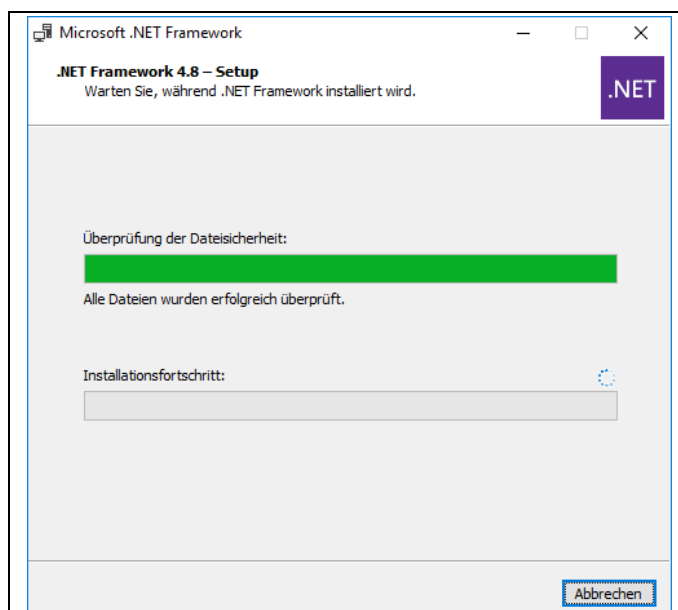


Abbildung 36: Anzeige Installationsfortschritt

Programme die .NET verwenden müssen geschlossen werden

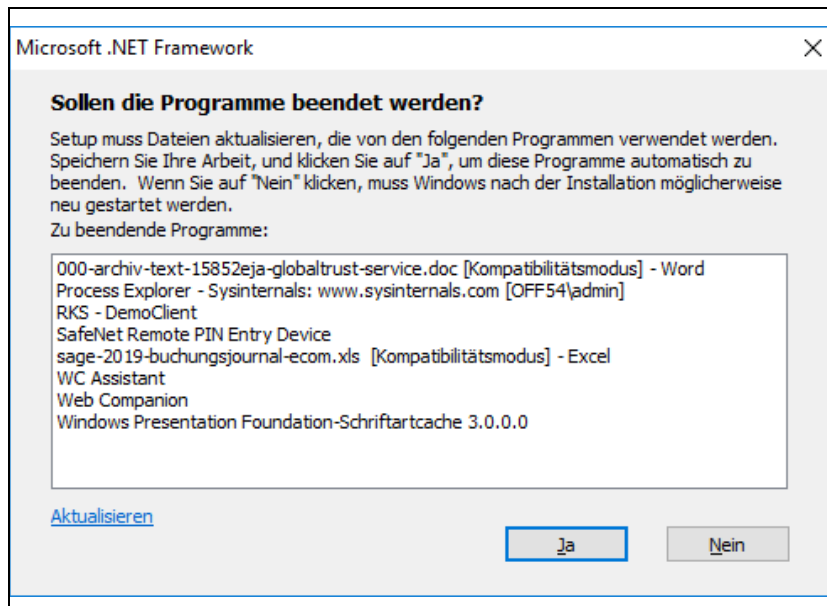


Abbildung 37: Liste Programme, die .NET verwenden

Ja ⇒

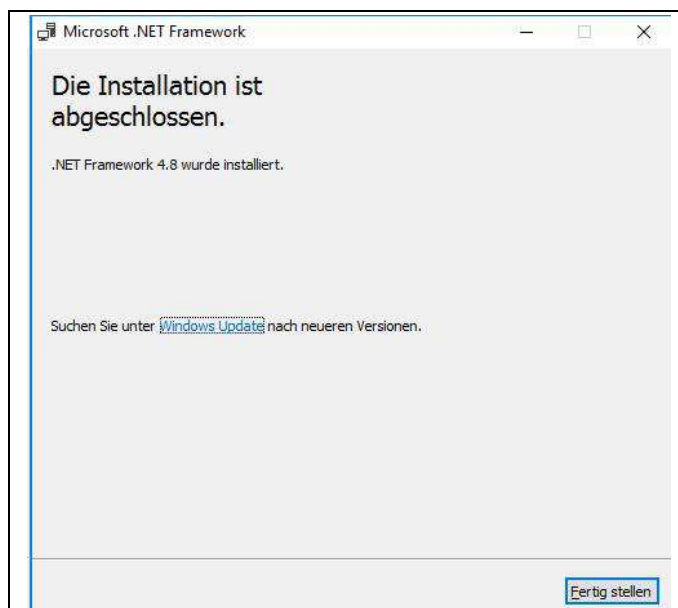


Abbildung 38: Information Abschluss .NET-Installation

Fertig stellen ⇒

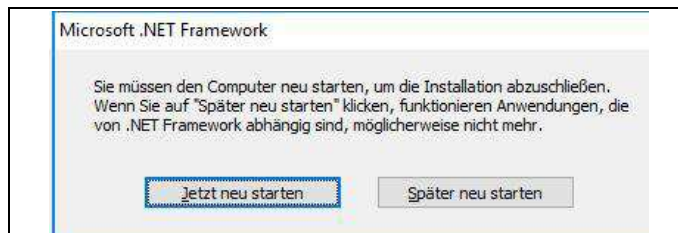


Abbildung 39: Aufforderung Computer neu starten

Später neu starten ⇒

Die Programme des Computers sollten manuell in geeigneter Reihenfolge geschlossen werden und kurzfristig ein Neustart erfolgen.

Hinweis!

Unter anderem kann es zu Einstellungsänderungen in Word kommen, zB Graphiken sind nicht mehr sichtbar: Datei ⇒ Optionen ⇒ Erweitert ⇒ Platzhalter für Graphiken: aktivieren und dann wieder deaktivieren

(5) Installation e-Sign Agent

25

C:\download\eSignAgent.msi ⇒ (Doppelclick) ⇒

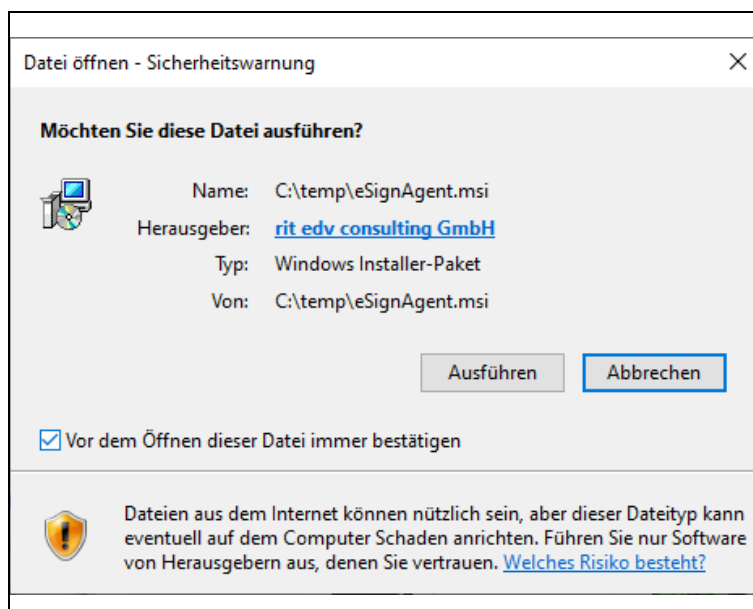


Abbildung 40: Installation e-Sign Agent I

Ausführen ⇨

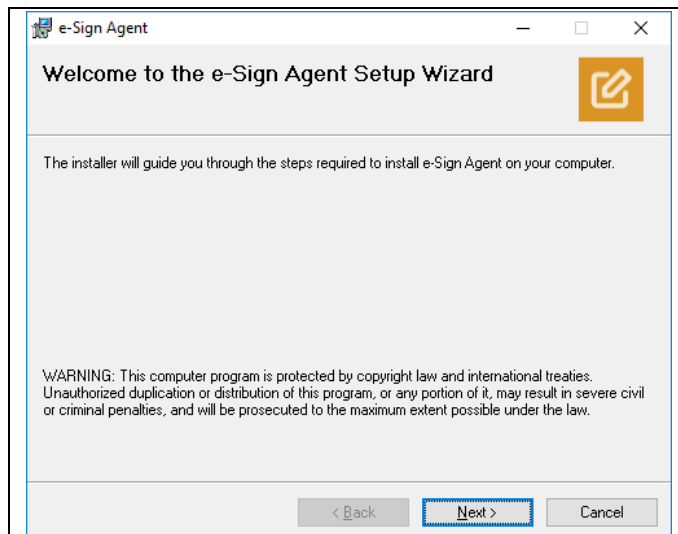


Abbildung 41: Installation e-Sign Agent I

Next ⇨

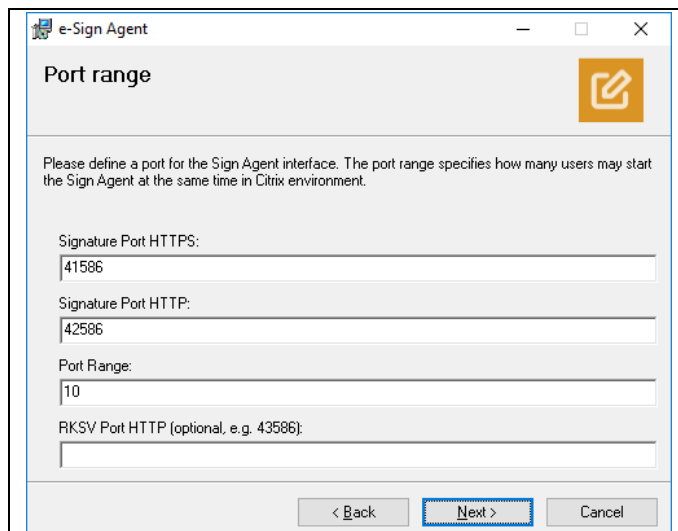


Abbildung 42: Installation e-Sign Agent II

Defaultwerte belassen
RKSX Port: nichts eintragen

Next ⇒

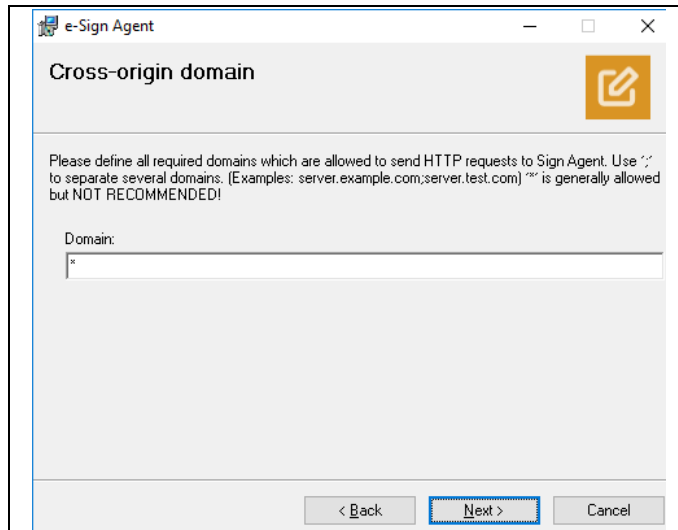


Abbildung 43: Installation e-Sign Agent III

Defaultwert belassen ⇒ Next ⇒

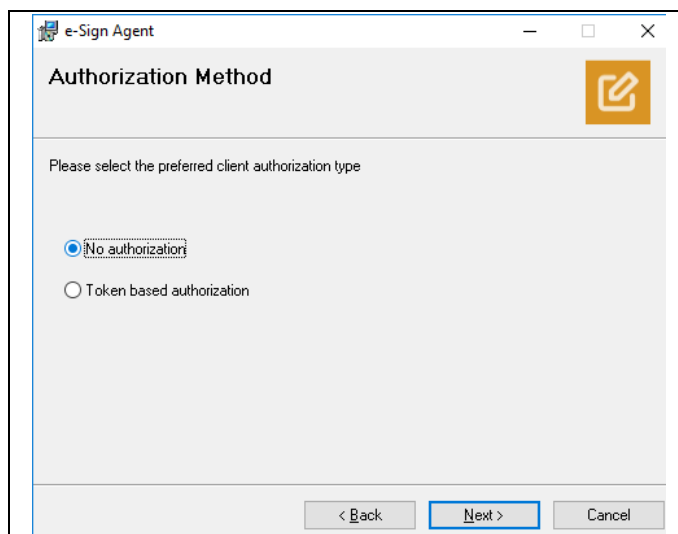


Abbildung 44: Installation e-Sign Agent IV

Defaultwert (No authorization) belassen ⇒ Next ⇒

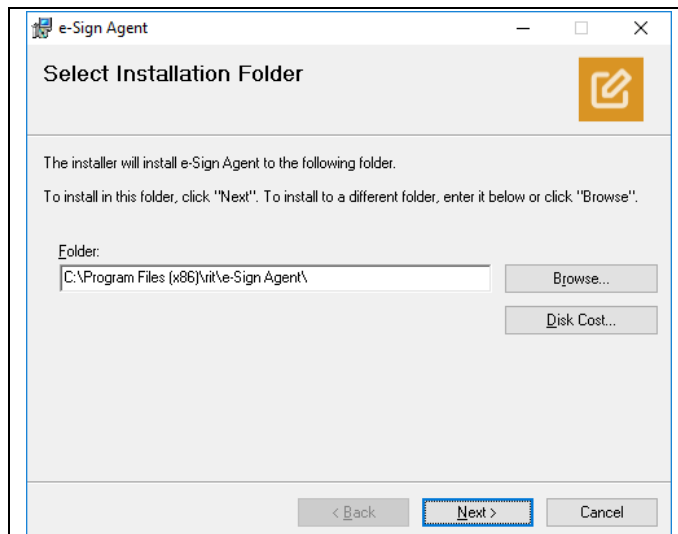


Abbildung 45: Installation e-Sign Agent V

Folder: C:\Program Files (x86)\rit\e-Sign Agent\

Next ⇒

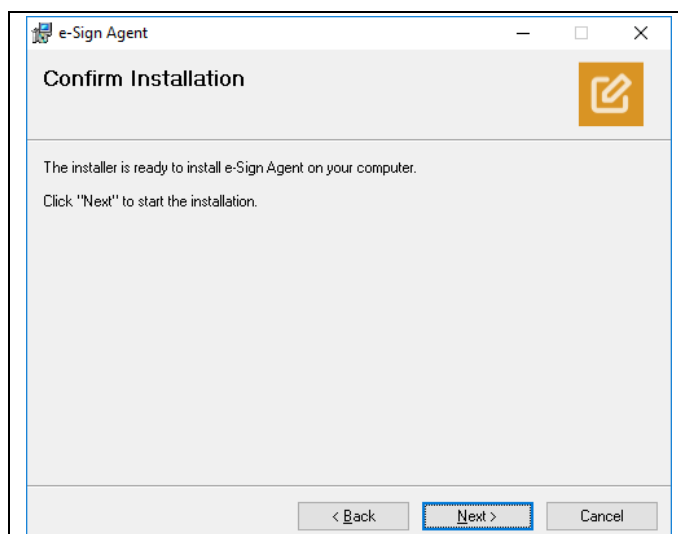


Abbildung 46: Installation e-Sign Agent VI

Next ⇒

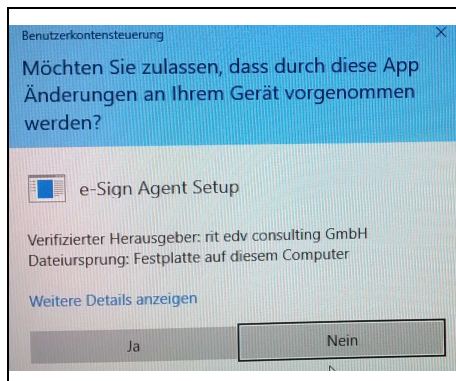


Abbildung 47: Installation e-Sign Agent VIII

Ja ⇒

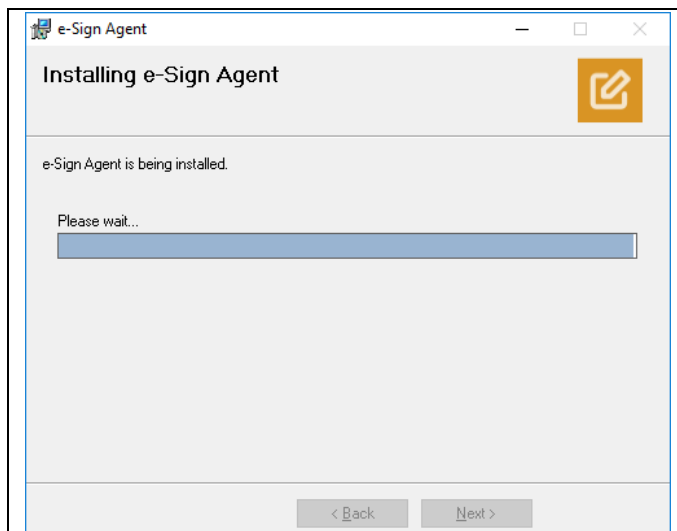


Abbildung 48: Installation e-Sign Agent VII

Hinweis

Die zusätzliche Bestätigung kann auch fallweise im Hintergrund liegen.

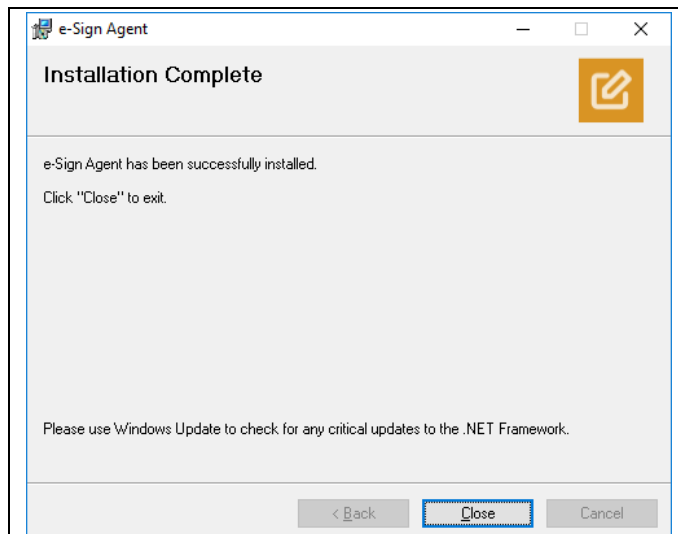


Abbildung 49: Installation e-Sign Agent IX

Close ⇒

Hinweis!

Stellen Sie sicher, dass in der Konfigurationsdatei "C:\Program Files (x86)\rit\e-Sign Agent\SignAgentConfig.json" der korrekte Server eingetragen ist:

- **Produktion:** <https://t2g.globaltrust.eu/trust2go>
- **Test:** <https://t2gtest.globaltrust.eu/trust2go>

Details zur Konfiguration ⇒ b) Konfiguration e-Sign Agent

(6) Deinstallation bestehende Version e-Sign Agent

31

Systemsteuerung ⇒ Alle Systemsteuerungselemente ⇒ Programme und Features ⇒

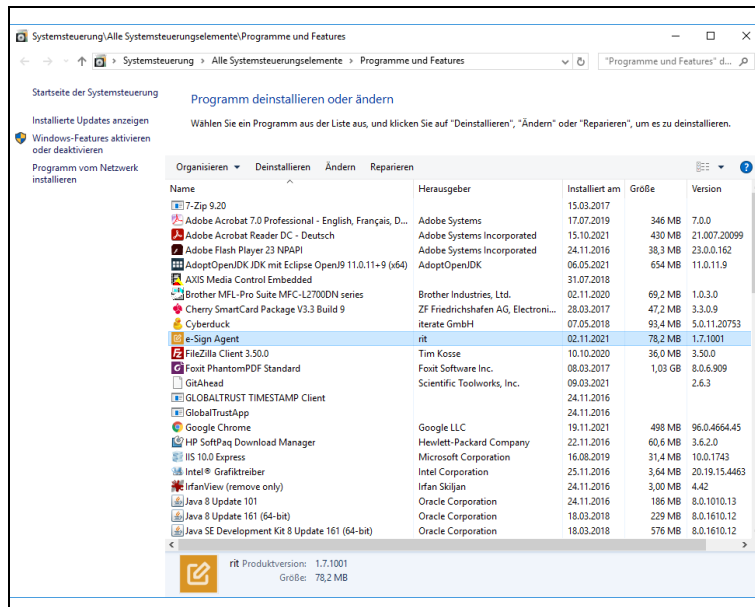


Abbildung 50: Deinstallation e-Sign Agent I

e-Sign Agent ⇒ (Rechtsklick) ⇒

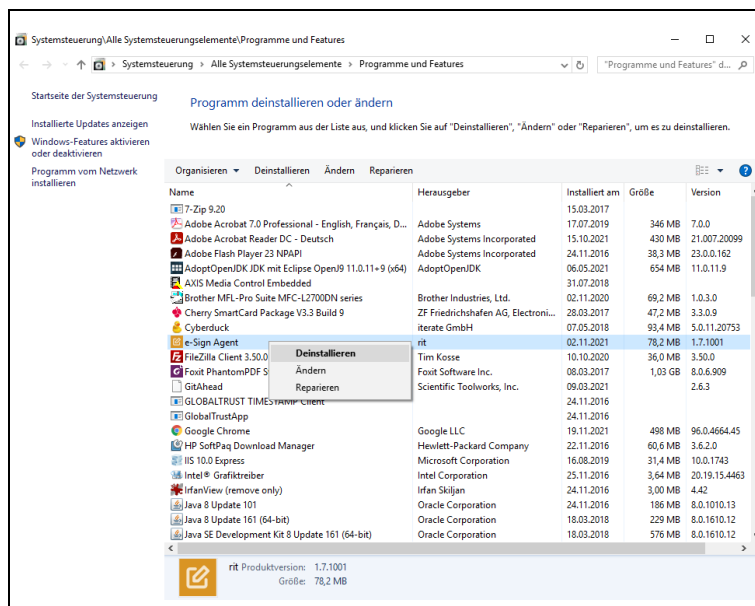


Abbildung 51: Deinstallation e-Sign Agent II

Deinstallieren ➔

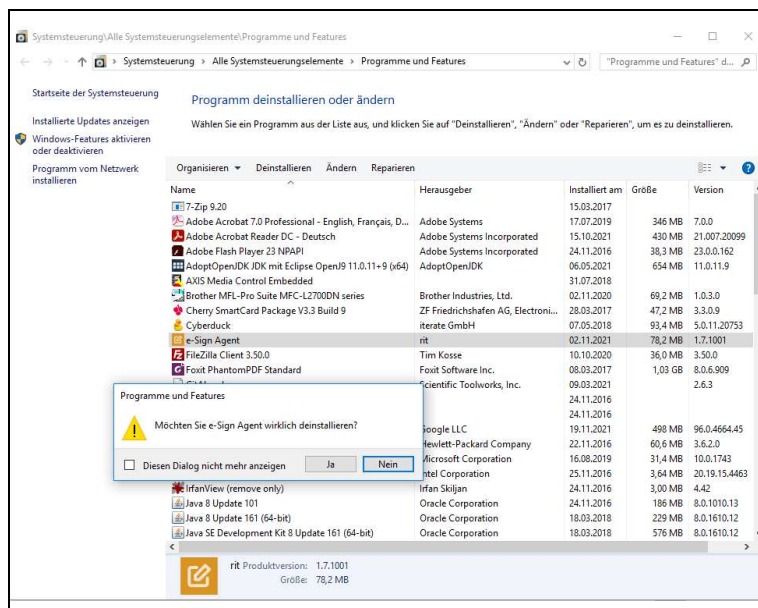


Abbildung 52: Deinstallation e-Sign Agent III

Ja ➔

Anzeige des Deinstallations-Status

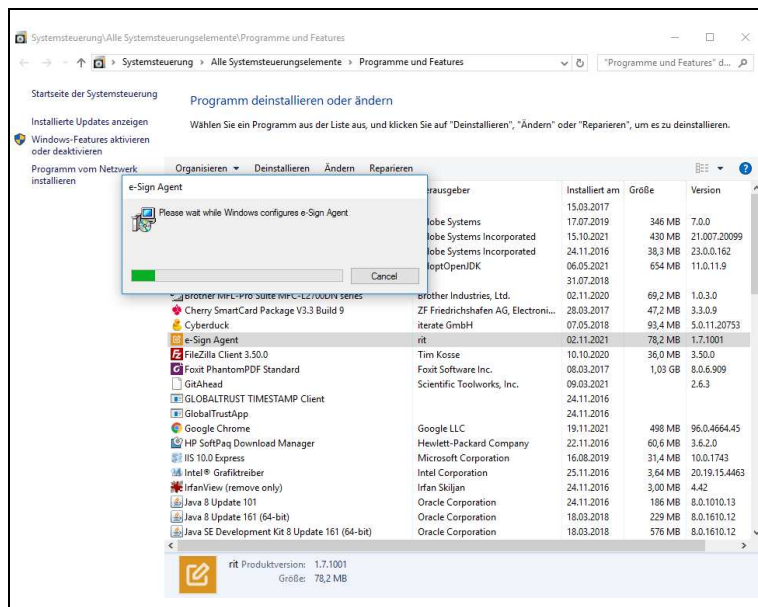


Abbildung 53: Deinstallation e-Sign Agent IV

Danach ist e-Sign Agent deinstalliert.

B) KONFIGURATION E-SIGN AGENT

33

(1) Konfiguration 'Trust2GoServer'

33

Nach Installation prüfen ob URL des Trust2Go-Servers <https://t2g²¹.globaltrust.eu/trust2go> in Konfiguration eingetragen ist.

C:\Program Files (x86)\rit\e-Sign Agent\SignAgentConfig.json

```
{
  "InterfaceSignatureMethods": {},
  "InterfaceConfigurations": {
    "SignatureHTTPS": {
      "Host": "127.0.0.1",
      "Port": 41586,
      "PortRangeLength": 10,
      "AuthorizationType": "None"
    },
    "SignatureHTTP": {
      "Host": "127.0.0.1",
      "Port": 42586,
      "PortRangeLength": 10,
      "AuthorizationType": "None"
    },
    "RKSV": {
      "Host": "127.0.0.1",
      "Port": 43586,
      "PortRangeLength": 10,
      "AuthorizationType": "None"
    }
  },
  "soapUser": "",
  "soapPassword": "",
  "soapCertificateSubject": "",
  "soapCertificateSerial": "",
  "Origins": [
    "*"
  ],
  "CorporateLicense": null,
  "Trust2GoPath": "https://t2gtest.globaltrust.eu/trust2go"
}
```

Eintrag "Trust2GoPath"

- Produktion: "https://t2g.globaltrust.eu/trust2go"
- Test: "https://t2gtest.globaltrust.eu/trust2go"

(2) Konfiguration Logging

33

e-Sign Agent schreibt in folgende Logdatei

\${USERPROFILE}\rit\e-Sign Agent\e-SignAgent.log

C:\Users\admin\rit\e-Sign Agent\e-SignAgent.log

C:\Program Files (x86)\rit\e-Sign Agent\SignAgent.log4net

```
<?xml version="1.0" encoding="utf-8" ?>
<!-- This section contains the log4net configuration settings -->
<log4net>
  <!-- Define some output appenders -->
  <appender name="ConsoleAppender" type="log4net.Appender.ConsoleAppender" >
    <layout type="log4net.Layout.PatternLayout">
      <conversionPattern value="%date [%thread] %-5level %logger - %message%newline" />
    </layout>
  </appender>
```

²¹ im Testbetrieb ist statt **t2g** ⇒ **t2gtest** zu verwenden

```

<appender name="RollingFileAppender" type="log4net.Appender.RollingFileAppender">
  <file value="{$USERPROFILE}\rit\e-Sign Agent\e-SignAgent.log" />
  <appendToFile value="true" />
  <rollingStyle value="Size" />
  <maxSizeRollBackups value="10" />
  <maximumFileSize value="1000KB" />
  <staticLogFileName value="true" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%date [%thread] %-5level %logger - %message%newline" />
  </layout>
</appender>

<!-- Setup the root category, add the appenders and set the default level -->
<root>
  <level value="INFO" />
  <appender-ref ref="ConsoleAppender" />
  <appender-ref ref="RollingFileAppender" />
</root>

<!-- To disable logging -->
<!-- log4net threshold="OFF" /-->

<logger name="SignLib.PdfSignature.WebServer">
  <level value="INFO" />
</logger>

<!--<logger name="SignAgent.pdfViewer">
  <level value="DEBUG" />
</logger>
<logger name="SignAgent.SettingsWindow">
  <level value="DEBUG" />
</logger>-->
</log4net>

```

Muster

C:\Users\admin\rit\e-Sign Agent\e-SignAgent.log

```

2021-09-22 15:49:39,704 [1] INFO SignAgent.App - Starting version 1.7.0.3 (32bit)
2021-09-22 15:49:39,720 [1] INFO SignAgent.App - User: admin, Domain: OFF54, Host: OFF54
2021-09-22 15:49:39,720 [1] INFO SignAgent.App - Argument: C:\temp\testpdf-fuer-trust2go-
vorlage.pdf
2021-09-22 15:49:39,829 [1] INFO SignAgent.Configuration.FileBasedConfiguration - Loading
configuration from C:\Program Files (x86)\rit\e-Sign Agent\SignAgentConfig.json
2021-09-22 15:49:39,986 [1] INFO SignAgent.SettingsWindow - Sign Agent installation dir:
C:\Program Files (x86)\rit\e-Sign Agent\
2021-09-22 15:49:40,736 [1] INFO SignAgent.Pdf.PDFService - Embedded HTTP server started on port
11000
2021-09-22 15:49:41,236 [1] INFO SignAgent.SettingsWindow - Opened HTTPS interface for PDF
Signature on port 41586
2021-09-22 15:49:41,736 [1] INFO SignAgent.SettingsWindow - Opened HTTP interface for PDF
Signature on port 42586
2021-09-22 15:49:41,845 [1] INFO SignAgent.Configuration.FileBasedConfiguration - Loading
configuration from C:\Program Files (x86)\rit\e-Sign Agent\SignAgentConfig.json
2021-09-22 15:49:45,049 [1] INFO SignAgent.Pdf.PdfSignature.PdfViewer - Window closing
2021-09-22 15:56:36,302 [1] INFO SignAgent.App - Activating version 1.7.0.3 (32bit)
2021-09-22 15:56:36,302 [1] INFO SignAgent.App - Argument: C:\temp\testpdf-fuer-trust2go-
vorlage.pdf
2021-09-22 15:56:36,302 [1] INFO SignAgent.Configuration.FileBasedConfiguration - Loading
configuration from C:\Program Files (x86)\rit\e-Sign Agent\SignAgentConfig.json
...

```

c) ANZEIGE VERSION E-SIGN AGENT

35

erfolgt über die Taskleiste (e-Sign Agent muss gestartet sein)

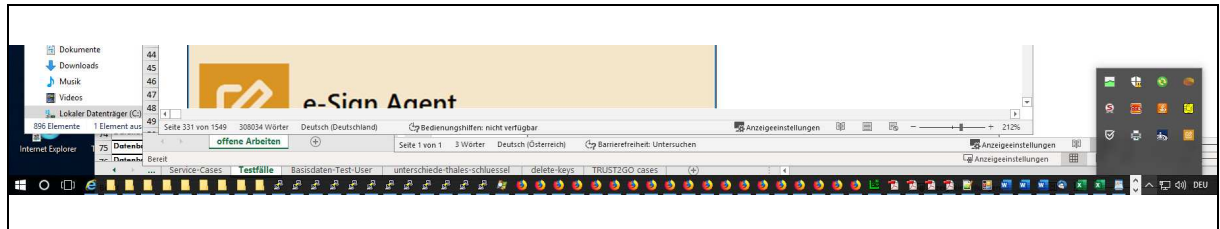


Abbildung 54: Anzeige Version e-Sign Agent I

Taskleiste ⇒  e-Sign Agent ⇒ Eigenschaften ⇒



Abbildung 55: Anzeige Version e-Sign Agent II

Hinweis

e-Sign Agent MUSS zumindest in der Version 1.9.7 installiert sein!

9 [ERSTREGAUTHAPP] (ERST)REGISTRIERUNG 'TRUST2GOAUTHAPP' - INKLUSIVE
AKTIVIERUNG QRSCD PRIVATE KEY

36

Voraussetzung

Die 'Trust2GoAuthApp' wurde aus dem Apple- oder Google-Store erfolgreich downgeloadet und installiert.

Warnung!

Im Zuge der Registrierung/Aktivierung müssen Sie einen AktivierungsPIN vergeben. Bewahren Sie diesen AktivierungsPIN gut auf. Er wird bei jeder Signatur verlangt und ist NUR Ihnen bekannt. Geht er verloren, muss ein neues Zertifikat - kostenpflichtig - ausgestellt werden.

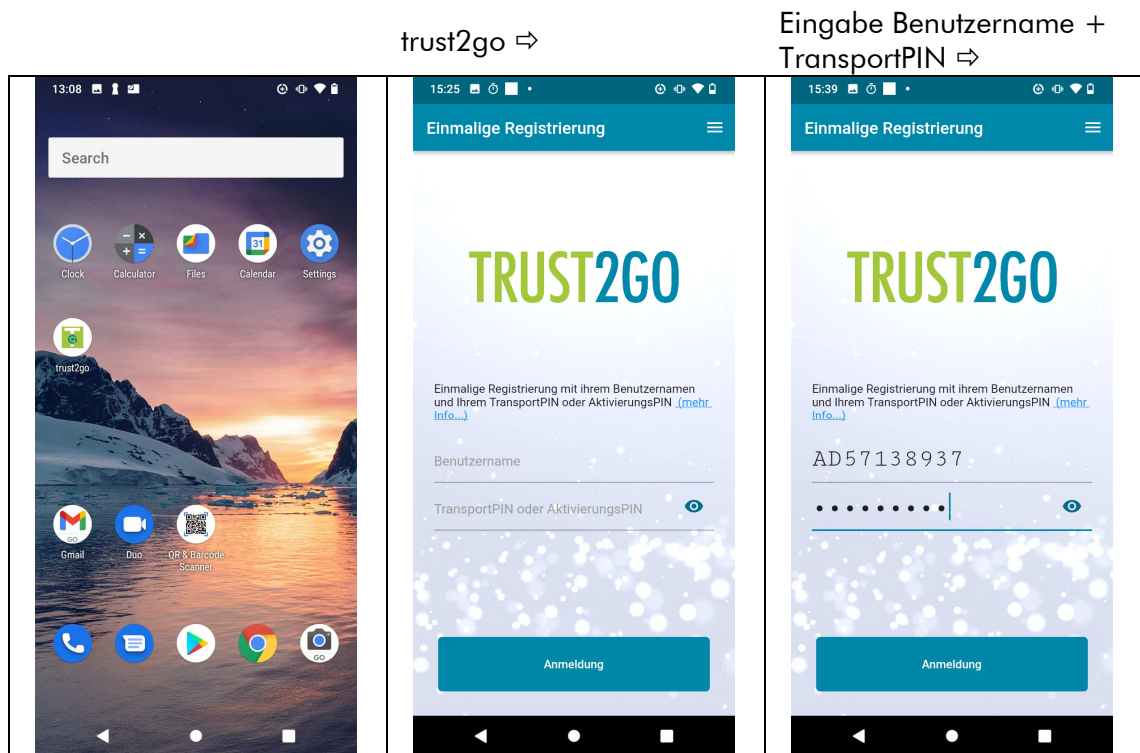


Abbildung 56: ErstRegistrierung AuthenticationApp I

"Ich stimme zu" ⇨

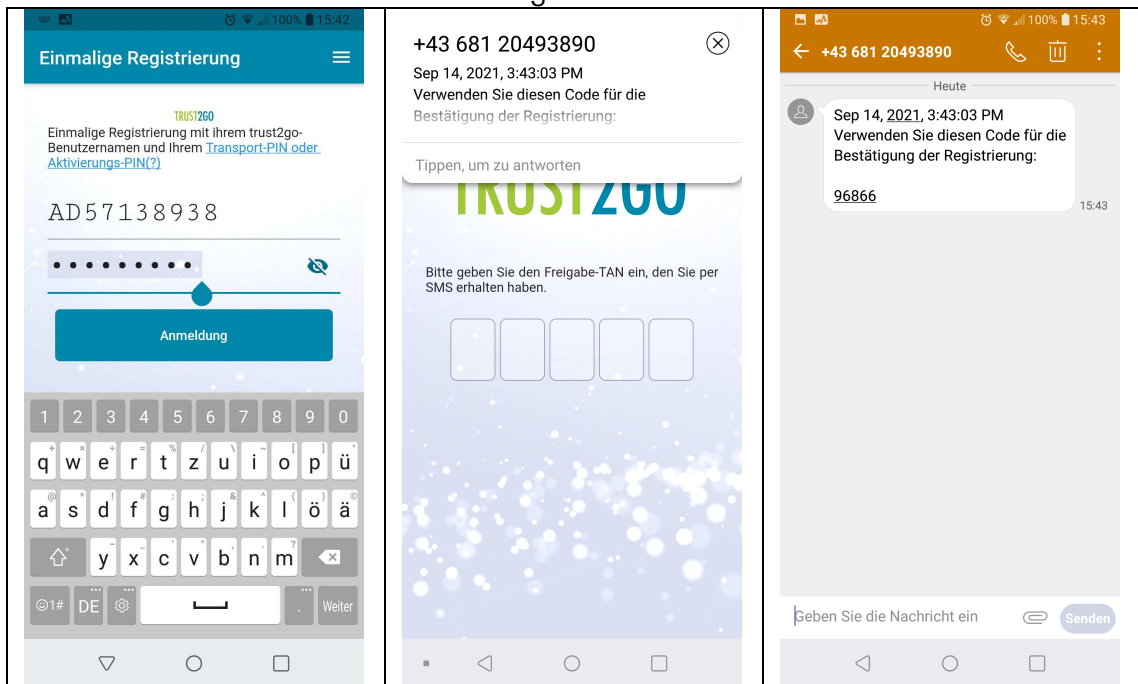
Signatordaten eingeben
Anmeldung ⇨Bestätigungscode in SMS-
Postfach abrufen ⇨

Abbildung 57: ErstRegistrierung AuthenticationApp II

Bestätigungscode
eingeben ⇨

AktivierungsPIN eingeben
und **merken** (min. 8
Stellen, Groß-
/Kleinschreibung + Ziffer
+ Sonderzeichen) ⇨

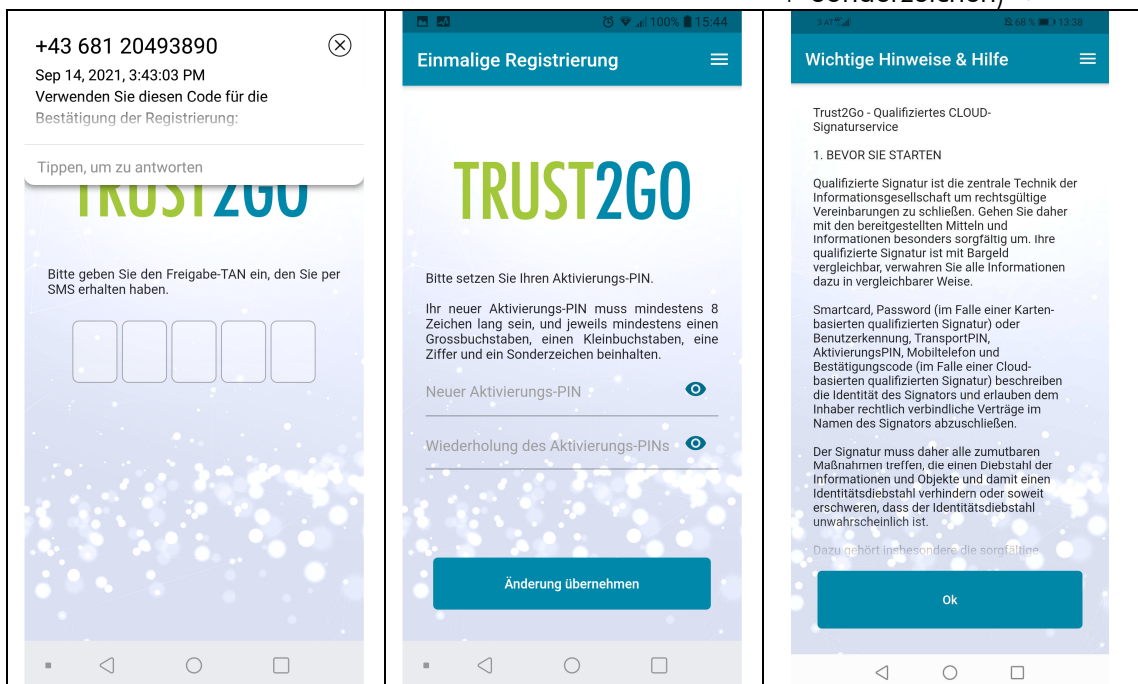


Abbildung 58: ErstRegistrierung AuthenticationApp III

OK ⇒

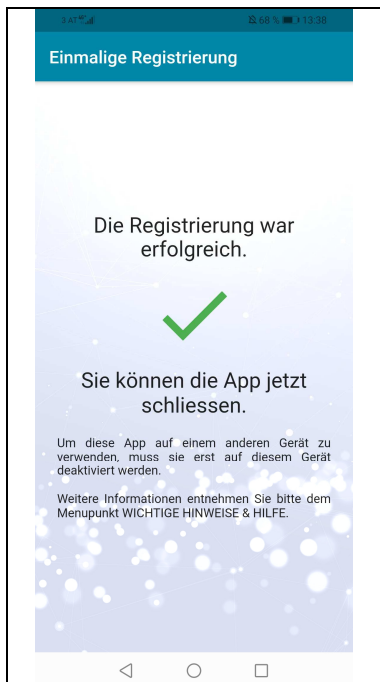


Abbildung 59: ErstRegistrierung AuthenticationApp IV

Ist ein ⇒ Signator registriert werden nach Start der 'Trust2GoAuthApp' in Abständen von mehreren Sekunden offene Signaturanfragen abgefragt. Weiters werden ab diesem Zeitpunkt automatisiert Änderungen der technischen Daten des Smartphones (zB Änderungen der Betriebssystemversion) an ⇒ Server Signing Application (SSA) übermittelt.

10 [ERSTREGAUTHWEB] (ERST)REGISTRIERUNG 'TRUST2GOWEB' - INKLUSIVE
AKTIVIERUNG QRSCD PRIVATE KEY

39

<https://t2g²².globaltrust.eu/trust2go/public/index.html>

Warnung!

Im Zuge der Registrierung/Aktivierung müssen Sie einen AktivierungsPIN vergeben. Bewahren Sie diesen AktivierungsPIN gut auf. Er wird bei jeder Signatur verlangt und ist NUR Ihnen bekannt. Geht er verloren, muss ein neues Zertifikat - kostenpflichtig - ausgestellt werden.

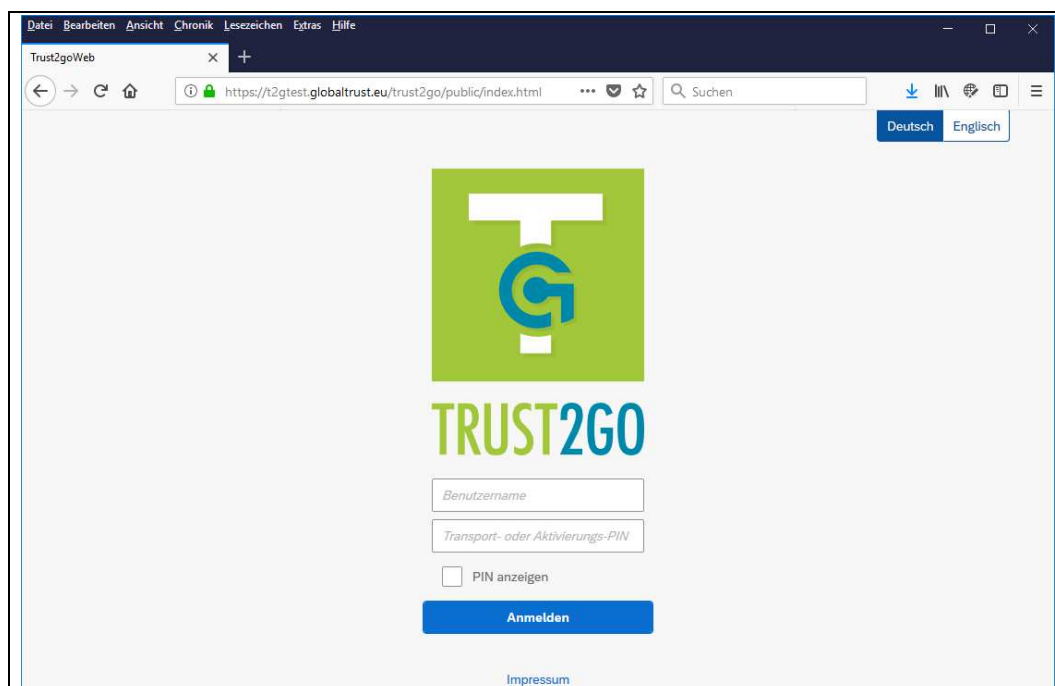


Abbildung 60: ErstRegistrierung WebService I

bei Erstregistrierung

Benutzername und **TransportPIN** laut Vertragsunterlagen eintragen

bei späteren Anmeldungen

Benutzername und **AktivierungsPIN** eintragen

²² NUR im Testbetrieb ist statt **t2g** ⇒ **t2gtest** zu verwenden

Anmelden ⇨

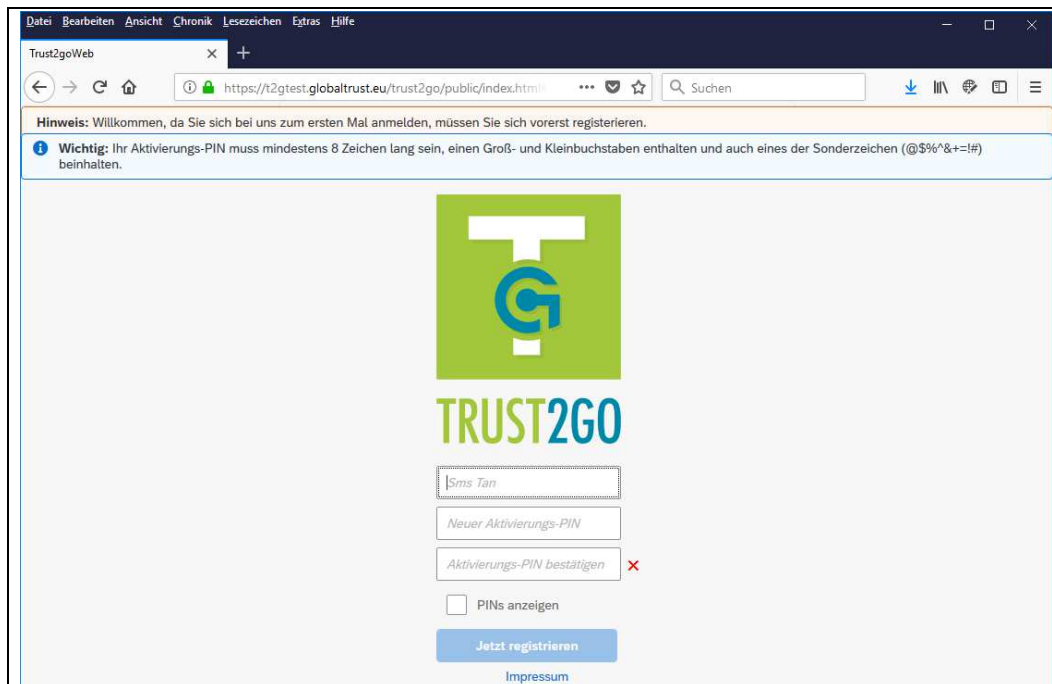


Abbildung 61: ErstRegistrierung Webservice II

SMS kommt auf zugewiesene Telefonnummer

Zulässige Zeichen ⇨ AktivierungsPIN:

Der ⇨ AktivierungsPIN muss mindestens 8 Zeichen lang sein, einen Groß- und Kleinbuchstaben enthalten und auch eines der Sonderzeichen (^ ° ! \$ % & / () = ? @) beinhalten.

Jetzt registrieren ⇒

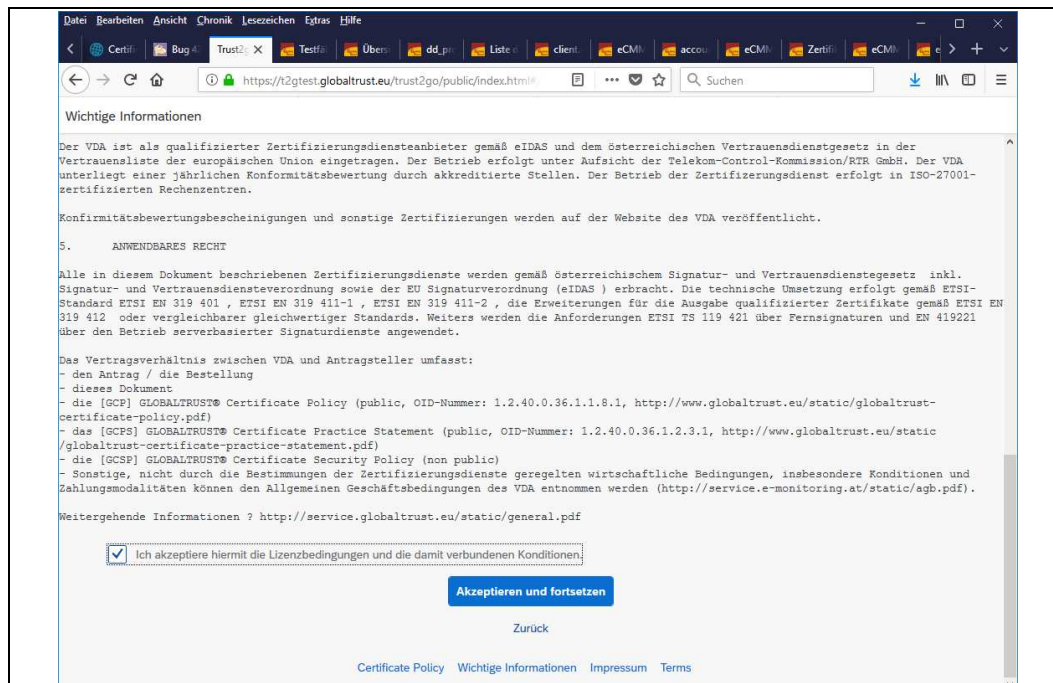


Abbildung 62: ErstRegistrierung WebService III

Zustimmen Lizenzbedingen ⇒ Akzeptieren und fortsetzen ⇒

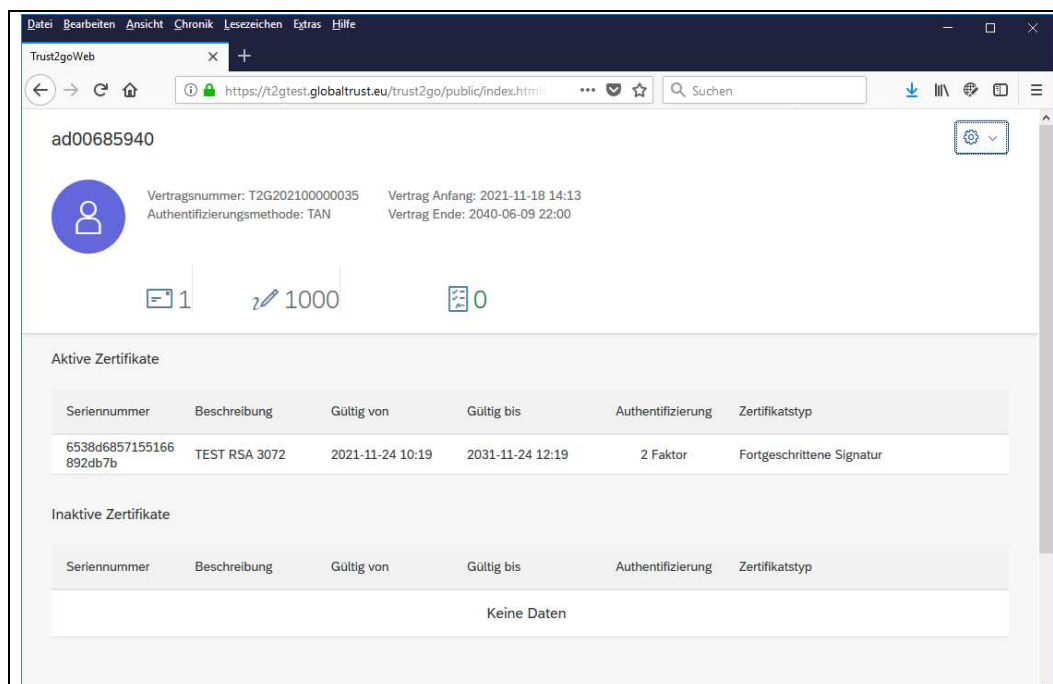


Abbildung 63: ErstRegistrierung WebService IV

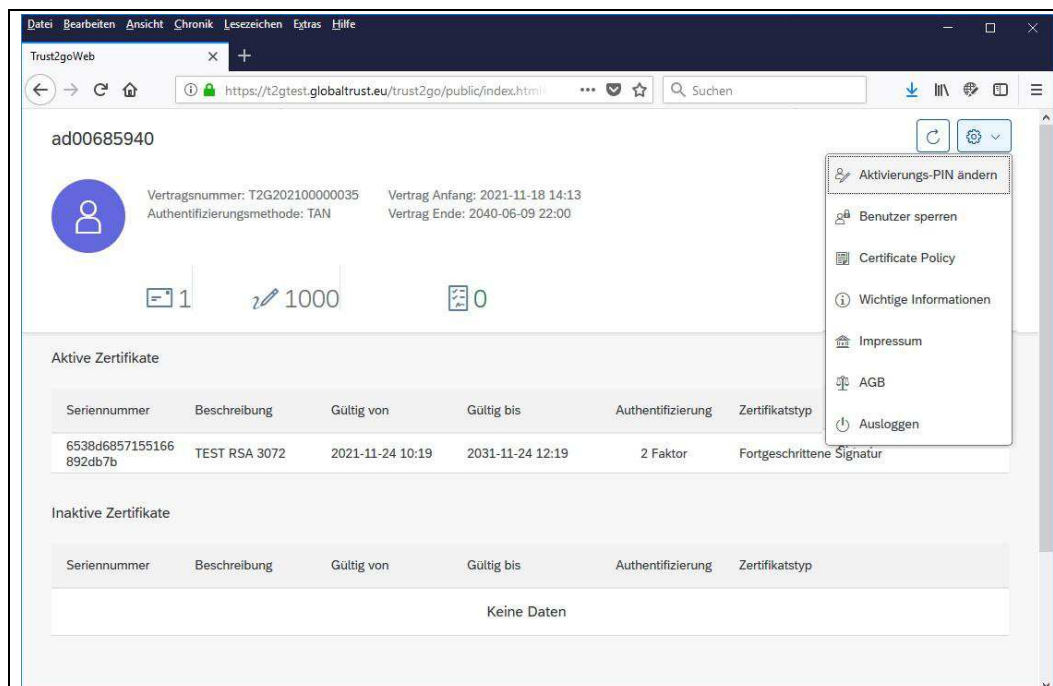
  [Zahnrad] ⇨

Abbildung 64: Erstregistrierung WebService V

Ausloggen ⇨

11 [UPDATEAUTHAPP] UPDATE 'TRUST2GOAUTHAPP'

43

Download des App-Updates folgt grundsätzlich dem Ablauf der Erst-Installation:

- ⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android (p119) oder
- ⇒ 7 [KompApplos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS (p120)

Das Update erfolgt gemäß den Vorgaben des jeweiligen Betriebssystems. Nach Update steht die neue Version zur Verfügung, es sind keine Trust2Go-spezifischen Schritte (Aktivierungen, Registrierungen, ...) erforderlich.

12 [AENDAKTPINAPP] ÄNDERUNG AKTIVIERUNGSPIN MIT 'TRUST2GOAUTHAPP'

44

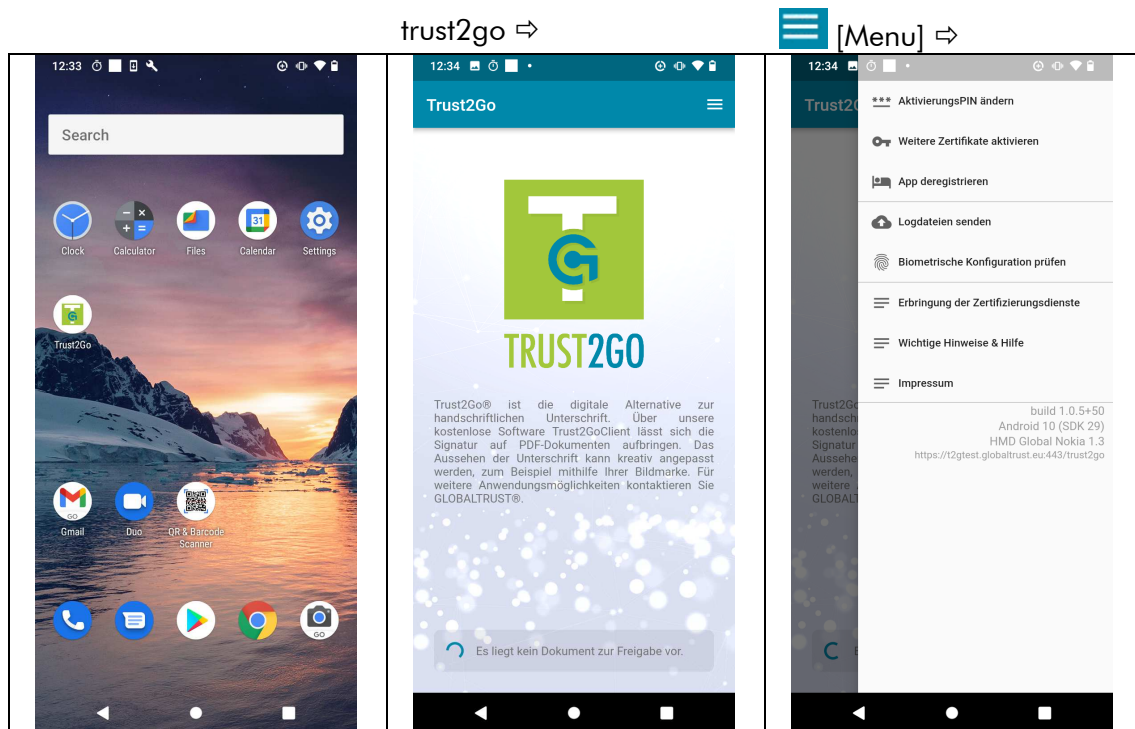


Abbildung 65: Änderung AktivierungsPIN I

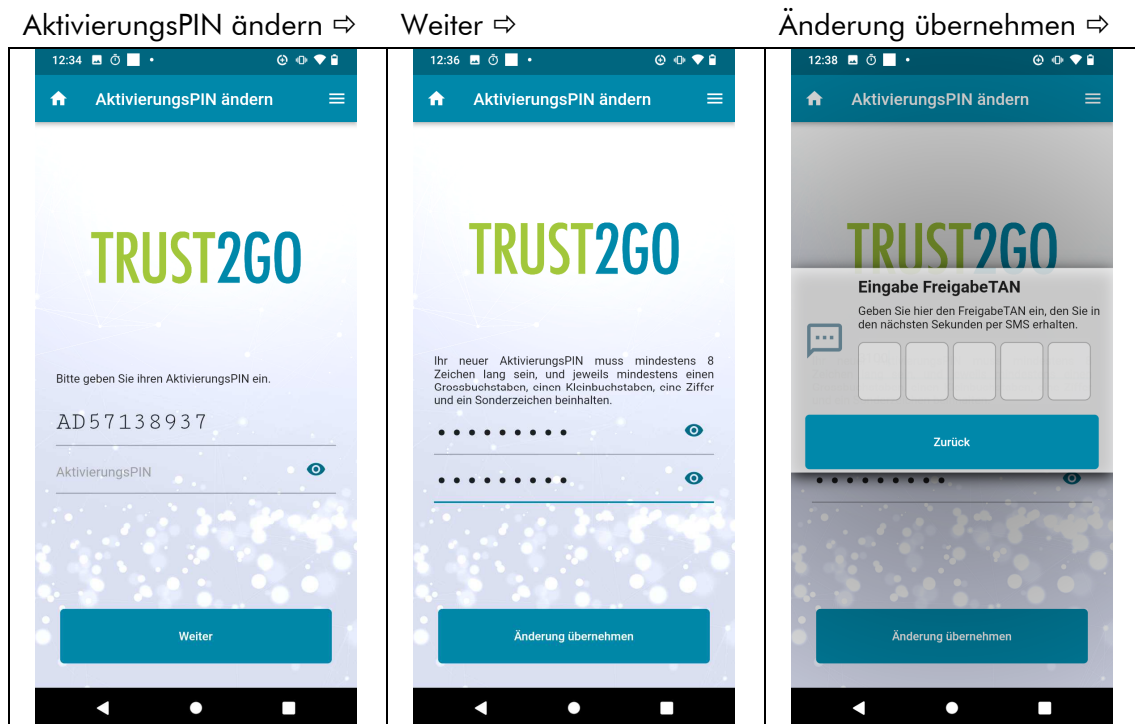


Abbildung 66: Änderung AktivierungsPIN II

per SMS erhaltenen
FreigabeTAN eingeben ⇒

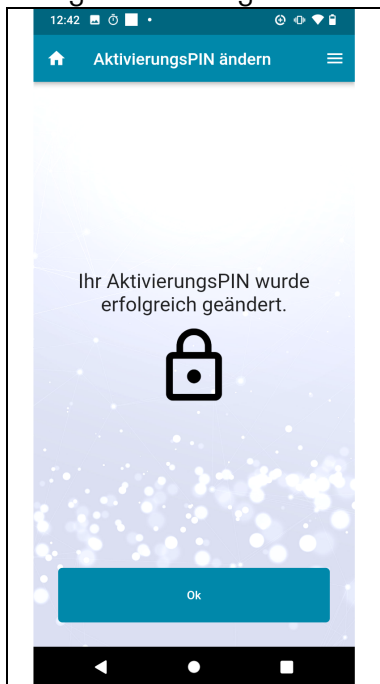
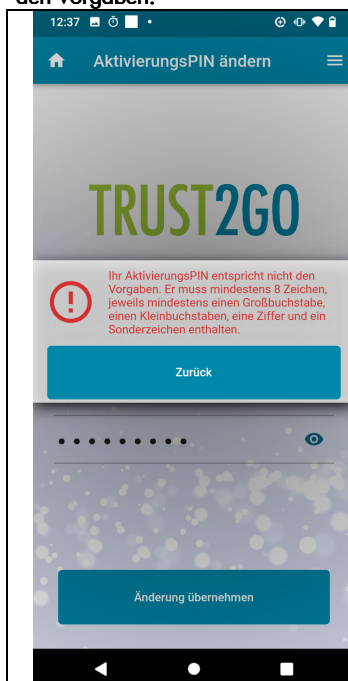


Abbildung 67: Änderung AktivierungsPIN III

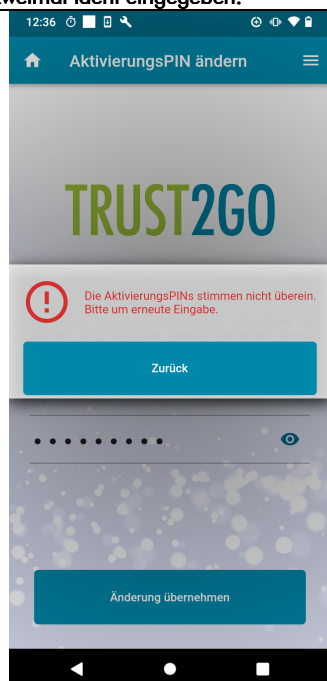
OK ⇒

Typische Fehlermeldungen

Neuer AktivierungsPIN entspricht nicht den Vorgaben.



Neuer AktivierungsPIN wurde nicht zweimal ident eingegeben.



Der per SMS übermittelte TAN wurde nicht korrekt eingegeben.

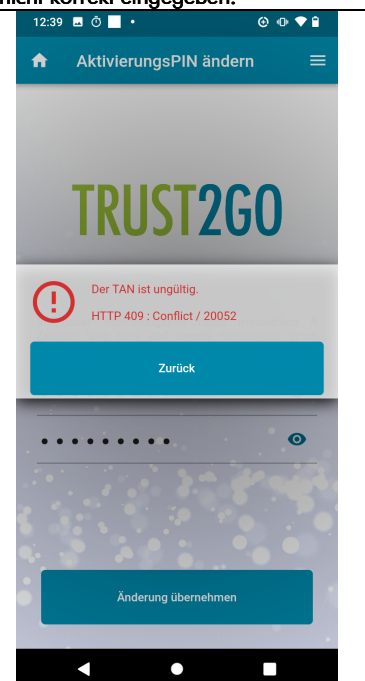


Abbildung 68: Änderung AktivierungsPIN - Fehlermeldungen

II	Dienst			A	DIENST-12 - "Trust2Go"
		3		[T2G-DOK3] Signator-Dokumentation	
					Trust2Go

In jedem Fehlerfall bleibt der bisherige AktivierungsPIN erhalten, die Änderung muss wiederholt werden.

Hinweis

Zertifikate, die noch nicht aktiviert wurden müssen mit dem übermittelten TransportPIN aktiviert werden. Sie sind von der Änderung des AktivierungsPINs nicht betroffen.

13 [AENDAKTPINWEB] ÄNDERUNG AKTIVIERUNGSPIN MITTELS 'TRUST2GoWEB' 47

<https://t2g²³.globaltrust.eu/trust2go/public/index.html>

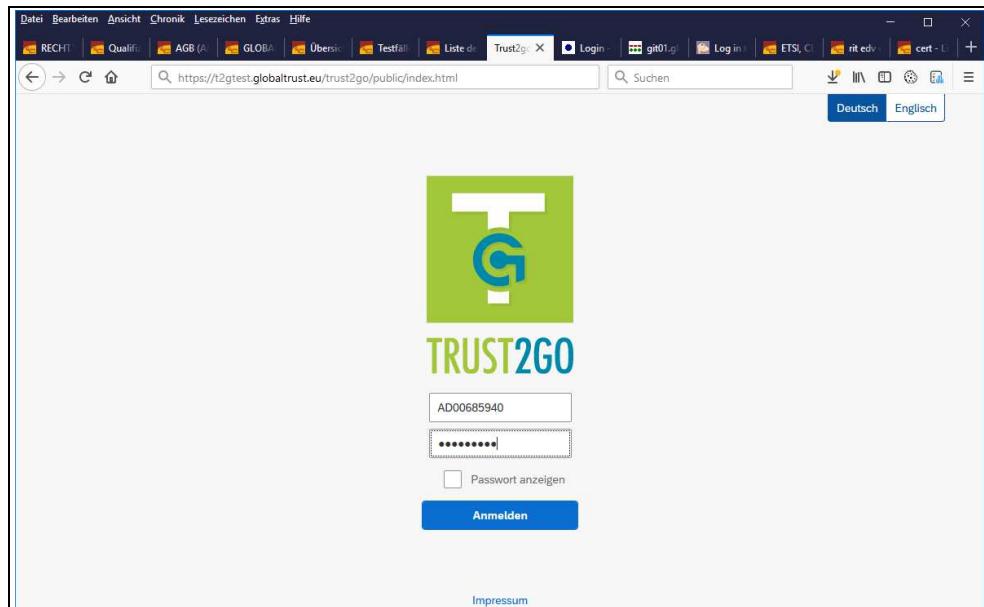


Abbildung 69: Änderung AktivierungSPIN Web I

Anmelden ⇒  [Zahnrad] ⇒

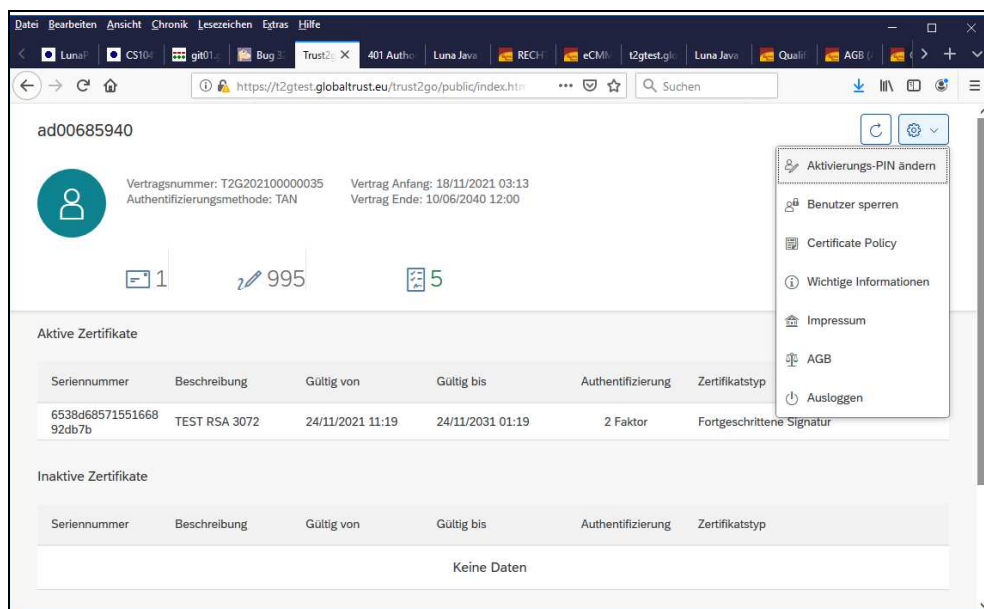


Abbildung 70: Änderung AktivierungSPIN Web II

²³ im Testbetrieb ist statt **t2g** ⇒ **t2gtest** zu verwenden

TransportPIN ändern ⇨

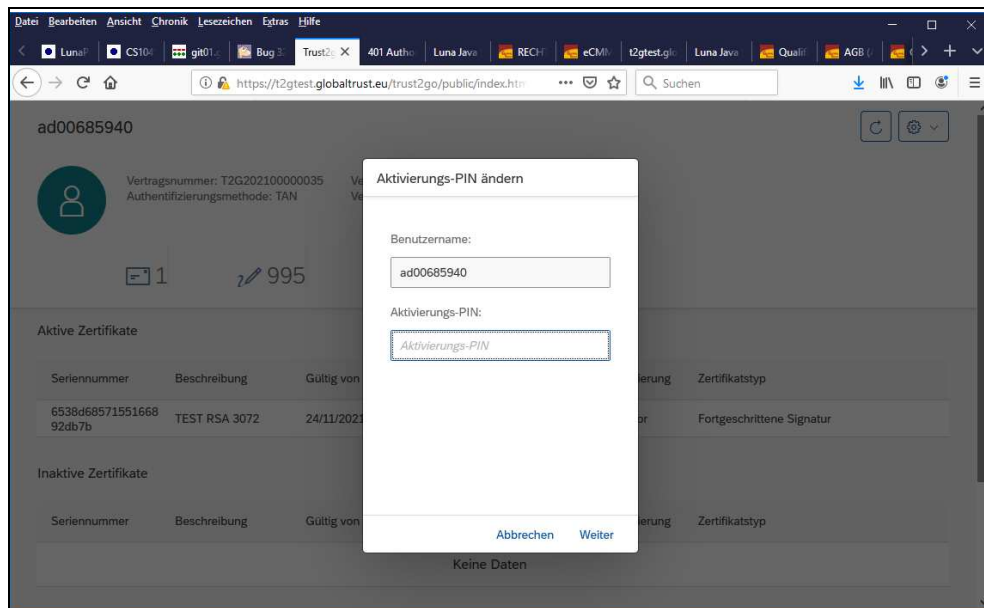


Abbildung 71: Änderung AktivierungsPIN Web III

Eingabe bisheriger AktivierungsPIN ⇨ Weiter ⇨

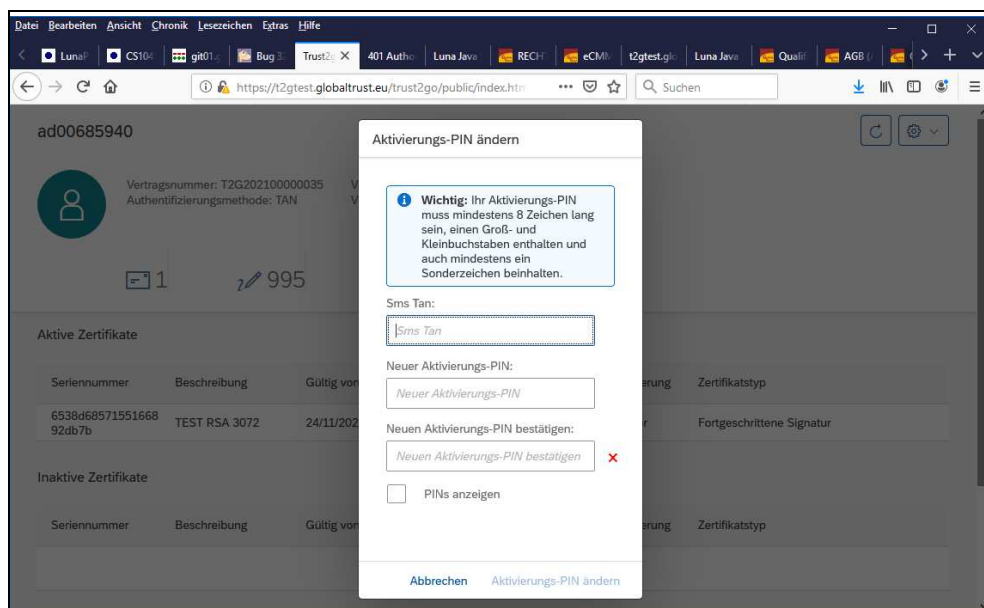


Abbildung 72: Änderung AktivierungsPIN Web IV

SMS + neuen AktivierungsPIN eingeben ⇒ AktivierungsPIN ändern ⇒

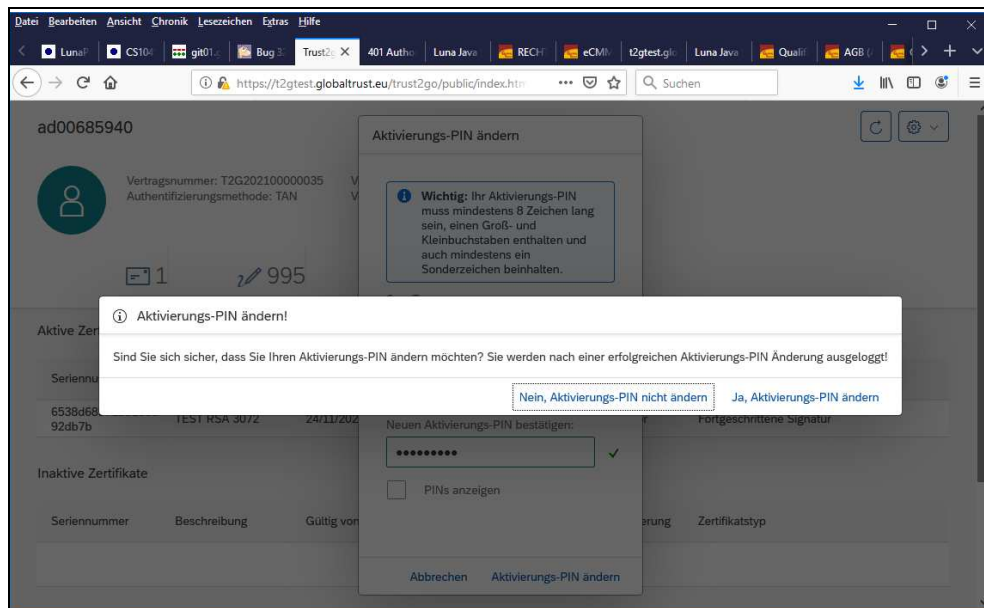


Abbildung 73: Änderung AktivierungsPIN Web V

Ja, AktivierungsPIN ändern ⇒

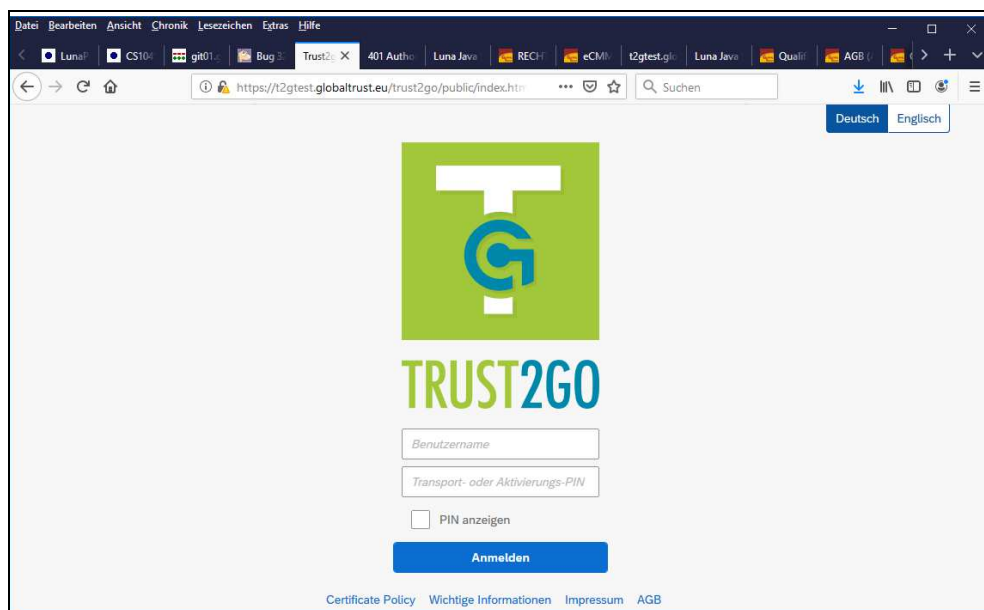


Abbildung 74: Änderung AktivierungsPIN Web VI

Anschließend ist die Neuanmeldung mit dem neuen ⇒ AktivierungsPIN möglich.

14 [AKTWEITPRIVKEYAPP] AKTIVIERUNG WEITERES ZERTIFIKAT(PRIVATE KEY) MITTELS
'TRUST2GOAUTHAPP'

50

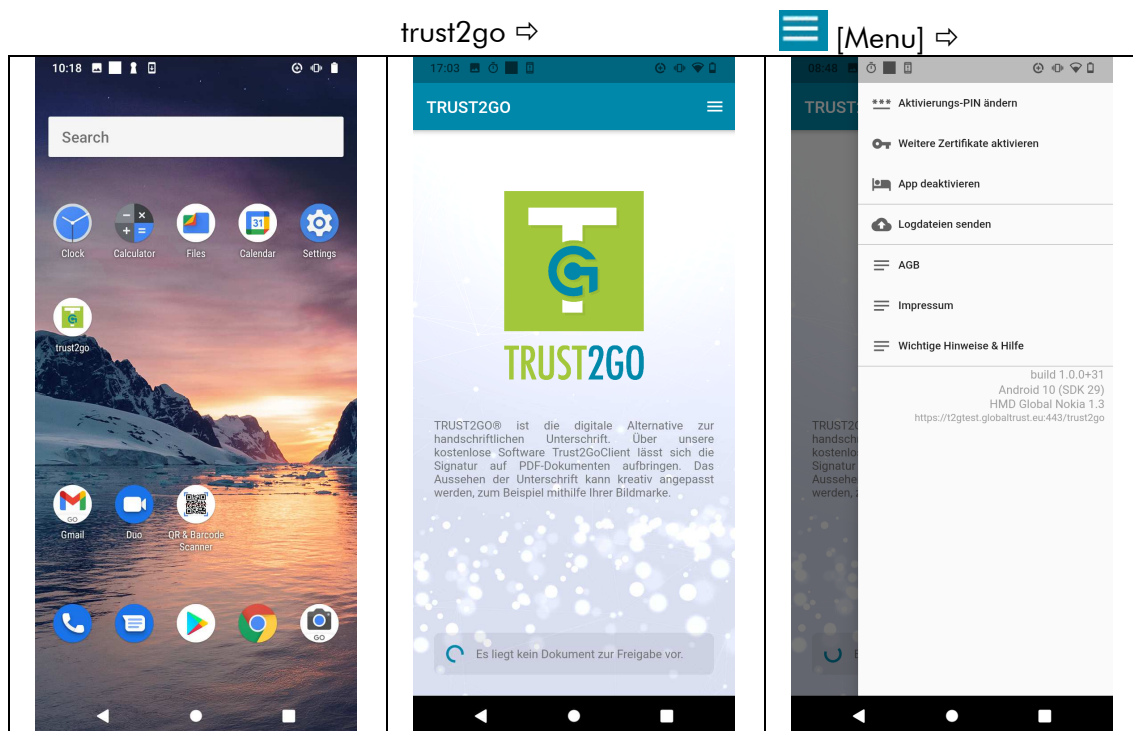


Abbildung 75: Aktivierung weiterer Private Key 'Trust2GoAuthApp' I

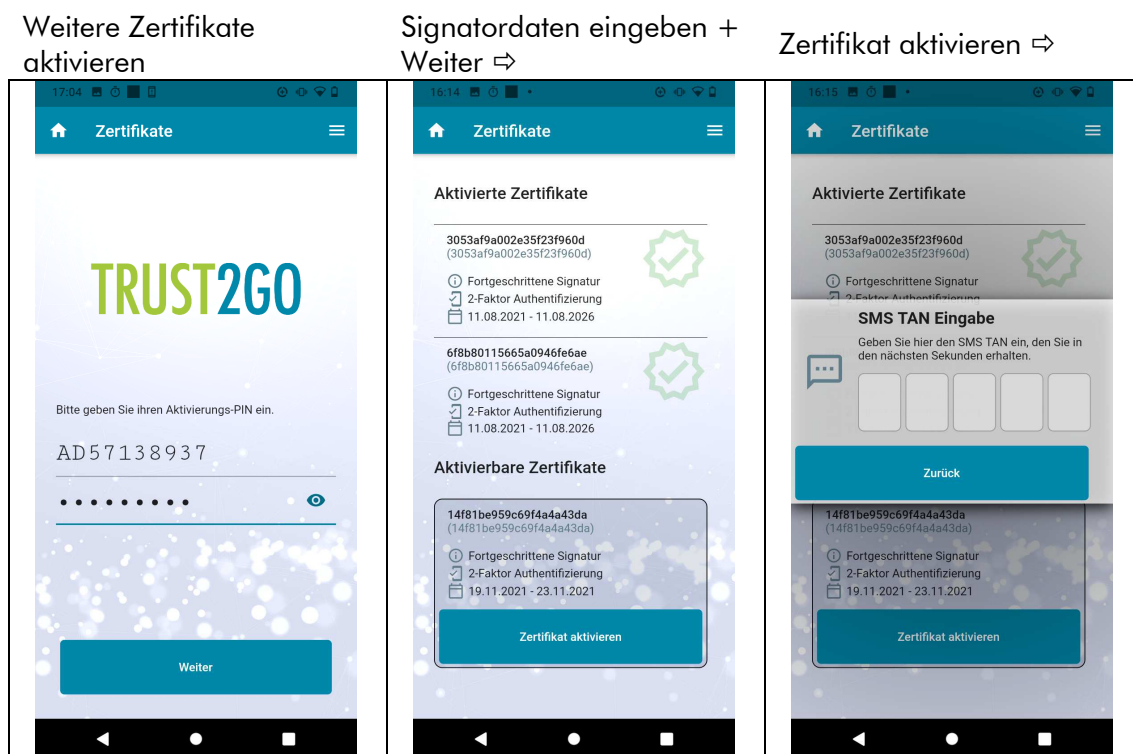


Abbildung 76: Aktivierung weiterer Private Key 'Trust2GoAuthApp' II

SMS TAN eingeben ⇨

TransportPIN des neuen
Zertifikats eingeben ⇨

Zertifikat aktivieren ⇨

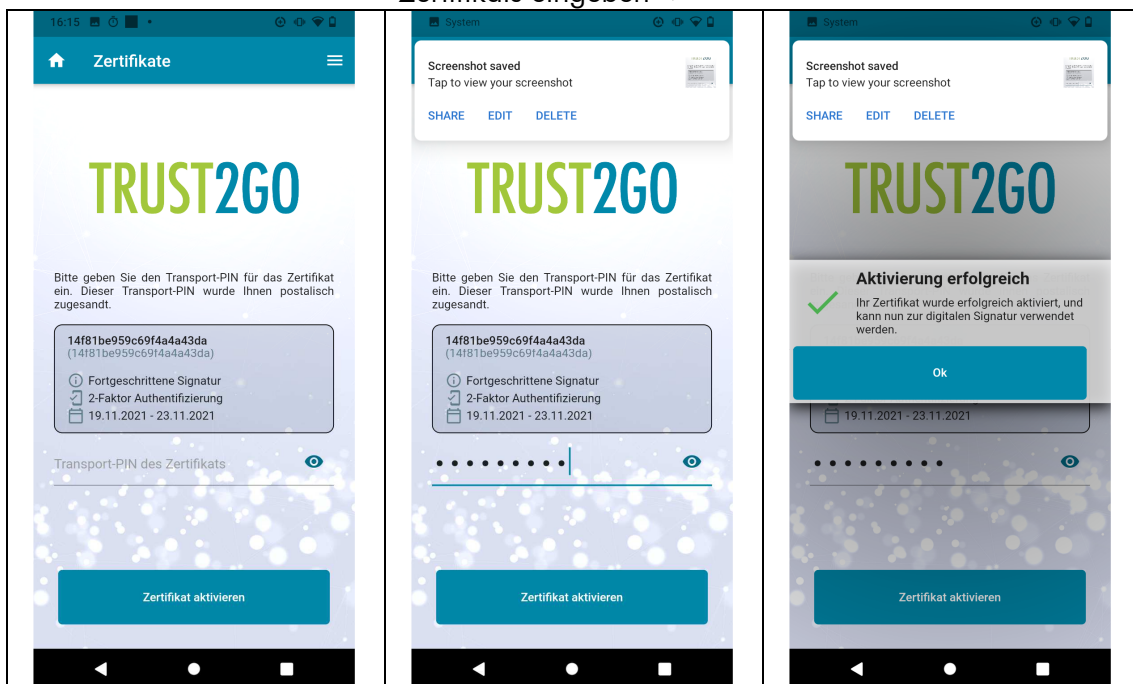


Abbildung 77: Aktivierung weiterer Private Key 'Trust2GoAuthApp' III

OK ⇨



Abbildung 78: Aktivierung weiterer Private Key 'Trust2GoAuthApp' IV

15 [AKTWEITPRIVKEYWEB] AKTIVIERUNG WEITEREN PRIVATE KEY MITTELS
'TRUST2GOWEB'

52

<https://t2g²⁴.globaltrust.eu/trust2go/public/index.html>

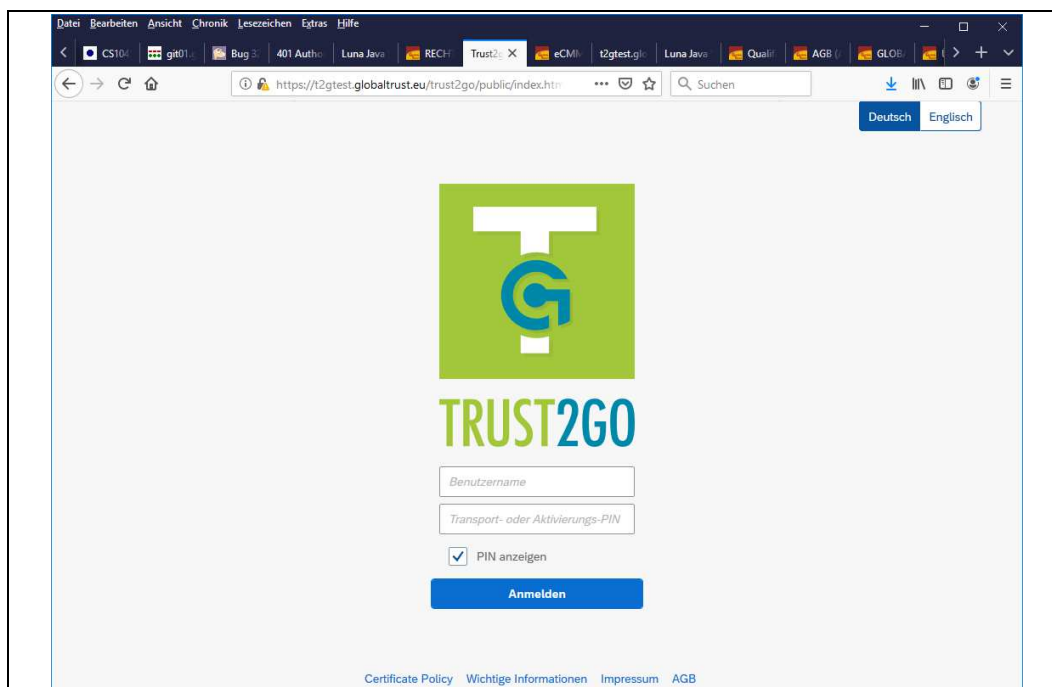


Abbildung 79: Aktivierung weiterer Private Key Web I

Eingabe Benutzername + AktivierungsPIN ⇒ Anmelden ⇒

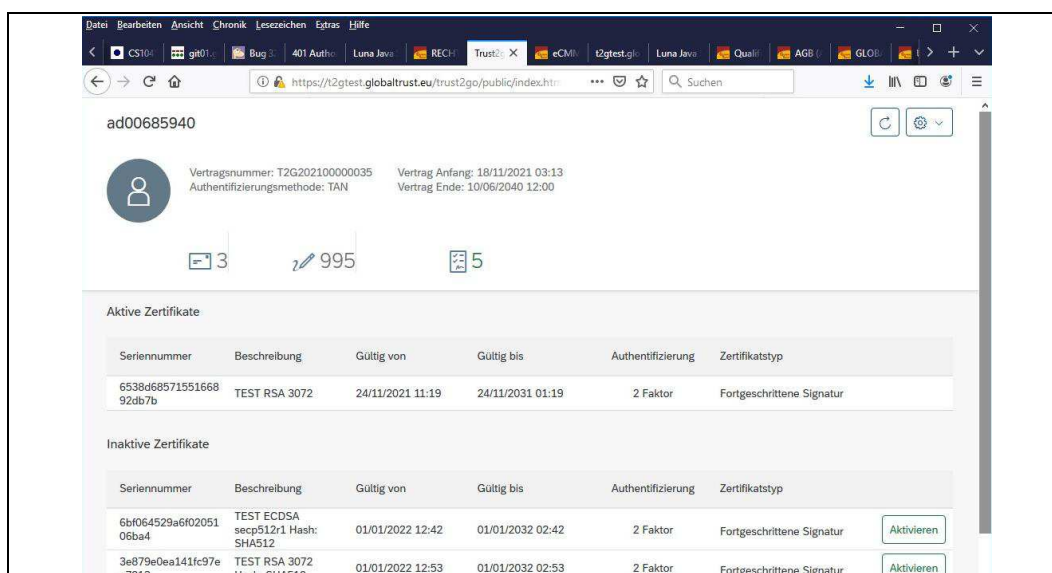


Abbildung 80: Aktivierung weiterer Private Key Web II

²⁴ im Testbetrieb ist statt **t2g** ⇒ **t2gtest** zu verwenden

Aktivieren ⇒

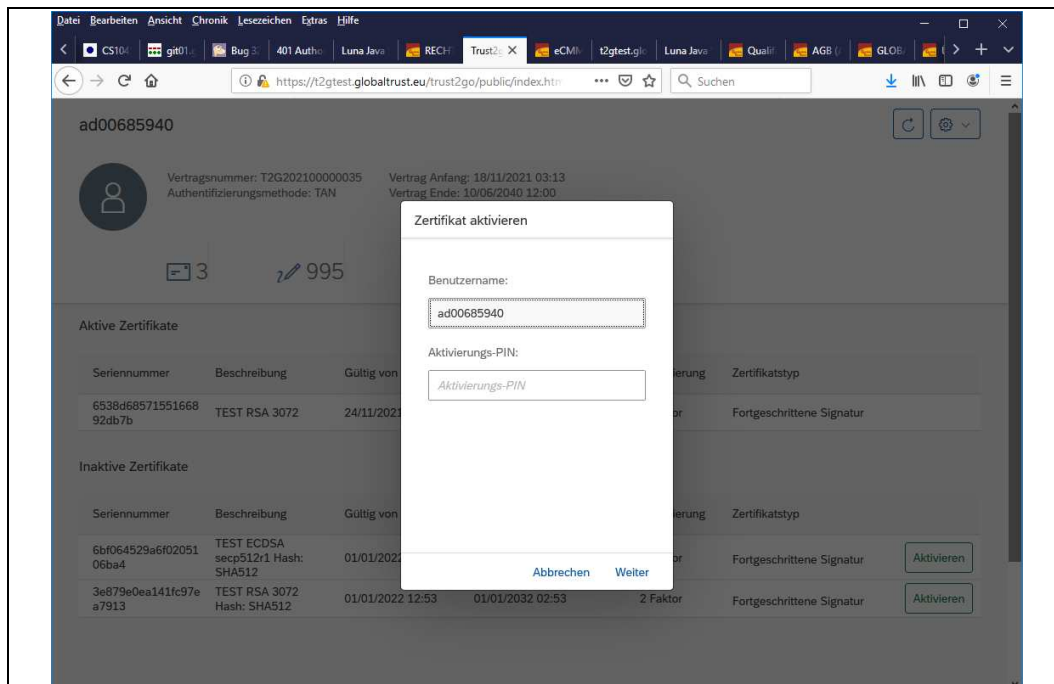


Abbildung 81: Aktivierung weiterer Private Key Web III

bestehenden AktivierungsPIN eingeben ⇒ Weiter ⇒

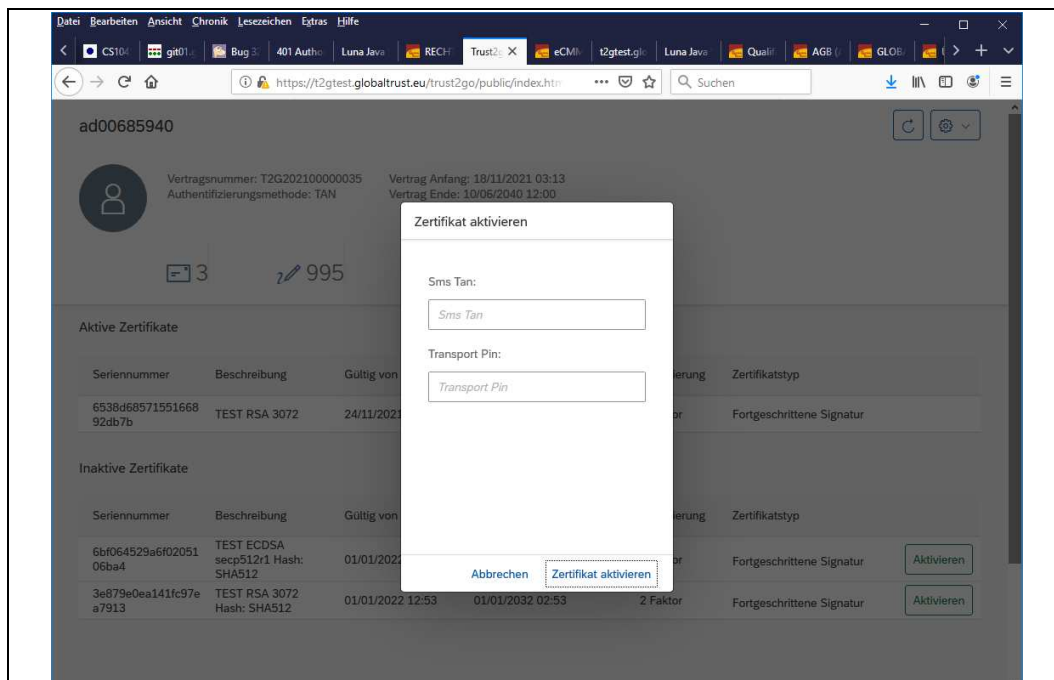


Abbildung 82: Aktivierung weiterer Private Key Web IV

SMSTan + TransportPIN des neuen Zertifikates ⇒ Zertifikat aktivieren ⇒

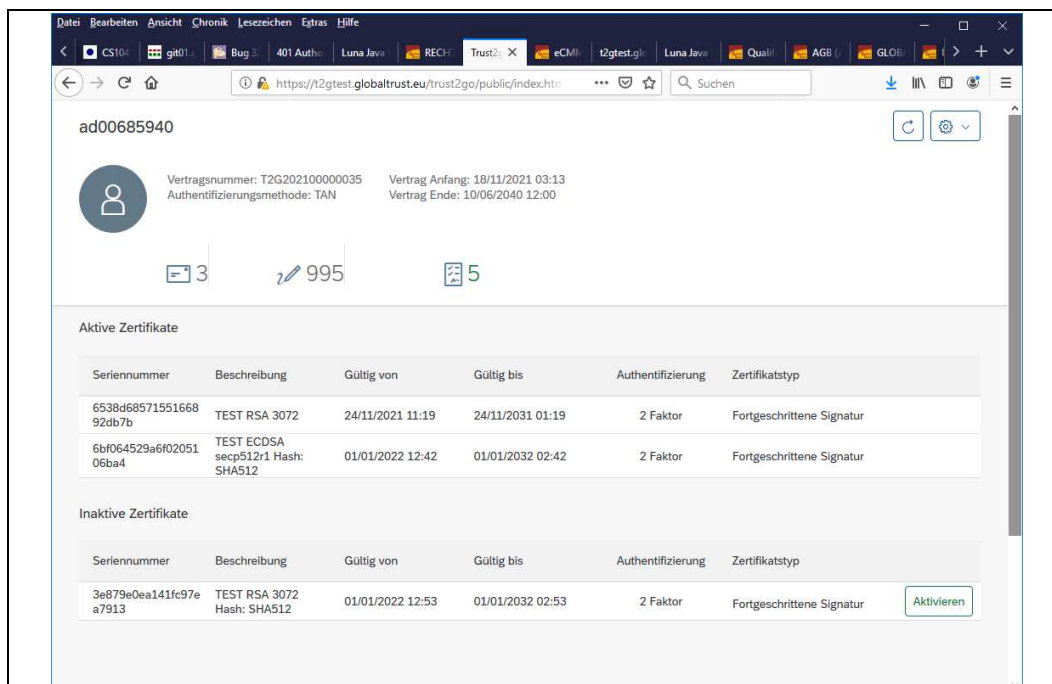



Abbildung 83: Aktivierung weiterer Private Key Web V

Im Anschluss können weitere Zertifikate aktiviert werden oder

 [Zahnrad] ⇒ Ausloggen ⇒

16 [ERSTQUALSIG] ERSTELLEN QUALIFIZIERTE SIGNATUR

55

A) ERSTELLEN QUALIFIZIERTE SIGNATUR IN PDF MITTELS 'TRUST2GOCLIENT' (E-SIGN AGENT) +
'TRUST2GOAUTHAPP'

55

Hinweis!

Dieser Ablauf ist bei fortgeschrittener Signatur mit 2-Faktor-Authentisierung ident.

Erforderliche Komponente(n) - Client

- Installation 'Trust2GoAuthApp':
 - ⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android (p119) **alternativ**
 - ⇒ 7 [KompAppIos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS (p120)
- Installation 'Trust2GoClient':
 - ⇒ 8 [KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent) (p125)

pdf-Datei ⇒ (Rechte Maustaste) ⇒ Öffnen mit ⇒

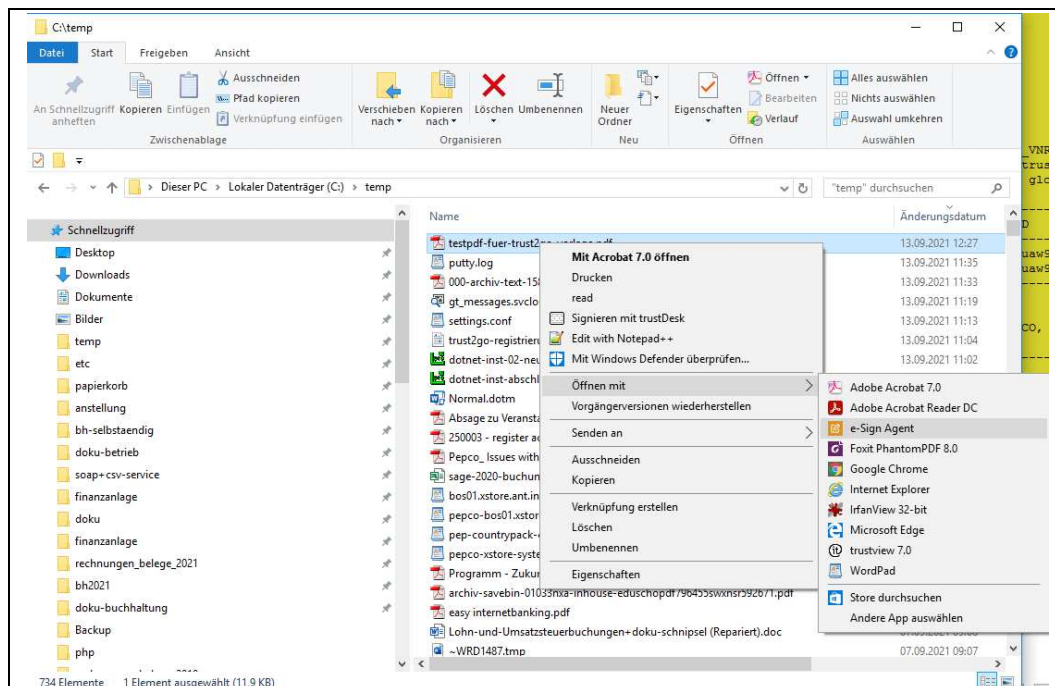


Abbildung 84: App-Signatur I - Dateiauswahl

e-Sign Agent ⇒ Trust2Go (im Feld "Unterschreiben mit:") auswählen ⇒

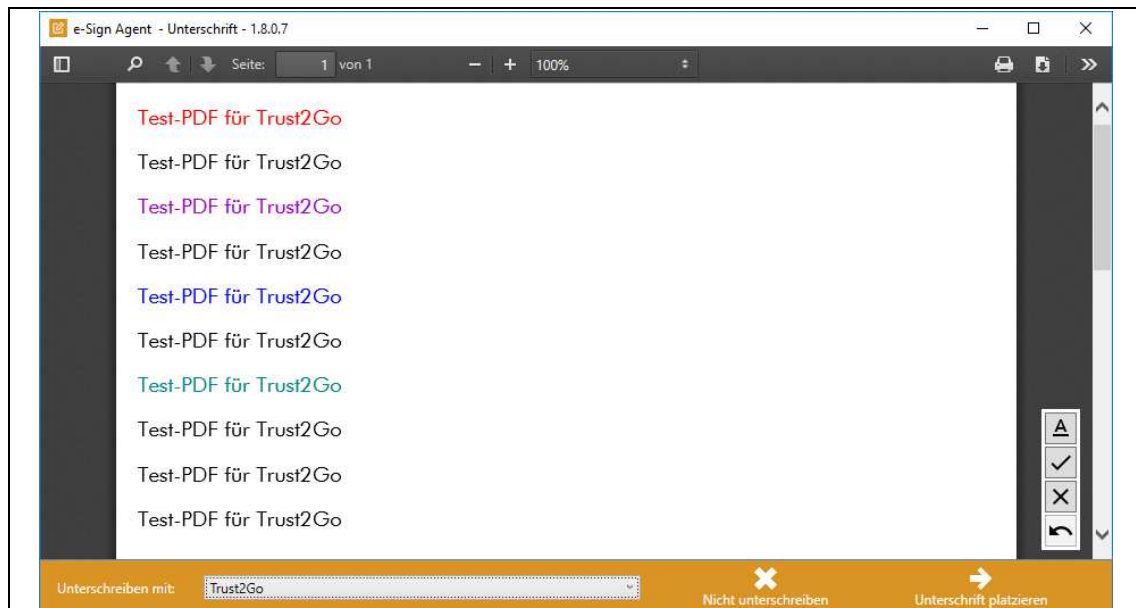


Abbildung 85: App-Signatur II - Serviceauswahl Trust2Go

Unterschreiben mit: Trust2GO ⇒ Unterschrift platzieren ⇒

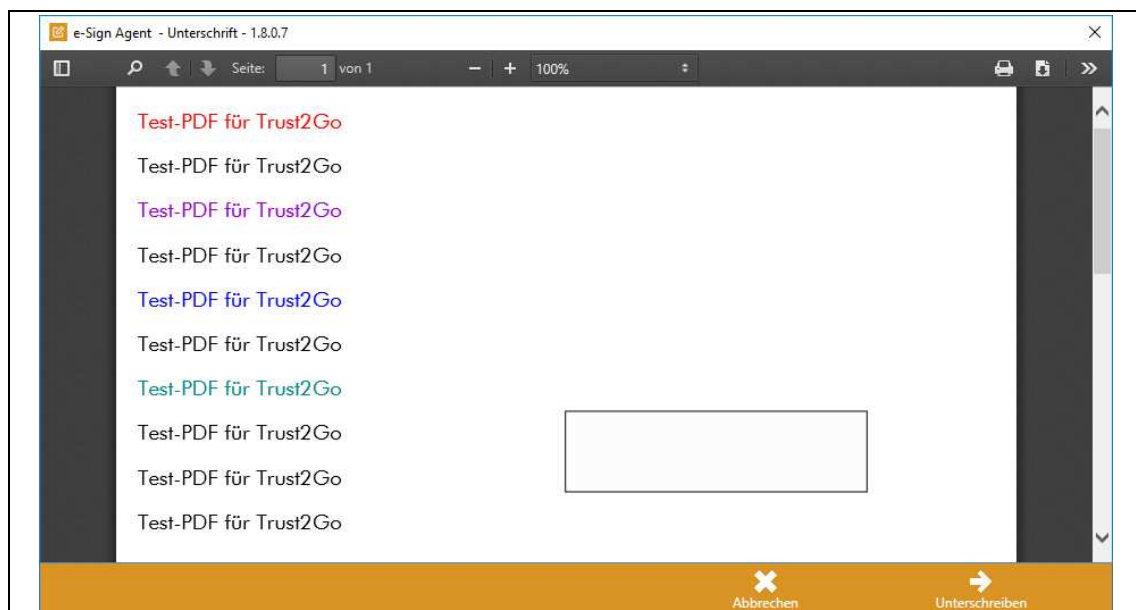


Abbildung 86: App-Signatur III - Unterschriftsfeld platzieren

Rechteck verschieben ⇨

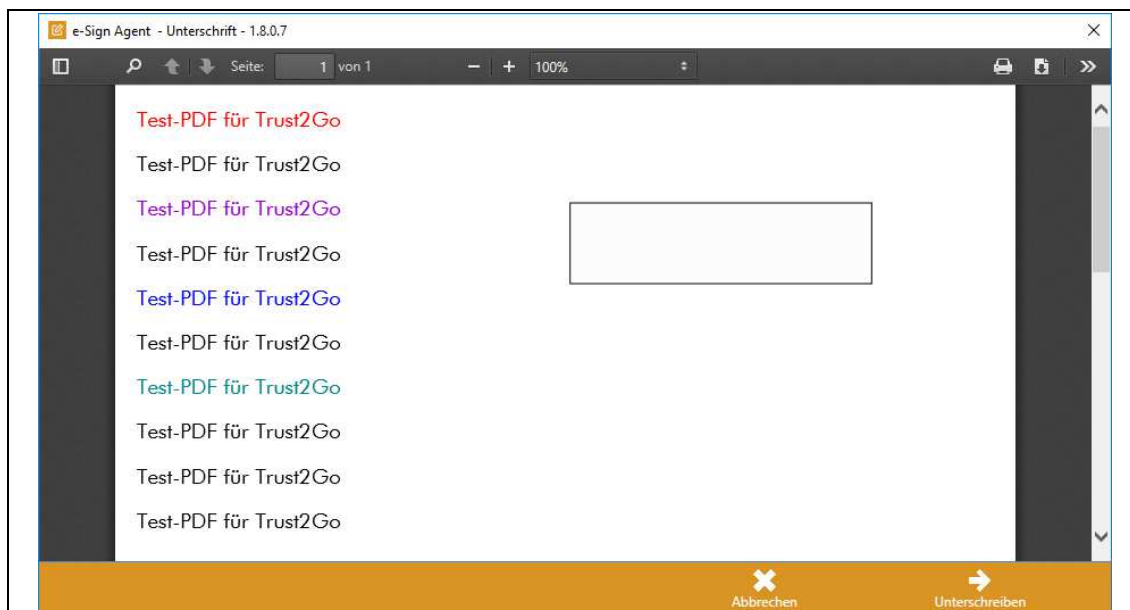


Abbildung 87: App-Signatur IV - Unterschriftsfeld verschieben (optional)

Unterschriften ⇨

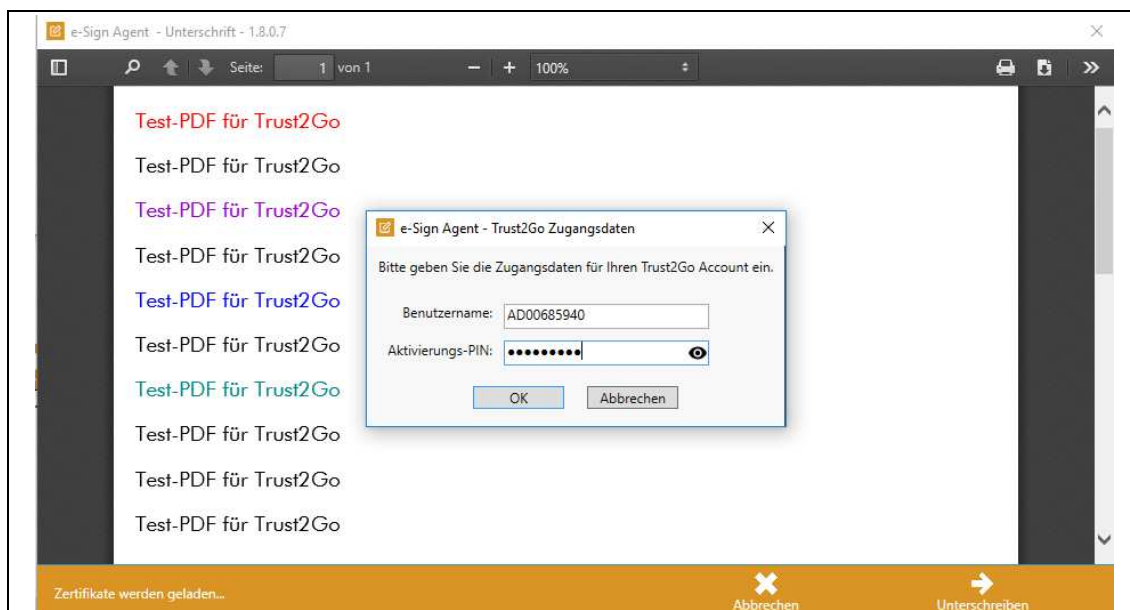


Abbildung 88: App-Signatur V - Signatordienst aufrufen

Speichern ⇒

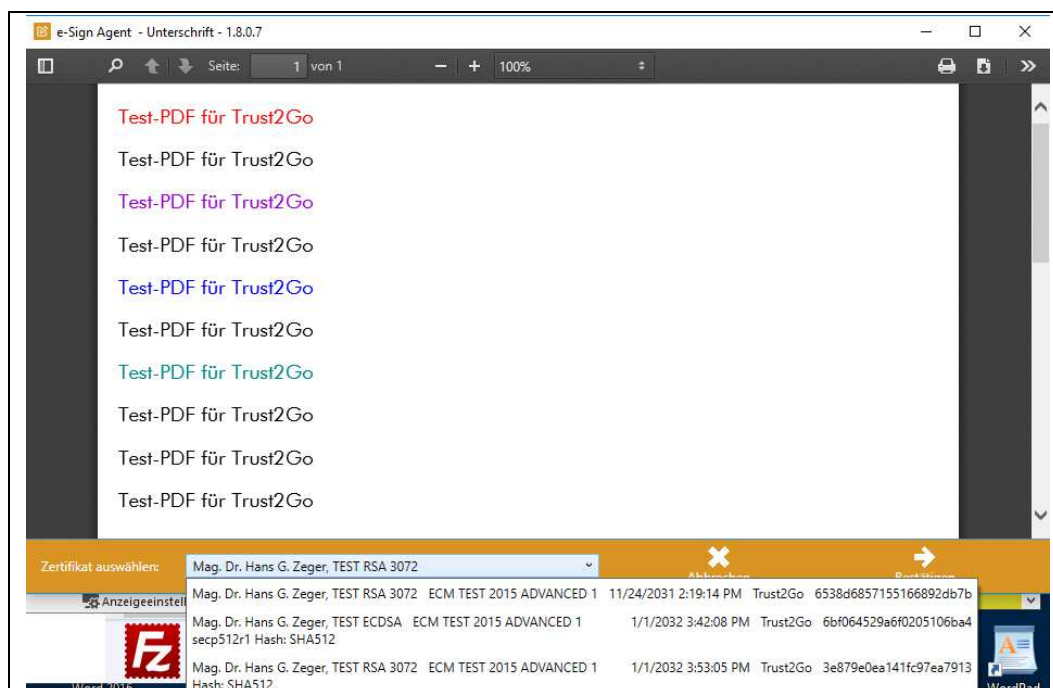


Abbildung 89: App-Signatur VI - Zertifikat auswählen

Zertifikat auswählen: geeignetes Zertifikat auswählen ⇒ Bestätigen ⇒

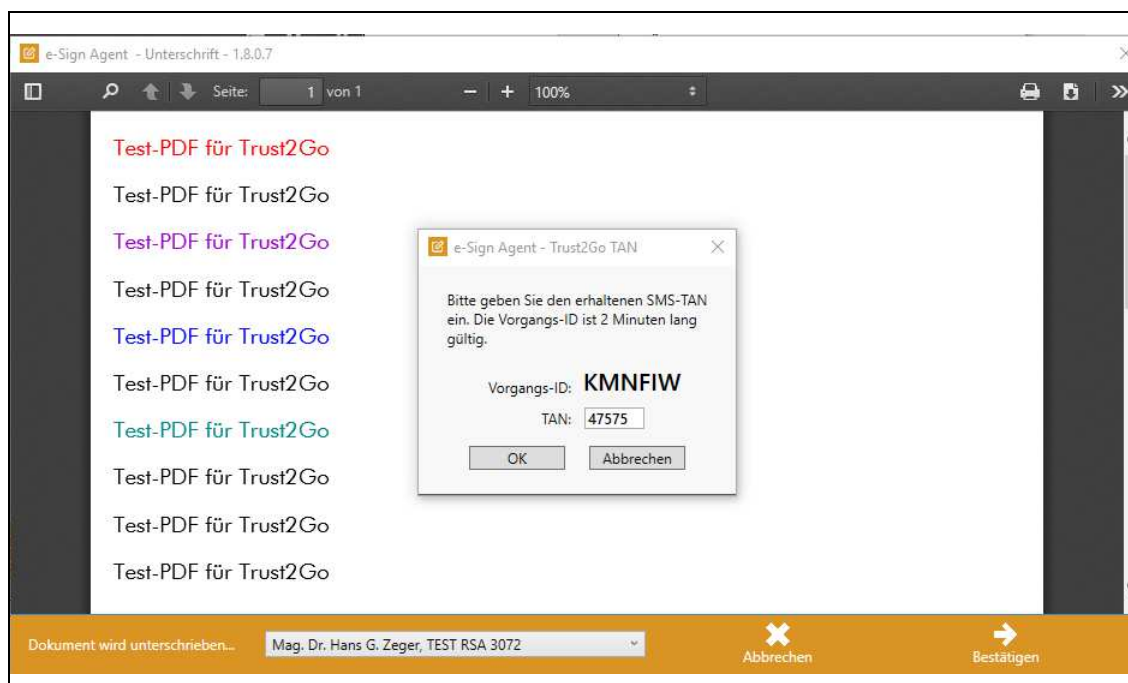


Abbildung 90: App-Signatur VII - Signatur starten - TAN-Bestätigung

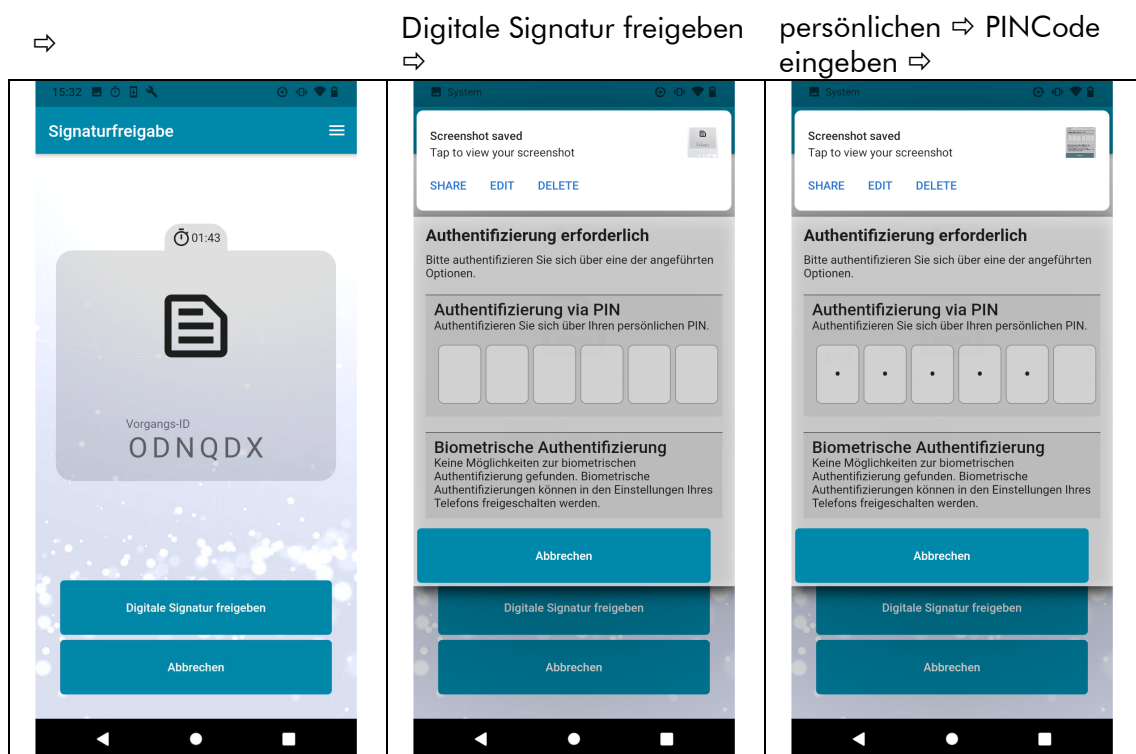


Abbildung 91: App-Signatur VIIla - bestätigen 2. Auth-Faktor mit 'Trust2GoAuthApp' I

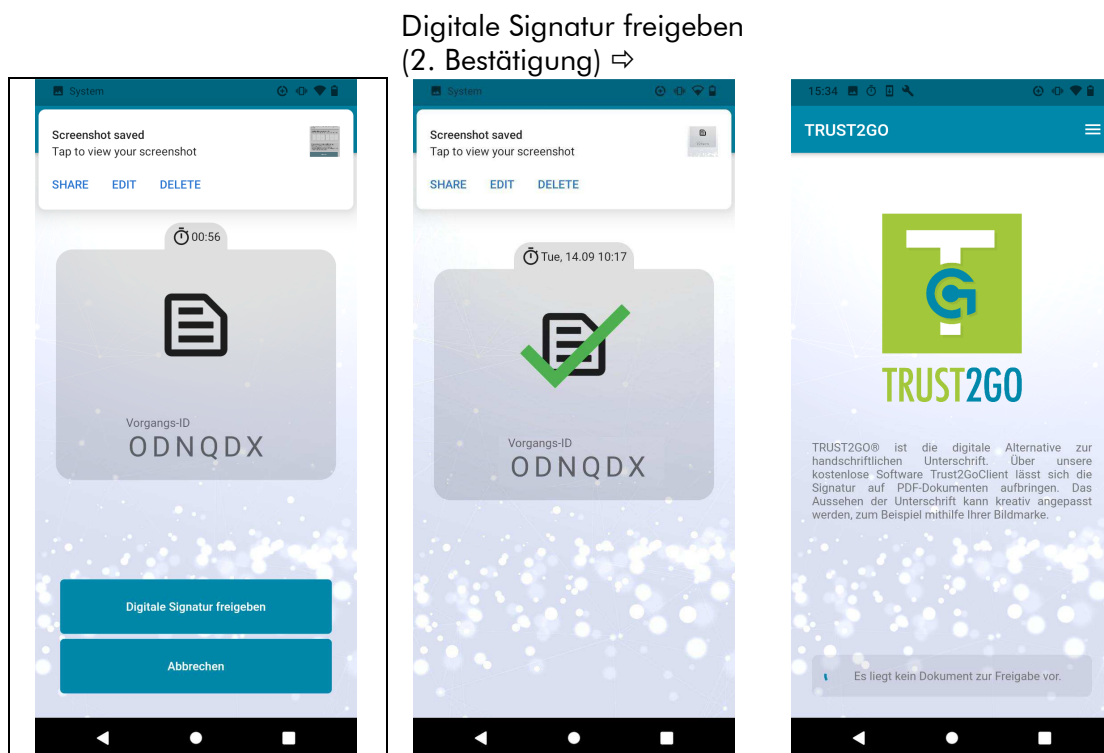


Abbildung 92: App-Signatur VIIlb - bestätigen 2. Faktor mit 'Trust2GoAuthApp' II

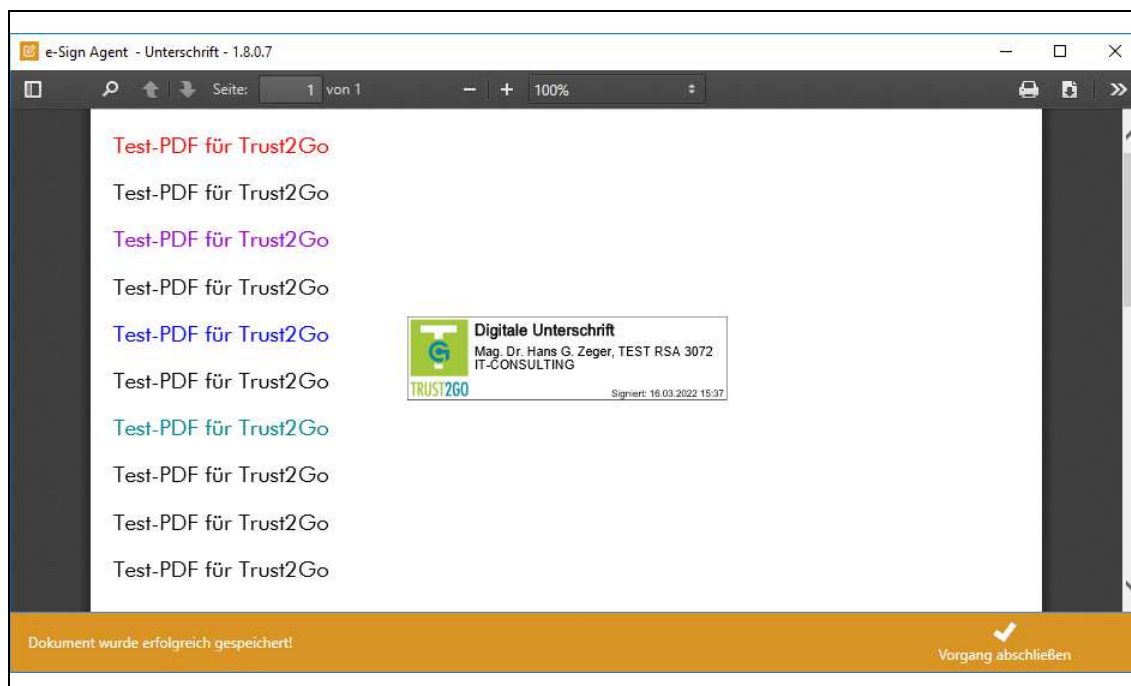


Abbildung 93: App-Signatur IX - Signatur im Dokument angebracht

Vorgang abschließen ⇨

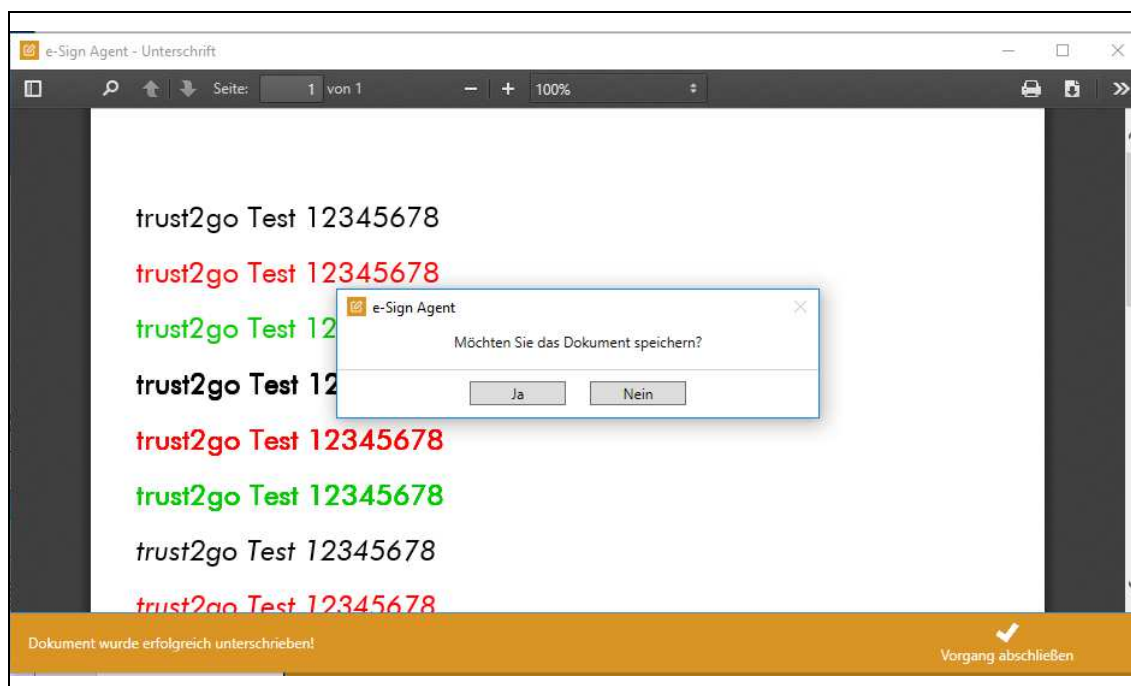


Abbildung 94: App-Signatur X - Anzeige signiertes Dokument

Ja ⇒

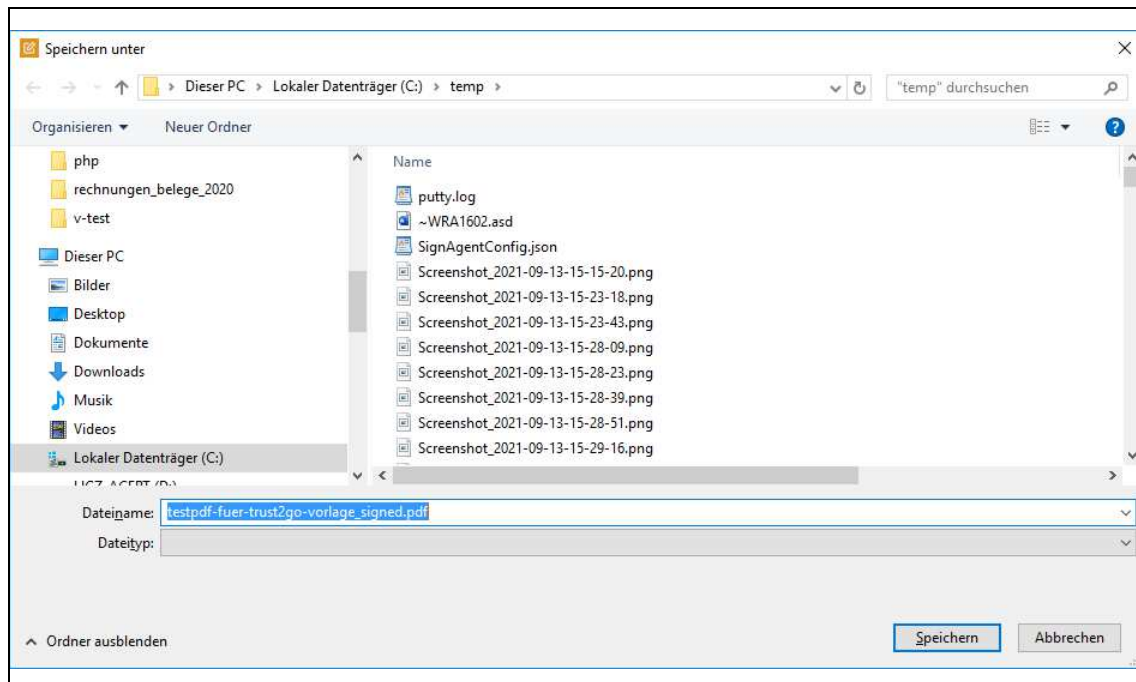


Abbildung 95: App-Signatur XI - Speichern signierte Datei

optional

Signaturcheck (⇒ 25 [SignCheckAdobe] Signaturcheck in Adobe Acrobat DC, p196)

B) ERSTELLEN QUALIFIZIERTE SIGNATUR IN PDF MIT 'TRUST2GOCLIENT' + SMS

62

Hinweis!

Dieser Ablauf ist bei fortgeschrittener Signatur mit 2-Faktor-Authentisierung ident.

Erforderliche Komponente(n) - Client

- Mobiltelefon für SMS-Empfang (Nummer laut Antrag)
- Installation 'Trust2GoClient':
⇒ 8 [KompEsign] Installation + Konfiguration 'Trust2GoClient' (e-Sign Agent) (p125)

pdf-Datei ⇒ (Rechte Maustaste) ⇒ Öffnen mit ⇒

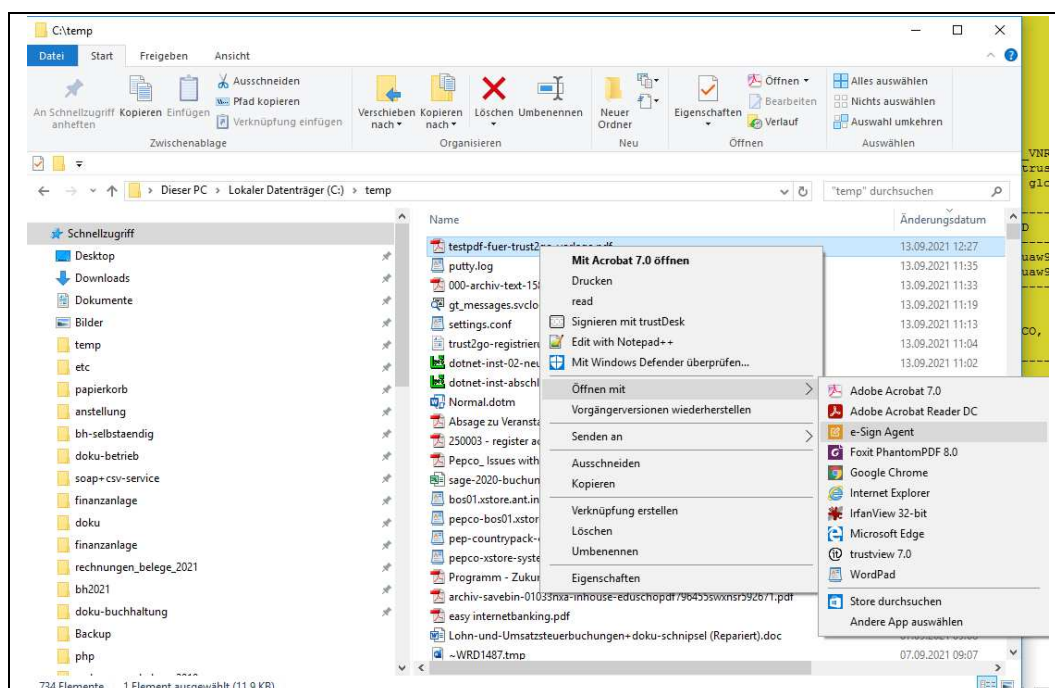


Abbildung 96: Web-Signatur I - Dateiauswahl

e-Sign Agent ⇨

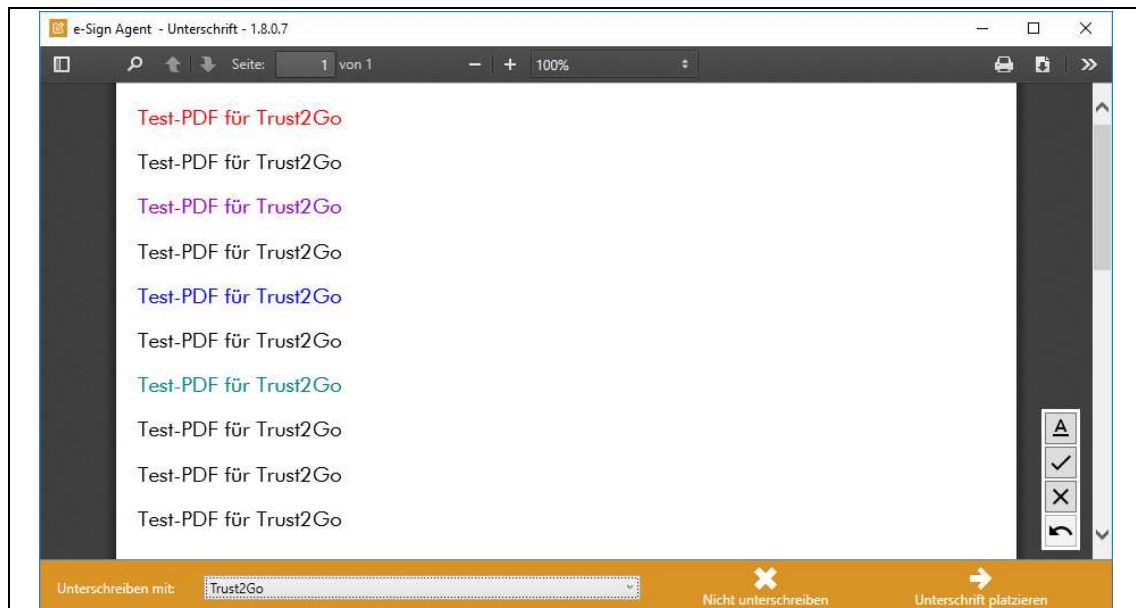


Abbildung 97: Web-Signatur II - Serviceauswahl Trust2Go

Unterschreiben mit: Trust2GO ⇨ Unterschrift platzieren ⇨

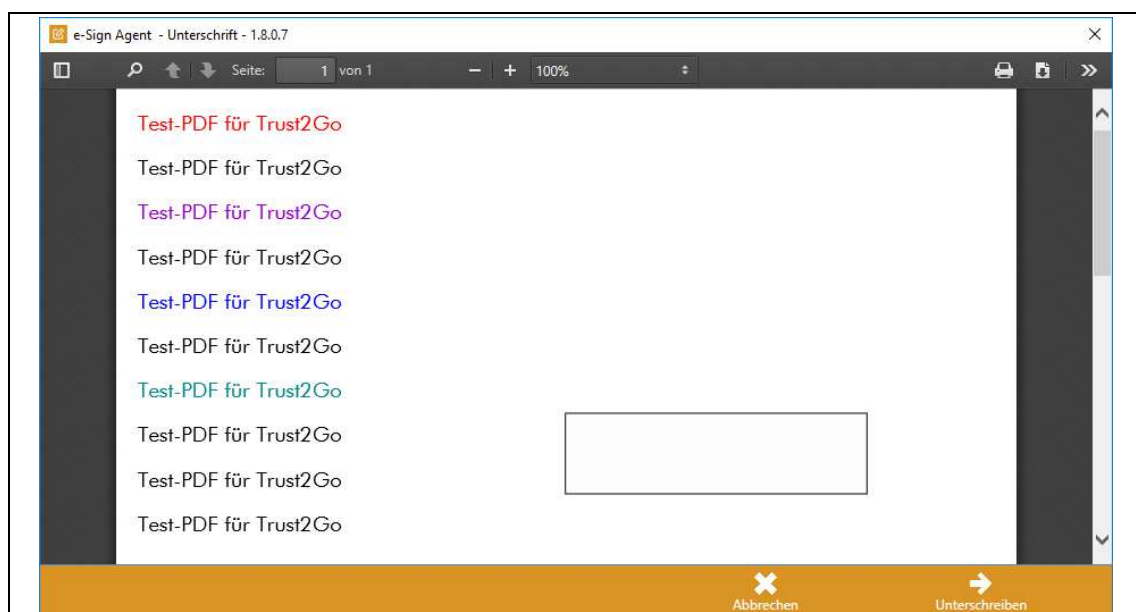


Abbildung 98: Web-Signatur III - Unterschriftsfeld platzieren

Rechteck verschieben ⇨

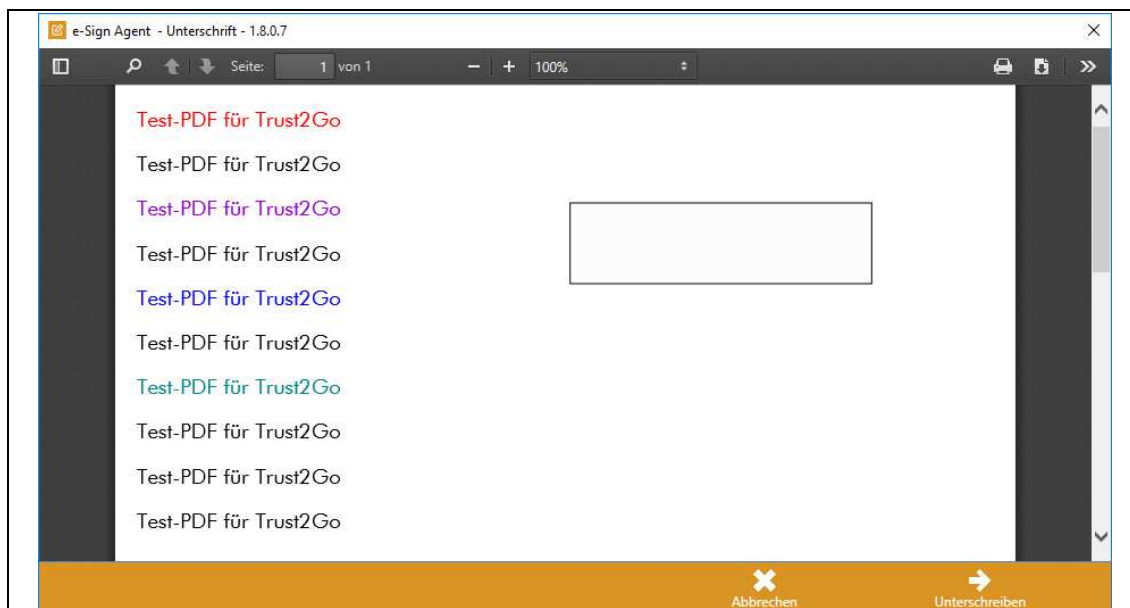


Abbildung 99: Web-Signatur IV - Unterschriftsfeld verschieben (optional)

Unterschriften ⇨

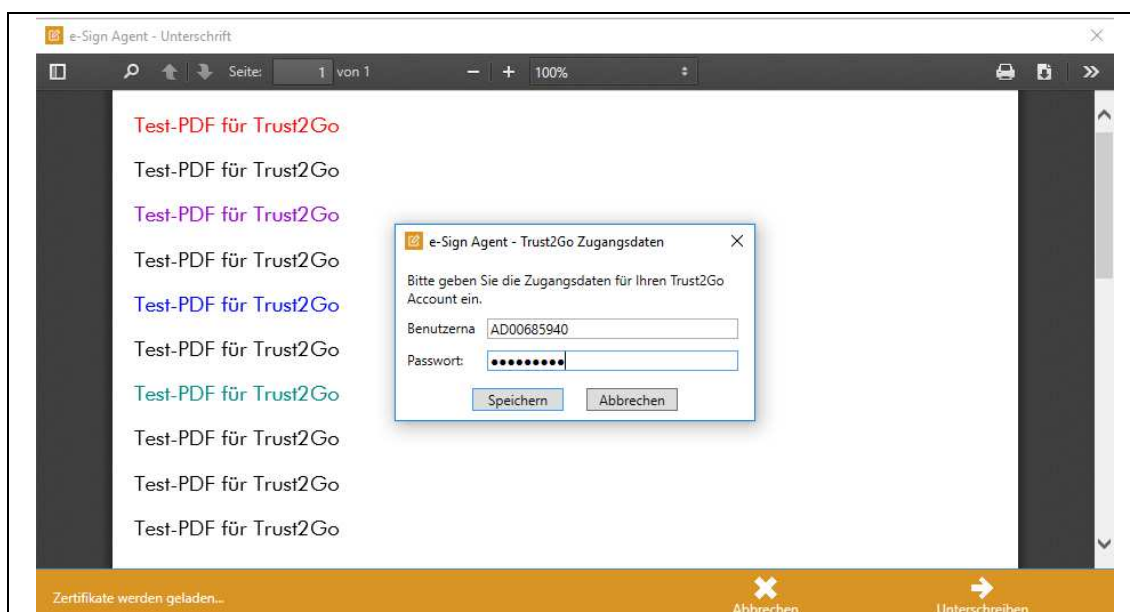


Abbildung 100: Web-Signatur V - Signaturdienst aufrufen

Speichern ⇒

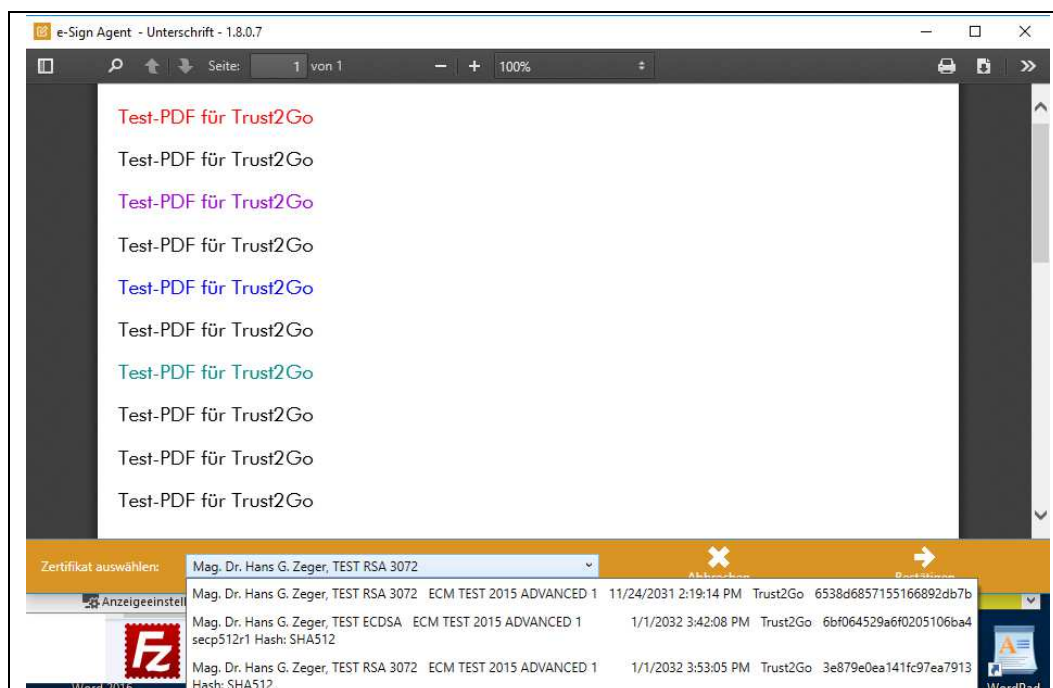


Abbildung 101: Web-Signatur VI - Zertifikat auswählen

Zertifikat auswählen: geeignetes Zertifikat auswählen ⇒ Bestätigen ⇒

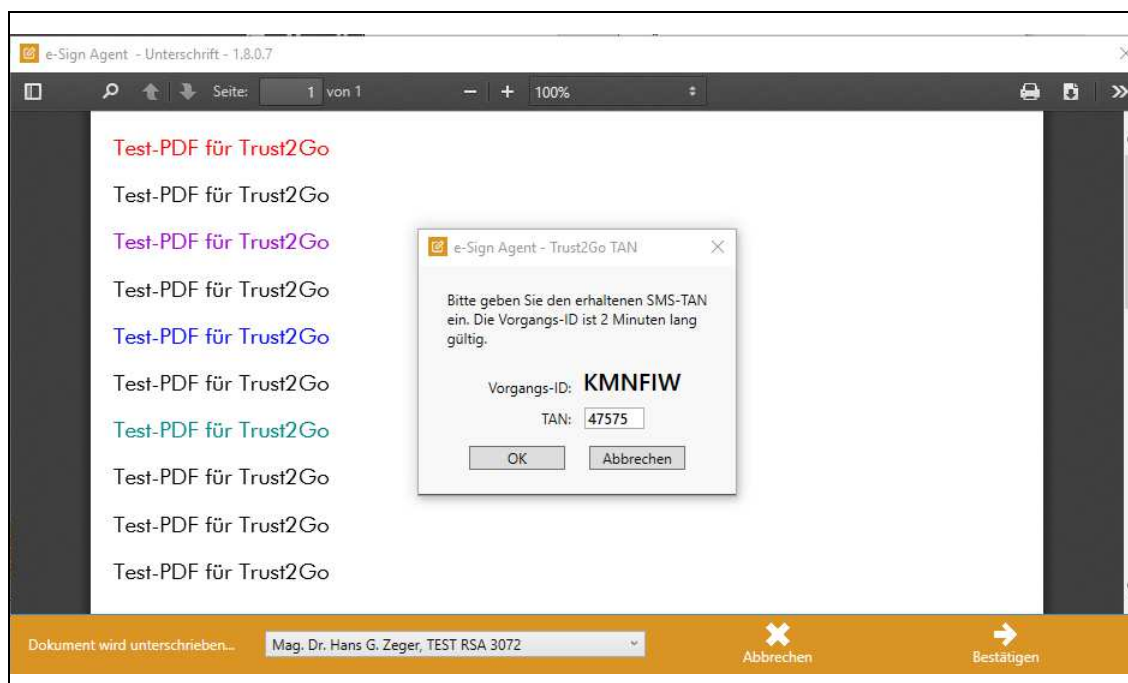


Abbildung 102: Web-Signatur VII - Signatur starten

TAN eingeben ⇒ OK ⇒

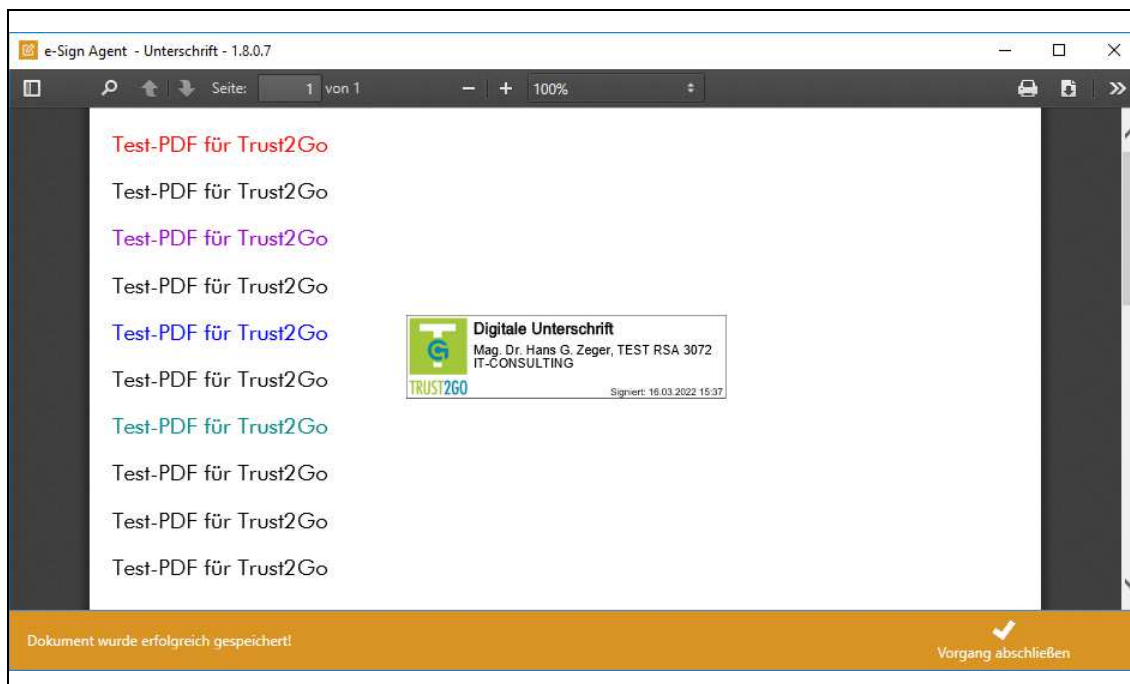


Abbildung 103: Web-Signatur VIII - Signatur im Dokument angebracht

Vorgang abschließen ⇒

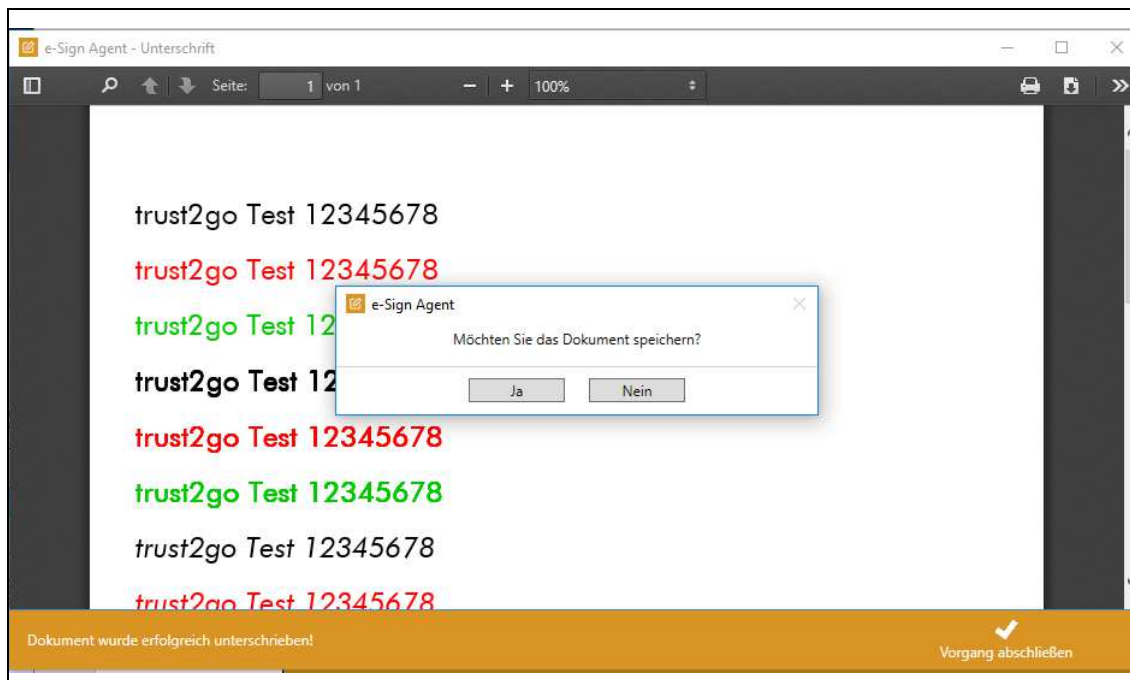


Abbildung 104: Web-Signatur IX - Anzeige signiertes Dokument

Ja ⇒

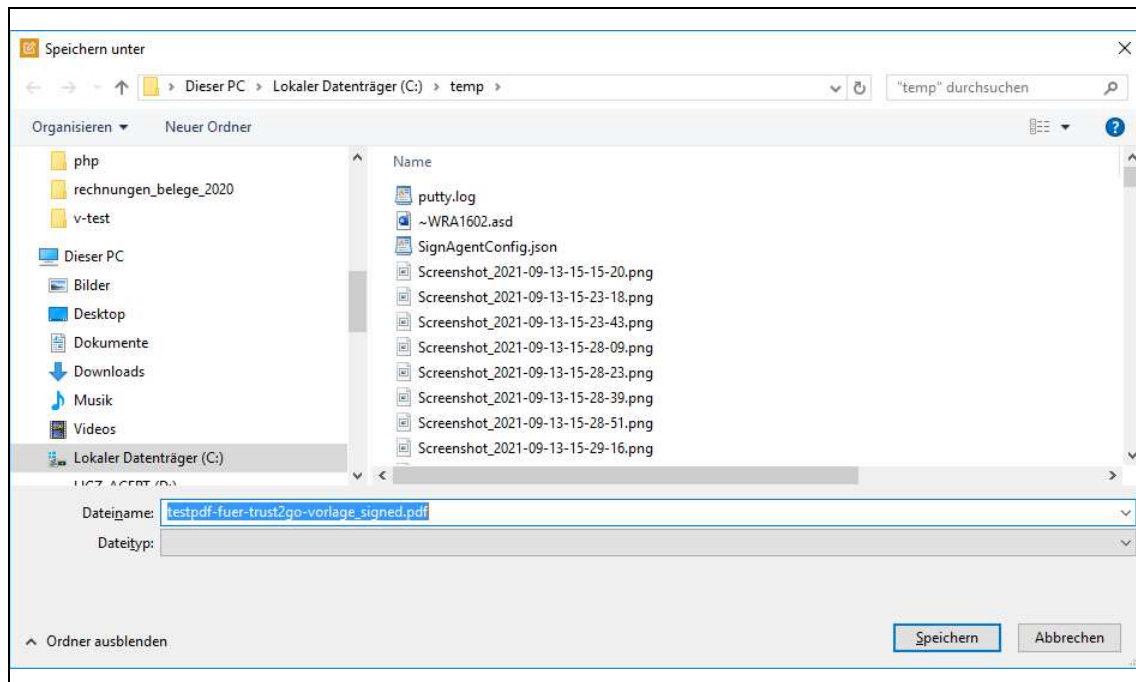


Abbildung 105: Web-Signatur XI - Speichern signierte Datei

optional

Signaturcheck (⇒ 25 [SignCheckAdobe] Signaturcheck in Adobe Acrobat DC, p196)

C) ERSTELLEN QUALIFIZIERTE SIGNATUR IN PDF MIT 'TRUST2GOAPI' + 'TRUST2GOAUTHAPP' 67

Anwendung abhängig von API-Implementation: kontaktieren Sie Ihren Trust2Go-Integrator

D) ERSTELLEN QUALIFIZIERTE SIGNATUR IN PDF MIT 'TRUST2GOAPI' + 'TRUST2GOWEB' 67

Anwendung abhängig von API-Implementation: kontaktieren Sie Ihren Trust2Go-Integrator

E) ERSTELLEN QUALIFIZIERTE SIGNATUR IN XML MIT 'TRUST2GOAPI' + 'TRUST2GOAUTHAPP' 67

Anwendung abhängig von API-Implementation: kontaktieren Sie Ihren Trust2Go-Integrator

F) ERSTELLEN QUALIFIZIERTE SIGNATUR IN XML MIT 'TRUST2GOAPI' + 'TRUST2GOWEB' 67

Anwendung abhängig von API-Implementation: kontaktieren Sie Ihren Trust2Go-Integrator

17 [DEREGAUTHAPP] DEREGISTRIERUNG MITTELS 'TRUST2GOAUTHAPP'

68

Wann ist eine DeRegistrierung mittels 'Trust2GoAuthApp' sinnvoll?

- es ist der Wechsel zu einem anderen Smartphone geplant
- es wird der \Rightarrow AuthenticationApp oder dem Smartphone nicht mehr vertraut
- es soll in Zukunft nur mehr SMS als \Rightarrow 2. Auth-Faktor verwendet werden
- es wird Trust2Go nicht mehr benötigt
- es erfolgt der Wechsel von Testsystem t2gtest.globaltrust.eu zum Produktionssystem t2g.globaltrust.eu

Hinweis

Eine DeRegistrierung hat keine Auswirkung auf die verwendeten Zertifikate. Sollen Zertifikate gesperrt oder widerrufen werden, ist gemäß Policy des VDA (\Rightarrow [GCP] 4.9 + [GCPS] 4.9) vorzugehen und ein Antrag des Signators an den VDA zu stellen.

Hinweis

Ist die in diesem Abschnitt beschriebene Deregistrierung mittels 'Trust2GoAuthApp' nicht (mehr) möglich, dann muss eine Deregistrierung durch den VDA erfolgen. Dazu muss der \Rightarrow Signator den Support des VDA kontaktieren (AktivierungspIN unbekannt).

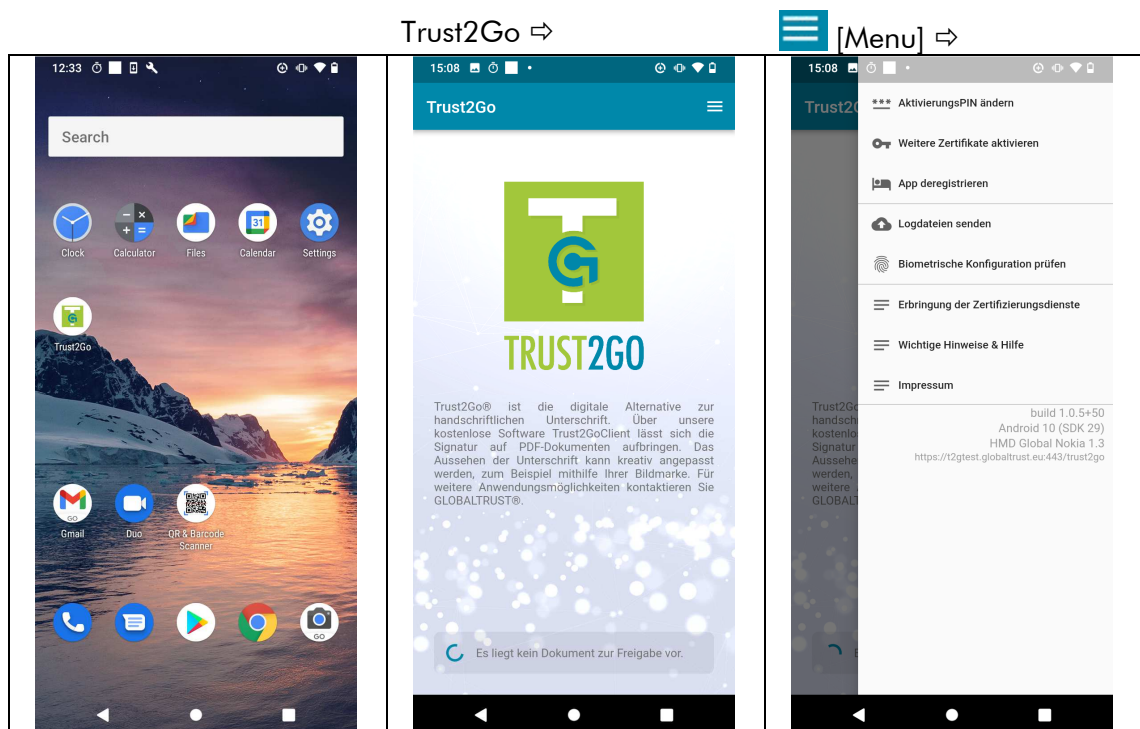


Abbildung 106: DeRegistrierung AuthenticationApp I

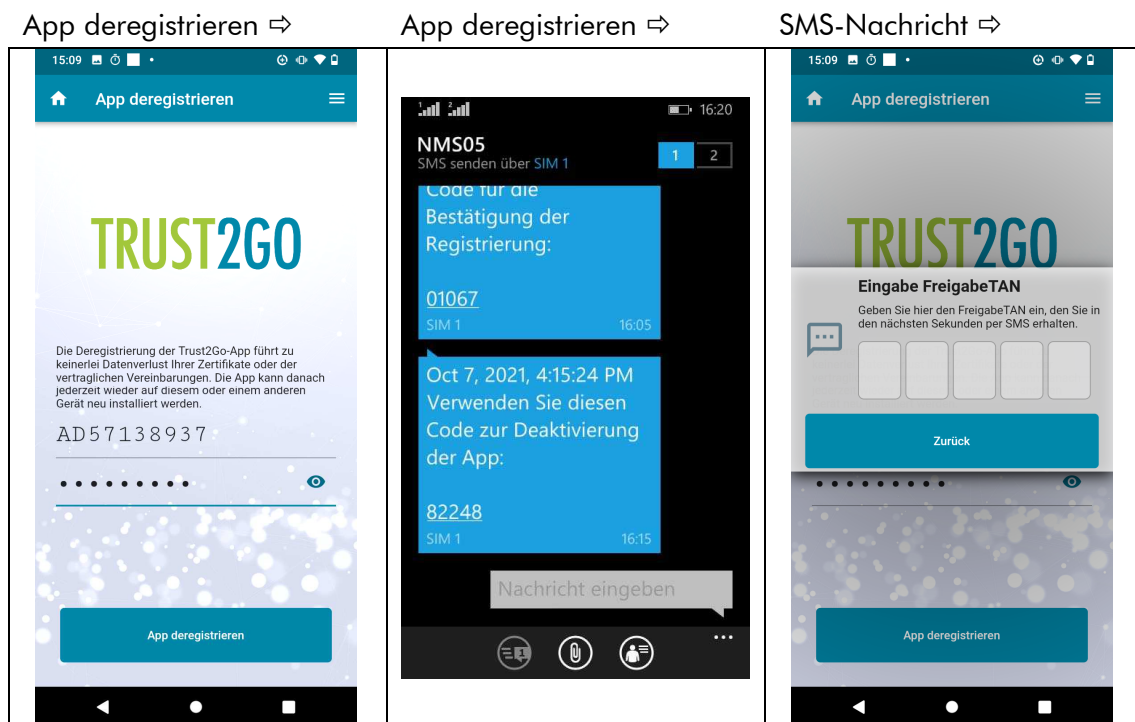


Abbildung 107: DeRegistrierung AuthenticationApp II

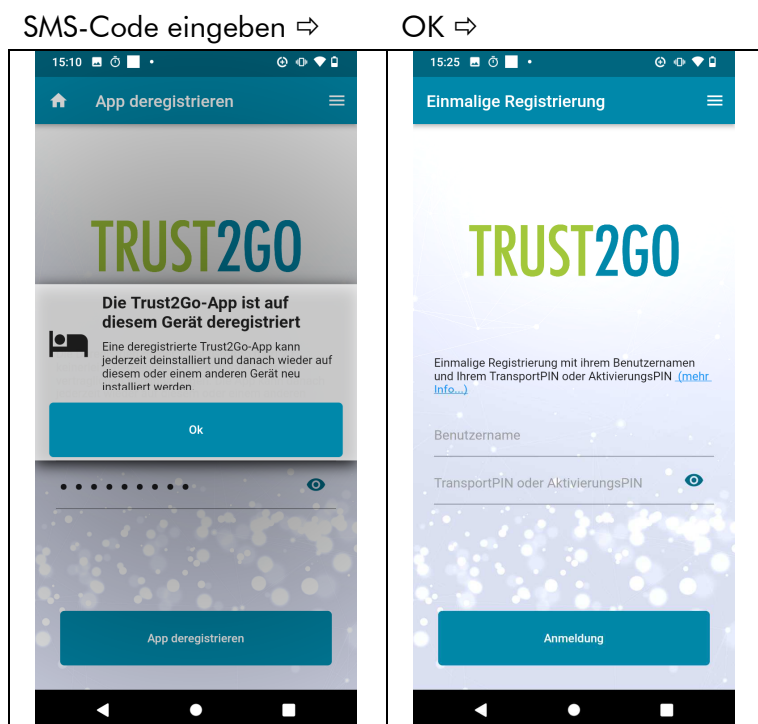


Abbildung 108: DeRegistrierung AuthenticationApp III

Anschließend kann die 'Trust2GoAuthApp' entfernt werden (rechts wischen) oder sie läuft im Hintergrund weiter.

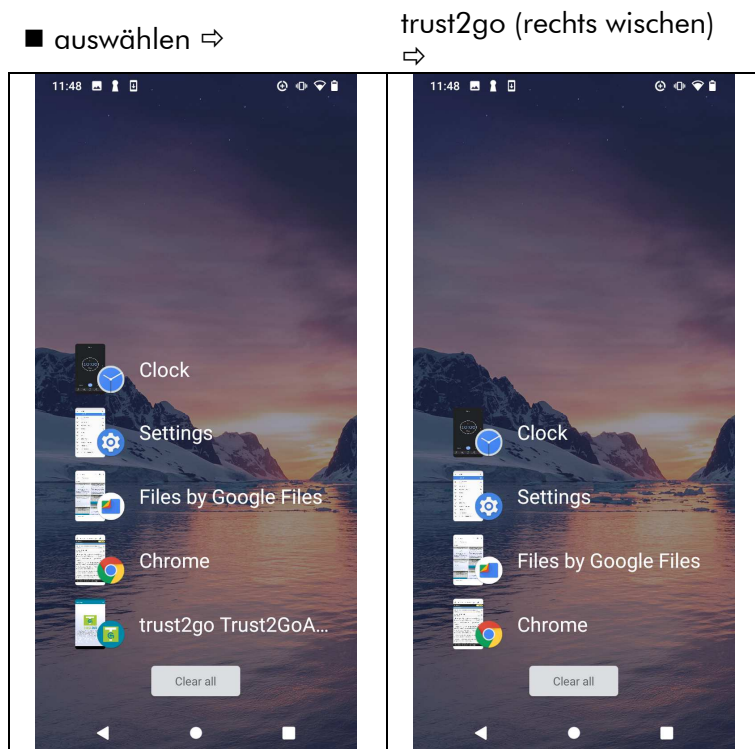


Abbildung 109: DeRegistrierung AuthenticationApp IV

Hinweis

Im Anschluss kann die 'Trust2GoAuthApp' auch deinstalliert werden ⇨ 19 [DeInstAuthApp]
Deinstallation 'Trust2GoAuthApp' (p182).

18 [DEREGAUTHWEB] DEREGISTRIERUNG MITTELS 'TRUST2GOWEB'

71

Wann ist eine DeRegistrierung mittels 'Trust2GoWeb' sinnvoll?

- es besteht kein Zugriff mehr auf das Smartphone

Hinweis

Eine DeRegistrierung hat keine Auswirkung auf die verwendeten Zertifikate. Sollen Zertifikate gesperrt oder widerrufen werden, ist gemäß Policy [GCP] 4.9 und [GCPS] 4.9 vorzugehen.

Hinweis

Ist die in diesem Abschnitt beschriebene Deregistrierung mittels 'Trust2GoAuthApp' nicht (mehr) möglich, dann muss eine manuelle Deregistrierung durchgeführt werden. Diese ist nur durch den VDA möglich. Dazu muss der ⇒ Signator den Support des VDA kontaktieren (AktivierungsPIN unbekannt).

<https://t2g²⁵.globaltrust.eu/trust2go/public/index.html>

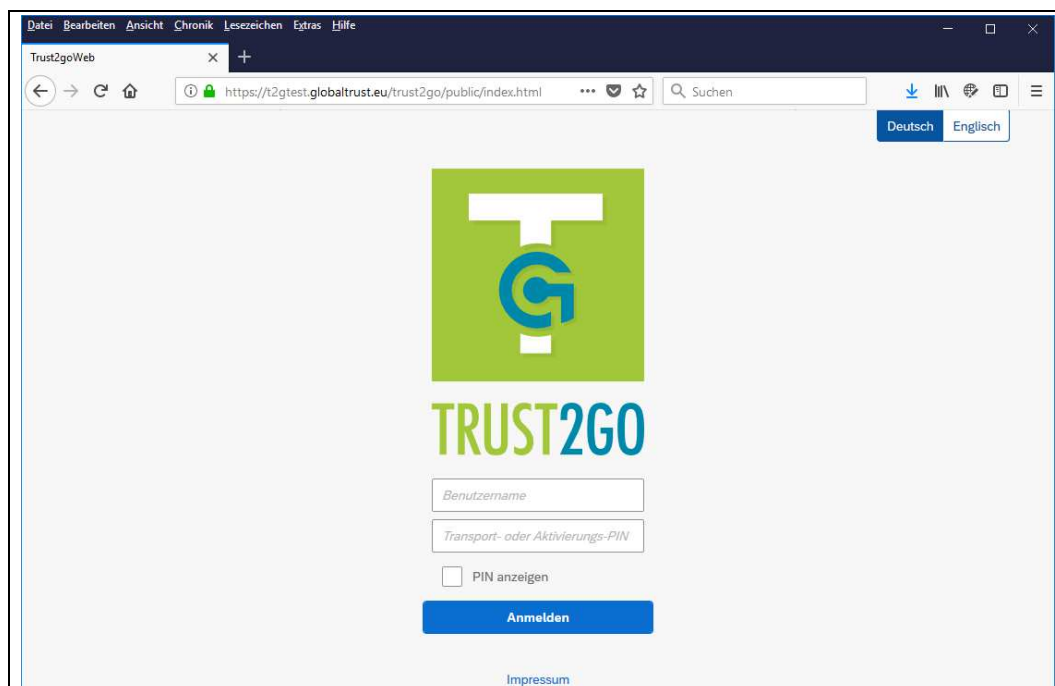


Abbildung 110: DeRegistrierung AuthenticationApp mittels Web I

²⁵ im Testbetrieb ist statt t2g ⇒ t2gtest zu verwenden

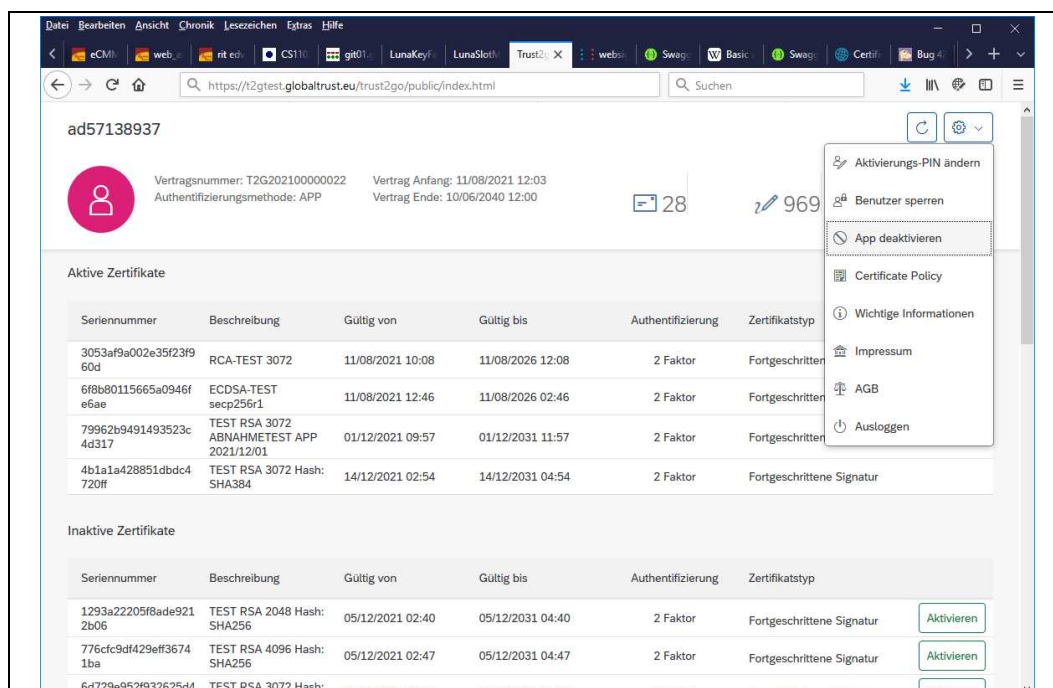
Anmelden ⇨  [Zahnrad] ⇨

Abbildung 111: DeRegistrierung AuthenticationApp mittels Web II

Hinweis

Der Menu-Punkt "App deregistrieren" erscheint nur, wenn der ⇨ Signator die ⇨ AuthenticationApp 'Trust2GoAuthApp' registriert hat.

'Trust2GoAuthApp' deregistrieren ⇨

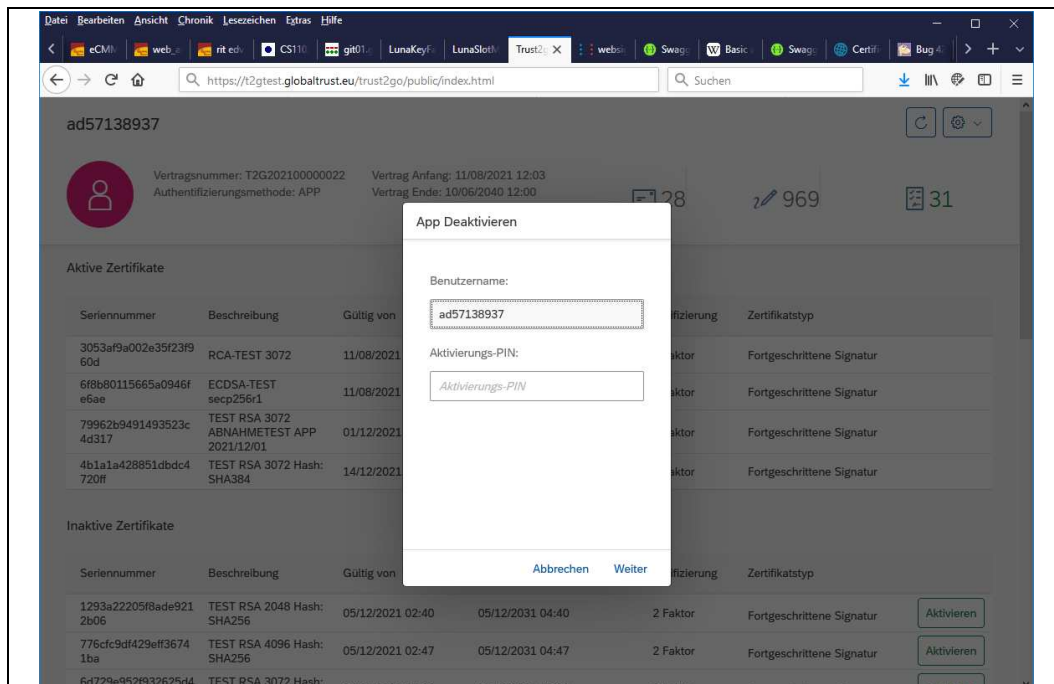


Abbildung 112: DeRegistrierung AuthenticationApp mittels Web III

Weiter ⇨

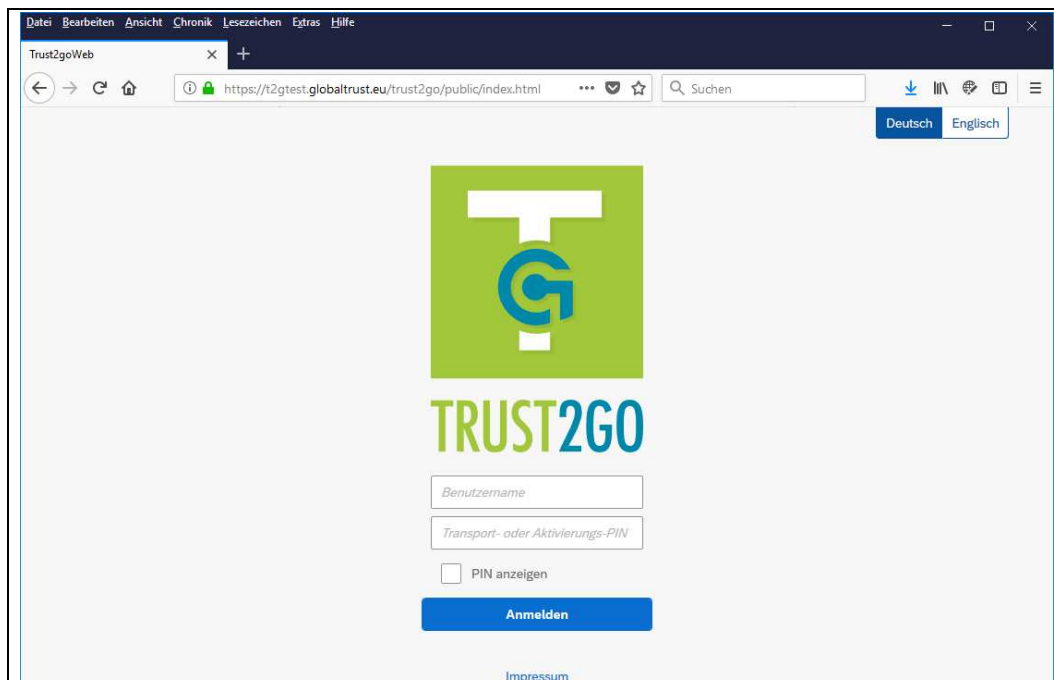


Abbildung 113: DeRegistrierung AuthenticationApp mittels Web IV

19 [DEINSTAUTHAPP] DEINSTALLATION 'TRUST2GOAUTHAPP'

74

Wann ist eine Deinstallation sinnvoll?

- es erfolgt der Wechsel von Testsystem t2gtest.globaltrust.eu zum Produktionssystem t2g.globaltrust.eu
- es ist der Wechsel zu einem anderen Smartphone geplant
- es wird Trust2Go nicht mehr benötigt

Hinweis

Eine Deinstallation der ⇒ AuthenticationApp ohne vorangegangener DeRegistrierung (⇒ 17 [DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp', p176) führt dazu, dass alle Zertifikate für den ⇒ Signator nicht mehr verwendbar sind. Eine neuerliche Nutzung kann nur mehr durch den VDA aufgehoben werden.

Hinweis

Ist die DeRegistrierung mittels 'Trust2GoAuthApp' oder 'Trust2GoWeb' nicht (mehr) möglich, dann muss die manuelle DeRegistrierung durchgeführt werden (AktivierungsPIN unbekannt).

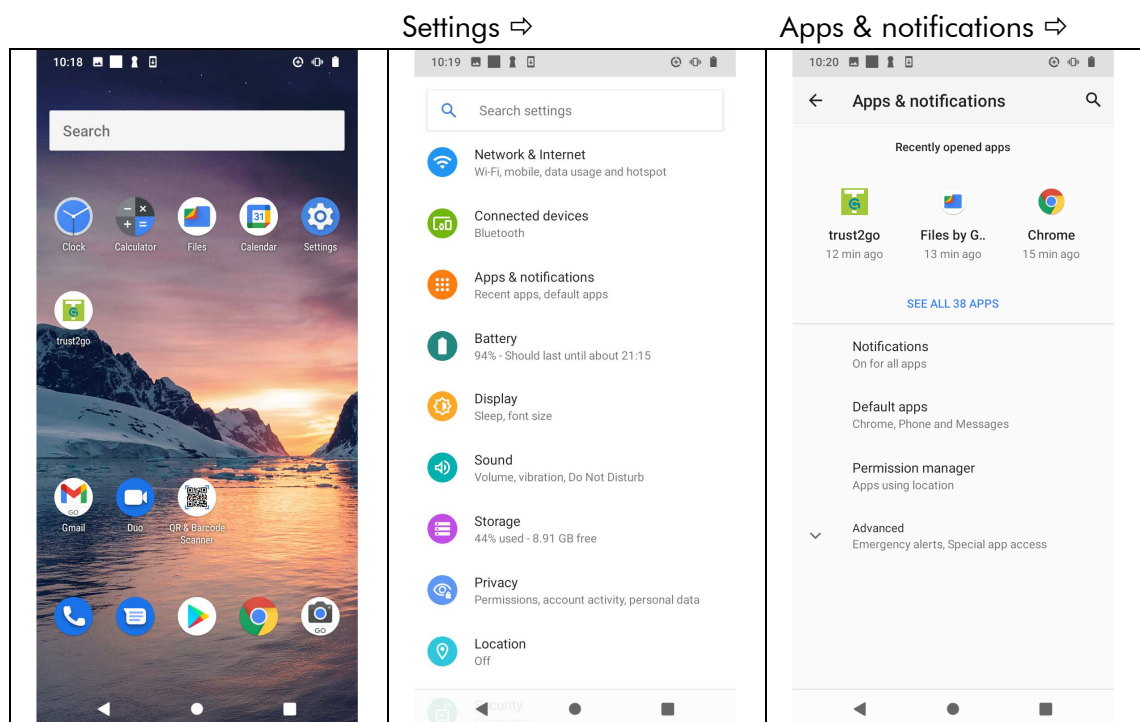


Abbildung 114: Deinstallation AuthenticationApp I

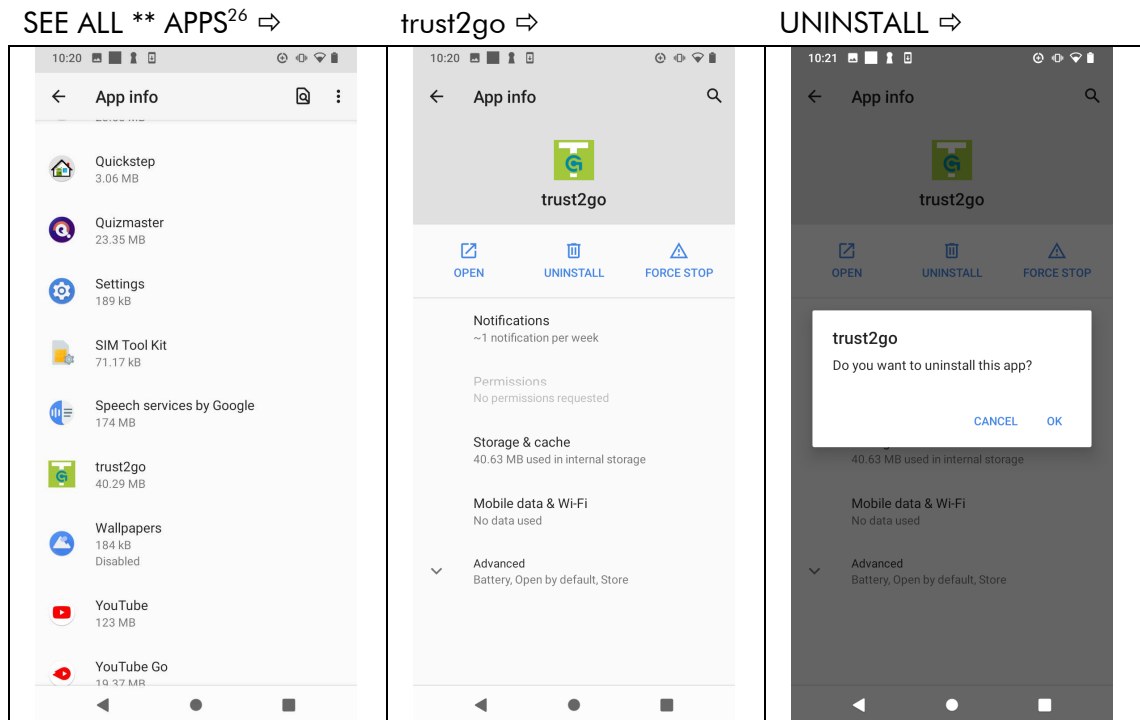


Abbildung 115: Deinstallation AuthenticationApp II

OK ⇒

20 [NEUREGAUTHAPP] NEUREGISTRIERUNG 'TRUST2GOAUTHAPP'

75

Hinweis!

Eine NeuRegistrierung der ⇒ AuthenticationApp ist möglich, wenn die 'Trust2GoAuthApp' deregistriert ist (⇒ 17 [DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp', p176).

Hinweis!

Wurde der AktivierungsPIN vergessen, erfolgt die DeRegistrierung durch den VDA.

Hinweis!

Wurde die 'Trust2GoAuthApp' deinstalliert (⇒ 19 [DeInstAuthApp] Deinstallation 'Trust2GoAuthApp', p182), muss vorab eine Installation erfolgen:

- ⇒ 6 [KompAppAndr] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version Android, p119 oder
- ⇒ 7 [KompApplos] Installation (Erst/Neu) Produktionsversion 'Trust2GoAuthApp' - Version IOS, p120).

²⁶ sofern trust2go nicht unter "Recently opened apps" aufscheint

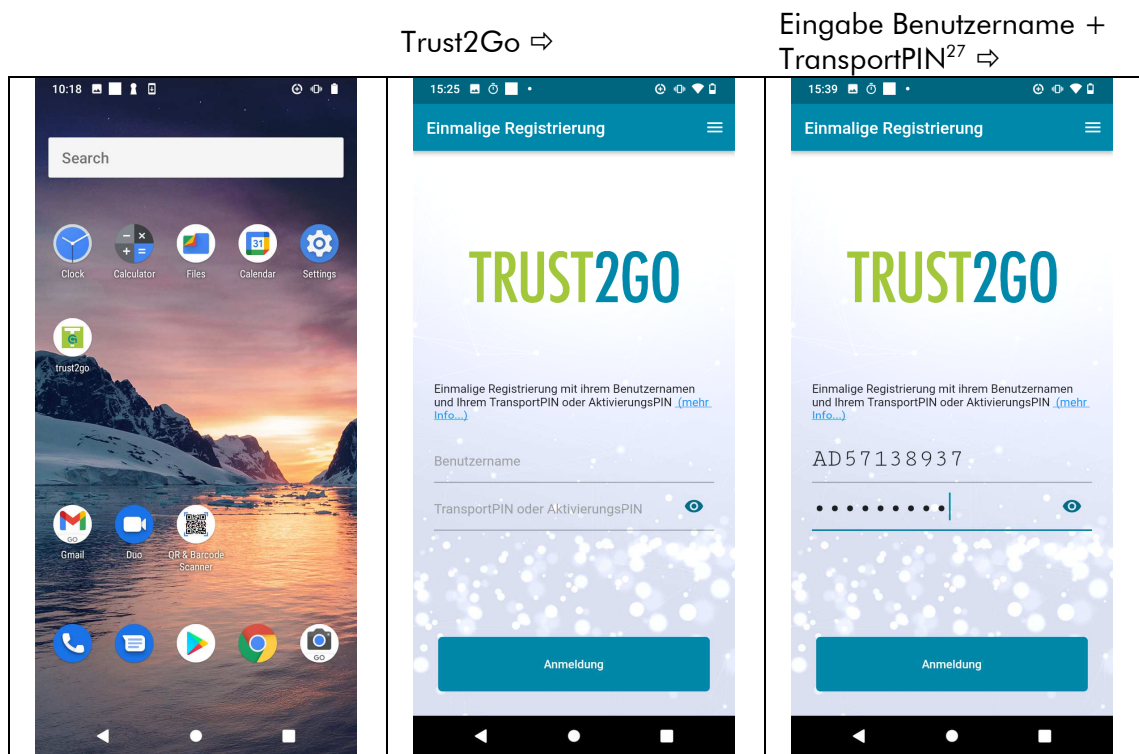


Abbildung 116: NeuRegistrierung AuthenticationApp I

²⁷ Erfolgt eine Neuregistrierung der App MIT vorheriger DeRegistrierung durch den Signator, dann ist der AktivierungsPIN einzugeben. Dies kann der Fall sein, wenn ein Smartphone neu installiert wird oder das Smartphone gewechselt wird.

Anmeldung ⇒

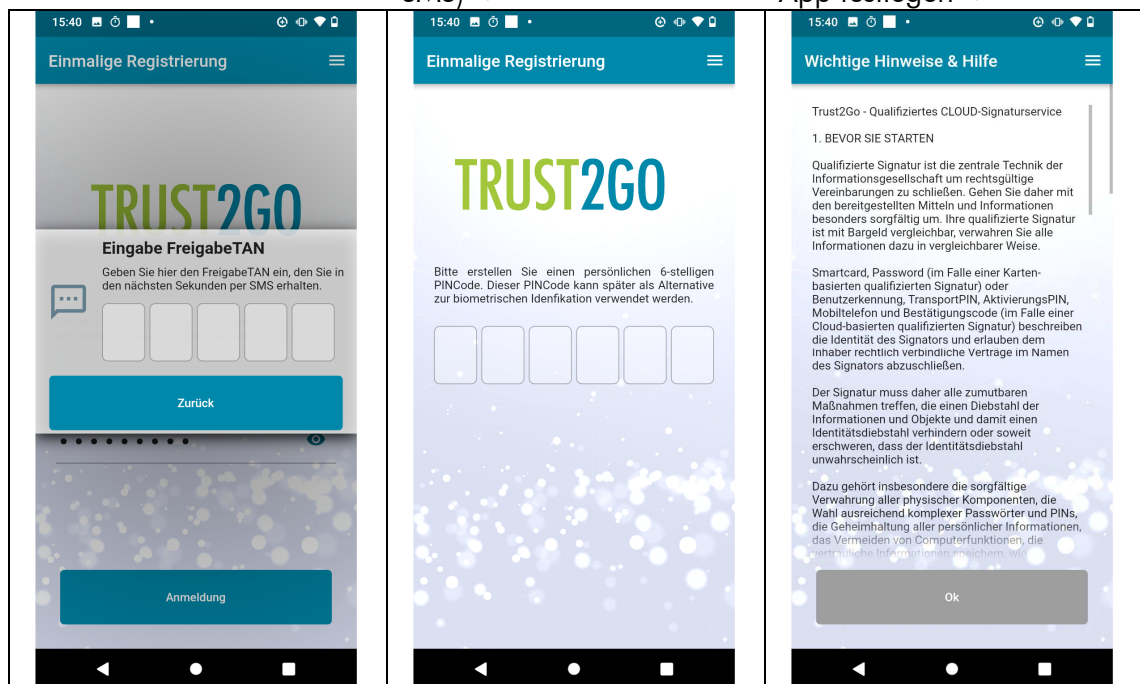
Eingabe FreigabeTAN (aus
SMS) ⇒persönlichen PIN-Code der
App festlegen ⇒

Abbildung 117: NeuRegistrierung AuthenticationApp II

an das Ende blättern ⇒

OK ⇒

Fortfahren ⇒

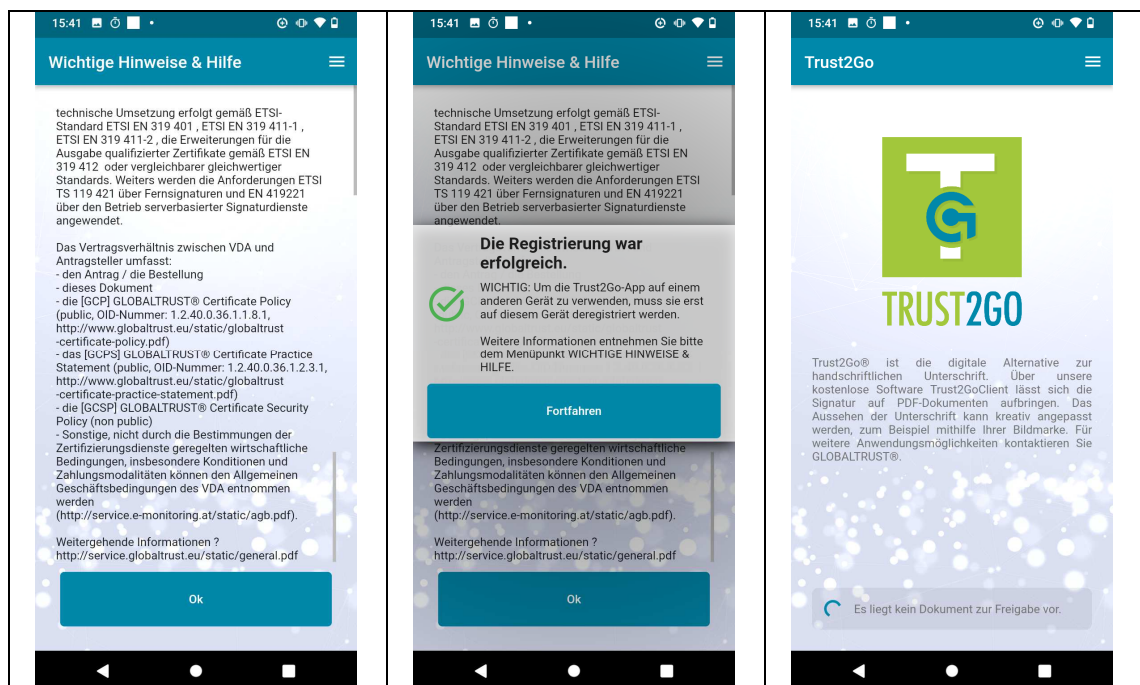


Abbildung 118: NeuRegistrierung AuthenticationApp III

Anschließend kann die 'Trust2GoAuthApp' entfernt werden (rechts wischen) oder sie läuft im Hintergrund weiter.

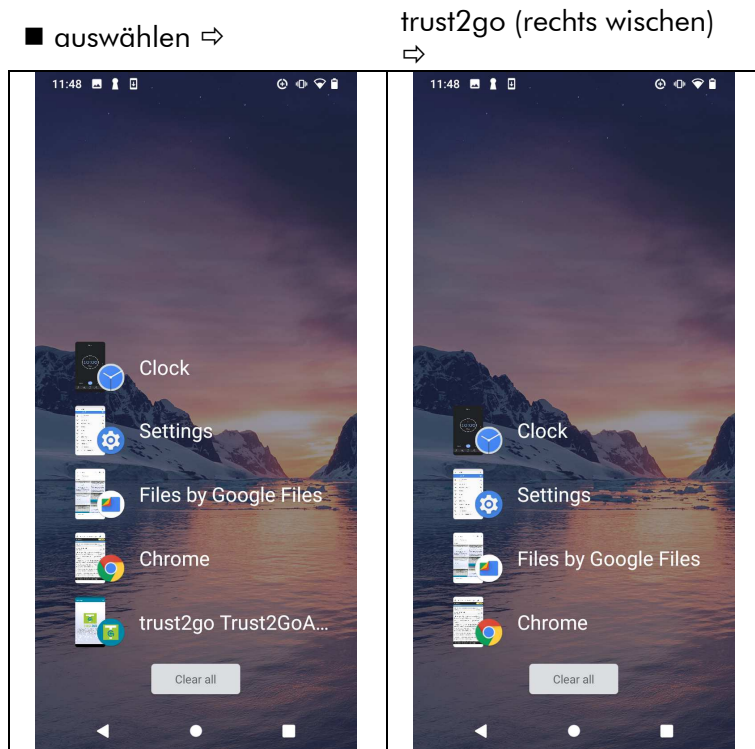


Abbildung 119: NeuRegistrierung AuthenticationApp IV

21 [SPERRESIGNATOR] SPERRE DURCH DEN SIGNATOR

79

Wenn ist eine Sperre sinnvoll?

- der ⇒ Signator hat die Kontrolle über seine ⇒ AuthenticationApp verloren, zB durch Verlust seines Smartphones oder das Smartphone mit einer gültigen Trust2Go-Installation ging kaputt

A) SPERRE SIGNATOR MITTELS 'TRUST2GoWEB'

79

Hinweis 1

Die Sperre erfordert zumindest die Kenntnis des Aktivierungspins. Ist dieser nicht mehr bekannt, muss umgehend der VDA informiert werden.

Hinweis 2

Ein Aufheben der Sperre ist nur durch den VDA möglich (⇒ 23 [AktAccount] Freigabe / Aufhebung Sperre, p192).

<https://t2g²⁸.globaltrust.eu/trust2go/public/index.html>

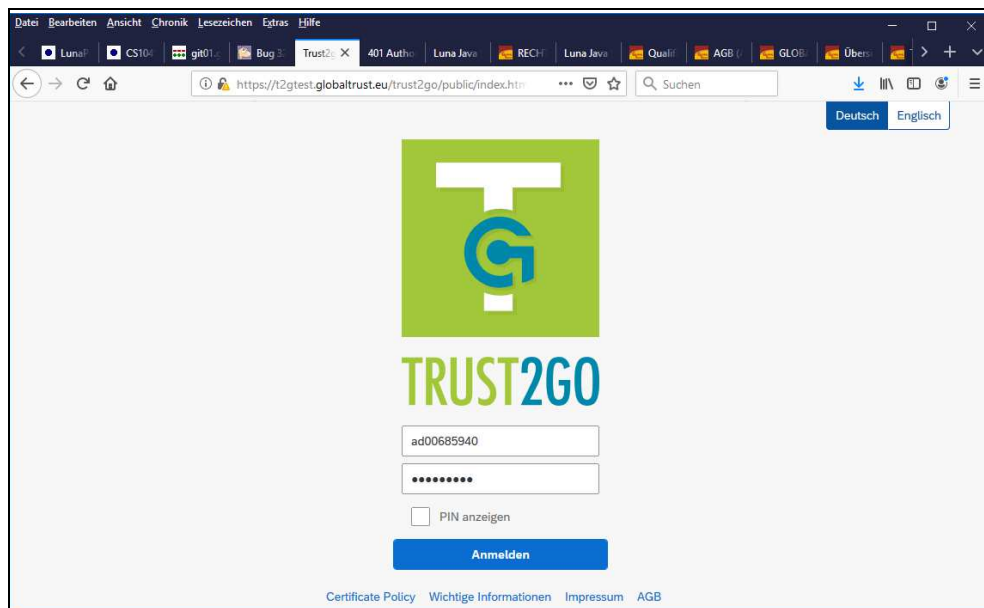


Abbildung 120: Sperre Signator Web I

Anmelden ⇒

²⁸ im Testbetrieb ist statt **t2g** ⇒ **t2gtest** zu verwenden

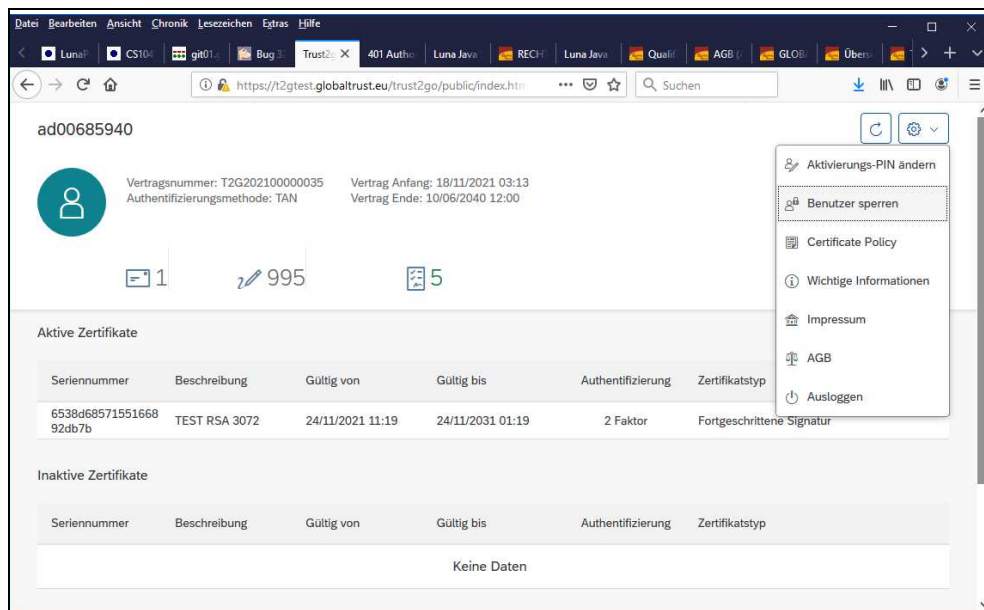


Abbildung 121: Sperre Signator Web II

 [Zahnrad] ⇒ Benutzer sperren ⇒

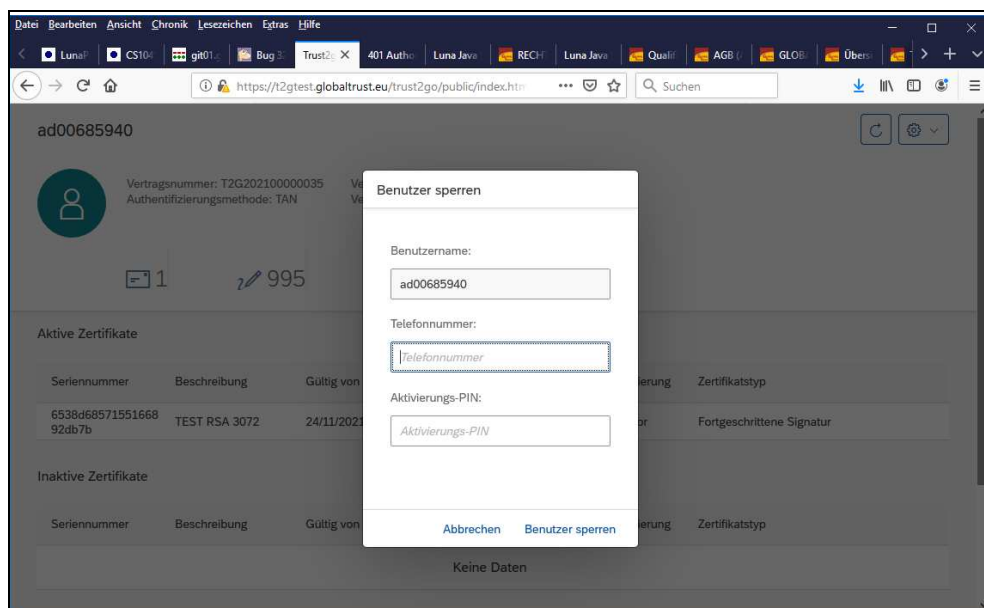


Abbildung 122: Sperre Signator Web III

Benutzer sperren ⇨

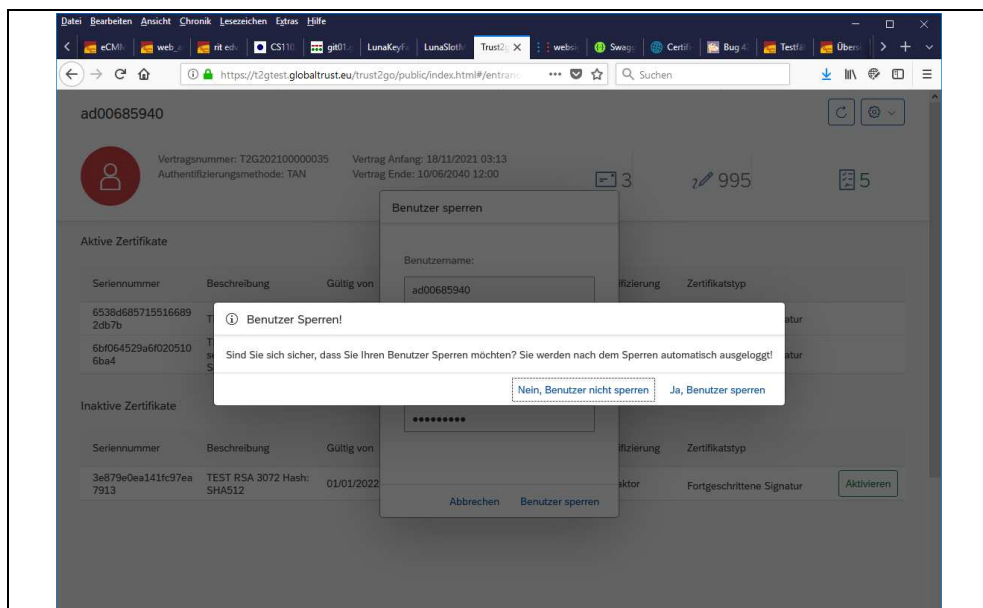


Abbildung 123: Sperre Signator Web IV

Ja, Benutzer sperren ⇨

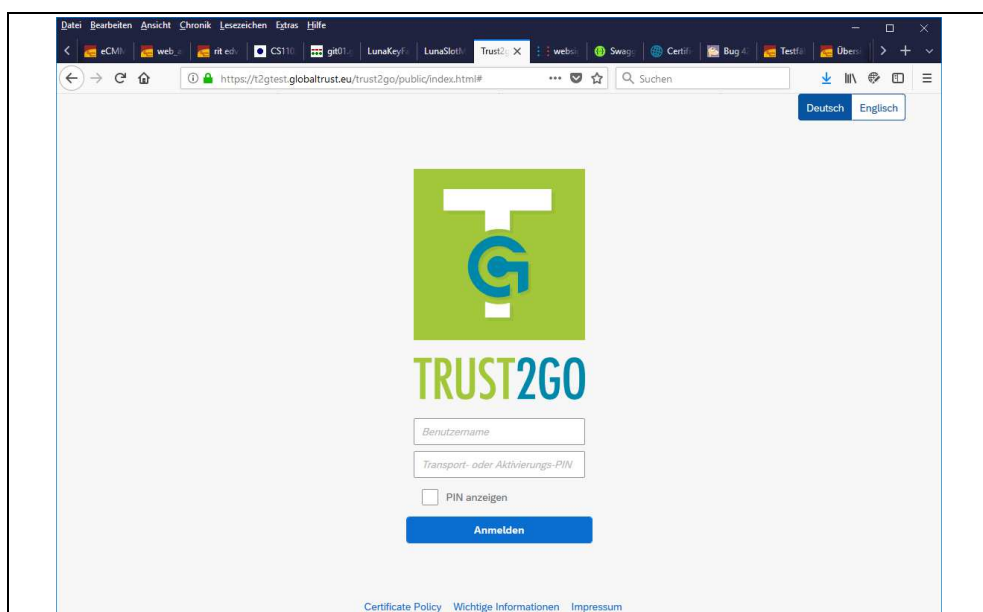


Abbildung 124: Sperre Signator Web V

ein neuerlicher Anmeldeversuch liefert folgendes Ergebnis

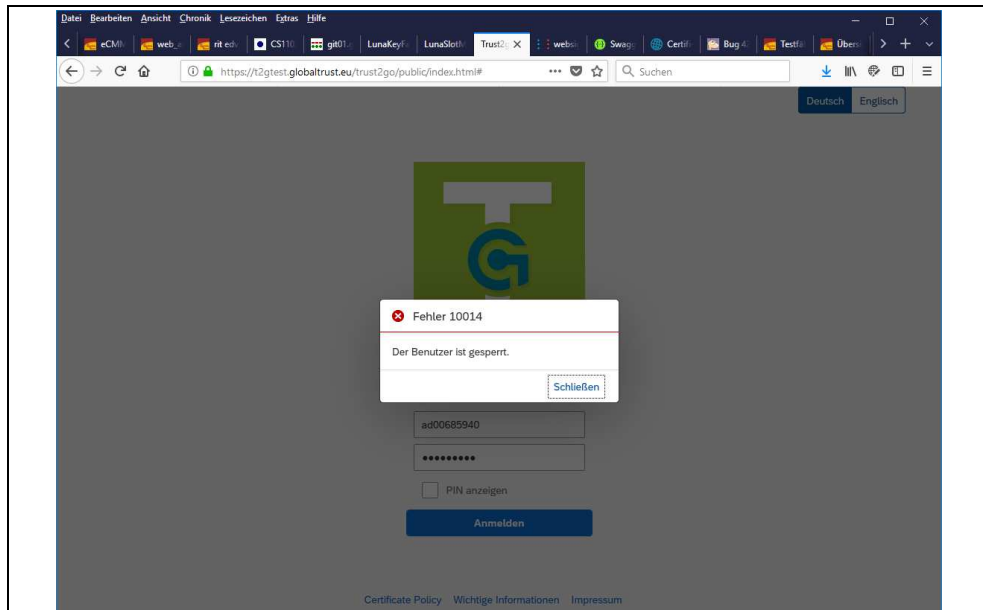


Abbildung 125: Sperre Signator Web VI

B) SPERRE SIGNATOR MITTELS 'TRUST2GOAUTHAPP'

82

nicht möglich

22 [SPERREVDA] SPERRE DURCH DEN VDA

83

Wenn ist eine Sperre sinnvoll?

- Der ⇒ Signator hat seinen ⇒ AktivierungsPIN vergessen.
- Der ⇒ Signator vertraut Trust2Go nicht mehr.

Sperrgründe unabhängig vom Signator

- Der VDA stellt Aktivitäten fest, die entgegen den Bestimmungen von Trust2Go durchgeführt werden.
- Der VDA stellt Aktivitäten fest, die dem VDA, dem ⇒ Signator oder Dritten schaden könnten.
- Dritte, die Gründe glaubhaft machen können, die eine rechtswidrige Verwendung von Trust2Go durch einen ⇒ Signator nahelegen.
- Technische Gründe, die Zweifel an der Zuverlässigkeit des Trust2Go-Betriebs ergeben.

Die Sperre erfolgt über die interne Verwaltung des VDA und erfordert entweder einen Antrag des ⇒ Signators (ohne Begründung) oder einen der vom ⇒ Signator unabhängigen Sperrgründe.

Zur Sperre ist kein Nachweis eines Schadens oder eines rechtswidrigen Verhaltens erforderlich. Es reicht, wenn die vorgebrachten Gründe glaubhaft bzw. plausibel sind.

Erfolgt die Sperre nicht auf Antrag des ⇒ Signators, dann wird dieser unverzüglich über die Sperre und den Grund per eMail verständigt.

23 [AKTACCOUNT] FREIGABE / AUFHEBUNG SPERRE

84

Gründe der Sperre eines Accounts

- Der ⇒ Signator hat seinen ⇒ AktivierungsPIN vergessen.
- Der ⇒ Signator mehr als fünfmal seinen ⇒ AktivierungsPIN falsch eingegeben.
- Der ⇒ Signator hat die Sperre über 'Trust2GoWeb' aktiviert (⇒ 21 [SperreSignator] Sperre durch den Signator, p187).
- Der VDA hat auf Grund objektiver Fakten berechnigte Zweifel an der korrekten Nutzung des Accounts und hat ihn gesperrt.

A) AUFHEBUNG SPERRE OHNE VERLUST DES AKTIVIERUNGSPIN (KEINE NEUAUSSTELLUNG ZERTIFIKATE)

84

- Signator beantragt Aufhebung gemäß Policy des VDA (schriftlich, telefonisch, eMail, Web-Formular): ⇒ [GCP] 4.9 + [GCPS] 4.9
- der Antrag wird gemäß Policy des VDA auf Authentizität geprüft: ⇒ [GCP] 4.9 + [GCPS] 4.9
- der VDA schaltet Account frei
- Signator kann 'Trust2GoAuthApp' und 'Trust2GoWeb' mit bisherigen ⇒ AktivierungsPIN weiter benutzen

B) AUFHEBUNG SPERRE NACH VERLUST DES AKTIVIERUNGSPIN UND NEUAUSSTELLUNG ZERTIFIKATE

84

Falls der ⇒ Signator seinen ⇒ AktivierungsPIN vergisst, gibt es keine Möglichkeit die ⇒ QRSCD Private Key wieder zu aktivieren. Es müssen neue Zertifikate und ⇒ QRSCD Private Keys ausgestellt und aktiviert werden.

Vorbereitung:

- Signator beantragt Aufhebung gemäß Policy des VDA melden (schriftlich, telefonisch, eMail, Web-Formular): ⇒ [GCP] 4.9 + [GCPS] 4.9
- diese Meldung wird gemäß Policy des VDA auf Authentizität geprüft: ⇒ [GCP] 4.9 + [GCPS] 4.9
- alle bisher ausgestellten Trust2Go-Zertifikate MÜSSEN werden widerrufen
- neue Zertifikate werden gemäß Policy des VDA mit ⇒ TransportPIN ausgestellt (⇒ [GCP] 4.3)
- Signator erhält die Zugangsdaten für die neuen Zertifikate
- Der VDA gibt den ⇒ 2. Auth-Faktor frei unbekannt)
- anschließend kann der ⇒ Signator das Zertifikat mittels 'Trust2GoAuthApp' oder 'Trust2GoWeb' aktivieren (abhängig vom bisher verwendeten ⇒ 2. Auth-Faktor)

(1) Aktivierung neues Zertifikat mittels 'Trust2GoAuthApp' 85

Anwendungsfall

- Signator verwendet 'Trust2GoAuthApp' als \Rightarrow 2. Auth-Faktor und möchte sie weiter verwenden
- es das neue Zertifikat analog zur Neuregistrierung aktiviert:
 \Rightarrow 20 [NeuRegAuthApp] NeuRegistrierung 'Trust2GoAuthApp', p183

(2) Aktivierung neues Zertifikat mittels 'Trust2GoWeb' 85

Anwendungsfall

- Signator verwendet SMS als \Rightarrow 2. Auth-Faktor und möchte sie weiter verwenden
- Es ist noch kein Zertifikat aktiviert
- der \Rightarrow Signator erstellt den \Rightarrow AktivierungsPIN und MUSS in derselben Session die neuen Zertifikate aktivieren (\Rightarrow 15 [AktWeitPrivKeyWeb] Aktivierung weiteren Private Key mittels 'Trust2GoWeb', p160)

Ablauf Ident zu 10 [ErstRegAuthWeb] (Erst)Registrierung 'Trust2GoWeb' - inklusive Aktivierung QRSCD Private Key

Hinweis

Fehlermeldung beim Versuch SMS als \Rightarrow 2. Auth-Faktor zu verwenden, obwohl eine \Rightarrow AuthenticationApp registriert ist.

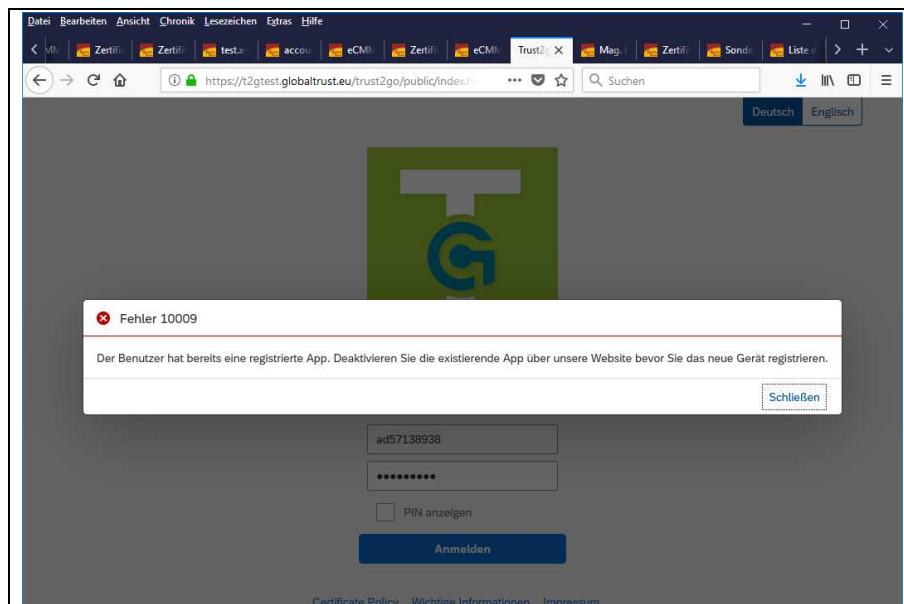


Abbildung 126: Fehlermeldung SMS zu aktivieren, obwohl AuthenticationApp registriert ist

24 [LOGAPP] ÜBERMITTLUNG LOGDATEN AUS 'TRUST2GOAUTHAPP'

86

Bei Problemen in der Nutzung der ⇒ AuthenticationApp hat der ⇒ Signator die Möglichkeit die lokalen Logdaten der 'Trust2GoAuthApp' an den VDA zu übermitteln.

Diese Funktion steht auch dann zur Verfügung, wenn der Benutzername - aus welchen Gründen auch immer - nicht mehr aktiv ist oder kein gültiger Vertrag zur Verfügung steht.

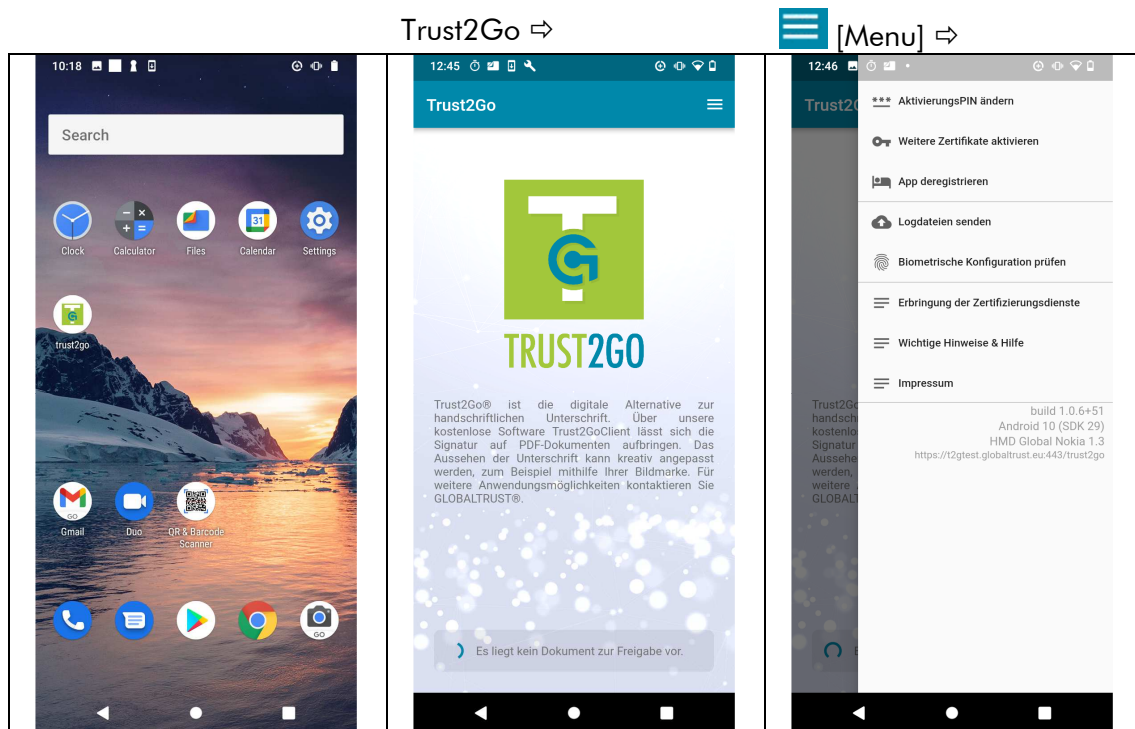


Abbildung 127: Versand Logdaten I

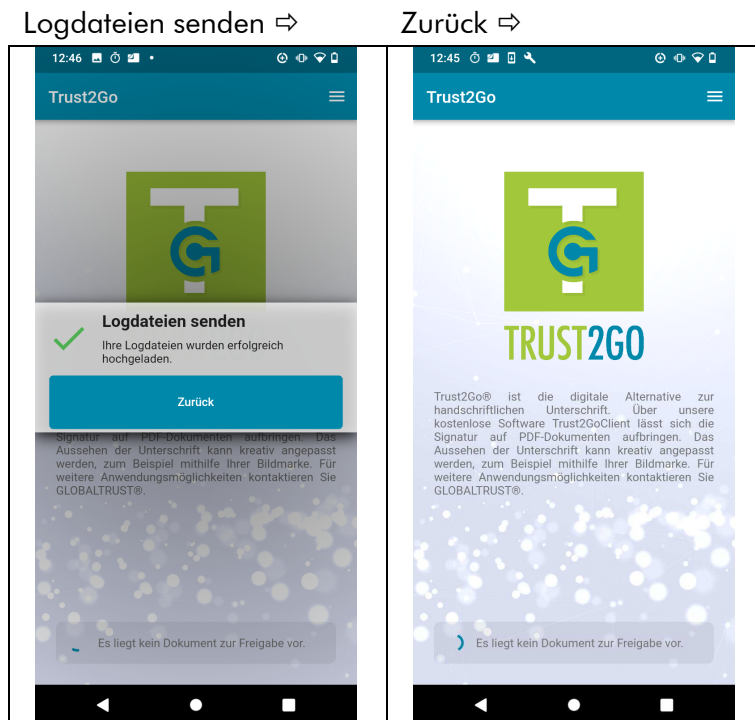


Abbildung 128: Versand Logdaten II

25 [SIGNCHECKADOBE] SIGNATURCHECK IN ADOBE ACROBAT DC

88

Hinweis

Der Prozess [SignCheckAdobe] ist kein Trust2Go-Prozess sondern stellt eine einfache Methode dar Trust2Go-Signaturen durch ein kostenloses und allgemein verfügbares Produkt eines Drittherstellers zu prüfen.

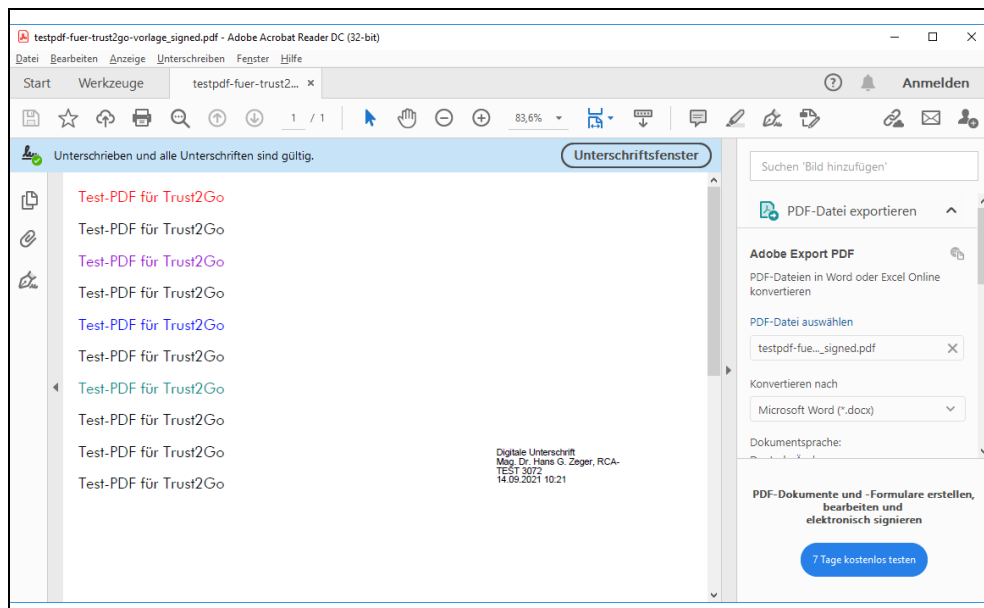


Abbildung 129: Signaturcheck I

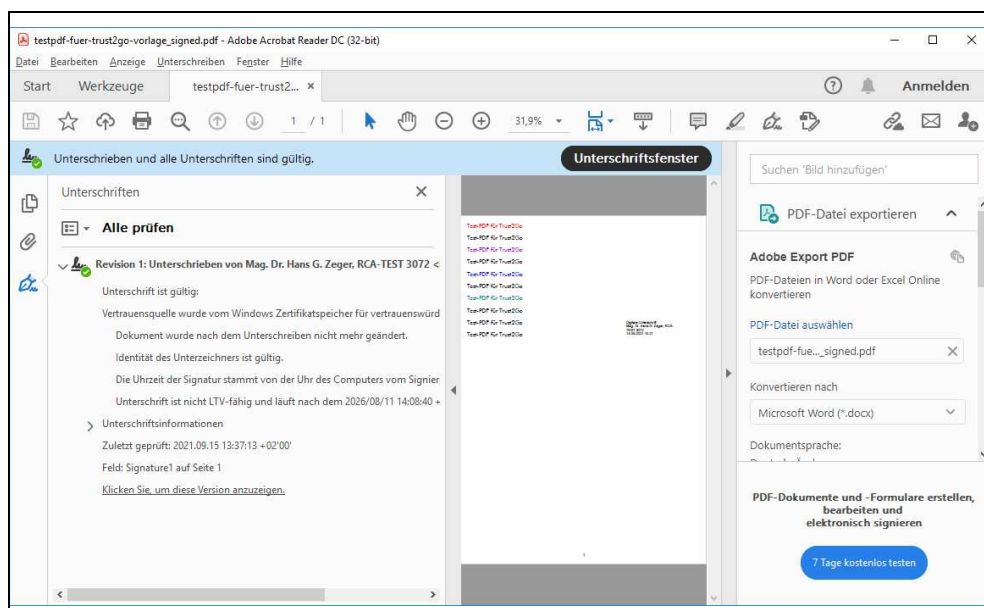


Abbildung 130: Signaturcheck II

"Revision 1" ⇒ (rechte Maustaste) ⇒

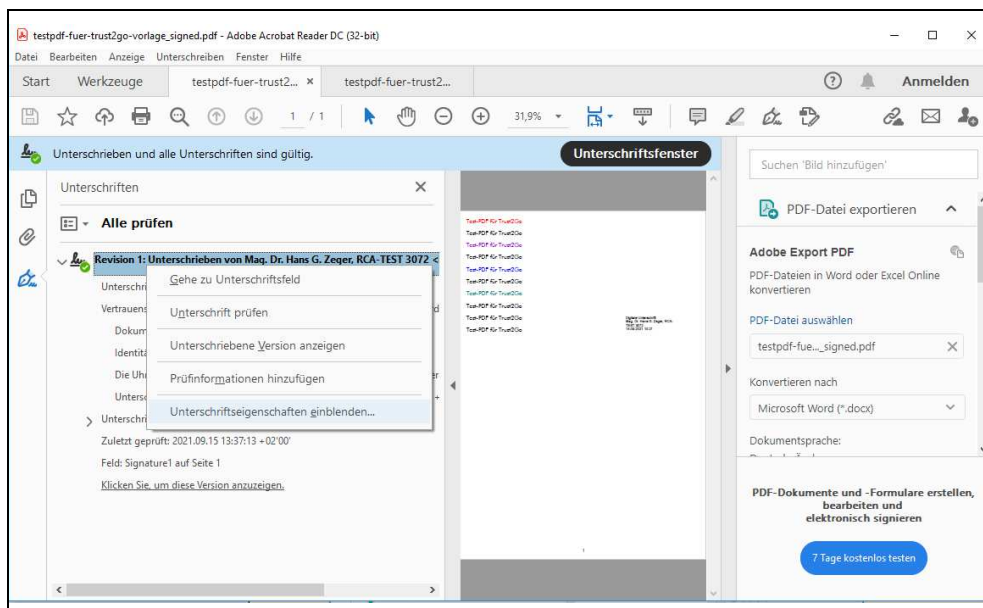


Abbildung 131: Signaturcheck III

Unterschriftseigenschaften einblenden... ⇒

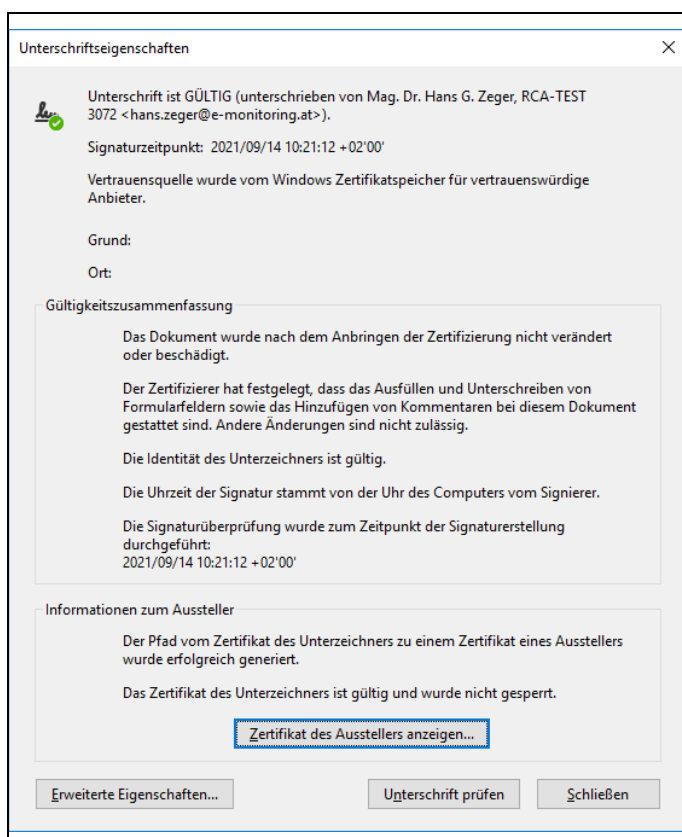


Abbildung 132: Signaturcheck IV

Zertifikat des Ausstellers anzeigen... ➞

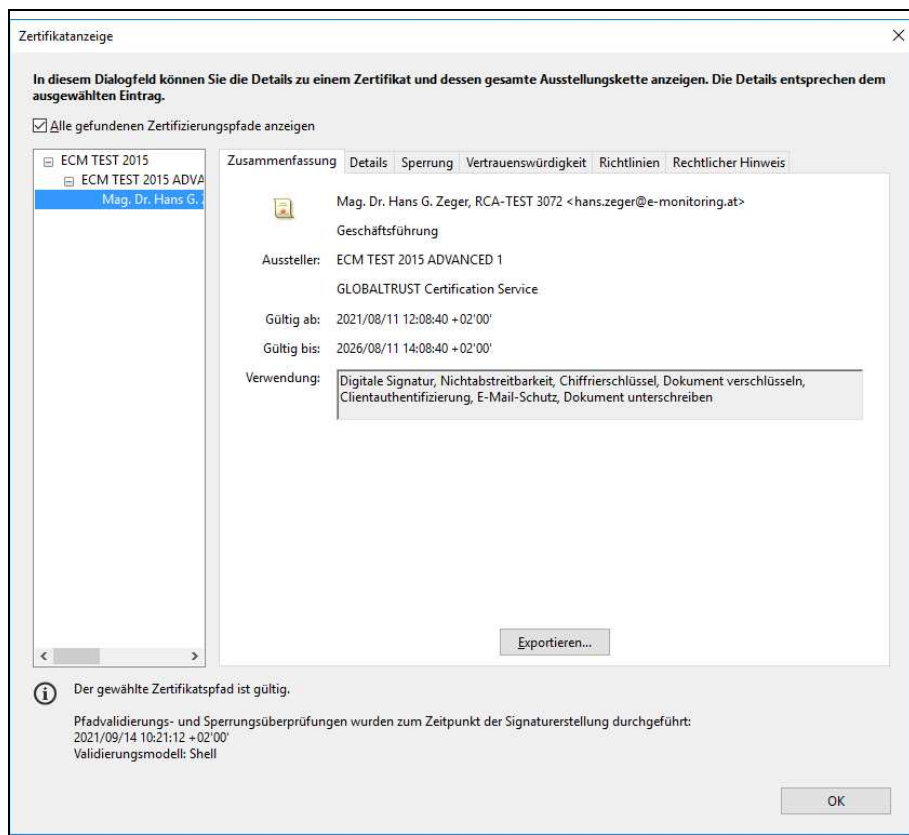


Abbildung 133: Signaturcheck V

OK ➞ Schließen ➞

26 [SIGNCHECKEU] TEST-TOOLS DER EUROPÄISCHEN KOMMISSION

91

Die erstellten ⇒ Signaturen erfüllen die Vorgaben der EU. Die Konformität kann durch externe Testtools geprüft werden.

- Digital Signature Service (DSS) Demo Tool:

Prüftool: <https://ec.europa.eu/cefdigital/DSS/webapp-demo/>

Info:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Start+using+Digital+Signature+Services+%28DSS%29+-+Demo#>

- ETSI Signature Conformance Checker (zT unvollständig/fehlerhaft)

(erfordert Registrierung als Benutzer)

Prüftool: <https://signatures-conformance-checker.etsi.org/pub/index.shtml>

Hinweis I

Sollte eine Konformitätsprüfung Fehlermeldungen bringen, dann sollte der ⇒ Signator den VDA unter Angabe des verwendeten Zertifikates, des Prüfergebnisses (Protokolle, Dateien, Screenshots) und eines signierten Dokuments informieren. Der VDA analysiert die Gründe für die fehlerhafte Prüfung und - sofern der Fehler in seinem Einflussbereich liegt - behebt den Fehler.

Hinweis II

Die Konformität mit den EU-Vorgaben garantiert noch keine automatische Anerkennung durch Software Dritter (Hersteller von Office-Paketen, pdf-Readern, Dokumentenmanagement-Systemen usw.). Es kann im Einzelfall erforderlich sein diese Produkte für den Einsatz von Trust2Go zu konfigurieren.

27 [CHANGESERV] WECHSEL 'TRUST2GOAUTHAPP' SERVER

92

Hinweis

Dieser Schritt darf nur erfolgen, wenn vorab die 'Trust2GoAuthApp' deregistriert wurde
⇒ 17 [DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp'

Erfolgt vorab keine Deregistrierung, dann kann weder die Produktions- noch die Test-Umgebung verwendet werden!

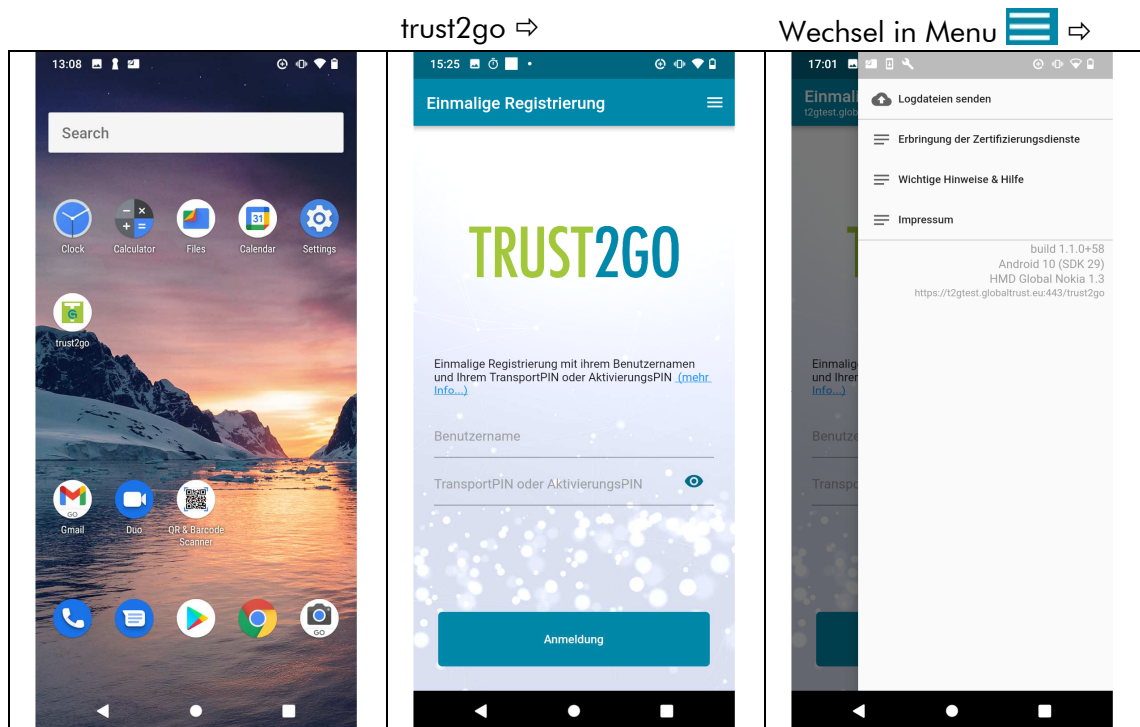


Abbildung 134: Wechsel Plattform I

ab Version 1.1.1-59: 5
mal Tab auf Leerfläche

25846 ⇨ erweitertes Menu
⇨

Switch to
[https://t2gtest\(test\)](https://t2gtest(test)) ⇨

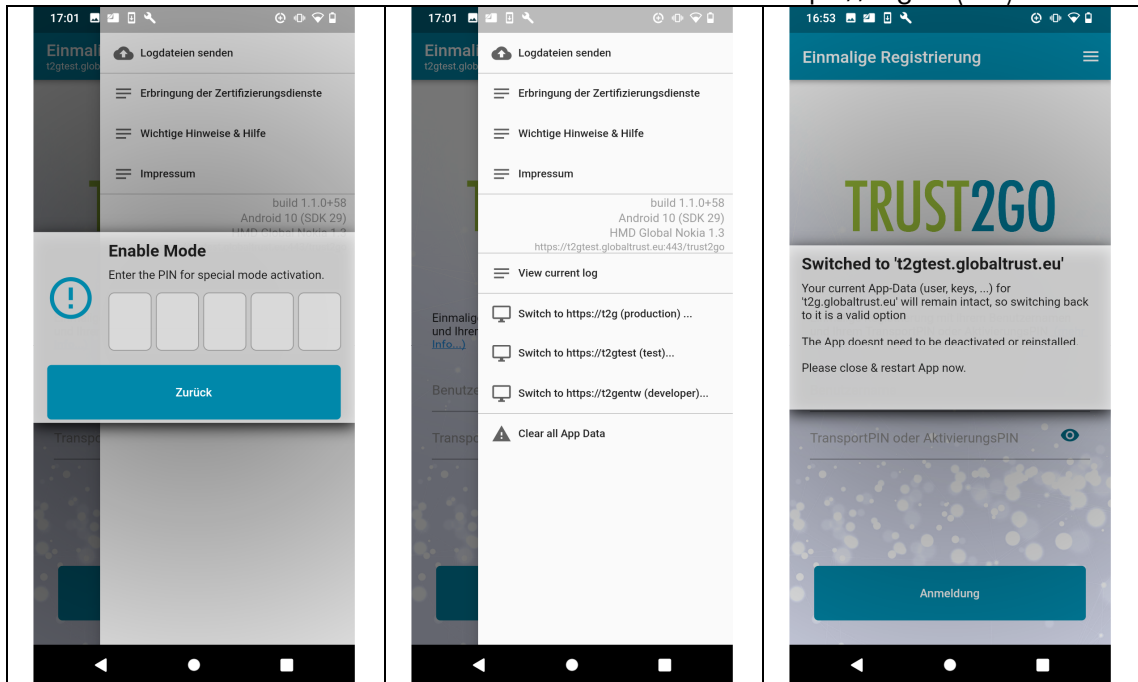


Abbildung 135: Wechsel Plattform II

Wechsel Task-Übersicht ⇨ ☐

Schließen App (rechts
wischen) ⇨

Wechsel zu Übersichtsseite
☐ ⇨

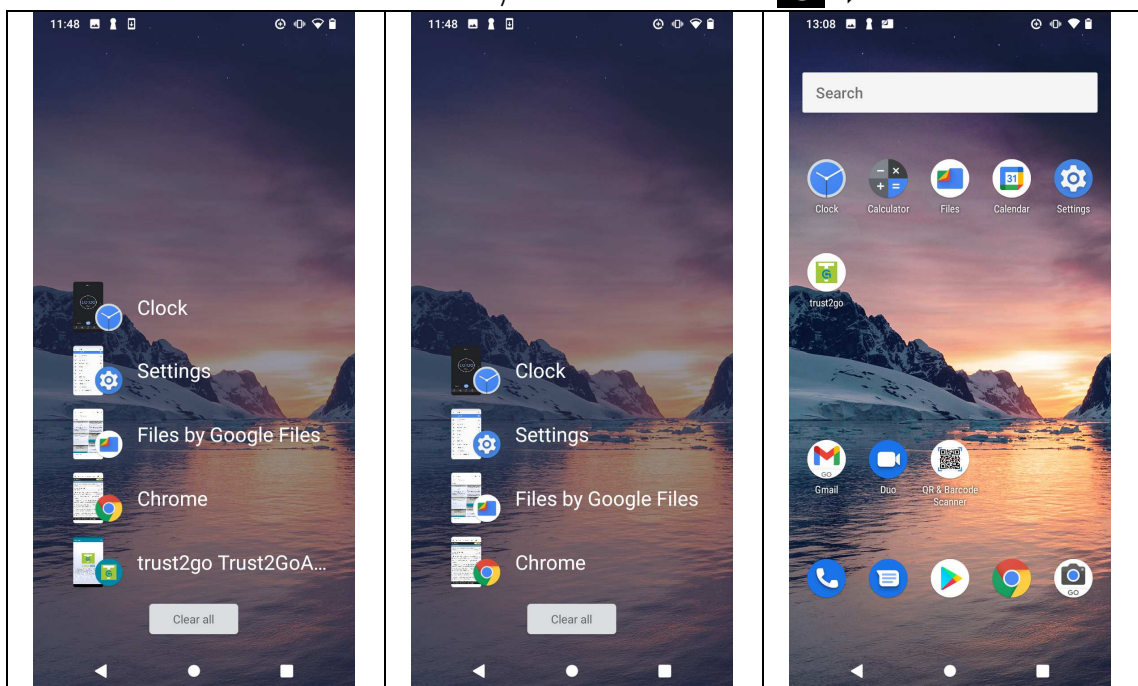


Abbildung 136: Wechsel Plattform III

28 [CHANGEENV] WECHSEL 'TRUST2GOAUTHAPP' ZWISCHEN TEST- UND PRODUKTIONS-UMGEBUNG

94

Dieser Abschnitt betrifft ausschließlich Nutzer von Testaccounts oder Nutzer, die zwischen Test- und Produktionsumgebung wechseln wollen.

Hintergrundinformation

Das Smartphone in Verbindung mit der 'Trust2GoAuthApp' stellt den gemäß eIDAS für qualifizierte Signaturen erforderlichen 2. Faktor bzw. Identitätsnachweis dar. Je Smartphone kann immer nur ein Identitätsnachweis gleichzeitig verarbeitet werden. Produktions- und Testumgebung sind vollständig getrennt, die 'Trust2GoAuthApp' auf einem Smartphone kann immer nur für eine Umgebung genutzt werden. Parallelnutzungen von mehreren Betriebsumgebungen oder mehreren Benutzernamen sind nicht möglich.

Drei Schritte zum Wechsel Test ⇔ Produktion erforderlich

- DeRegistrierung der 'Trust2GoAuthApp' in bestehender Umgebung
⇒ 17 [DeRegAuthApp] DeRegistrierung mittels 'Trust2GoAuthApp'
- Wechsel der Umgebung (Wechsel des Trust2Go-Servers)
⇒ 27 [ChangeServ] Wechsel 'Trust2GoAuthApp' Server
- Registrierung der 'Trust2GoAuthApp' in neuer Umgebung
⇒ 9 [ErstRegAuthApp] (Erst)Registrierung 'Trust2GoAuthApp' - inklusive Aktivierung QRSCD Private Key

TIPP

Es wird empfohlen für Test- und Produktionsumgebung denselben ⇔ AktivierungsPIN zu verwenden. Der ⇔ AktivierungsPIN ist den jeweiligen Zertifikaten fix zugeordnet. Geht der ⇔ AktivierungsPIN verloren gibt es keine Möglichkeit mehr die Zertifikate weiter zu benutzen und sie müssen widerrufen werden.

Hinweis

Wurden keine neuen Zertifikate angefordert bzw. sind alle bisherigen Zertifikate aktiviert, dann fällt der Teilschritt "Aktivierung QRSCD Private Key" weg.

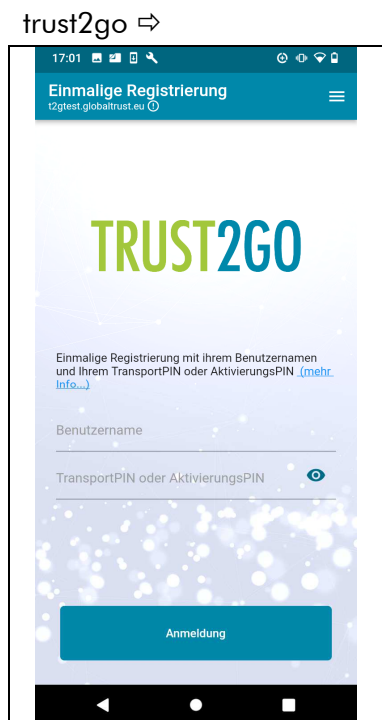


Abbildung 137: Wechsel Plattform IV

Hinweis

Sollen sowohl Test-Zertifikate als auch Produktions-Zertifikate verwendet werden, muss VOR jedem Wechsel zwischen Test und Produktion die 'Trust2GoAuthApp' der vorgegebene Ablauf wiederholt werden.

Ein Wechsel zwischen Test- und Produktionsumgebung OHNE vorherige Deregistrierung ist nicht möglich.

Keine Deinstallation der 'Trust2GoAuthApp'

Keinesfalls sollte die 'Trust2GoAuthApp' deinstalliert werden. Erfolgt eine Deinstallation ohne vorherige DeRegistrierung werden die Zertifikate des Signators aus Sicherheitsgründen gesperrt!

Last overall page of this sector: 203