A-Trust GmbH
Landstraßer Hauptstraße 1b E02, A-1030 Wien
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.a-trust.at

A-Trust GmbH
Liste der empfohlenen Komponenten und Verfahren

Version: 1.7.28
Datum: 24.10.2024

Datum	Rev	Autor:in	Änderungen
3.4.2009	1.7.4	Gregor Jöbstl	Kobil TriCAP Reader
10.9.2009	1.7.5	Gregor Jöbstl	MOCCA (Online BKU) hinzugefügt, STARCOS SPK 2.3 Karte entfernt
22.12.2009	1.7.6	Gregor Jöbstl	STARCOS 3.4 Health AHC C1 hinzugefügt
2.2.2010	1.7.7	Gregor Jöbstl	cyberJack e-com plus hinzugefügt
8.6.2010	1.7.8	Gregor Jöbstl	Namenänderungen bei A-Trust Software, Aufnahme A-Trust Bürgerkartensoftware, Entfernung des Kobil EMV-TriCAP Kartenlesers
28.6.2010	1.7.9	Gregor Jöbstl	Aufnahme von div. Webbrowsern, Aufnahme Cherry ST-2000 Smartcard Reader
13.1.2011	1.7.10	Gregor Jöbstl	Aufnahme Cherry ST-2xxx Smartcard Reader (FW 6.01)
07.6.2011	1.7.11	Gregor Jöbstl	Aufnahme von ACOS EMV-A05V1, Namesänderung bei a.sign MultiSign
10.10.2011	1.7.12	Gregor Jöbstl	Towitoko CHIPDRIVE entfernt
06.07.2012	1.7.13	Ramin Sabet	SecSigner, a.sign Client Version
16.01.2013	1.7.14	Ramin Sabet	trustView Version angepasst, Adobe Reader Version angepasst
10.03.2014	1.7.15	Ramin Sabet	trustView Signaturformate, Handy-Signatur Signaturformate, A-Trust BKU Signaturformate angepasst
28.04.2017	1.7.16	Ramin Sabet	A-Trust TanApp (3.2), Acrobat Versionen (5.7), hotPDFSign entfernt, alte SmartCards entfernt (2), BDC EDV -> BDC IT-Engineering GmbH, SignCube Version (4), trustDesk Version (4), MBS und hotSign Version (5.4),
23.05.2017	1.7.17	Ramin Sabet	Webbrowserversionen (5.2)
21.07.2017	1.7.18	Ramin Sabet	Adresse, Logo
14.02.2018	1.7.18	Ramin Sabet	Kartenleser-Kompatibilität (3)
27.02.2019	1.7.19	Ramin Sabet	QWACS (7)
07.03.2019	1.7.20	Ramin Sabet	Adobe Reader (5.7)
24.07.2019	1.7.21	Ramin Sabet	StarCOS entfernt (2)
16.06.2020	1.7.22	RS, JC	Adobe Reader (5.7) Mobile PDF (5.8)
21.07.2022	1.7.23	IH	FIDO Token (6)
26.07.2022	1.7.24	IH	FIDO 2 Level 2 (6), Logo
27.02.2023	1.7.25	IH	Signaturkarten ACOS-IDv2.0

01.08.2023	1.7.26	RS, IH	a.sign PDF, a.sign MultiSign entfernt Anpassungen Kartenleser (3), empfohlene Browser (3.1), App (3.2), Signaturapplikationen (4), sichere Anzeige (5.2), Adobe Acrobat und Adobe Reader (5.7), FIDO Liste (6)
16.08.2023	1.7.27	RS, IH	BDC HotSign, Openlimit entfernt
24.10.2024	1.7.28	IH	Signaturkarten ACOS-04, ACOS-05 entfernt Änderung TanApp zu A-Trust Signatur App

Tabelle 1: Dokumentenhistorie

Inhaltsverzeichnis

1 Allgemeines

Die von A-Trust GmbH empfohlenen Komponenten und Formate für Sichere Signaturen behandeln eine qualitätsgesicherte Arbeitsumgebung der zertifikatsinhabenden Person, die mit einer von A-Trust GmbH ausgestellten Signaturerstellungseinheit (Smartcard) eine sichere digitale Signatur erstellt.
Das Hauptaugenmerk der A-Trust GmbH Empfehlung wurde auf die folgenden Aspekte gelegt:

- Signaturerstellungseinheit (Karte)
- PIN Eingabe (Kartenleser)
- Signaturanwendungen (Hashverfahren)
- Software zur vertrauenswürdigen Anzeige

Diese Liste wird stets aktuell gehalten und stellt die jeweils am Markt verfügbaren und von A-Trust GmbH empfohlenen Produkte zur Erstellung sicherer Signaturen dar. Die A-Trust GmbH Empfehlung umfasst die Kompatibilität der angeführten Komponenten mit den Smart Card- und Zertifikatsprodukten von A-Trust GmbH, sowie die Korrektheit der Zertifizierungen und Bescheinigungen.

D. h., dass die angeführten Produkte schon im Rahmen der Evaluierungen auf das Zusammenwirken mit A-Trust GmbH Produkten geprüft wurden. Um sicherzustellen, dass die unterschiedlichen Komponenten (wie z. B. Kartenleser und Viewer) miteinander kompatibel sind, müssen dazu unbedingt die Informationen der Hersteller berücksichtigt werden.

1.1 Voraussetzungen für eine vertrauenswürdige Einsatzumgebung

Die signierende Person muss an seinen Signaturarbeitsplatz besondere Bedingungen stellen, um die sichere Signaturerstellung in einer vertrauenswürdigen Einsatzumgebung zu gewährleisten:

- Wenn der Rechner mehr als einer Person zugänglich ist oder eine Internetverbindung besteht, muss regelmäßig für einen aktuellen Virenschutz gesorgt werden.
- Einrichtung einer lokalen Firewall (z. B. Windows Firewall).
- Die vom herstellenden Unternehmen des Betriebssystems empfohlenen Sicherheitsupdates müssen installiert werden.
- Die von A-Trust GmbH empfohlenen Komponenten und Verfahren müssen stets in der aktuellen Version verwendet werden (Secure Viewer, Treibersoftware für Kartenleser).

2 Signaturkarten

Die nachstehende Liste weist alle von A-Trust GmbH für Sichere Signaturen ausgegebenen Signaturerstellungseinheiten aus. Eine sichere Signatur ist nur unter Verwendung des als 'Signaturzertifikats' bezeichneten Schlüssel der Sicheren Signaturerstellungseinheit (SSCD) möglich.

- Smart Card mit Chip Infineon SLE78CFX*P und Betriebssystem CardOS V5.3 QES, V1.0
- Smart Card mit Chip Infineon SLC52GXX448 oder SLC52GXX348 und Betriebsystem ACOS-IDv2.0

3 Kartenleser

Die PIN (Personal Identification Number) ist eine Ziffernfolge, die auch als Aktivierungsdaten für die Signaturerstellung bezeichnet wird. A-Trust GmbH empfiehlt ausschließlich Kartenlesegeräte mit eigenem Nummerneingabefeld für die sichere PIN-Eingabe. Der Schutz der PIN für die sichere Signatur kann nur durch Eingabe am Nummernfeld eines von A-Trust GmbH empfohlenen Kartenlesegeräts gewährleistet werden.

Es ist zu beachten, dass diese Liste nichts über die Kompatibilität der Karten zu den Kartenlesegeräten aussagt, sondern nur ob die jeweiligen Produkte für die Erstellung einer qualifizierten Signatur geeignet sind. Die jeweils aktuellsten Kartenleser sind unter http://www.a-trust.at/reader zu finden.

3.1 Sichere Eingabe von Aktivierungsdaten im Browser in Verbindung mit a.sign premium mobile (Handy-Signatur)

Für die sichere Eingabe von Aktivierungsdaten in Verbindung mit a.sign premium mobile werden folgende Browser Applikationen in den jeweils aktuellsten Versionen empfohlen:

- Microsoft Edge (Microsoft Corporation)
- Firefox (Mozilla Foundation)
- Opera (Opera Software ASA)
- Safari (Apple Inc.)
- Google Chrome (Google Inc.)

A-Trust GmbH empfiehlt den lokalen Signaturarbeitsplatz (lokaler PC) durch geeignete und dem Stand der Technik entsprechende Maßnahmen (Antiviren Software, Firewalls, etc...), vor dem unerlaubten Abfangen und Mitlesen der Aktivierungsdaten durch dritte zu schützen. Weiters empfiehlt A-Trust GmbH sämtliche Browserfunktionen, die ein Speichern der Feldeingaben (Aktivierungsdaten) zum Ziel haben, für die Benutzung von a.sign premium mobile zu deaktivieren (z. B. Autovervollständigung, Speichern von Passworten).

3.2 Sichere Eingabe von Aktivierungsdaten in der A-Trust Signatur App

Für die Eingabe von Aktivierungsdaten wurde eine Software für mobile Endgeräte entwickelt, welche die Kommunikation mit dem Server übernimmt. Ausgelöst kann eine Signatur durch die App mittels biometrischer Daten beziehungsweise dem GerätePIN werden. Diese App existiert für folgende Betriebssysteme:

- Android
- Apple iOS

A-Trust GmbH empfiehlt auf den mobilen Endgeräten - falls unterstützt - eine aktuelle Version einer Sicherheitssoftware einzusetzen, um das Endgerät vor Schadsoftware zu schützen. Dies kann ein komplizierter Schritt sein, der abhängig von dem eingesetzten Endgerät unterschiedlich durchzuführen ist, wird A-Trust GmbH eine Zusammenfassung der Möglichkeiten/Empfehlungen veröffentlichen und die Signierenden in der Belehrung darauf hinweisen.

4 Signaturapplikationen

Die Signaturapplikation berechnet den Hashwert des zu signierenden Dokuments und wird zur Aufbringung der Signatur verwendet. Die angeführten Produkte wurden auf die einwandfreie Implementierung von kryptographisch sicheren Hashverfahren geprüft und sind für Sichere Signaturen geeignet.

Hinweis: Diese Produkte können häufig deckungsgleich mit denen der sicheren Anzeige sein!

- a.sign client Version 1.3 (A-Trust GmbH)
- a.sign Bürgerkartensoftware Version 1.x (A-Trust GmbH)
- trustDesk ab Version 4.0 (IT Solution GmbH)
- Signatursoftware MBS Modul zur Erstellung sicherer Signaturen (BDC IT-Engineering GmbH)
  - für Java Integration v1.0.9
  - für C/C++ Integration v1.0.9
  - für Java Integration v2.0.2
  - für C/C++ Integration v2.0.2

  Hinweis: Das MBS-Modul ist integrierter Bestandteil des Electronic Banking MBS-Paketes.
- SecSigner Version 5.0 (SecCommerce Informationssysteme GmbH)
- MOCCA (Modular Open Citizen Card Architecture), Version entsprechend Die österreichische Bürgerkarte - Version 1.2

5 Software zur vertrauenswürdigen Anzeige

Unter vertrauenswürdiger Anzeige versteht man Produkte, die gewährleisten, dass nur die der signierenden Person dargestellten Daten auch tatsächlich signiert werden. Es werden auch die empfohlenen Dokumenten Formate, die von diesen Produkten sicher angezeigt werden können, angeführt.
Nachfolgend finden Sie die von A-Trust GmbH empfohlenen Produkte:

5.1 a.sign Bürgerkartensoftware Version 1.x (A-Trust GmbH)

Die zu signierenden Dokumente entsprechen der SecurityLayer Spezifikation 1.2 des Bundes [1]. Achtung es gibt auch eine nicht aktuelle Version 1.2: http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20080220/

5.1.1 text/xml

Die a.sign Bürgerkartensoftware benutzt XML als Dokumentenformat.

5.1.2 text/plain

Für die Darstellung der Daten wird UTF-8 verwendet.

5.1.3 application/pdf

Für die Darstellung wird ein installierter Adobe Reader vorausgesetzt, oder zum Download angeboten.

5.2 Webbrowser zur sicheren Anzeige in Verbindung mit a.sign premium mobile (Handysignatur)

Zur sicheren Anzeige der Signaturdaten in Verbindugn mit a.sign premium mobile (Handysignatur) werden folgende Browserapplikationen in der jeweils aktuellsten Version empfohlen:

- Microsoft Edge (Microsoft Corporation)
- Firefox (Mozilla Foundation)
- Opera (Opera Software ASA)
- Safari (Apple Inc.)
- Google Chrome (Google Inc.)

Als Dokumentenformate werden text/plain und text/xml eingesetzt.

5.2.1 text/xml

a.sign premium mobile benutzt XML als Dokumentenformat. Die zu signierenden Dokumente entsprechen der SecurityLayer Spezifikation 1.2 des Bundes.

5.2.2 text/plain

Für die Darstellung der Daten wird UTF-8 verwendet.

5.2.3 application/pdf

Für die Darstellung wird ein Link auf das PDF angeboten, welchen die signierende Person zum Download/Anzeige nutzen kann.

5.3 trustview secure viewer (IT Solution GmbH) Versionen: 2.1.1 rel. 9

http://www.a-sit.at/pdfs/bescheinigungen_sig/1035_Gutachten_TrustView_2_1_1R9_kurzfassung_final_S_S.pdf

trustView ist Bestandteil unterschiedlicher Distributionen und kann als trustDesk Basic, trustDesk Professional, trustDesk Business und diversen Kundenanpassungen (zB.: trustDesk BAIK-Archiv oder trustDesk GOG-Archiv) ausgeliefert werden.

Zur Signaturverifikation ist diese Version geeignet, da Sie laut Herstellerangaben neben SHA-1 auch SHA256 Signaturen verifizieren kann. Ab der Version, welche in Kapitelr 4 angeführt wird, ist die Standardeinstellung bei der Hash-Berechnung im Rahmen der Signatuerstellung SHA256.

5.3.1 text/xml

Siehe Bescheinigung A-SIT

5.3.2 cms

Siehe Bescheinigung A-SIT

5.4 Signatursoftware MBS Modul zur Erstellung sicherer Signaturen (BDC IT-Engineering GmbH)

- für Java Integration v1.0.9
- für C/C++ Integration v1.0.9
- für Java Integration v2.0.2
- für C/C++ Integration v2.0.2

Das MBS Modul zur Erstellung sicherer Signaturen benutzen als Characterset ein eingeschränktes ISO 8859-1. Diese Versionen unterstützen nach Herstellerangabe nur noch SHA256 zur Signaturerstellung.

Zeichen	Hexwert
Linefeed	0x0a
Space	0x20
#	0x23
-	0x2d
.	0x2e
0-9	0x30-0x39
A-Z	0x41-0x5a
a-z	0x61-0x7a
Ä	0xc4
Ö	0xd6
Ü	0xdc
ß	0xdf
ä	0xe4
ö	0xf6
ü	0xfc

5.5 SecSigner 3.6 (SecCommerce Informationssysteme GmbH)

Die folgenden Daten-/Dokumentformate werden von SecSigner unterstützt.

5.5.1 Reiner Text (plain text)

Für die Darstellung der Daten wird der Standardzeichensatz verwendet, den das Betriebssystem bereitstellt. Das ist in Europa das Characterset nach ISO 8859-1.

5.5.2 HTML (Subset)

Es werden folgende Tags des HTML 2.0 Standards unterstützt:
A, ADDRESS, B, BASE, BIG, BLOCKQUOTE, BR, CENTER, CITE, CODE, COMMENT, DD, DIR, DL, DT, EM, FONT, H1, H2, H3, H4, H5, H6, HEAD, HTML, HR, I, KBD, LI, LISTING, MENU, OL, P, PRE, SAMP, SMALL, STRONG, TABLE, TITLE, TT, TR, TD, UL, VAR, XMP.

Die HTML-Seite wird mit den Anzeigeoptionen

- ”Text”,
- ”HTML einfarbig” oder
- ”HTML mehrfarbig”

dargestellt, die die signierende Person zur Laufzeit des Signierprozesses vor der eigentlichen Signatur selbst beliebig auswählen und wechseln kann. Die HTML-Darstellung nutzt die im HTML-Dokument enthaltenen Formatierungs- und Farbinformationen zur Darstellung, wobei

der Hintergrund immer und unabhängig von der Farbinformation der HTML-Seite weiß dargestellt wird. In der Darstellungsoption "HTML einfarbig" wird der in der HTML-Seite enthaltene Text unabhängig von der Farbinformation der HTML-Seite schwarz dargestellt. In der Darstellungsoption "HTML mehrfarbig" wird der Text mit der Farbinformation der HTML-Seite dargestellt, mit folgender Ausnahme: unterscheidet sich die im HTML-Dokument definierte Textfarbe nicht deutlich genug von der Hintergrundfarbe "weiß", wird schwarz als Textfarbe verwendet.

5.5.3 PDF-A (ab Version 3.4)

Die Software SecSigner kann ab Version 3.4 auch zur Anzeige und Sicheren Signatur von Dokumenten im PDF-A Format verwendet werden.

5.6 Openlimit SignCubes Viewer (OPENLiMiT SignCubes AG)

Die Software Openlimit SignCubes Viewer ist integraler Bestandteil der Openlimit SignCubes Basiskomponenten und ist zur sichern Anzeige von Text, TIFF und PDF (1.7) Dokumenten geeignet.

5.7 Adobe Acrobat und Adobe Acrobat Reader

Die Applikationen der Adobe Acrobat Familie sollten immer auf dem neusten Stand gehalten werden. Es wird empfohlen Acrobat DC und Acrobat Reader DC mindestens in der Version 2020.009.20063.

Folgende Plugins oder Applikationen können in Kombination mit den Adobe Produkten verwendet werden.

- HotPDFVerify Version 2.18 (BDC IT-Engineering GmbH)
- e-sign for SAP Solution Version 2.3 (rit EDV-Consulting GmbH)

Auf Mobilen Plattformen wird empfohlen folgende Versionen der Adobe Produkte zu verwenden:

- Android Adobe: in der neuesten Version
- iOS Adobe: in der neuesten Version

5.8 PDF Viewer auf mobilen Plattformen

Auf mobilen Plattformen werden folgende PDF Viewer empfohlen:

- Android PDF Renderer welcher mit dem Betriebssystem Android >= 8 ausgeliefert wird.
- iOS Safari Webkit Engine welche mit dem Betriebssystem iOS >= 10 ausgeliefert wird.

Es soll darauf geachtet werden, stets die neuesten Updates für das Mobiltelefon zu installieren.

6 FIDO

Als zweiten Faktor zur Auslösung der ID Austria kann neben dem Mobiltelefon auch ein FIDO Token verwendet werden. Der Token muss mindestens eine FIDO 2 Level 2 Zertifizierung haben. A-Trust unterstützt nur folgende Token: https://www.a-trust.at/fido

7 QWACS

Qualifizierte Webseiten Authentifizierungs Zertifikate (QWACS)

Keine Bestimmungen.

Literatur

[1] Arno Hollosi, Gregor Karlinger, Thomas Rössler, and Martin Centner. Transportprotokolle für die Applikationsschnittstelle Security-Layer der österreichischen Bürgerkarte. https://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114/bindings/bindings.html, 2014. [Online; accessed 2023-08-14].