



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

Liste der empfohlenen Komponenten und Verfahren

Version: 1.7.25
Datum: 27.02.2023

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, STAR-COS 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, Namensänderung 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 (5.10) hotPDFSign entfernt BDC EDV -> BDC IT-Engineering GmbH SignCube Version (4) trustDesk Version (4) MBS und hotSign Version (5.4) alte SmartCards entfernt (2)
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 (5.10)
24.07.2019	1.7.21	Ramin Sabet	StarCOS entfernt (2)
16.06.2020	1.7.22	RS, JC	Adobe Reader (5.10) Mobile PDF (5.11)
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

Tabelle 1: Dokumentenhistorie

Inhaltsverzeichnis

1	Allgemeines	4
1.1	Voraussetzungen für eine vertrauenswürdige Einsatzumgebung	4
2	Signaturkarten	5
3	Kartenleser	6
3.1	Sichere Eingabe von Aktivierungsdaten im Browser in Verbindung mit a.sign premium mobile (Handy-Signatur)	7
3.2	Sichere Eingabe von Aktivierungsdaten in der TanApp (Handy-Signatur)	7
4	Signaturapplikationen	8
5	Software zur vertrauenswürdigen Anzeige	9
5.1	a.sign Bürgerkartensoftware Version 1.x (A-Trust GmbH)	9
5.1.1	text/xml	9
5.1.2	text/plain	9
5.1.3	application/pdf	9
5.2	Webbrowser zur sicheren Anzeige in Verbindung mit a.sign premium mobile (Handysignatur)	9
5.2.1	text/xml	10
5.2.2	text/plain	10
5.2.3	application/pdf	10
5.3	trustview secure viewer (IT Solution GmbH) Versionen: 2.1.1 rel. 9	10
5.3.1	text/xml	10
5.3.2	cms	10
5.4	Signatursoftware MBS Modul zur Erstellung sicherer Signaturen (BDC IT-Engineering GmbH)	10
5.5	BDC HotSign, Signatur-Client zur Erstellung sicherer Signaturen, Version 2.0.0 Rel. 09.07.2015 (BDC IT-Engineering GmbH)	11
5.5.1	text/plain	11
5.5.2	text/xml	12
5.5.3	text/html	13
5.6	SecSigner 3.6 (SecCommerce Informationssysteme GmbH)	22
5.6.1	Reiner Text (plain text)	22
5.6.2	HTML (Subset)	22
5.6.3	PDF-A (ab Version 3.4)	22
5.7	Openlimit SignCubes Viewer (OPENLiMiT SignCubes AG)	23
5.8	a.sign PDF	23
5.9	a.sign MultiSign	23
5.10	Adobe Acrobat und Adobe Acrobat Reader	23
5.11	PDF Viewer auf mobilen Plattformen	24
6	FIDO	25

1 Allgemeines

Die von A-Trust empfohlenen Komponenten und Formate für Sichere Signaturen behandeln eine qualitätsgesicherte Arbeitsumgebung der zertifikatsinhabenden Person, die mit einer von A-Trust ausgestellten Signaturerstellungseinheit (Smartcard) eine sichere digitale Signatur erstellt. Das Hauptaugenmerk der A-Trust 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 empfohlenen Produkte zur Erstellung sicherer Signaturen dar. Die A-Trust Empfehlung umfasst die Kompatibilität der angeführten Komponenten mit den Smart Card- und Zertifikatsprodukten von A-Trust, sowie die Korrektheit der Zertifizierungen und Bescheinigungen.

D. h., dass die angeführten Produkte schon im Rahmen der Evaluierungen auf das Zusammenwirken mit A-Trust 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 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 für Sichere Signaturen ausgegebenen Signaturerstellungseinheiten aus. Ein Sichere Signatur ist nur unter Verwendung des als 'Signaturzertifikats' bezeichneten Schlüssel der Sicheren Signaturerstellungseinheit (SSCD) möglich.

- Smart Card mit Chip NXP SmartMx P5CC037V0A und Betriebssystem ACOS EMV-A04V1, Configuration B und Digital Signature Application a-sign Premium
- Smart Card mit Chip Infineon SLE66CX360PE und Betriebssystem ACOS EMV-A05V1, Configuration B und Digital Signature Application a-sign Premium
- Smart Card mit Chip Infineon SLE78CFX*P und Betriebssystem CardOS V5.3 QES, V1.0
- Smart Card mit Chip Infineon SLC52GXX448 oder SLC52GXX348 und Betriebssystem ACOS-IDv2.0

3 Kartenleser

Die PIN (Personal Identification Number) ist eine Ziffernfolge, die auch als Aktivierungsdaten für die Signaturerstellung bezeichnet wird. A-Trust 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 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.

Nachfolgend die von A-Trust empfohlenen Kartenlesegeräte:

- Kobil KAAN Professional Firmware Version 2.0.8
- Kobil KAAN Advanced Version K104R3, Firmware Version 1.02
- Cherry PC-Tastaturen mit integriertem Chipkartenterminal
G83-6700LQZxx/01
G81-7015LQZxx/01
G81-8015LQZxx/01
G81-12000LTZxx/01
- Chipkartenterminal der Familie Cherry Smartboard xx44, Firmware Version 1.04
- Cherry SmartTerminal ST-2000U (Part. no.: ST-2000UCZ, ST-2000UCZ-R), Firmware Version 5.11
- Cherry SmartTerminal ST-2xxx (Part No. ST-20xxUxZ-x/xx HWV03), Firmwareversion: 6.01
- cyberJack e-com Chipkartenleser mit Tastatur und Display Firmware Version 2.0
- cyberJack pinpad Chipkartenleser mit Tastatur Firmware Version 2.0 und 3.0
- cyberJack pinpad Stapelsignatur mit Tastatur Firmware Version 4.0
- cyberJack secoder mit Tastatur Version 3.0
- cyberJack e-com plus Chipkartenleser mit Tastatur und Display Version 3.0
- Siemens Chipkartenleser-Tastatur KB SCR Pro, Firmware Version 1.06
- Chipkartenterminal der Familie CardMan Trust CM3621/CM3821, Firmware Version 6.00 der Omnikey GmbH

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 empfohlen:

- Internet Explorer (Microsoft Corporation), ab Version 8
- Firefox (Mozilla Foundation), ab Version 3.5.5
- Opera (Opera Software ASA), ab Version 10.54
- Safari (Apple Inc.), ab Version 5
- Google (Google Inc.), Chrome ab Version 5.0

A-Trust 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 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 TanApp (Handy-Signatur)

Für die Eingabe von Aktivierungsdaten wurde eine Software für mobile Endgeräte entwickelt, welche die Kommunikation mit dem Server übernimmt. Diese empfängt die TAN und übernimmt deren Anzeige. Alternativ kann über die Option SPEED-SIGN im Browser ein QR-Code angezeigt werden, welcher in der TanAPP abfotografiert wird und so an den Server übermittelt wird. Diese App existiert für folgende Betriebssysteme:

- Android
- Apple iOS
- BlackBerry
- Windows Phone

A-Trust 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 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)
- a.sign PDF Version 1.x.x.0 (A-Trust GmbH) (vormals VPDFSign)
- a.sign MultiSign Version 1.x.x.0 (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.

- BDC HotSign, Signatur-Client zur Erstellung sicherer Signaturen (BDC IT-Engineering GmbH)
 - Version 2.0
- SecSigner Version 5.0 (SecCommerce Informationssysteme GmbH)
- Openlimit SignCubes Basiskomponenten Version 2.10 (OPENLiMiT SignCubes AG)
- 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 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. Siehe Link: <https://www.buergerkarte.at/konzept/securitylayer/spezifikation/20140114/>. 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 Verbindung mit a.sign premium mobile (Handysignatur) werden folgende Browserapplikationen empfohlen:

- Internet Explorer (Microsoft Corporation), ab Version 11
- Edge (Microsoft Corporation), ab Version 40
- Firefox (Mozilla Foundation), ab Version 48
- Opera (Opera Software ASA), ab Version 37
- Safari (Apple Inc.), nur macOS, ab Version 9.1.3
- Google (Google Inc.), Chrome ab Version 50.0

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 Signatuererstellung.

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 BDC HotSign, Signatur-Client zur Erstellung sicherer Signaturen, Version 2.0.0 Rel. 09.07.2015 (BDC IT-Engineering GmbH)

Die folgenden Datenformate werden von hot:Sign unterstützt

5.5.1 text/plain

Die Daten werden ohne Interpretation der Formatierung angezeigt. Bei der Interpretation des Inhalts ist das Character-Set relevant, in dem die Daten vorliegen, dazu kann das Character-Encoding als zusätzlicher Parameter übergeben werden. Wird kein Character-Encoding angegeben, werden die Daten als ISO-8859-1 interpretiert.

Liste aller unterstützten Character-Sets:

ANSI_X3.4-1968	Cp869	Cp1124
Big5	Cp870	Cp1258
Big5-HKSCS	Cp871	Cp1381
Cp037	Cp874	Cp1383
Cp273	Cp875	Cp33722
Cp277	Cp918	EUC_CN
Cp278	Cp921	EUC_JP
Cp280	Cp922	EUC_JP_LINUX
Cp284	Cp930	EUC_KR
Cp285	Cp933	EUC_TW
Cp297	Cp935	ISO2022JP
Cp420	Cp937	ISO8859_1
Cp424	Cp939	ISO8859_2
Cp437	Cp942	ISO8859_3
Cp500	Cp942C	ISO8859_4
Cp737	Cp943	ISO8859_5
Cp775	Cp943C	ISO8859_6
Cp838	Cp948	ISO8859_7
Cp850	Cp949	ISO8859_8
Cp852	Cp949C	ISO8859_1
Cp855	Cp950	ISO8859_9
Cp856	Cp964	ISO8859_13
Cp857	Cp970	ISO8859_15_FDIS
Cp860	Cp1006	MS874
Cp861	Cp1025	MS932
Cp862	Cp1026	SJIS
Cp863	Cp1097	TIS620
Cp864	Cp1098	UTF8
Cp865	Cp1112	UnicodeLittleUnmarked
Cp866	Cp1122	
Cp868	Cp1123	

5.5.2 text/xml

Die Daten werden als XML-Daten interpretiert und die XML-Elemente werden hierarchisch dargestellt. Als Einrückungszeichen werden jeweils vier Leerzeichen verwendet.

Liste der zulässigen Character-Sets

ANSI_X3.4-1968	EBCDIC-CP-IT	ISO-8859-1
Big5	EBCDIC-CP-NL	ISO-8859-2
EBCDIC-CP-AR1	EBCDIC-CP-NO	ISO-8859-3
EBCDIC-CP-AR2	EBCDIC-CP-ROECE	ISO-8859-4
EBCDIC-CP-CA	EBCDIC-CP-SE	ISO-8859-5
EBCDIC-CP-CH	EBCDIC-CP-US	ISO-8859-6
EBCDIC-CP-DK	EBCDIC-CP-YU	ISO-8859-7
EBCDIC-CP-ES	EUC-JP	ISO-8859-8
EBCDIC-CP-FI	EUC-KR	ISO-8859-9
EBCDIC-CP-FR	GB2312	Shift_JIS
EBCDIC-CP-GB	KOI8-R	UTF-8
EBCDIC-CP-HE	ISO-2022-JP	Windows-31J
EBCDIC-CP-IS	ISO-2022-KR	

5.5.3 text/html

Die Daten werden nach dem HTML-Standard interpretiert und angezeigt, die zulässigen Character-Encodings entsprechen den Character-Sets für "text/xml". Der HTML Sprachumfang ist eingeschränkt und die zulässigen HTML Elemente in einem XML-Schema festgelegt. Wenn die vorliegenden Daten nicht dem spezifiziertem HTML Sprachumfang entsprechen, wird der Signaturvorgang abgebrochen. Zusätzlich werden die verwendbaren Text- und Hintergrundfarben eingeschränkt.

XML-Schema für den HTML-Sprachumfang:

```
<?xml version="1.0" encoding="UTF-8" ?>
<xs:schema targetNamespace="http://www.w3.org/1999/xhtml"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="http://www.w3.org/1999/xhtml">
  <xs:group name="Heading.class">
    <xs:choice>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element ref="h1" />
        <xs:element ref="h2" />
        <xs:element ref="h3" />
        <xs:element ref="h4" />
        <xs:element ref="h5" />
        <xs:element ref="h6" />
      </xs:choice>
    </xs:choice>
  </xs:group>
  <xs:group name="List.class">
    <xs:choice>
```

```
<xs:choice minOccurs="0" maxOccurs="unbounded">
  <xs:element ref="ul" />
  <xs:element ref="ol" />
  <xs:element ref="dl" />
</xs:choice>
</xs:choice>
</xs:group>
<xs:group name="Block.class">
  <xs:choice>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element ref="p" />
      <xs:element ref="blockquote" />
      <xs:element ref="table" />
      <xs:element ref="hr" minOccurs="0" maxOccurs="unbounded" />
      <xs:group ref="List.class" />
    </xs:choice>
  </xs:choice>
</xs:group>
<xs:group name="Block.mix">
  <xs:choice>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:group ref="Heading.class" />
      <xs:group ref="Text.class" />
      <xs:group ref="Block.class" />
    </xs:choice>
  </xs:choice>
</xs:group>
<xs:group name="Flow.mix">
  <xs:choice>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:group ref="Block.class" />
      <xs:group ref="Text.class" />
    </xs:choice>
  </xs:choice>
</xs:group>
<xs:group name="Text.class">
  <xs:choice>
    <xs:choice minOccurs="0" maxOccurs="unbounded">
      <xs:element ref="font" />
      <xs:element ref="br" />
      <xs:element ref="tt" />
      <xs:element ref="i" />
      <xs:element ref="b" />
      <xs:element ref="big" />
    </xs:choice>
  </xs:choice>
</xs:group>
```

```
<xs:element ref="sub" />
  <xs:element ref="sup" />
</xs:choice>
</xs:choice>
</xs:group>
<xs:simpleType name="Color">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Black" />
    <xs:enumeration value="black" />
    <xs:enumeration value="Silver" />
    <xs:enumeration value="silver" />
    <xs:enumeration value="Gray" />
    <xs:enumeration value="gray" />
    <xs:enumeration value="White" />
    <xs:enumeration value="white" />
    <xs:enumeration value="Maroon" />
    <xs:enumeration value="maroon" />
    <xs:enumeration value="Red" />
    <xs:enumeration value="red" />
    <xs:enumeration value="Purple" />
    <xs:enumeration value="purple" />
    <xs:enumeration value="Fuchsia" />
    <xs:enumeration value="fuchsia" />
    <xs:enumeration value="Green" />
    <xs:enumeration value="green" />
    <xs:enumeration value="Lime" />
    <xs:enumeration value="lime" />
    <xs:enumeration value="Olive" />
    <xs:enumeration value="olive" />
    <xs:enumeration value="Yellow" />
    <xs:enumeration value="yellow" />
    <xs:enumeration value="Navy" />
    <xs:enumeration value="navy" />
    <xs:enumeration value="Blue" />
    <xs:enumeration value="blue" />
    <xs:enumeration value="Teal" />
    <xs:enumeration value="teal" />
    <xs:enumeration value="Aqua" />
    <xs:enumeration value="aqua" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="FontSize">
  <xs:restriction base="xs:string">
    <xs:enumeration value="-1" />
  </xs:restriction>
</xs:simpleType>
```



```
<xs:enumeration value="+1" />
<xs:enumeration value="+2" />
<xs:enumeration value="+3" />
<xs:enumeration value="+4" />
<xs:enumeration value="2" />
<xs:enumeration value="3" />
<xs:enumeration value="4" />
<xs:enumeration value="5" />
<xs:enumeration value="6" />
<xs:enumeration value="7" />
</xs:restriction>
</xs:simpleType>
<xs:simpleType name="FontFace">
  <xs:restriction base="xs:string">
    <xs:enumeration value="Arial" />
    <xs:enumeration value="arial" />
    <xs:enumeration value="Times New Roman" />
    <xs:enumeration value="times new roman" />
    <xs:enumeration value="Verdana" />
    <xs:enumeration value="verdana" />
    <xs:enumeration value="courier new" />
    <xs:enumeration value="Courier New" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Length">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="1000" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="restrictedLength">
  <xs:restriction base="xs:string">
    <xs:pattern value="\\d2%" />
    <xs:pattern value="\\d1%" />
    <xs:pattern value="100%" />
    <xs:pattern value="\\d1" />
    <xs:pattern value="\\d2" />
    <xs:pattern value="\\d3" />
    <xs:pattern value="\\d4" />
    <xs:pattern value="10000" />
    <xs:pattern value="\\d1px" />
    <xs:pattern value="\\d2px" />
    <xs:pattern value="\\d3px" />
    <xs:pattern value="\\d4px" />
  </xs:restriction>
</xs:simpleType>
```

```
    <xs:pattern value="10000px" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Pixels">
  <xs:restriction base="xs:integer">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="1000" />
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="Number">
  <xs:restriction base="xs:nonNegativeInteger" />
</xs:simpleType>
<xs:complexType name="empty.type" />
  <xs:attributeGroup name="CellVAlign.attrib">
    <xs:attribute name="valign">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="top" />
          <xs:enumeration value="middle" />
          <xs:enumeration value="bottom" />
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:attributeGroup>
  <xs:attributeGroup name="CellHAlign.attrib">
    <xs:attribute name="align">
      <xs:simpleType>
        <xs:restriction base="xs:NMTOKEN">
          <xs:enumeration value="left" />
          <xs:enumeration value="center" />
          <xs:enumeration value="right" />
        </xs:restriction>
      </xs:simpleType>
    </xs:attribute>
  </xs:attributeGroup>
  <xs:complexType name="body.type" mixed="true">
    <xs:group ref="Block.mix" />
    <xs:attribute name="bgcolor" type="Color" />
    <xs:attribute name="text" type="Color" />
  </xs:complexType>
  <xs:element name="body" type="body.type" />
  <xs:simpleType name="FPI">
    <xs:restriction base="xs:normalizedString" />
  </xs:simpleType>
```

```
<xs:complexType name="html.type">
  <xs:sequence>
    <xs:element ref="head" minOccurs="0" />
    <xs:element ref="body" />
  </xs:sequence>
  <xs:attribute name="version" type="FPI" fixed="XHTML1.1" />
</xs:complexType>
<xs:element name="html" type="html.type" />
<xs:element name="title" type="xs:string" />
<xs:group name="head.content">
  <xs:sequence>
    <xs:element ref="title" minOccurs="0" />
  </xs:sequence>
</xs:group>
<xs:complexType name="head.type">
  <xs:group ref="head.content" />
</xs:complexType>
<xs:element name="head" type="head.type" />
<xs:complexType name="blockquote.type" mixed="true">
  <xs:group ref="Block.mix" />
</xs:complexType>
<xs:element name="blockquote" type="blockquote.type" />
<xs:complexType name="heading.type" mixed="true">
  <xs:group ref="Text.class" />
  <xs:attributeGroup ref="CellHAlign.attrib" />
</xs:complexType>
<xs:element name="h1" type="heading.type" />
<xs:element name="h2" type="heading.type" />
<xs:element name="h3" type="heading.type" />
<xs:element name="h4" type="heading.type" />
<xs:element name="h5" type="heading.type" />
<xs:element name="h6" type="heading.type" />
<xs:complexType name="p.type" mixed="true">
  <xs:group ref="Text.class" />
  <xs:attributeGroup ref="CellHAlign.attrib" />
</xs:complexType>
<xs:element name="p" type="p.type" />
<xs:complexType name="dt.type" mixed="true">
  <xs:group ref="Text.class" />
</xs:complexType>
<xs:element name="dt" type="dt.type" />
<xs:complexType name="dd.type" mixed="true">
  <xs:group ref="Flow.mix" />
</xs:complexType>
```

```
<xs:element name="dd" type="dd.type" />
  <xs:group name="dl.content">
    <xs:choice>
      <xs:element ref="dt" />
      <xs:element ref="dd" />
    </xs:choice>
  </xs:group>
<xs:complexType name="dl.type" mixed="true">
  <xs:group ref="dl.content" minOccurs="1" maxOccurs="unbounded" />
</xs:complexType>
<xs:element name="dl" type="dl.type" />
<xs:complexType name="li.type" mixed="true">
  <xs:group ref="Flow.mix" />
</xs:complexType>
<xs:element name="li" type="li.type" />
<xs:complexType name="ol.type">
  <xs:sequence>
    <xs:element ref="li" minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>
<xs:element name="ol" type="ol.type" />
<xs:complexType name="ul.type">
  <xs:sequence>
    <xs:element ref="li" minOccurs="1" maxOccurs="unbounded" />
  </xs:sequence>
</xs:complexType>
<xs:element name="ul" type="ul.type" />
<xs:attributeGroup name="table.attlist">
  <xs:attribute name="width" type="restrictedLength" />
  <xs:attribute name="border" type="Pixels" />
  <xs:attribute name="cellspacing" type="Length" />
  <xs:attribute name="cellpadding" type="Length" />
  <xs:attribute name="bgcolor" type="Color" />
  <xs:attribute name="align">
    <xs:simpleType>
      <xs:restriction base="xs:NMTOKEN">
        <xs:enumeration value="left" />
        <xs:enumeration value="center" />
        <xs:enumeration value="right" />
      </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
</xs:attributeGroup>
<xs:group name="table.content">
```

```
<xs:choice>
  <xs:element ref="tr" minOccurs="1" maxOccurs="unbounded" />
</xs:choice>
</xs:group>
<xs:complexType name="table.type" mixed="true">
  <xs:group ref="table.content" />
  <xs:attributeGroup ref="table.attlist" />
</xs:complexType>
<xs:element name="table" type="table.type" />
<xs:attributeGroup name="tr.attlist">
  <xs:attribute name="bgcolor" type="Color" />
  <xs:attributeGroup ref="CellHAlign.attrib" />
  <xs:attributeGroup ref="CellVAlign.attrib" />
</xs:attributeGroup>
<xs:group name="tr.content">
  <xs:choice>
    <xs:element ref="th" minOccurs="0" maxOccurs="unbounded" />
    <xs:element ref="td" minOccurs="0" maxOccurs="unbounded" />
  </xs:choice>
</xs:group>
<xs:complexType name="tr.type">
  <xs:group ref="tr.content" />
  <xs:attributeGroup ref="tr.attlist" />
</xs:complexType>
<xs:element name="tr" type="tr.type" />
<xs:attributeGroup name="td.attlist">
  <xs:attribute name="nowrap" fixed="nowrap" />
  <xs:attribute name="bgcolor" type="Color" />
  <xs:attribute name="text" type="Color" />
  <xs:attribute name="rowspan" type="Length" default="1" />
  <xs:attribute name="colspan" type="Length" default="1" />
  <xs:attributeGroup ref="CellHAlign.attrib" />
  <xs:attributeGroup ref="CellVAlign.attrib" />
</xs:attributeGroup>
<xs:complexType name="td.type" mixed="true">
  <xs:group ref="Block.mix" />
  <xs:attribute name="height" type="restrictedLength" />
  <xs:attribute name="width" type="restrictedLength" />
  <xs:attributeGroup ref="td.attlist" />
</xs:complexType>
<xs:element name="td" type="td.type" />
<xs:attributeGroup name="th.attlist">
  <xs:attribute name="nowrap" fixed="nowrap" />
  <xs:attribute name="bgcolor" type="Color" />
```

```
<xs:attribute name="width" type="restrictedLength" />
<xs:attribute name="height" type="restrictedLength" />
<xs:attribute name="rowspan" type="Length" default="1" />
<xs:attribute name="colspan" type="Length" default="1" />
<xs:attributeGroup ref="CellHAlign.attrib" />
<xs:attributeGroup ref="CellVAlign.attrib" />
</xs:attributeGroup>
<xs:complexType name="th.type" mixed="true">
  <xs:group ref="Block.mix" />
  <xs:attributeGroup ref="th.attlist" />
</xs:complexType>
<xs:element name="th" type="th.type" />
<xs:element name="br" type="empty.type" />
<xs:element name="b" type="xs:string" />
<xs:element name="big" type="xs:string" />
<xs:element name="i" type="xs:string" />
<xs:element name="sub" type="xs:string" />
<xs:element name="sup" type="xs:string" />
<xs:element name="tt" type="xs:string" />
<xs:element name="hr" type="empty.type" />
<xs:attributeGroup name="font.attlist">
  <xs:attribute name="size" type="FontSize" />
  <xs:attribute name="color" type="Color" />
  <xs:attribute name="face" type="FontFace" />
</xs:attributeGroup>
<xs:complexType name="font.type" mixed="true">
  <xs:group ref="Text.class" minOccurs="0" maxOccurs="unbounded" />
  <xs:attributeGroup ref="font.attlist" />
</xs:complexType>
<xs:element name="font" type="font.type" />
</xs:schema>
```

Folgende Farben können wahlweise als Text- bzw. Hintergrundfarbe verwendet werden:

Black	Silver	Gray	White	Maroon
Red	Purple	Fuchsia	Green	Lime
Olive	Yellow	Navy	Blue	Teal
Aqua				

Die Verwendung einer Farbe sowohl für den Text als auch für den Hintergrund wird ausgeschlossen. Zusätzlich werden noch die folgenden Farbkombinationen ausgeschlossen:

Navy	Black
Olive	Gray
Yellow	White
Purple	Maroon
Red	Fuchsia
Teal	Green
Aqua	Lime

5.6 SecSigner 3.6 (SecCommerce Informationssysteme GmbH)

Die folgenden Daten-/Dokumentformate werden von SecSigner unterstützt.

5.6.1 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.

5.6.2 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 Anzeigoptionen

- "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.

5.6.3 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.

5.7 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.

5.8 a.sign PDF

a.sign PDF (vormals VPDFSign) stellt die jeweils aktuelle Seite eines geöffneten PDF-Dokuments als Bild (tiff) dar. Um etwaige dynamische Inhalte des PDF-Dokuments auszuschließen und die Anzeige zum Zeitpunkt der Signatur einzufrieren bietet a.sign PDF die Möglichkeit, während des Signiervorganges, das PDF-Dokument in ein sicheres PDF-Dokumente zu wandeln. Dabei wird aus jeder einzelnen Seite des PDF-Dokuments ein Bild angefertigt. Die so entstandenen Bilder werden in einem zweiten Arbeitsschritt wieder zu einem PDF-Dokument zusammengefügt, welches dann signiert wird. Auf diese Art und Weise werden sämtliche dynamische Inhalte des PDF-Dokuments zum Zeitpunkt der Signatur fixiert und eine veränderte Anzeige zu einem späteren Zeitpunkt ist ausgeschlossen.

5.9 a.sign MultiSign

a.sign MultiSign bietet wie a.sign PDF die Möglichkeit, ein PDF Dokumente in eine sicheres PDF-Dokument ohne dynamische Inhalt, zu wandeln (siehe 5.8). Im Unterschied zu a.sign PDF wird für die Anzeige der Dokumente die jeweilige Anwendung verwendet, die mit PDF-Dokumenten assoziiert ist (in den meisten Fällen Adobe Reader).

5.10 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, Acrobat 2017 und Acrobat Reader 2017 mindestens in der Version 2017.011.30171 und Acrobat 2015 und Acrobat Reader 2015 mindestens in der Version 2015.006.30523 zu verwenden (https://helpx.adobe.com/mena_en/security/products/acrobat/apsb20-24.html).

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

- a.sign MultiSign Version 1.x.x.0 (A-Trust GmbH)
- 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 mindestens folgende Versionen der Adobe Produkte zu verwenden:

- Android Adobe: 20.4.0.13615
- iOS Adobe: Version 20.05.01

5.11 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:

- GoTrust Idem Key (USB-A/NFC)
- GoTrust Idem Key (USB-C/NFC)

Nähere Informationen können auch unter <https://www.a-trust.at/fido> abgerufen werden.

7 QWACS

Qualifizierte Webseiten Authentifizierungs Zertifikate (QWACS)
Keine Bestimmungen.