A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr 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 Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium seal

Version: 1.0.1
Datum: 13.02.2019

Inhaltsverzeichnis

Rev	Autor	Änderungen
1.0.0	RS, PT	Initiale Version
1.0.1	RS	Feedback Auditor

Tabelle 1: Dokumentenhistorie

1 Einführung

1.1 Überblick

Die Anwendungsvorgaben (Certificate Policy) enthalten ein Regelwerk, das den Einsatzbereich eines Zertifikats für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert.

Die Certificate Policy für qualifizierte a.sign premium seal Zertifikate gilt entsprechend der Verordnung (EU) 910/2014 [eIDAS-VO] und dem österreichischen Signatur- und Vertrauensdienstegesetz [SVG], die an Endbenutzer ausgestellt werden, auf sicheren Siegelerstellungseinheiten basieren und für die Erstellung qualifizierter Siegel geeignet sind.

1.2 Dokumentidentifikation

Name der Richtlinie:	A-Trust Anwendungsvorgaben (Certificate Policy) für qualifizierte Zertifikate a.sign premium seal für qualifizierte Siegel
Version:	1.0.1 / 13.02.2019
Object Identifier:	1.2.040.0.17 (A-Trust) .1 (CP) .11.1 (a.sign premium seal) .1.0.1 (Version) vorliegende Version

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

Die vorliegende Policy ist in Übereinstimmung mit ETSI EN 319 411-2 Klasse "qcp-legal-qscd" [Object Identifier: 0.4.0.194112.1.3] (siehe [ETSI 319 411]).

1.3 Anwendungsbereich

Diese a.sign premium seal Anwendungsvorgaben gelten für qualifizierte Zertifikate gem. Artikel 38 [eIDAS-VO], welche ausschließlich für juristische Personen ausgestellt werden. Der Schlüssel des Siegelerstellers darf ausschließlich für das Erstellen von Siegel genutzt werden.

Elektronische Siegel, die in Übereinstimmung mit diesen Anwendungsvorgaben und unter Verwendung der von A-Trust empfohlenen Komponenten und Verfahren erstellt wurden, sind qualifizierte Siegel im Sinne von Artikel 3 [eIDAS-VO].

Ausgestellt werden a.sign premium seal Zertifikate auf folgende geeignete Chipkarten:

- a.sign premium seal Standardkarten, wobei es eine bei A-Trust bestellte reine Siegelkarte oder eine signaturfähige Karte mit zusätzlichen Funktionen (z. B. Maestrokarte, Mastercard, Mitgliedsausweis etc.) sein kann.

Zu den empfohlenen Komponenten und Verfahren gehören:

- ein von A-Trust empfohlenes Hash-Verfahren,
- die sichere Eingabe der Signatur PIN, bei welcher der Signator ausschließen kann, dass die PIN anderen Personen zukommt oder über den Signaturvorgang hinaus gespeichert wird,
- die sichere Anzeige der zu besiegelnden Daten, die alle zu besiegelnden Daten inhaltlich unverändert darstellen kann.

Nur mit einem qualifizierten Zertifikat, welches auf der von einer Bestätigungsstelle (z.B. A-SIT) bescheinigten sicheren Siegelerstellungseinheit wie in Kapitel 3.2.8 beschrieben basiert, kann ein qualifiziertes Siegel erstellt werden.

Der Siegelersteller ist sich bewusst, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten Siegeln bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren A-Trust für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.

1.4 Übereinstimmung mit der Policy

A-Trust verwendet den Object Identifier aus Kapitel 1.2 nur für die Erstellung von Zertifikaten, anlässlich deren Ausgabe die Regelungen der gegenständlichen Policy für qualifizierte Zertifikate für qualifizierte Siegel Beachtung fanden.

2 Verpflichtungen und Haftung

2.1 Verpflichtungen des Zertifizierungsdiensteanbieters

A-Trust verpflichtet sich, dass alle Anforderungen dieser Anwendungsvorgabe und der Zertifizierungsrichtlinie erfüllt sind, die sich insbesondere auf die folgenden Aspekte erstrecken:

- Die Zertifikate für Siegelersteller werden im Einklang mit dieser Anwendungsvorgabe und der Zertifizierungsrichtlinie erstellt und können ausgesetzt, widerrufen oder verlängert werden.
- Die Zertifizierungsstelle arbeitet im Einklang mit dem der Aufsichtsbehörde vorgelegten Sicherheits- und Zertifizierungskonzept.
- Die Zertifizierungsstelle beschäftigt ausschließlich qualifiziertes Personal.
- Die Zertifizierungsstelle kommt ihrer Informationspflicht hinsichtlich Siegelersteller und Aufsichtsbehörden nach.
- Die Zertifizierungsstelle sorgt durch geeignete Maßnahmen (technisch, organisatorisch, infrastrukturell und personell) für den Schutz des privaten Schlüssels der Zertifizierungsstelle.
- Der Einsatz des privaten Schlüssels der Zertifizierungsstelle erfolgt ausschließlich zum Signieren der Zertifikate der Siegelersteller und zum Signieren der Widerrufsinformationen.
- Die Zertifizierungsstelle veröffentlicht alle ausgestellten Zertifikate (sofern dies bei der Ausstellung vom Inhaber gewünscht wird). Bei Widerruf und Aussetzung eines Zertifikats wird der betroffene Siegelersteller benachrichtigt. Ein nicht veröffentlichtes Zertifikat wird bei einer Aussetzung oder einem Widerruf in die Widerrufsliste aufgenommen. Wenn der Widerruf aufgrund einer Neuaktivierung stattfindet, im Zuge derer der Signator über den Widerruf des bestehenden Zertifikates informiert wird, kann diese Verständigung ausbleiben.
- A-Trust hat insbesondere die Verpflichtung eine Liste der für eine qualifizierte Siegelerstellung und -prüfung zu verwendenden Komponenten und Verfahren zur erstellen und aktuell zu halten und diese den Siegelersteller und Überprüfern von Zertifikaten jederzeit zugänglich zu machen.

2.2 Verpflichtungen der Zertifikatsinhaber

Die Siegelersteller haben sich an die Richtlinien dieses Dokuments zu halten. Dies betrifft insbesondere folgende Aspekte:

- Die Siegelersteller verpflichten sich die Allgemeinen Geschäftsbedingungen [AGB] zusammen mit der a.sign premium seal Anwendungsvorgabe (Policy), der Zertifizierungsrichtlinie und den Entgeltbestimmungen von A-Trust als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Siegelersteller ist für die Richtigkeit der Angaben verantwortlich, die er bei der Registrierung macht und wirkt gemäß den in der Zertifizierungsrichtlinie angegebenen Verfahren zur Identitätsfeststellung und Authentifikation mit.
- Der Siegelersteller ist verpflichtet, seinen privaten Schlüssel angemessen zu schützen. Dies umfasst insbesondere keinen Zugriff durch unautorisierte Personen auf die a.sign premium seal Karte zuzulassen und die Aktivierungsdaten (PIN) des privaten Schlüssels geheim zu halten.
- Falls nötig initiiert der Siegelersteller unverzüglich die Aussetzung oder den Widerruf seines Zertifikats. Wird die Aussetzung nicht in einem vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.
- Der Siegelersteller setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und die zugehörigen Anwendungsvorgaben (Policy).
- Der Siegelersteller ist sich bewusst, dass A-Trust eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten Signaturen bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren A-Trust für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.
- Es muss weiters dafür Sorge getragen werde, dass auf dem PC-Arbeitsplatz, an welchem das qualifizierte Siegel erstellt wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu soll er die folgenden Vorgaben von A-Trust einhalten:
  - Der Siegelersteller muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf seinen PC-Arbeitsplatz und die darauf befindlichen Programmcodes zu verhindern.
  - A-Trust verpflichtet den Siegelersteller sich an die Empfehlungen des Herstellers des von ihm verwendeten Betriebssystems sowie an die Empfehlungen der Hersteller der anderen Software-Produkte, die er installiert hat, zu halten.
- Der Siegelersteller ist verpflichtet die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

2.3 Verpflichtungen der Zertifikatsnutzer

Den Zertifikatsnutzern von a.sign premium seal Zertifikaten (Siegelempfänger) wird empfohlen, vor der Akzeptanz folgende Prüfungen durchzuführen:

- Der Zertifikatsnutzer prüft das digitale Siegel.
- Der Zertifikatsnutzer prüft die Gültigkeit des Zertifikats.
- Die Zertifikatsnutzer prüft, ob das Zertifikat zweckgemäß (d.h. für die Erstellung eines Siegel) eingesetzt wurde.

Wenn der Überprüfer eines Zertifikats eine qualifizierte Siegelprüfung durchzuführen beabsichtigt, dann empfiehlt ihm A-Trust die Verwendung der für eine qualifizierte Überprüfung eines Siegels empfohlenen Komponenten und Verfahren.

2.4 Haftung

A-Trust haftet als Aussteller von qualifizierten Zertifikaten gemäß Artikel 13 [eIDAS-VO].

3 Anforderung an die Erbringung von Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von qualifizierten Zertifizierungsdiensten ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Zertifikatsgenerierung, Zertifikatsausgabe, Aussetzungs- und Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Zertifizierungsrichtlinie (CPS)

A-Trust hat die nachfolgend aufgelisteten Maßnahmen ergriffen, um die für die Erbringung von Zertifizierungsdiensten nötige Sicherheit und Verlässlichkeit zu gewährleisten:

1. A-Trust hat eine Risikoanalyse erstellt, um die möglichen Risiken abzuschätzen und die sich daraus ergebenden Sicherheitsanforderungen und Umsetzungsmaßnahmen zu bestimmen.
2. A-Trust hat alle nötigen Vorgangsweisen und Prozeduren, um die Anforderungen aus der Anwendungsvorgabe zu erfüllen, in ihrem Sicherheitskonzept dargestellt.
3. Die Zertifizierungsrichtlinie für a.sign premium seal (siehe [CPS]) benennt die Verpflichtungen aller externen Vertragspartner, die Dienstleistungen für A-Trust unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.
4. A-Trust macht allen Siegelerstellern und Überprüfern von elektronischen Signaturen die Zertifizierungsrichtlinie und jegliche Dokumentation, die die Übereinstimmung mit dieser Anwendungsvorgabe dokumentiert, zugänglich (siehe Kapitel 3.3.4).
5. Die Geschäftsführung der A-Trust stellt das alleinige Entscheidungsgremium dar, das für die Genehmigung der Zertifizierungsrichtlinie für a.sign premium seal verantwortlich ist.
6. Die Geschäftsführung der A-Trust trägt auch die Verantwortung für die ordnungsgemäße Implementierung der Zertifizierungsrichtlinie für a.sign premium seal.
7. A-Trust hat einen Revisionsprozess zur Überprüfung der Vorgangsweisen der Zertifizierung aufgesetzt, der auch Maßnahmen zur Wartung der Zertifizierungsrichtlinie für a.sign premium seal umfasst.
8. A-Trust wird zeitgerecht über beabsichtigte Änderungen informieren, die in der Zertifizierungsrichtlinie vorgenommen werden sollen, und wird nach Genehmigung derselben entsprechend Punkt 5 dieses Absatzes eine überarbeitete Version der Zertifizierungsrichtlinie für a.sign premium seal entsprechend Kapitel 3.3.4 unverzüglich zugänglich machen.

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der A-Trust Schlüssel

Die Generierung der von A-Trust zur Erbringung von Zertifizierungsdiensten verwendeten Schlüssel erfolgt in Übereinstimmung mit den Bestimmungen der Artikel 19, 24 [eIDAS-VO]:

1. Die Erzeugung der Schlüssel wird von dazu autorisiertem Personal (siehe Rollenmodell in Kapitel 3.4.3), mindestens im Vier-Augen-Prinzip in einer physisch abgesicherten Umgebung durchgeführt (siehe 3.4.4).
2. Die Schlüssel werden in einer Siegelerstellungseinheit (Hardware Security Modul) erstellt, die einem Bestätigungsverfahren bei A-SIT unterzogen wurde und zur Erstellung fortgeschrittener Siegel geeignet ist.
3. Für die Schlüsselgenerierung wird ein Algorithmus verwendet, der für qualifizierte Zertifikate als geeignet angesehen wird.
4. Die Schlüssellänge und der Algorithmus sind für qualifizierte Zertifikate geeignet und entsprechen dem Durchführungsbeschluss zur [eIDAS-VO] (EU) 2015/1506 und den Empfehlungen der Expertengruppe der European Electronic Signature Standardisation Initiative.

3.2.2 Speicherung der CA-Schlüssel

A-Trust stellt sicher, dass die privaten Schlüssel geheim gehalten werden und ihre Integrität bewahrt bleibt.

Die Schlüssel sind in einem Hardware Security Modul gespeichert, welches die Anforderungen aus § 2 (7) [SVV] erfüllt.

3.2.3 Verteilung der öffentlichen CA-Schlüssel

A-Trust stellt durch die folgenden Maßnahmen sicher, dass die Integrität und Authentizität der öffentlichen Schlüssel anlässlich der Verteilung gewahrt bleibt:

- Ausstellung und Veröffentlichung eines selbst signierten Root-Zertifikates.

Das Zertifikat des CA-Schlüssels zur Signatur von a.sign premium seal Zertifikaten wird den Zertifikatsinhabern durch Veröffentlichung im Rahmen des Verzeichnisdienstes zugänglich gemacht. A-Trust gewährleistet die Authentizität dieses Zertifikats.

3.2.4 Schlüsseloffenlegung

Eine Offenlegung der geheimen CA-Schlüssel ist nicht vorgesehen.

3.2.5 Verwendungszweck von CA-Schlüsseln

Der private Schlüssel der Zertifizierungsstelle wird nur für die Erstellung von a.sign premium seal Zertifikaten und für die Signatur der zugehörigen Widerrufslisten oder Antworten von OCSP Anfragen innerhalb von physisch abgesicherten Räumlichkeiten verwendet.

3.2.6 Ende der Gültigkeitsperiode von CA-Schlüsseln

Geheime Schlüssel zur Signatur von a.sign premium seal Zertifikaten werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Die Zertifikate über die Schlüssel der A-Trust Zertifizierungsstelle werden spätestens alle zehn Jahre erneuert.

Eine Archivierung der geheimen Schlüssel ist nicht vorgesehen.

3.2.7 Erzeugung der Schlüssel für die Siegelersteller

Die Schlüssel werden im Hochsicherheitsbereich des Kartenherstellers in den a.sign premium seal Karten erzeugt, auf welche anschließend die persönlichen Daten des Siegelerstellers aufgebracht werden. Ein Zertifikat für das Signaturschlüsselpaar wird noch nicht erstellt. Dies geschieht erst im Zuge des Registrierungsprozesses, indem der Siegelersteller zuverlässig identifiziert und authentisiert wird.

3.2.8 Sicherheit der a.sign premium seal Karte

Die Schlüssel der Signatoren werden auf einer den Anforderungen entsprechenden Chipkarte, der a.sign premium seal Karte, gespeichert. Es handelt sich bei der a.sign premium seal Karte um eine von einer Bestätigungsstelle (wie z.B. A-SIT) nach Artikel 30 [eIDAS-VO] bescheinigte Smartcard, welche eine sichere Siegelerstellungseinheit darstellt und die Erzeugung und Speicherung der Siegelerstellungsdaten ermöglicht ([ACOS-04], [ACOS-05], [CardOS5.3]). Auf den von A-Trust als a.sign premium seal Karten eingesetzten Smartcards mit zertifiziertem Chip ist sicher gestellt, dass es durch andere auf der Karte befindliche Applikationen zu keiner Beeinflussung der Signaturfunktion kommen kann.

3.3 Lebenszyklus des Zertifikats

3.3.1 Registrierung des Siegelerstellers

Die Maßnahmen zur Identifikation und Registrierung des Siegelerstellers entsprechen den Anforderungen des Artikels 24 [eIDAS-VO] und stellen sicher, dass der Antrag auf Ausstellung eines qualifizierten Zertifikats korrekt, vollständig und autorisiert ist.

Die Angaben des Siegelerstellers werden in zwei Kategorien eingeteilt. Dies sind zum einen die erforderlichen und zum anderen die optionalen Angaben. Es sind folgende Daten aufzunehmen:

- Name für das a.sign premium seal Zertifikat: Vollständiger Firmenwortlaut und ggf. die Registriernummer gemäß der amtlichen Eintragung
  Im Falle einer natürlichen Person: den Namen der Person
- Die Angabe der Firmen-Adresse ist optional.
- Im Falle eines Zertifikates im Sinne von Artikel 34 [PSD II-Verordnung] können zusätzlich folgende Attribute aufgenommen werden:
  - Die Rolle des Zahlungsdienstleisters, die eine oder mehrere der folgenden Funktionen umfassen kann:
    * Kontoführung
    * Zahlungsauslösung
    * Kontoinformation
    * Ausstellung kartenbasierter Zahlungsinstrumente
  - den Namen der zuständigen Behörden, bei denen der Zahlungsdienstleister eingetragen ist.

Die Angaben des Antragstellers werden bei der Aktivierung der Karte in der Registrierungsstelle durch den Registration Officer überprüft.

Authentisierung von Individuen Die Identität des Vertreters des Antragsstellers ist durch eine qualifizierte elektronische Signatur oder durch Vorlage eines amtlichen Lichtbildausweises nachzuweisen.

Die Vertretungsbefugnis des Vertreters des Antragstellers ist durch Vorlage einer vom gesetzlichen Vertreters des Antragsstellers gefertigten Vollmacht nachzuweisen.

Authentisierung von Organisationen Als Voraussetzung für die Beantragung eines qualifizierten Zertifikats für ein qualifiziertes elektronisches Siegel a.sign premium seal, muss die Identität und ggf. die Adresse des Firmensitzes des Antragstellers überprüft werden. Wenn der Antragsteller im Österreichischen Firmenbuch

eingetragen ist, erfolgt die Überprüfung der Identität und ggf. der Adresse des Firmensitzes des Antragstellers durch die Registrierungsstelle mittels Abfrage des Firmenbuches. Anderenfalls hat der Vertreter des Antragstellers die Identität und ggf. die Adresse des Firmensitzes des Antragstellers durch Vorlage eines notariell beglaubigten amtlichen Registerauszuges nachzuweisen. Eine Ausstellung von a.sign premium seal Zertifikaten ist derzeit nur für juristische Personen möglich, deren Firmensitz in der Europäischen Union liegt. Wenn der Antragsteller keine registrierte juristische Person ist, erfolgt die Überprüfung der Identität und ggf. der Adresse des Firmensitzes des Antragstellers mittels Vorlage von notariell beglaubigten Dokumenten aus denen die Identität und die Adresse des Antragstellers hervorgeht.

Qualifizierte Zertifikate, die auf die Namen Max Mustermann, Test Zupfer, Test Test, Musterfrau Maxine lauten oder deren Namen mit „XXX“ beginnen, werden von der A-Trust GmbH zu Testzwecken ausgestellt. Aus diesem Grund wird bei Ausstellung von qualifizierten Zertifikaten auf die genannten Namen keine Identitätsprüfung durchgeführt.

3.3.2 Erneute Registrierung/Rezertifizierung

Der Siegelersteller kann nach einem Widerruf ein Ersatzprodukt bestellen und analog der Erstregistrierung aktivieren. Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben.

3.3.3 Ausstellung von Zertifikaten

Die mit den Schlüsseln versehene a.sign premium seal Karte wird entweder an die zuständige Registrierungsstelle weitergeleitet und der Signator nimmt sie dort entgegen oder der Signator ist bereits im Besitz einer signaturfähigen Karte.

Persönliche Ausstellung:

Für die Ausstellung der Zertifikate des Antragstellers wird dieser persönlich in einer Registrierungsstelle vorstellig. Der Registration Officer stellt die Zertifikate aus, wenn

- er die Identität des Antragstellers anhand eines gültigen, amtlichen Lichtbildausweises (zulässige Ausweise siehe Kapitel 3.3.1) überprüft hat,
- der Antragsteller belehrt wurde und
- die Allgemeinen Geschäftsbedingungen [AGB] akzeptiert hat.

Online-Ausstellung:

Im Zuge der Online-Ausstellung ist es für den Signator notwendig die Identität mittels des Aktivierungscodes (mittels RSa Brief an den Signator übermittelt) und des beim Antrag selbst gewählten Widerrufspasswortes zu bestätigen. Alternativ hierzu kann eine Bestätigung der Identität durch einen Dritten erfolgen, sofern die initiale Identitätsfeststellung und Ausgabe der Zugangsdaten zu deren Onlineportal den Anforderungen des Artikel 24(1) Lit d [eIDAS-VO] entspricht. Diese Bestätigung wird in elektronischer Form, durch diesen Dritten signiert, vor der Zertifikatsausstellung an A-Trust übermittelt. Im Rahmen der weitern Schritte können die Personendaten nicht mehr geändert werden. Es wird ausschließlich auf bereits verifizierte Personendaten zur Ausstellung des Zertifikats zurück gegriffen, die von der Karten ausgebenden Stelle an die A-Trust zur Verwendung frei gegeben und übermittelt werden.

Die Webanwendung bietet dem Signator noch vor Aktivierung des Zertifikats die Möglichkeit sich die Unterrichtung und die Allgemeinen Geschäftsbedingungen [AGB] anzusehen und auf einem eigenen dauerhaften Datenträger zu speichern.

In den Ausstellungsfällen gilt die Ausstellung als abgeschlossen, wenn der Signaturvertrag des Signators unterschrieben ist und das Zertifikat ausgestellt wurde. A-Trust unterscheidet nicht, ob der unterschriebene Signaturvertrag in physischer (Papier) oder elektronischer Form unterzeichnet vorliegt.

Durch die folgenden Maßnahmen wird sicher gestellt, dass Ausstellung, Verlängerung und Neuausstellung von Zertifikaten in sicherer Weise erfolgen und den Anforderungen des [SVG] und des [eIDAS-VO] entsprechen.

1. Die Zertifikate werden gem. den Bestimmungen in Anhang I [eIDAS-VO] als X.509 v3 Zertifikate erstellt. Die in den Zertifikaten enthaltenen Angaben sind insb. die folgenden:
    - Versionsnummer des Zertifikats: es werden Zertifikate der Version 3 (codiert mit dem Wert 2) ausgestellt
    - Seriennummer des Zertifikats
    - Bezeichnung des Zertifikatsausstellers
    - Beginn und Ende der Gültigkeit des Zertifikats
    - Bezeichnung des Zertifikatsinhabers
    - öffentlicher Schlüssel (mit Angabe des Algorithmus)
    - Angabe des Algorithmus für die Signatur des Zertifikats
    - Signatur über das Zertifikat
    - Zertifikatserweiterungen, wie z.B.:
        - Bezeichnung als qualifiziertes Zertifikat
        - Informationen über die anzuwendende Policy bzw. CPS
        - Zertifikatsverwendung

- Information zum Auffinden der CRL
- Optionales Behördenkennzeichen und ggf. ein optionaler Verwaltungsbezeichner.

2. Das Zertifikat wird bei der Registrierung auf Veranlassung der Registrierungsstelle erzeugt, nachdem der Antragsteller identifiziert und die Korrektheit aller Daten durch ihn bestätigt wurde. Das Verfahren ist für Verlängerung und Neuausstellung identisch.

3. Das Signatur-Schlüsselpaar der a.sign premium seal Karte wurde anlässlich der Initialisierung der Karte erstellt.

4. Für alle a.sign premium seal Karten gilt:

   - Jedem Siegelersteller wird eine innerhalb der A-Trust einmalig vergebene und eindeutige Identifikationsnummer (CIN) zugeordnet. Diese Identifikationsnummer ist Teil des hervorgehobenen Namens und stellt damit seine Eindeutigkeit sicher.
   - Die in der Registrierungsstelle aufgenommenen Daten werden signiert und verschlüsselt (SSL) an die Zertifizierungsstelle übertragen. Vertraulichkeit und Integrität sämtlicher Daten ist damit sicher gestellt.
   - Alle RA-Mitarbeiter sind mit Signaturkarte ausgestattet. Die Authentizität der übermittelten Registrierungsdaten wird durch Verifizierung der Signatur des RA-Mitarbeiters überprüft.

3.3.4 Bekanntmachung der Vertragsbedingungen

A-Trust macht den Signatoren und Überprüfern von Signaturen die Bedingungen betreffend die Benutzung des qualifizierten Zertifikats durch Veröffentlichung der nachfolgenden Dokumente auf der A-Trust Homepage zugänglich:

- der gegenständlichen Anwendungsvorgabe (Certificate Policy),
- des Zertifizierungsrichtlinie für a.sign premium seal, siehe [CPS],
- der Allgemeinen Geschäftsbestimmungen [AGB],
- der Belehrungen für den Signator,
- der sonstigen Mitteilungen.

Änderungen werden dem Signator mittels Bekanntmachung auf der A-Trust Homepage und gegebenenfalls per Mail oder Brief mitgeteilt

3.3.5 Veröffentlichung der Zertifikate

Von A-Trust ausgestellte Zertifikate werden den Signatoren und, je nach Vereinbarung mit dem Signator, den Überprüfern folgendermaßen verfügbar gemacht.

- Anlässlich der Erstellung eines Zertifikats wird dieses am Ende des Registrierungsvorgangs auf die a.sign premium seal Karte des Signators gespeichert.
- Wenn der Signator damit einverstanden ist, wird das Zertifikat im Verzeichnisdienst von A-Trust veröffentlicht.
- Die Bedingungen für die Benutzung eines Zertifikats werden von A-Trust allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
- Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen "a.sign premium seal" einfach herstellbar.
- Der Verzeichnisdienst ist 7 Tage 24 Stunden verfügbar. Unterbrechungen von mehr als 30 Minuten werden gemäß § 5 (5) [SVV] als Störfälle dokumentiert.
- Der Verzeichnisdienst ist öffentlich und international zugänglich.

3.3.6 Aussetzung und Widerruf

a.sign premium seal Zertifikate können vorübergehend ausgesetzt werden. Diese Aussetzung kann auch in einen endgültigen Widerruf umgewandelt werden. Ebenso ist ein sofortiger und permanenter Widerruf des Zertifikats möglich. Der Signator wird von einer erfolgten Aussetzung oder einem Widerruf informiert.

Die Vorgangsweisen für das Auslösen von Aussetzung und Widerruf sind in der Zertifizierungsrichtlinie für a.sign premium seal (siehe [CPS]) dokumentiert, insbesondere:

- wer berechtigt ist einen Widerruf zu beantragen,
- wie ein Widerrufsantrag gestellt werden kann,
- die Umstände unter denen eine Aussetzung möglich ist,
- die Mechanismen für die Bereitstellung von Statusinformationen und
- die maximale Zeitdauer, die zwischen Einlangen eines Widerrufsantrags und der Veröffentlichung des Widerrufs, verstreichen kann.

Eine Aussetzung oder ein Widerruf kann durch den Signator vorgenommen werden. Dies kann wie folgt geschehen:

- Der Signator wendet sich per Telefon an den Widerrufsdienst.
- Der Signator bzw. der Vertretungsbefugte veranlasst den Widerruf per Fax.
- Bei Vergessen des Passworts für den Widerruf kann der Signator keinen Widerruf, sondern nur eine Aussetzung beantragen.

Dabei ergeben sich einige Anforderungen an den Ablauf der jeweiligen Alternative. Diese werden nachfolgend aufgeführt.

- Telefonat: Der Signator kann rund um die Uhr einen Widerruf per Telefon vornehmen. Die Authentifikation erfolgt nur über das Aussetzungs- und Widerrufs-Passwort, welches der Antragsteller bei der Bestellung bzw. Registrierung selbst festgelegt hat.
  Die für einen Widerruf benötigten Informationen lassen sich wie folgt zusammenfassen:
  - Persönliche Daten (vollständiger Name, Geburtstag und -ort),
  - Passwort für den Widerruf,
  - Identifikationsnummer des Signators (CIN), Kartennummer oder Seriennummer des Zertifikats.
- Fax: Der Signator kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss das Aussetzungs- und Widerrufs-Passwort sowie die vollständige Seriennummer oder die Kartennummer des zu widerrufenden Zertifikats beinhalten.
- Fax: Der Vertretungsbefugte bzw. eine bevollmächtigte Person kann von 0 bis 24 Uhr einen Widerruf per Fax vornehmen. Das Fax muss einen Hinweis auf seine Vertretungsbefugnis sowie die vollständige Seriennummer oder die Kartennummer des zu widerrufenden Zertifikats beinhalten.
- Besuch in einer Registrierungsstelle: Der Signator benötigt dazu einen gültigen, amtlichen Lichtbildausweis. Der RO teilt dem Signator die Zertifikatsnummer und das Passwort für den Widerruf mit, womit der Signator anschließend den Widerruf beim Widerrufsdienst veranlassen kann.

Ausgesetzte und widerrufene Zertifikate werden in einer Widerrufsliste (CRL) unter Berücksichtigung der nachfolgenden Regelungen veröffentlicht:

- Die aktuelle Update-Frequenz der Widerrufsliste ist im Internet über die Web-Seite der A-Trust abrufbar.
- Jede Widerrufsliste enthält den Zeitpunkt der geplanten Ausgabe der nächsten Liste.

- Falls erforderlich kann eine neue Widerrufsliste auch vorzeitig veröffentlicht werden.
- Jede Widerrufsliste ist mit dem Zertifizierungsschlüssel signiert.

Widerrufslisten werden als X.509 Version 2 CRLs ausgegeben. Die wesentlichen Angaben in den CRLs sind die folgenden:

- Versionsnummer der CRL: Version 2 (codiert mit dem Wert 1)
- Bezeichnung des Ausstellers
- Zeitpunkt der CRL-Ausstellung sowie der nächsten geplanten Ausstellung
- Information über die in der CRL enthaltenen Zertifikate:
  - Seriennummer,
  - Zeitpunkt der Eintragung in die CRL,
  - Eintragungsgrund
- CRL-Erweiterungen
- Angabe des Algorithmus für die Signatur über die CRL
- Signatur über die CRL.

Die Widerrufsdienste sind täglich 24 Stunden verfügbar. Spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgt eine Aktualisierung der Widerrufsliste. Widerrufslisten sind täglich 24 Stunden abfragbar. Im Fall von Systemausfällen kommen die in der Zertifizierungsrichtlinie für a.sign premium seal (siehe [CPS]) genannten Vorkehrungen zum Tragen, um die Auswirkungen möglichst gering zu halten. Statusinformationen über Zertifikate können auch online mittels OCSP abgefragt werden. Die Integrität und Authentizität der OCSP-Antworten sind durch eine Signatur gesichert.

3.4 A-Trust Verwaltung

3.4.1 Sicherheitsmanagement

Es gelten folgenden Bestimmungen:

- A-Trust ist für alle Prozesse im Rahmen der Zertifizierungsdienste verantwortlich; dies gilt auch für die an Vertragspartner ausgelagerten Dienste. Die Verantwortlichkeiten der Vertragspartner sind klar geregelt und Kontrollen zur Überprüfung der ordnungsgemäßen Tätigkeit eingerichtet. Die für die Sicherheit relevanten Vorgehensweisen sind in der Zertifizierungsrichtlinie für a.sign premium seal veröffentlicht.

- Die Geschäftsführung von A-Trust ist unmittelbar verantwortlich für die Definition der Sicherheitsrichtlinien und deren Kommunikation an die mit sicherheitsrelevanten Vorgängen befassten Mitarbeiter.
- Die Sicherheitsinfrastruktur von A-Trust wird laufend überprüft und an sich ändernde Anforderungen angepasst. Jegliche Änderungen, die einen Einfluss auf das Ausmaß der erreichten Sicherheit haben, sind von der Geschäftsführung der A-Trust zu genehmigen.
- Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden von A-Trust dokumentiert und entsprechend der Dokumentation implementiert und gewartet.
- Der Betrieb des Rechenzentrums der A-Trust ist ausgelagert. Der Dienstleister ist an die Wahrung der Informationssicherheit vertraglich gebunden.

3.4.2 Informationsklassifikation und -verwaltung

A-Trust stellt sicher, dass alle Daten und Informationen in geeigneter Weise abgesichert sind.

In der Risiko- und Bedrohungsanalyse sind alle Informationsbestände verzeichnet und gem. ihrer Schutzwürdigkeit klassifiziert.

3.4.3 Personelle Sicherheitsmaßnahmen

Das Personal der A-Trust und deren Beschäftigungsmodalitäten sind geeignet, das Vertrauen in die Abwicklung der Zertifizierungsdienste zu stärken. Insbesondere wird Wert gelegt auf:

- A-Trust beschäftigt ausschließlich Personal, welches gemäß Artikel 24 (2) [eIDAS-VO] über das benötigte Fachwissen, die Qualifikation und Erfahrung für die jeweilige Position verfügt.
- Sicherheitsrelevante Funktionen und Verantwortlichkeiten werden in den jeweiligen Stellenbeschreibungen dokumentiert. Funktionen, von denen die Sicherheit der Zertifizierungsdienste abhängt, sind eindeutig identifiziert.
- Für alle Mitarbeiter der A-Trust (unabhängig ob in einem temporären oder ständigen Beschäftigungsverhältnis angestellt) sind klare Stellenbeschreibungen ausgearbeitet, in denen die Pflichten, Zugriffsrechte und Minimalkompetenzen dargelegt sind.
- Die Ausübung sowohl der administrativen als auch der Managementfunktionen steht im Einklang mit den Sicherheitsrichtlinien.

- Alle Leitungsfunktionen sind mit Personen besetzt, die über Erfahrung mit der Technologie digitaler Signaturen und mit der Führung von Personal verfügen, das Verantwortung für sicherheitskritische Tätigkeiten trägt.
- Alle Mitarbeiter, denen vertrauenswürdige Positionen zugeordnet sind, werden von Interessenskonflikten, die einer unvoreingenommenen Erfüllung der Aufgaben entgegenstehen könnten, frei gehalten.
- Alle vertrauenswürdigen Positionen sind in der Zertifizierungsrichtlinie (siehe [CPS]) im Detail beschrieben.
- Die Zuweisung der Positionen erfolgt mit formeller Ernennung durch die Geschäftsführung.
- A-Trust beschäftigt keine Personen, die strafbare Handlungen begangen haben, die sie für eine vertrauenswürdige Position ungeeignet erscheinen lassen. Eine Beschäftigung erfolgt erst nach einer diesbezüglichen Überprüfung.

3.4.4 Physikalische und organisatorische Sicherheitsmaßnahmen

Es ist sichergestellt, dass der Zutritt zu Räumlichkeiten, in denen sicherheitskritische Funktionen ausgeübt werden, abgesichert ist und Risken einer physischen Beschädigung der Vermögenswerte minimiert sind. Insbesondere gilt:

- Der Zutritt zu den Räumlichkeiten, in denen Zertifizierungs- und Widerrufsdienste erbracht und in denen die a.sign premium seal Karten initialisiert werden, ist auf autorisiertes Personal beschränkt. Die Systeme, die die Zertifikate ausstellen, sind vor Gefährdung durch Umweltkatastrophen geschützt.
- Es werden Maßnahmen ergriffen, um den Verlust, die Beschädigung oder die Kompromittierung von Anlagen und die Unterbrechung des Betriebes zu verhindern.
- Weitere Maßnahmen gewährleisten, dass eine Kompromittierung oder ein Diebstahl von Daten und datenverarbeitenden Anlagen nicht möglich ist.
- Die Systeme für Zertifikatsgenerierung, die Kartenbereitstellung und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
- Die Abgrenzung der Systeme für Zertifikatsgenerierung, Kartenbereitstellung und Widerrufsdienste erfolgt durch klar definierte Sicherheitszonen d.h. durch räumliche Trennung von anderen organisatorischen Einheiten und physischen Zutrittsschutz.
- Die Sicherheitsmaßnahmen inkludieren den Gebäudeschutz, die Computersysteme selbst und alle sonstigen Einrichtungen, die für deren Betrieb unerlässlich sind. Der Schutz der Einrichtungen für die Zertifikatserstellung, Kartenproduktion und

Bereitstellung der Widerrufsdienste umfasst physische Zutrittskontrolle, Abwendung von Gefahren durch Naturgewalten, Feuer, Rohrbrüche und Gebäudeeinstürze, Schutz vor Ausfall von Versorgungseinheiten, Diebstahl, Einbruch und Systemausfällen.

- Die unautorisierte Entnahme von Informationen, Datenträgern, Software und Einrichtungsgegenständen, welche zu den Zertifizierungsdiensten gehören, wird durch Kontrollmaßnahmen verhindert.

3.4.5 Betriebsmanagement

A-Trust stellt sicher, dass das Zertifizierungssystem sicher und korrekt betrieben und das Risiko des Versagens minimiert wird. Insbesondere gilt:

- Die Integrität der Computersysteme und Informationen ist gegen Viren und böswillige oder unautorisierte Software geschützt.
- Schaden durch sicherheitskritische Zwischenfälle und Fehlfunktionen wird durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren verhindert.
- Datenträger werden vor Beschädigung, Diebstahl und unautorisiertem Zugriff geschützt.
- Für die Ausführung von sicherheitskritischen und administrativen Aufgaben, die sich auf die Erbringung der Zertifizierungsdienste auswirken, sind Verfahrensweisen definiert und in Kraft gesetzt.
- Datenträger werden je nach ihrer Sicherheitsstufe (siehe Kapitel 3.4.2) behandelt und aufbewahrt. Nicht mehr benötigte Datenträger, die vertrauliche Daten beinhalten, werden in sicherer Weise vernichtet.
- Kapazitätserfordernisse werden beobachtet und künftige Entwicklungen prognostiziert, sodass stets die angemessene Prozessorleistung und Speicherplatz zur Verfügung stehen.
- Auf Zwischenfälle wird so rasch wie möglich reagiert, um die sicherheitskritischen Vorkommnisse auf ein Minimum zu begrenzen. Alle Zwischenfälle werden baldmöglichst aufgezeichnet.

Die sicherheitskritischen Funktionen im Rahmen der Zertifizierungs- und Widerrufsdienste werden von den gewöhnlichen Funktionen strikt getrennt.

Sicherheitskritische Funktionen inkludieren:

- Operationale Funktionen und Verantwortungen

- Planung und Abnahme von Sicherheitssystemen
- Schutz vor Schadsoftware
- Allgemeine Wartungstätigkeiten
- Netzwerkadministration
- Aktive Überprüfung von Log-Files und Prüfberichten, Analyse von Zwischenfällen
- Datenträgerverwaltung und –sicherheit
- Daten- und Softwareaustausch

Diese Aufgaben werden von A-Trust-Sicherheitsbeauftragten geregelt, können aber von operativem Personal (unter Beaufsichtigung) gem. Sicherheitskonzept und Stellenbeschreibungen durchgeführt werden.

3.4.6 Zugriffsverwaltung

A-Trust stellt durch die nachfolgenden Maßnahmen sicher, dass der Zugriff auf das Zertifizierungssystem ausschließlich auf ordnungsgemäß autorisierte Personen beschränkt ist.

- Sicherungsmaßnahmen wie z.B. Firewalls bewahren das interne Netzwerk vor Zugriffen durch Dritte.
- Vertrauliche Daten werden geschützt, wenn sie über unsichere Netzwerke ausgetauscht werden, wie z.B. die Registrierungsdaten.
- Eine Benutzerverwaltung, die den verschiedenen Funktionen unterschiedliche Zugriffsrechte einräumt, ist eingerichtet; insbesondere werden sicherheitsrelevante von nicht sicherheitskritischen Funktionen sorgfältig getrennt. Änderungen in den Zugriffsrechten werden im System sofort nachgezogen. Die Kontrolle der Benutzerverwaltung ist Teil des internen Audits.
- Zugriff auf Informationen und Anwendungen ist auf Grund der vergebenen Zugriffsrechte eingeschränkt. Die dafür geltenden Definitionen sind im Zertifizierungsrichtlinie für a.sign premium seal (siehe [CPS]) angeführt. Administrative und den laufenden Betrieb betreffende Funktionen sind streng getrennt. Die Verwendung von System-Utility-Programmen ist besonders eingeschränkt.
- Das Personal muss sich vor jedem kritischen Zugriff auf Applikationen, die in Zusammenhang mit dem Zertifikatsmanagement stehen, authentifizieren.
- Die Zugriffe werden in Log-Dateien aufgezeichnet. Das Personal wird für die ausgeführten Tätigkeiten zur Verantwortung gezogen.

- Eine Wiederverwendung von Datenspeichern führt nicht zur Offenlegung von vertraulichen Daten an nicht autorisierte Personen.
- Komponenten des lokalen Netzwerks befinden sich in einer physisch gesicherten Umgebung und die Konfiguration wird periodisch überprüft.
- Die Entdeckung von unautorisierten und/oder außergewöhnlichen Zugriffsversuchen auf die eigentliche Zertifizierungsstelle und die Widerrufsdienste wird durch geeignete Maßnahmen gesichert, sodass ggf. sofort Gegenmaßnahmen ergriffen werden können. Dies geschieht durch die Führung und Auswertung von CA-Logfiles und Firewall-Logfiles.
- Ändernde Zugriffe (Löschungen, Hinzufügungen) auf die Verzeichnis- und Widerrufsdienste werden durch Passworteingabe abgesichert.
- Versuche des unautorisierten Zugriffs auf Verzeichnis- und Widerrufsdienste werden aufgezeichnet.

3.4.7 Entwicklung und Wartung vertrauenswürdiger Systeme

A-Trust verwendet vertrauenswürdige Systeme und Produkte, die gegen Veränderung geschützt sind.

- Eine Analyse der Sicherheitsanforderungen muss im Stadium der Design- und Anforderungsspezifikation im Rahmen jedes Entwicklungsprojekts erfolgen, das von A-Trust oder von Dritten im Auftrag von A-Trust durchgeführt wird.
- Änderungskontrollprozeduren existieren für die Erstellung von geplanten Programmversionen, sonstigen Änderungen und Fehlerbehebungen.

3.4.8 Erhaltung des ungestörten Betriebes und Behandlung von Zwischenfällen

A-Trust wird sich bemühen, nach Katastrophenfällen, inklusive der Kompromittierung eines Zertifizierungsschlüssels, den Betrieb so rasch wie möglich wieder aufzunehmen. Insbesondere ist vorgesehen:

- Der Notfallsplan von A-Trust sieht die (vermutete) Kompromittierung des privaten Zertifizierungsschlüssels als Katastrophenfall vor.
- Sollte dieser Fall eintreten, so hat A-Trust die Aufsichtsstelle gemäß des Artikels 19 (2) [eIDAS-VO], die Signatoren, die auf die Sicherheit der Zertifizierungsdienste vertrauenden Personen und ggf. andere Zertifizierungsdiensteanbieter, mit denen Vereinbarungen bestehen, davon zu unterrichten und mitzuteilen, dass die Widerrufs- und Zertifikatsinformationen nicht mehr als zuverlässig anzusehen sind.

- Zertifikate und Widerrufslisten werden als nicht mehr gültig gekennzeichnet.

3.4.9 Einstellung der Tätigkeit

Gemäß Artikel 24 (2) Lit. a [eIDAS-VO] wird A-Trust die Einstellung der Tätigkeit unverzüglich der Aufsichtsstelle anzeigen und sicher stellen, dass eine eventuelle Beeinträchtigung der Dienstleistung gegenüber Signatoren und vertrauenden Parteien möglichst gering gehalten wird.

1. Vor Beendigung der Dienstleistung werden
   - alle Signatoren, Zertifizierungsdiensteanbieter und sonstige Parteien, mit denen A-Trust eine geschäftliche Verbindung unterhält, direkt, sowie jene Parteien, die auf die Zuverlässigkeit der Zertifizierungsdienste vertrauen, durch Veröffentlichung von der Einstellung unterrichtet,
   - die Verträge mit Subunternehmern (Registrierungsstellen, Kartenhersteller etc.) zur Erbringung von Zertifizierungsdiensten beendet,
   - Vorkehrungen zur Übernahme der Verzeichnis- und Widerrufsdienste sowie der Aufzeichnungen gemäß Kapitel 3.4.11 durch einen anderen Zertifizierungsdiensteanbieter getroffen,
   - die privaten Schlüssel von A-Trust von der Nutzung zurückgezogen und in Entsprechung zu Abschnitt 3.2.6 zerstört.
2. Die Abdeckung der Kosten für o.a. Vorkehrungen sind durch Gesellschaftergarantien abgedeckt.
3. Das Zertifizierungsrichtlinie von A-Trust (siehe [CPS]) benennt die Vorkehrungen, die bei Einstellung der Tätigkeit getroffen werden, insbesondere jene Vorkehrungen
   - für die Benachrichtigung der betroffenen Personen und Organisationen,
   - für die Übertragung der Verpflichtungen auf Drittparteien und
   - wie der Widerrufsstatus von nicht abgelaufenen Zertifikaten gehandhabt wird.

3.4.10 Übereinstimmung mit gesetzlichen Regelungen

A-Trust handelt grundsätzlich in Übereinstimmung mit den gesetzlichen Regelungen und Auflagen gemäß [SVG] und [eIDAS-VO], insbesondere sind nachfolgende Punkte sicher gestellt:

- Wichtige Aufzeichnungen werden vor Verlust, Zerstörung und Verfälschung bewahrt.

- Die Anforderungen des Datenschutzgesetzes [DSG] werden befolgt.
- Nötige technische und organisatorische Maßnahmen wurden ergriffen, um persönliche Daten vor unautorisierter und ungesetzlicher Verarbeitung sowie vor versehentlicher Zerstörung oder Beschädigung zu schützen.
- Den Signatoren wird versichert, dass die an A-Trust übermittelten Informationen nur mit ihrem Einverständnis, mit gerichtlichem Beschluss oder auf Basis gesetzlicher Regelungen offen gelegt werden.

3.4.11 Aufbewahrung der Informationen zu qualifizierten Zertifikaten

Alle Informationen, die in Zusammenhang mit qualifizierten Zertifikaten stehen, werden entsprechend [SVG] aufbewahrt. Insbesondere gilt:

1. Die Vertraulichkeit und Integrität der aktuellen sowie der archivierten Datensätze ist gewahrt.
2. Die Datensätze zu qualifizierten Zertifikaten werden vollständig und vertraulich in Übereinstimmung mit der veröffentlichten Zertifizierungsrichtlinie (siehe [CPS]) archiviert.
3. Aufzeichnungen bezüglich qualifizierter Zertifikate werden für die Beweisführung der ordnungsgemäßen Zertifizierung im Rahmen gerichtlicher Auseinandersetzungen verfügbar gemacht. Zusätzlich hat der Signator zu den Registrierungs- und sonstigen persönlichen Daten, die ihn betreffen, Zugang.
4. Die Aufzeichnungen umfassen auch den genauen Zeitpunkt des Eintretens wichtiger Ereignisse, die in Zusammenhang mit der Systemumgebung, dem Schlüssel- und dem Zertifikatsmanagement stehen.
5. Die Dokumentation entsprechend Artikel 24 (2) Lit. h [eIDAS-VO] wird gemäß § 10 (3) [SVG] für 35 Jahre elektronisch aufbewahrt. Das Antragsformular (Signaturvertrag) wird für drei Jahre in der betreffenden Registrierungsstelle im Original aufbewahrt.
6. Alle Aufzeichnung erfolgen derart, dass sie innerhalb der Aufbewahrungsfrist nicht leicht gelöscht oder zerstört werden können.
7. Die spezifischen Ereignisse und Daten die aufgezeichnet werden, sind in der Zertifizierungsrichtlinie (siehe [CPS]) dokumentiert.
8. Insbesondere werden alle Registrierungsinformationen, inkl. jener, die im Zusammenhang mit der Verlängerung der Gültigkeitsdauer von Zertifikaten stehen, elektronisch aufbewahrt.

9. Die aufzuzeichnenden Registrierungsinformationen beinhalten insbesondere:
   - die Art des Identifikationsdokuments, das anlässlich der Registrierung vorgelegt wurde,
   - die Daten des Identifikationsdokuments,
   - die Aufbewahrungsstelle der elektronischen Kopien der Antragsdokumente inklusive der Archivierung der Ausweisdaten,
   - die Akzeptanz der vertraglichen Vereinbarungen
   - vom Signator gewählte und akzeptierte Zertifikatsinhalte,
   - Angabe der Registrierungsstelle und des zuständigen Mitarbeiters.
10. Die Vertraulichkeit der Daten der Signatoren ist gewährleistet.
11. Es werden alle Ereignisse, die den Lebenszyklus der CA-Schlüssel von A-Trust betreffen, aufgezeichnet.
12. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.
13. Es werden alle Ereignisse, die im Zusammenhang mit der Generierung der Schlüssel der Signatoren stehen, aufgezeichnet.
14. Es werden alle Ereignisse, die im Zusammenhang mit der Initialisierung und Personalisierung der a.sign premium seal Karte stehen aufgezeichnet.
15. Alle Anträge auf Aussetzung, Aussetzungsaufhebung und Widerruf und die damit verbundenen Informationen werden aufgezeichnet. Dies inkludiert die Bandaufzeichnung der Telefonate und die Archivierung von Anträgen per Fax (siehe Kapitel 3.3.6).

3.5 Organisatorisches

A-Trust ist als Organisation zuverlässig und hält die folgenden Richtlinien strikt ein:

3.5.1 Allgemeines

- Alle Richtlinien und Vorgehensweisen sind nicht-diskriminierend.
- Die Dienstleistungen von A-Trust stehen allen Personen zur Verfügung, die über einen in Österreich ausgestellten amtlichen Lichtbildausweis (die zulässigen Lichtbildausweise sind auf der A-Trust Homepage aufgezählt) oder einen international gültigen Reisepass in deutscher und/oder englischer Sprache verfügen.
- A-Trust ist eine juristische Person (Gesellschaft mit beschränkter Haftung).

- A-Trust verfügt über Systeme zur Qualitätssicherung und Gewährleistung der Informationssicherheit, die den angebotenen Zertifizierungsdiensten angemessen sind.
- Die Haftung, insbesondere diejenige zur Schadenswiedergutmachung, entspricht den Bestimmungen des [SVG] und [eIDAS-VO] (siehe Kapitel 2.4).
- Hinsichtlich der finanziellen Ausstattung befolgt A-Trust die Bestimmungen des Artikels 24 (2) Lit. c [eIDAS-VO].
- Das von A-Trust beschäftigte Personal verfügt entsprechend den Bestimmungen [eIDAS-VO] (siehe auch Kapitel 3.4.3) über die nötige Schulung, Training, technisches Wissen und Erfahrung und ist in ausreichender Zahl vorhanden, um den geplanten Umfang der Zertifizierungsdienste bewerkstelligen zu können.
- Es sind Richtlinien und Vorgehensweisen für die Behandlung von Beschwerden und Streitfällen vorhanden, die von Kunden oder anderen Parteien an die A-Trust herangetragen werden und die Erbringung ihrer Dienstleistungen betreffen.
- Die rechtlichen Beziehungen zu Subunternehmern, die Dienstleistungen für A-Trust erbringen, sind vertraglich geregelt und ordnungsgemäß dokumentiert.
- Es gibt keine aktenkundigen Gesetzesverletzungen seitens A-Trust.

3.5.2 Zertifikatserstellungs- und Widerrufsdienste

Die für die Erbringung von Zertifizierungs- und Widerrufsdiensten vorgesehenen organisatorischen Einheiten sind hinsichtlich ihrer Entscheidungen über die Erbringung, Aufrechterhaltung und Beendigung der Dienstleistungen der A-Trust unabhängig von anderen Gesellschaften. Die Geschäftsführung und das Personal, das vertrauliche und leitende Funktionen ausübt, sind frei von kommerziellem, finanziellem und sonstigem Druck, der das Vertrauen in ihre Tätigkeit negativ beeinflussen könnte.

Die für die Zertifizierungs- und Widerrufsdienste bestimmten Einheiten verfügen über eine dokumentierte Struktur, die die Unvoreingenommenheit der Aufgabenausführung gewährleistet.

A Anhang

A.1 Begriffe und Abkürzungen

a.sign premium seal Karte	Eine Prozessorchipkarte, die geheime Schlüssel des Karteninhabers enthält und zur Erstellung und Verifizierung digitaler Signaturen dient.
Aktivierungsdaten	Daten, die zur Aktivierung der Schlüssel benötigt werden.
Anwender	Person, die die Dienstleistungen der Zertifizierungsstelle der A-Trust nutzt. Anwender sind sowohl Zertifikatsinhaber als auch Zertifikatsnutzer.
Audit	Von externen Personen durchgeführte Sicherheitsüberprüfung.
CA (Certification Authority), Zertifizierungsdiensteanbieter	Eine Person oder Stelle, die Zertifikate ausstellt oder anderweitige elektronische Signaturdienste öffentlich anbieten darf.
CA-Schlüssel	Schlüssel der CA, die zur Ausstellung von Zertifikaten und dem Unterschreiben von Widerrufslisten (Zertifizierung) verwendet werden.
CA-Zertifikat, Zertifizierungsstellenzertifikat	Zertifikat der Zertifizierungsstelle, das zur Signatur der Zertifikate der Signatoren und der zugehörigen CRLs dient
Certification Policy, Policy	Ein Regelwerk, das den Einsatzbereich eines Zertifikates für eine bestimmte Benutzergruppe und/oder Anwendungsklasse festhält.
Certification Practice Statement, CPS, Zertifizierungsrichtlinie	Aussagen über die bei der Ausstellung von Zertifikaten von einem Zertifizierungsdiensteanbieter eingehaltenen Vorgehensweise
Dienste (CA-Dienste)	Überbegriff für angebotene Dienstleistungen wie Verzeichnisdienst, Statusauskunft und Zeitstempeldienst
Dienste-Schlüssel	Schlüssel eines Dienstes (z.B. Signaturschlüssel zur Signatur von Statusauskünften)
Digitale Signatur	Elektronische Signatur, die mit Hilfe von Verfahren der asymmetrischen Kryptographie erzeugt wird.
E-Mail	Electronic Mail; Nachrichten, die in digitaler Form über computerbasierte Kommunikationswege versandt oder empfangen werden.
Elektronische Signatur	Eine Signatur in digitaler Form, die in Daten enthalten ist, Daten beigefügt wird oder logisch mit ihnen verknüpft ist und von einem Unterzeichner verwendet wird, um zu bestätigen, dass er den Inhalt dieser Daten billigt. Sie ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.

Gültigkeitsmodell	Modell, nach dem die Prüfung der Gültigkeit von Zertifikaten und Signaturen vorgenommen wird.
Hardware Security Modul, HSM	Elektronisches System zur sicheren Speicherung von Schlüsseln und zur Berechnung und Verifizierung von Signaturen.
Integrität (von Daten)	Ein Zustand, in dem Daten weder von Unbefugten verändert noch zerstört wurden.
Kettenmodell	Gültigkeitsmodell, nach dem eine gültige Anwendung des Schlüssels dann erfolgt, wenn zum Zeitpunkt der Anwendung das Zertifikat gültig ist und das übergeordnete Zertifikat zum Zeitpunkt der Erstellung des eingesetzten Zertifikats gültig war.
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheim zuhaltende Daten.
LDAP	Lightweight Directory Access Protocol ist ein Standard Protokoll für Verzeichnisdienste (LDAP Server) im Internet.
OCSP	Online Certificate Status Protocol, Protokoll für die Statusauskunft
OID	Object Identifier, eine Ganzzahl, durch die ein Objekt (z.B. Policy) eindeutig identifiziert wird.
Öffentlicher Schlüssel	Öffentlicher Teil eines Schlüsselpaares. Er ist Bestandteil eines Zertifikates und wird zur Überprüfung von Digitalen Signaturen bzw. zur Verschlüsselung von Nachrichten/Daten verwendet.
PIN	Personal Identification Number (Aktivierungsdaten)
Privater Schlüssel, geheimer Schlüssel	Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren sowie zum Entschlüsseln von Nachrichten/Dokumenten erforderlich ist und geheim gehalten werden muss.
Public-Key Infrastructure, PKI	Ein kryptografisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Der öffentliche Teil dieses Schlüsselpaars kann jedermann zugänglich gemacht werden, der Informationen verschlüsseln oder eine digitale Signatur prüfen will, der geheime (private) Teil wird von seinem Besitzer sicher bewahrt und kann Daten entschlüsseln oder eine digitale Signatur erstellen.
Qualifiziertes Zertifikat	Zertifikat, welches den Bestimmungen des Anhang I [eIDAS-VO] entspricht.
Qualifiziertes Zertifikat für Siegel	Zertifikat, welches den Bestimmungen des Anhang III [eIDAS-VO] entspricht.

Registrierungsstelle, Registration Authority, RA	Eine vertrauenswürdige Einrichtung, welche die Überprüfung der Identität der Zertifikatsbewerber im Namen des Zertifizierungsdiensteanbieters unter Berücksichtigung der Zertifizierungsrichtlinien durchführt und selbst keine Zertifikate ausstellt.
RFC	Request for Comments, Artikel über Standards und Protokolle im Internet. Neue Standards werden zunächst vorgeschlagen und zur Diskussion gestellt (daher "mit der Bitte um Stellungnahme"). Erst nachdem sie ausdiskutiert und für gut befunden worden sind, werden sie unter einer RFC-Nummer veröffentlicht.
Root-CA, Root-Zertifizierungsstelle	Die Root-CA ist die oberste CA in der Zertifizierungshierarchie der A-Trust. Sie stellt die Zertifikate für die nachgeordneten CAs aus.
Root-Zertifikat, Stammzertifikat, Root-CA Zertifikat	Zertifikat des Root-Keys, der zur Signatur der Zertifikate der Zertifizierungsstellen und der zugehörigen CRLs dient
RSA	Signatur- und Verschlüsselungsverfahren; benannt nach Rivest, Shamir und Adleman
Schlüsselpaar	Ein privater Schlüssel und der dazugehörige öffentliche Schlüssel. Abhängig vom verwendeten Algorithmus kann man mit Hilfe des öffentlichen Schlüssels eine digitale Unterschrift, die mit dem dazu gehörigen privaten Schlüssel erstellt wurde, verifizieren bzw. mit dem privaten Schlüssel Daten entschlüsseln, welche mit dem zugehörigen öffentlichen Schlüssel verschlüsselt wurden.
Siegelersteller	Eine juristische Person, die ein elektronisches Siegel erstellt, Zertifikatsinhaber
Siegelersteller	Eine juristische Person, die ein elektronisches Siegel erstellt
Siegelerstellungsdaten	Siegelerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Siegelersteller zur Erstellung einer elektronischen Signatur verwendet werden.
Siegelprüfdaten	Siegelprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung eines elektronischen Siegels verwendet werden.
Aussetzung	Eine Aussetzung ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines a.sign premium seal Zertifikats.
Statusauskunft	Dienst, bei dem die Anwender Auskunft über den aktuellen Status (gültig oder widerrufen) eines Zertifikates abrufen können.

URI	Uniform Resource Identifier, spezifiziert eine bestimmte Datei auf einem bestimmten Server, Oberbegriff für URL (Uniform Resource Locator) und URN (Universal Resource Name).
Verifizierung (einer digitalen Signatur)	Feststellung, dass eine digitale Signatur mit dem privaten Schlüssel, der zu dem in einem gültigen Zertifikat beinhalteten öffentlichen Schlüssel gehört, erstellt wurde und die Nachricht sich nach der Signatur nicht verändert hat.
Verzeichnis (-dienst)	Dienst, bei dem die Anwender Zertifikate der CA oder anderer Anwender sowie CRLs abrufen können. Der Zugriff wird über LDAP realisiert.
Widerruf	Der irreversible Vorgang der vorzeitigen Beendigung der Gültigkeit eines Zertifikats ab einem bestimmten Zeitpunkt.
X.509	Der ITU-Standard für Zertifikate. X.509 v3 beschreibt Zertifikate, die mit verschiedenen Zertifikatserweiterungen erstellt werden können
Zeitstempel	Digitale Signatur von digitalen Daten und einem Zeitpunkt. Mit Hilfe eines Zeitstempels kann nachgewiesen werden, dass digitale Dokumente zu einem bestimmten Zeitpunkt existiert haben. Um Manipulationen zu verhindern, soll der Zeitstempel nur von einer vertrauenswürdigen Instanz (z.B. Zertifizierungsstelle) ausgestellt werden.
Zertifikatsinhaber	Anwender, dessen Schlüssel und persönliche Daten im Zertifikat der A-Trust festgehalten sind, auch Siegelersteller genannt.
Zertifikatsnutzer, Signaturempfänger	Anwender, der Zertifikate über die Schlüssel und Daten anderer nutzt, um Siegel zu prüfen.
Zertifikats-Widerrufsliste, CRL	Eine digital signierte Datenstruktur, die widerrufene und ausgesetzte Zertifikate anführt, welche von einem bestimmten Zertifizierungsdiensteanbieter ausgestellt wurden.

A.2 Referenzdokumente

[AGB] Allgemeine Geschäftsbedingungen (AGB) A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH (A-Trust) für qualifizierte und fortgeschrittene Zertifikate Version 7.0

[Policy] A-Trust Certificate Policy für qualifizierte a.sign premium seal Zertifikate für sichere Signaturen

[eIDAS-VO] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

[SVG] Bundesgesetz über elektronische Signaturen und Vertrauensdieste für elektronische Transaktionen (Signatur und Vertrauensdienstegesetz - SVG)
StF: BGBl. I Nr. 50/2016 (NR: GP XXV RV 1145 AB 1184 S. 134. BR: 9594 AB 9607 S. 855.)

[SVV] Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – SVV) StF: BGBl. II Nr. 208/2016

[CPS] A-Trust Zertifizierungsrichtlinie für qualifizierte a.sign premium seal Zertifikate für sichere Signaturen, in der jeweils aktuellen Version.

[Policy] A-Trust Certificate Policy für qualifizierte a.sign premium seal Zertifikate für sichere Signaturen

[ETSI 319 411] Policy and security requirements for Trust Service Providers issuing certificates - ETSI EN 319 411-2 v2.2.2 (April 2018)

[DSG] Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.)

[RFC3647] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003

[A-SIT-e-card-G3] A-SIT Bescheinigung nach § 18 (5) SigG: Sichere Signaturerstellungseinheit STARCOS 3.4 Health AHC C1, 21.12.2009

[A-SIT-ACOS-03] A-SIT Bescheinigung nach § 18 (5) SigG: Sichere Signaturerstellungseinheit ACOS EMV-A03V0 Konfiguration B, 13.12.2006 und Sichere Signaturerstellungseinheit ACOS EMV-A03V1 Konfiguration B, 13.02.2006

[ACOS-04] T-Systems GEI GmbH bestätigt nach § 15 Abs. 7 S. 1, 17 Abs. 1 SigG sowie § 15 Abs. 1 und 4, § 11 Abs. 3 SigV (Deutschland): Signaturerstellungseinheit ACOS EMV-A04V1 Konfiguration B, 18.07.2008 (Nachtrag: 18.05.2009)

[ACOS-05] A-SIT Bescheinigung nach § 18 (5) SigG: Sichere Signaturerstellungseinheit ACOS EMV-A05V1, Konfiguration A+B, (23-06-2016), Referenznummer A-SIT-VI-15-062

[CardOS5.3] A-SIT Bescheinigung nach § 1 (5) SigG: Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0,(24.06.2016) ,Referenznummer A-SIT-VI-16-057

[PSD II-Verordnung] DELEGIERTE VERORDNUNG (EU) 2018/389 DER KOMMISSION vom 27. November 2017

[ETSI TS 119 495] Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

[DSGVO] VERORDNUNG (EU) 2016/679 vom 27. April 2016