FLZ

einfach sicher

FLZ - Anstalt
Wirtschaftspark 25, FL - 9492 Eschen
Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350
https://www.flz.li

# FLZ
# Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate lisign qualified mobile

Version: 1.0.3
Datum: 08.09.2020

# Inhaltsverzeichnis

| Rev | Datum | Autor | Änderungen |
|---|---|---|---|
| 1.0.3 | 08.09.2020 | RS, PT | Kontaktdaten |
| 1.0.2 | 23.07.2020 | MI, PT | eIDAS Anpassungen |
| 1.0.1 | 25.04.2018 | RS | initiale version |

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 lisign qualified mobile Anwendungsvorgabe (Certificate Policy) für qualifizierte Signaturen gilt entsprechend der Verordnung (EU) 910/2014 [eIDAS-VO] und dem liechtensteinischen Signatur- und Vertrauensdienstegesetz [SVG] für qualifizierte Zertifikate, die an Endbenutzer ausgestellt werden, auf sicheren Signaturerstellungseinheiten basieren und für die Erstellung qualifizierter Signaturen geeignet sind.

## 1.2 Dokumentidentifikation

| | |
|---|---|
| Name der Richtlinie: | FLZ Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate lisign qualified mobile |
| Version: | 1.0.3 / 08.09.2020 |
| Object Identifier: | 1.2.040.0.17 (A-Trust) .4 (CP FLZ) .2 (lisign qualified mobile) .1.0.3 (Version) vorliegende Version |

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert und wird auch für FLZ verwendet.

Die vorliegende Policy ist in Übereinstimmung mit ETSI EN 319 411-2 Klasse “ qcp-natural-qscd” [Object Identifier: 0.4.0.194112.1.2] (siehe [ETSI 319 411]).

## 1.3 Anwendungsbereich

Die lisign qualified mobile Anwendungsvorgaben gelten für qualifizierte Zertifikate gem. Artikel 3 Z 15 [eIDAS-VO], welche ausschließlich an Endbenutzer ausgestellt werden. Der zertifizierte Schlüssel des Signators darf ausschließlich für das Erstellen von Signaturen genutzt werden.

Elektronische Signaturen, die in Übereinstimmung mit diesen Anwendungsvorgaben und unter Verwendung der von FLZ empfohlenen Komponenten und Verfahren erstellt wurden, sind qualifizierte Signaturen im Sinne Artikel 3 Z 12 [eIDAS-VO].

Qualifizierte Signaturen, die auf Basis eines qualifizierten lisign qualified mobile Zertifikats für qualifizierte Signaturen erstellt wurden, sind in ihrer Rechtswirkung gemäß Artikel 25 Z 2 [eIDAS-VO] einer eigenhändigen Unterschrift grundsätzlich gleichgestellt.

Nur mit einem qualifizierten Zertifikat, welches auf einer qualifizierten Signaturerstellungseinheit gem. Artikel 3 Z 23 [eIDAS-VO] basiert, kann eine qualifizierte Signatur erstellt werden.

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

## 1.4 Übereinstimmung mit der Policy

FLZ 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 Signaturen Beachtung finden.

# 2 Verpflichtungen und Haftung

## 2.1 Verpflichtungen des Zertifizierungsdiensteanbieters

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

- Die Zertifikate für Signatoren 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 gegenüber Signatoren 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 Signatoren und zum Signieren der Widerrufsinformationen.
- Die Zertifikate der Signatoren können im FLZ Verzeichnisdienst veröffentlicht werden, der Signator hat stets die Möglichkeit eine Veröffentlichung abzulehnen. Bei Aussetzung eines Zertifikats wird der betroffene Signator benachrichtigt. Ein nicht veröffentlichtes Zertifikat wird bei einer Aussetzung oder einem Widerruf in die Widerrufsliste aufgenommen.
- FLZ hat insbesondere die Verpflichtung, eine Liste der für eine qualifizierte Signaturerstellung und -prüfung zu verwendenden Komponenten und Verfahren zu erstellen und aktuell zu halten und diese den Signatoren und Überprüfern von Zertifikaten jederzeit zugänglich zu machen.

## 2.2 Verpflichtungen der Signatoren

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

- Die Signatoren verpflichten sich die Allgemeinen Geschäftsbedingungen [AGB] zusammen mit dieser lisign qualified mobileAnwendungsvorgabe (Certificate Policy), der Zertifizierungsrichtlinie [CPS], der Unterrichtung, die Liste der empfohlenen Komponente, den Antrag/Signaturvertrag und den Entgeltbestimmungen von FLZ als Grundlage für den abgeschlossenen Vertrag anzuerkennen.
- Der Signator 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 Signator ist verpflichtet, seine für das Auslösen der Signatur nötigen Komponenten angemessen zu schützen. Dies umfasst insbesondere das Verhindern des Zugriffs durch unautorisierte Personen auf die SIM-Karte/Mobiltelefon und das vom Signator gewählte Signaturpasswort.
- Falls nötig, initiiert der Signator unverzüglich die Aussetzung oder den Widerruf seines Zertifikats. Wird die Aussetzung nicht nach dem in der Zertifizierungsrichtilinie [CPS] vorgegebenen Zeitraum aufgehoben, so erfolgt automatisch ein Widerruf des Zertifikats.
- Der Signator setzt sein Zertifikat nur zu dem im Zertifikat angegebenen Zweck ein. Maßgeblich hierfür sind die zum Zeitpunkt der Ausstellung des Zertifikats gültige Zertifizierungsrichtlinie und dieser Anwendungsvorgabe (Policy).
- Der Signator ist sich bewusst, dass FLZ eine Liste mit empfohlenen technischen Komponenten und Verfahren für die Erstellung von qualifizierten Signaturen bereitstellt und dass bei der Verwendung anderer Komponenten und Verfahren FLZ für Schäden, die durch diese verursacht werden, nicht haftbar gemacht werden kann.
- Es muss weiters dafür Sorge getragen werden, dass sowohl auf dem PC-Arbeitsplatz als auch auf dem eingesetzten Mobiltelefon, auf welchem qualifizierte Signatur erstellt/ausgelöst wird, kein unbefugt eingebrachter Programmcode zur Anwendung kommt. Dazu sollen folgende Vorgaben von FLZ eingehalten werden:
  - Der Signator muss alle notwendigen technischen und organisatorischen Maßnahmen ergreifen, um unbefugten Zugriff auf seinen PC-Arbeitsplatz sowie sein Mobiltelefon und die darauf befindlichen Programmcodes zu verhindern.
  - Der Signator verpflichtet sich, 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 (z.B. Virenscanner, Firewall).
  - Der Signator hat die notwendigen Maßnahmen zu ergreifen, um sich gegen Phishing zu schützen (Kontrolle der SSL Verbindung bzw. des zugrunde liegenden Zertifikats)

- Der Signator ist verpflichtet, die jeweiligen nationalen Ausfuhrbestimmungen sowie etwaige nationale Nutzungsbeschränkungen bei einer Verwendung im Ausland zu beachten.

## 2.3 Verpflichtungen der Signaturempfänger

Den Zertifikatsnutzern von lisign qualified mobile Zertifikaten (Signaturempfänger) wird empfohlen, vor der Akzeptanz folgende Prüfungen durchzuführen:

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

Wenn der überprüfende Signaturempfänger eines Zertifikats eine Signaturprüfung durchzuführen beabsichtigt, dann empfiehlt ihm FLZ die Verwendung der für eine qualifizierte Überprüfung einer Signatur empfohlenen Komponenten und Verfahren.

## 2.4 Haftung

FLZ haftet als Aussteller von qualifizierten Zertifikaten gem. den Bestimmungen in Artikel 13 [eIDAS-VO].

# 3 Anforderungen an die Erbringung von Vertrauensdiensten

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

## 3.1 Zertifizierungsrichtlinie (CPS)

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

1. FLZ hat eine Risikoanalyse erstellt, um die möglichen Risiken abzuschätzen und die sich daraus ergebenden Sicherheitsanforderungen und Umsetzungsmaßnahmen zu bestimmen.
2. FLZ hat alle nötigen Vorgangsweisen und Prozeduren, um die Anforderungen aus der Anwendungsvorgabe zu erfüllen, in ihrem Sicherheitskonzept dargestellt.
3. Die Zertifizierungsrichtlinie für lisign qualified mobile (siehe [CPS]) benennt die Verpflichtungen aller externen Vertragspartner, die Dienstleistungen für FLZ unter Beachtung der jeweils anwendbaren Policies und Richtlinien erbringen.
4. FLZ macht allen Signatoren und Signaturempfängern 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 FLZ stellt das alleinige Entscheidungsgremium dar, das für die Genehmigung der Zertifizierungsrichtlinie für lisign qualified mobile verantwortlich ist.
6. Die Geschäftsführung der FLZ trägt die Verantwortung für die ordnungsgemäße Implementierung der Zertifizierungsrichtlinie für lisign qualified mobile.
7. FLZ hat einen Revisionsprozess zur Überprüfung der Vorgangsweisen der Zertifizierung aufgesetzt, der auch Maßnahmen zur Wartung der Zertifizierungsrichtlinie für lisign qualified mobile umfasst.
8. FLZ 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 lisign qualified mobile entsprechend Kapitel 3.3.4 unverzüglich zugänglich machen.

## 3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

### 3.2.1 Erzeugung der FLZ Schlüssel

Die Generierung der von FLZ zur Erbringung von Zertifizierungsdiensten eingesetzten Schlüssel, erfolgt auf einer Signaturerstellungseinheit in Übereinstimmung mit den Bestimmungen aus Artikel 29 [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 Signaturerstellungseinheit (Hardware Security Modul) erstellt, die einem Bestätigungsverfahren bei A-SIT unterzogen wurde und zur Erstellung qualifizierter Signaturen 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 werden entsprechend den Stand der Technik regelmäßig neu evaluiert und gegebenenfalls angepasst.

### 3.2.2 Speicherung der CA-Schlüssel

FLZ 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 Art 4 (4) [SVV] erfüllt.

### 3.2.3 Verteilung der öffentlichen CA Schlüssel

FLZ 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 lisign qualified mobile Zertifikaten wird den Zertifikatsinhabern durch Veröffentlichung im Rahmen des Verzeichnisdienstes zugänglich gemacht. FLZ 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 lisign qualified mobile 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 lisign qualified mobile Zertifikaten werden verwendet, solange die verwendeten Algorithmen den Sicherheitserwartungen entsprechen. Die Zertifikate über die Schlüssel der FLZ Zertifizierungsstelle werden spätestens alle zehn Jahre erneuert.

Eine Archivierung der geheimen Schlüssel ist nicht vorgesehen.

### 3.2.7 Erzeugung der Schlüssel für die Signatoren

Die Schlüssel werden im Hochsicherheitsbereich des FLZ Rechenzentrums auf einer Signaturerstellungseinheit (Hardware Security Modul) erzeugt, welche die Anforderungen aus Artikel 29 [eIDAS-VO] erfüllt.

Es werden entsprechende Maßnahmen gesetzt, dass der private Schlüssel des Signators das HSM nicht in unverschlüsselter Form verläßt.

## 3.3 Lebenszyklus des Zertifikats

### 3.3.1 Registrierung des Signators

Die Identifikation von Zertifikatswerbern erfolgt durch assoziierte Registrierungsstellen.

Die Maßnahmen zur Identifikation und Registrierung des Signators 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 Signators werden in zwei Kategorien eingeteilt. Dies sind zum einen die erforderlichen und zum anderen die optionalen Angaben. Es sind folgende Daten aufzunehmen:

Qualifizierte lisign qualified mobile Zertifikate enthalten zumindest:

- Name für das lisign qualified mobile Zertifikat: Nachname und Vorname sind erforderlich. Bei Namensteilen welche die Maximallänge des technischen Zertifikatsstandards überschreiten, können diese entsprechend ihrer Reihenfolge entfallen.
  Im Falle von Standard lisign qualified mobile können Signatoren statt des Namens auch ein Pseudonym wählen. Der korrekte und vollständige Name muss der Registrierungsstelle und Zertifizierungsstelle auch bei Verwendung eines Pseudonyms bekannt sein.
- Die Angabe der postalischen oder einer elektronischen Adresse ist erforderlich.
- Die Angabe der Meldeadresse ist optional.
- Optional können im Namen des Zertifikatswerbers die Attribute OrganizationName mit dem Inhalt "Berufsbezeichnung" (z.B. Rechtsanwalt) und OrganizationalUnit mit einem eindeutigen Code (z.B. Rechtsanwaltscode) als Inhalt vergeben werden. Diese Attribute werden nur vergeben, wenn die ausstellende Registrierungsstelle, z.B. Rechtsanwaltskammer, die Korrektheit dieser Angaben sicher stellt.
  Das Attribut OrganizationName kann auch bei Behördenzertifikaten nach Bekanntgabe der Behörde vergeben werden (siehe Kapitel 4.1).

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

**Authentisierung von Individuen** Die Angaben des Antragstellers werden bei der Ausstellung des Zertifikates in der Registrierungsstelle durch den Registration Officer überprüft. Der Antragsteller beweist seine Identität durch das Vorlegen eines gültigen, amtlichen Lichtbildausweises. Dabei sind die folgenden Ausweise zulässig:

- ein in Liechtenstein ausgestellter amtlicher Lichtbildausweis oder
- ein international gültiger Reisepass in deutscher und/oder englischer Sprache.

Es ist ebenfalls zulässig, dass der Signator ein neues qualifiziertes Zertifikat, mittels einer qualifizierten Signatur aktiviert. In diesem Falle ist keine erneute Registrierung / Rezertifizierung erforderlich. Sollten sich personenbezogene Daten geändert haben, muss eine erneute Registrierung / Rezertifizierung erfolgen.

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

Gemäß Artikel 24 (1) [eIDAS-VO] Lit d können weitere Identifizierungsmethoden von einer Konformitätsbewertungsstelle bestätigt werden.

**Authentisierung von Organisationen** Keine Bestimmungen.

Als Antrag wird verstanden, wenn der Signator entweder selbst oder durch bevollmächtigte Dritte freiwillig seine Personendaten an die FLZ übermittelt, um in den Besitz eines lisign qualified mobile Zertifikates zu kommen. Es wird ebenfalls die persönliche Kontaktaufnahme mit einer Registrierungsstelle zur Aktivierung eines Zertifikats, wie auch die Nutzung einer entsprechenden Webanwendung zur Aktivierung eines Zertifiats als Antrag verstanden. Die Freiwilligkeit bestätigt der Signator mit dem Akzeptieren des zustande kommenden Antrages.

Qualifizierte Zertifikate, die auf die Namen Max Mustermann, Test Zupfer, Test Test, Musterfrau Maxine lauten oder deren Namen mit XXX beginnen, werden von der FLZ 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 Signator kann nach einem Widerruf ein Ersatzprodukt bestellen und analog der Erstregistrierung aktivieren. Dabei sind allfällige Änderungen in den personenbezogenen Daten anzugeben.

Es ist ebenfalls zulässig, dass ein neues lisign qualified mobile Zertifikat, mittels einer noch gültigen qualifizierten oder fortgeschrittenen Signatur durch den Signator selbst aktiviert wird. In diesem Falle ist keine erneute Registrierung / Rezertifizierung erforderlich.

### 3.3.3 Ausstellung von Zertifikaten

Durch die folgenden Maßnahmen wird sicher gestellt, dass Ausstellung, Verlängerung und Neuausstellung von Zertifikaten in sicherer Weise erfolgen und den Anforderungen von [SVG] und der [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
  - Geburtsdatum des Zertifikatsinhabers (optional), verpflichtend bei Minderjährigen Anhang I [eIDAS-VO]
  - Optionales Behördenkennzeichen und ggf. ein optionaler Verwaltungsbezeichner.

2. Das Zertifikat wird nach der Identifizierung des Zertifikatswerbers und Bestätigung der Korrektheit aller Daten ausgestellt. Das Verfahren ist für Verlängerung und Neuausstellung identisch.

3. Für alle lisign qualified mobile Zertifikate gilt:

   - Jedem Signator wird eine innerhalb der FLZ 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.

### 3.3.4 Bekanntmachung der Vertragsbedingungen

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

- der gegenständliche Anwendungsvorgabe (Certificate Policy),
- des Zertifizierungsrichtlinie für lisign qualified mobile, siehe [CPS],
- der Allgemeinen Geschäftsbestimmungen [AGB],
- der Unterrichtung für den Signator,
- der sonstigen Mitteilungen,
- die Entgeltbestimmungen
- der Signaturvertrag (Antrag)
- die FLZ Liste der empfohlenen Komponenten und Verfahren.

Änderungen werden dem Signator mittels Bekanntmachung auf der FLZ Homepage und gegebenenfalls per Mail oder Brief mitgeteilt.

### 3.3.5 Veröffentlichung der Zertifikate

Von FLZ ausgestellte Zertifikate werden den Signatoren und, je nach Vereinbarung mit dem Signator, den Signaturempfängern folgendermaßen verfügbar gemacht.

- Wenn der Signator damit einverstanden ist, wird das Zertifikat im Verzeichnisdienst von FLZ veröffentlicht.
- Die Bedingungen für die Benutzung eines Zertifikats werden von FLZ allen Beteiligten zur Kenntnis gebracht (siehe Kapitel 3.3.4).
- Die Identifikation der anzuwendenden Bestimmungen ist durch die eindeutige Zuordnung zum Produktnamen "lisign qualified mobile" einfach herstellbar.
- Der Verzeichnisdienst ist 7 Tage 24 Stunden verfügbar. Unterbrechungen von mehr als 30 Minuten werden gemäß Art 8 (5) [SVV] als Störfälle dokumentiert.
- Der Verzeichnisdienst ist öffentlich und international zugänglich.

### 3.3.6 Aussetzung und Widerruf

lisign qualified mobile 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 informiert, sofern FLZ Kontaktinformationen (Adresse, email, ...) bekanntgeben wurden.

Die Vorgangsweisen für das Auslösen von Aussetzung und Widerruf sind in der Zertifizierungsrichtlinie für lisign qualified mobile (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 wendet sich an eine Registrierungsstelle oder öffentliche Stelle, um über diese benatragte Zertifikate widerrufen zu lassen.
- Der Signator bzw. der Vertretungsbefugte veranlasst den Widerruf per Fax.
- Bei Vergessen des Passworts für den Widerruf kann nur eine Aussetzung beantragt werden.

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 Widerruf-Passwort, welches der Antragsteller bei der Bestellung bzw. Registrierung erhalten bzw. selbst festgelegt hat.
  Die für einen Widerruf benötigten Informationen lassen sich wie folgt zusammenfassen:
  - Persönliche Daten des Antragsstellers (vollständiger Name, Geburtstag und -ort),
  - Passwort für den Widerruf,
  - Identifikationsnummer des Signators (CIN) 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 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 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:

- 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 lisign qualified mobile (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 FLZ Verwaltung

### 3.4.1 Sicherheitsmanagement

Es gelten folgende Bestimmungen:

- FLZ 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 lisign qualified mobile veröffentlicht.

- Die Geschäftsführung von FLZ ist unmittelbar verantwortlich für die Definition der Sicherheitsrichtlinien und deren Kommunikation an die mit sicherheitsrelevanten Vorgängen befassten Mitarbeiter.
- Die Sicherheitsinfrastruktur von FLZ 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 FLZ zu genehmigen.
- Alle Sicherheitsmaßnahmen und sicherheitsrelevanten Funktionen zur Bereitstellung der Zertifizierungsdienste werden von FLZ dokumentiert und entsprechend der Dokumentation implementiert und gewartet.
- Der Betrieb des Rechenzentrums der FLZ ist ausgelagert. Der Dienstleister ist an die Wahrung der Informationssicherheit vertraglich gebunden.

### 3.4.2 Informationsklassifikation und -verwaltung

FLZ 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 FLZ und deren Beschäftigungsmodalitäten sind geeignet, das Vertrauen in die Abwicklung der Zertifizierungsdienste zu stärken. Insbesondere wird Wert gelegt auf:

- FLZ 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 FLZ (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.
- FLZ 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 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 und die Widerrufsdienste werden in einer gesicherten Umgebung betrieben, sodass eine Kompromittierung durch unautorisierte Zugriffe nicht möglich ist.
- Die Abgrenzung der Systeme für Zertifikatsgenerierung 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 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

FLZ 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, Schad- oder unautorisierte Software geschützt.
- Schaden durch sicherheitskritische Zwischenfälle und Fehlfunktionen wird durch entsprechende Aufzeichnungen und Fehlerbehebungsprozeduren mitigiert.
- 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 FLZ-Sicherheitsbeauftragten gehandhabt, können aber von operativem Personal (unter Beaufsichtigung) gem. Sicherheitskonzept und Stellenbeschreibungen durchgeführt werden.

### 3.4.6 Zugriffsverwaltung

FLZ 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 lisign qualified mobile (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

FLZ 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 FLZ oder von Dritten im Auftrag von FLZ 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

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

- Der Notfallsplan von FLZ sieht die (vermutete) Kompromittierung des privaten Zertifizierungsschlüssels als Katastrophenfall vor.
- Sollte dieser Fall eintreten, so hat FLZ 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 FLZ 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 FLZ 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, 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 FLZ 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 FLZ (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 und der [DSGVO] 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. Die Dokumentation entsprechend Artikel 24 (2) Lit. h [eIDAS-VO] wird gemäß Art 9 (4) [SVG] für 35 Jahre elektronisch aufbewahrt. Das Antragsformular wird für drei Jahre in der betreffenden Registrierungsstelle im Original aufbewahrt.
5. Alle Aufzeichnung erfolgen derart, dass sie innerhalb der Aufbewahrungsfrist nicht leicht gelöscht oder zerstört werden können.
6. Die spezifischen Ereignisse und Daten die aufgezeichnet werden, sind in der Zertifizierungsrichtlinie (siehe [CPS]) dokumentiert.
7. Insbesondere werden alle Registrierungsinformationen, inkl. jener, die im Zusammenhang mit der Verlängerung der Gültigkeitsdauer von Zertifikaten stehen, elektronisch aufbewahrt.
8. Die aufzuzeichnenden Registrierungsinformationen beinhalten insbesondere:
    - die Art und Daten der zur Identifikation herangezogenen Dokumente

- 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.

9. Die Vertraulichkeit der Daten der Signatoren ist gewährleistet.
10. Es werden alle Ereignisse, die den Lebenszyklus der CA-Schlüssel von A-Trust betreffen, aufgezeichnet.
11. Es werden alle Ereignisse, die den Lebenszyklus der Zertifikate betreffen, aufgezeichnet.
12. Es werden alle Ereignisse, die im Zusammenhang mit der Generierung der Schlüssel der Signatoren stehen, aufgezeichnet.
13. Alle Anträge auf Aussetzung, Aussetzungsaufhebung und Widerruf und die damit verbundenen Informationen werden aufgezeichnet.

## 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 Anforderungen unter 3.3.1 erfüllen.
- 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 der [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

| | |
|---|---|
| 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. |

| | |
|---|---|
| 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. |
| Signator | Eine natürliche Person, die eine elektronische Signatur erstellt, Zertifikatsinhaber |
| Signaturerstellungsdaten | Signaturerstellungsdaten sind einmalige Daten wie Codes oder private Signaturschlüssel, die von dem Signator zur Erstellung einer elektronischen Signatur verwendet werden. |
| Signaturprüfdaten | Signaturprüfdaten sind Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden. |
| Aussetzung | Eine Aussetzung ist ein zeitlich begrenztes vorübergehendes Aussetzen der Gültigkeit eines lisign qualified mobile 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 Signator genannt. |
| Zertifikatsnutzer, Signaturempfänger | Anwender, der Zertifikate über die Schlüssel und Daten anderer nutzt, um Signaturen 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] FLZ Allgemeine Geschäftsbedingungen (AGB) für qualifizierte, fortgeschrittene und einfache Zertifikate V2.0

[Policy] FLZ Certificate Policy für qualifizierte lisign qualified mobile 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] Gesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz; SigVG) Liechtensteinisches Landesgesetzblatt, Jahrgang 2019, Nr. 114, ausgegeben am 29. April 2019

[SVV] Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung; SigVV) Liechtensteinisches Landesgesetzblatt, Jahrgang 2019, Nr. 180, ausgegeben am 12. Juli 2019

[CPS] FLZ Zertifizierungsrichtlinie für qualifizierte lisign qualified mobile Zertifikate für sichere Signaturen, in der jeweils aktuellen Version.

[Policy] FLZ Certificate Policy für qualifizierte lisign qualified mobile 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)

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

[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 ğ 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