fidentity

Practice Statement

Versionskontrolle

Version	Datum	Verfasser	Anmerkung
1	01.10.2022	Thorsten Hau	**Erste Version**
2	01.2.2023	Thorsten Hau	**Identitätsattribute in Abschnitt 5 hinzugefügt**
3	27.3.2023	Franziska Ackermann	**Fehlende Links und Formatierungsprobleme korrigiert**
4	15.04.2024	Naira Orlando	**Übersetzung EN - DE, Formatierung angepasst**

1. Referenzdokumente

1.1. Swisscom CP/CPS ZertES (CH): PDF (DE), PDF (EN)

1.2. Swisscom CP/CPS EIDAS (EU): PDF, und Zeitstempel: PDF

Swisscom AGB:

	CH / ZertES	EU / EIDAS
DE	PDF	PDF
EN	PDF	PDF

ETSI 119 461

2. Abkürzungen und Definitionen

CPS = Certification Practices Statement (Regelungen für den Zertifizierungsbetrieb).

Die im CPS von Swisscom verwendeten Definitionen werden durchweg in diesem Dokument verwendet.

3. Allgemeine Anmerkungen

fidentity fungiert als Registrierungsstelle (RA-Partner), die Antragsteller (natürliche Personen, die ein Dokument mit einer qualifizierten Signatur signieren wollen) identifiziert und authentifiziert, Anträge auf qualifizierte Signaturdienste erfasst und prüft, die Antragsunterlagen (Dokumente, Vollmachten etc.) archiviert und die Daten an die Zertifizierungsstelle weiterleitet. fidentity ist vertraglich verpflichtet, die von Swisscom in seinem Practice Statement definierten Prozesse für Registrierung, Zertifikatsausstellung, Widerruf und Archivierung einzuhalten.

Die Stellung von Swisscom Trust Services als TSP nach Schweizer und EU-Recht kann hier überprüft werden:
- Trust-Liste der Schweiz
- Trust-Liste der EU

fidentity ist bestrebt, eine Verfügbarkeit von 99,9 % zu gewährleisten.

4. Zertifikate

Qualifizierte Signaturen, die bei der Nutzung von fidentity erstellt werden, werden mit von Swisscom Trust Services ausgestellten Zertifikaten erstellt.

Antragsteller und/oder vertrauende Parteien können wählen, ob die Signatur nach EU-Recht (EIDAS) oder nach Schweizer Recht (ZertES) gültig sein soll.

Der DN (Distinguished Name, eindeutiger Name) ist wie folgt strukturiert:

Element	X.520 Attribut	Inhalt
Angezeigter Name	commonName (gemeinsamer Name)	cn=<FName LName> (gemäss MRZ, keine Zwischennamen)
Identität	Pseudonym	Pseudonym=<ID-document number> (gemäss MRZ)
Land	countryName (Name des Landes)	c=< 3-digit countrycode> Ausstellendes Land gemäss MRZ
Einzigartigkeit	serialNumber (Seriennummer)	serialNumber=fid<Process ID> (fidentity-Prozess-ID)
Organisation	organisation	o=<fidentity AG>
Organisatorische Einheit	organizational Unit	ou=<Identity and Signing>

Testzertifikate müssen sowohl im Common Name (CN) als auch in der Organisationsbeschreibung den Ausdruck «TEST» enthalten.
Die ausgestellten Zertifikate sind gemäss der Swisscom-Richtlinie kurzlebig (10 Minuten) und können nur für den jeweiligen Signaturvorgang verwendet werden.

5. Identifizierung

fidentity validiert Antragstelleridentitäten gemäss Anwendungsfall 9.2.3.4 «Anwendungsfall für unbeaufsichtigte Fernidentitätsprüfung – automatisierter Betrieb» aus der ETSI-Norm 119 461.

Die Identitätsattribute werden aus dem Ausweisdokument gesammelt, das der Nutzer während des Identifizierungsprozesses vorlegt. Die Daten werden sowohl von den Bildern des Dokuments als auch von dem im Dokument eingebetteten NFC-Chip erfasst. Diese Attribute sind:

- Nummer des Dokuments
- Ablaufdatum des Dokuments
- Gesichtsbild
- Namen (gemäss NFC und MRZ, möglicherweise gekürzt)
- Nationalität
- Ausstellendes Land
- Geburtsdatum
- Geschlecht

fidentity akzeptiert Ausweisdokumente, die zusammengenommen die nachstehenden Anforderungen erfüllen:

- elektronische, maschinenlesbare Reisedokumente (eMRTDs) gemäss ICAO 9303.
- Dokumente, die zur Einreise in die Schweiz zugelassen sind.
- Dokumente, die technisch mit seinem Dienst kompatibel sind.

Die akzeptierten Dokumente sind in der veröffentlichten Liste der akzeptierten Dokumente abschliessend aufgeführt. Die Liste kann von Zeit zu Zeit aktualisiert werden.

6. Authentifizierung

fidentity authentifiziert die Antragsteller für den jeweiligen Identifizierungs- und Signaturvorgang (innerhalb der Nutzersitzung). Die Authentifizierung erfolgt durch die Sitzungsinformationen und den Identifizierungsprozess. Der Antragsteller erhält keine Zugriffsmöglichkeiten, um später weitere Signaturvorgänge durchzuführen.

7. Einwilligung

Alle Antragsteller müssen die folgenden Allgemeinen Geschäftsbedingungen (AGB) akzeptieren, wenn Sie den fidentity-Dienst nutzen:

- AGB von Swisscom Trust Services in seiner Eigenschaft als TSP
- AGB von fidentity als Beauftragter von Swisscom Trust Services TSP

8. Datenschutz

fidentity speichert die Daten, die während des Identifizierungs- und Signaturprozesses entstehen, soweit es dies für notwendig erachtet.

Die Datenschutzrichtlinie von fidentity ist in der auf der Website des Unternehmens veröffentlichten Datenschutzrichtlinie dargelegt.

Anfragen zum Datenschutz können an info@fidentity.ch gerichtet werden.

9. Physische, verfahrenstechnische und personelle Sicherheitskontrollen

9.1. Rechenstandorte

Die Systeme von fidentity befinden sich in Rechenzentren. Die wichtigen Komponenten sind redundant und befinden sich in der Schweiz. Die Trustcenter bieten angemessene Schutz- und Infrastrukturschutzmassnahmen und entsprechen den gesetzlichen Anforderungen.

Die Rechenzentren verfügen über eine unterbrechungsfreie Stromversorgung (No-Break). Im Falle eines Stromausfalls wird der Strom durch ein Notstromaggregat erzeugt.

In den Trustcentern sorgen redundante Klimaanlagen für eine angemessene Raumtemperatur und Luftfeuchtigkeit.

Die Serverräume für die technische Infrastruktur bieten ausreichenden Schutz vor Wasserschäden.

Es gibt Brandschutzvorschriften. Die Trustcenter verfügen insbesondere über eine ausreichende Anzahl von Brandmeldeanlagen und Feuerlöschern.

Die Datenspeichergeräte werden in verschlossenen Räumen oder Schränken aufbewahrt. Wenn sich Datenspeichergeräte mit sensiblen Daten nicht in einem Swisscom-Rechenzentrum befinden, werden sie in einem Tresor aufbewahrt.

Alle Daten auf elektronischen Datenspeichergeräten oder auf Papier werden auf professionelle Art und Weise vernichtet und anschliessend entsorgt.

Backups werden auf physisch getrennten Systemen aufbewahrt.

9.2. Verfahrenstechnische Kontrollen

Vertrauensvolle Aufgaben müssen von Personen übernommen werden, die einer regelmässigen Überprüfung unterzogen werden. Bei diesen Personen kann es sich um Mitarbeiter oder Auftragnehmer von fidentity handeln. Sie haben Zugang zu den Systemen von fidentity und können Vorgänge durchführen, die erhebliche Auswirkungen auf die Vertraulichkeit, Integrität, Verfügbarkeit oder Compliance haben können.

Zu den zuverlässigen Personen gehören unter anderem Administratoren, Engineers, Sicherheitsbeauftragte und verantwortliche Manager.

Die Funktionen und Zuständigkeiten der Personen in vertrauenswürdigen Funktionen sind so verteilt, dass eine Person nicht allein handeln kann, um Sicherheitsmassnahmen zu umgehen und die Vertrauenswürdigkeit der RA-Vorgänge zu untergraben.

Die Zuweisung von vertrauenswürdigen Funktionen an Personen wird jährlich überprüft.
Der technische Zugang zu den IT-Systemen erfolgt über eine starke Authentifizierung oder über Benutzer-ID und Passwort.

fidentity schreibt eine Trennung der Aufgaben vor, um die Anhäufung unvereinbarer Funktionen auf eine Person zu verhindern und damit Interessenkonflikten vorzubeugen, das Vier-Augen-Prinzip durchzusetzen und schädigendes Verhalten zu verhindern.

Die Mitarbeiter von fidentity, die für den Betrieb der Plattform und die Überwachung verantwortlich sind, erfüllen die gesetzlichen Anforderungen, insbesondere im Hinblick auf Fachwissen, Zuverlässigkeit, Erfahrung und Qualifikationen.

Alle Mitarbeiter mit Zugang zu den IT-Systemen von fidentity müssen einen Auszug aus dem Strafregister und aus dem Betreibungsregister vorlegen.

Nur qualifizierte Mitarbeiter werden von fidentity beschäftigt. Ein Mitarbeiter erhält erst dann die Berechtigung zur Ausübung einer bestimmten Funktion, wenn er die erforderliche fachliche Qualifikation nachweisen kann.

Alle Mitarbeiter erhalten regelmässige Schulungen (mindestens alle 12 Monate) zu bewährten Praktiken im Bereich des Datenschutzes.

Unbefugte Handlungen, die die Sicherheit der IT-Systeme gefährden oder gegen Datenschutzvorschriften verstossen, werden disziplinarisch geahndet.

Die Mitarbeiter haben Zugang zu Lehrmaterial, Betriebsunterlagen und Verfahrensanweisungen.

9.3. Rückverfolgbarkeit

Die folgenden Ereignisse werden protokolliert:

- Zugriff, Start und Herunterfahren, Abstürze, Fehler, Änderungen
- Änderungen an privaten Schlüsseln
- Physischer Zugang zur Infrastruktur
- Änderungen an diesem Dokument

Jedes Ereignis wird mit einem Zeitstempel versehen und die ausführende Person oder der ausführende Prozess wird angegeben.

Die Protokolldaten werden an einen zentralen Protokollserver übertragen und vor Zugriff, Löschung und Manipulation geschützt.

9.4. Archivierung

fidentity archiviert die gesetzlich vorgeschriebenen Identifikationsdaten für die gesetzlich vorgeschriebene Zeit:

- Schweizer (ZertES) konforme QES: mindestens 11 Jahre
- EU (eIDAS) konforme QES: mindestens 35 Jahre

fidentity ergreift geeignete Massnahmen, um sicherzustellen, dass die Daten weder unbefugt gelesen oder kopiert, noch verändert oder gelöscht werden können.

9.5. Kompromittierung und Notfallwiederherstellung

fidentity setzt umfassende und effektive Verfahren zur Aufdeckung und Behandlung von Vorfällen und Schwachstellen ein.

Der Dienst wird nach einem Notfall nur dann wieder aufgenommen, wenn die Sicherheit gewährleistet ist.

9.6. Beendigung des Dienstes

Wenn die Identifizierungs- und Signaturdienste beendet werden, werden die folgenden Massnahmen ergriffen:

1. Benachrichtigung des TSP (Swisscom) mindestens 30 Tage vor Beendigung des Geschäftsbetriebs
2. Übermittlung der archivierten Identifikationsdaten an Swisscom
3. die Kundenorganisationen werden unverzüglich über die Einstellung des Geschäftsbetriebs informiert
4. eine Mitteilung über die Einstellung des Geschäftsbetriebs auf der Website veröffentlicht wird

9.7. Aktivierungsdaten

Aktivierungsdaten für Signaturen, die privaten Schlüssel der Abonnenten bleiben innerhalb der Swisscom-Trustcenter. Der Abonnent autorisiert die Verwendung seines privaten Schlüssels über die Aktivierungsdaten, d. h. die Identifizierungssitzungsinformationen und die eMRTD-Validierung.
Aktivierungsdaten müssen die Anforderungen der Stufe 2 (Sole Control Assurance Level 2) erfüllen.

9.8. IT-Sicherheitskontrollen

fidentity führt mehrere Arten von Sicherheitskontrollen durch:

- Laufende externe Penetrationstests zur Aufdeckung von Schwachstellen in der Verteidigung gegen unbekannte oder neuartige Angriffe.
- Jährliche Penetrationstests zur Überprüfung des gesamten Dienstes auf bekannte Schwachstellen.

- Ein definierter Änderungsprozess, der von einer Software unterstützt wird, die vollständige Transparenz und Prüfung von Änderungen gewährleistet.
- Laufende automatisierte und manuelle Überprüfungen von Änderungen
- Metriken für Codequalität

Darüber hinaus werden folgende Sicherheitsmassnahmen implementiert:
- Restriktive Zugangskontrolle
- Die Benutzerauthentifizierung und -autorisierung basiert auf den «Need-to-know"- und «Need-to-do"-Prinzipien.
- Perimeterschutz: Virenschutz, Einsatz von Firewall-Kaskaden und Web Application Firewall (WAF).
- Verwendung aktueller Software-Releases und rechtzeitige Installation von sicherheitsrelevanten Software-Updates erst nach Tests auf einem Staging-System.

Das Sicherheitsmanagement umfasst die folgenden Aspekte:
- Jährliche Audits (Konformitätsprüfung durch eine akkreditierte Konformitätsbewertungsstelle)
- Regelmässige Bewertung und Entwicklung des Sicherheitskonzepts (jährlich)

fidentity besteht aus Mikrodiensten, die in separate Teilnetzwerke aufgeteilt und durch eine mehrschichtige Firewall und WAF geschützt sind.

10. Compliance

Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen von digitalen Zertifikaten (Bundesgesetz über die elektronische Signatur, [ZertES]), Stand 1. Januar 2017

Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG [eIDAS-VO], in der Fassung vom 29.01.2015

Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – [SVG]) vom 01.07.2016

Verordnung über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdiensteverordnung – [SVV]) vom 02.08.2016

ETSI TS 119 461 V1.1.1 (2021-07) «Elektronische Signaturen und Infrastrukturen (ESI); Richtlinien- und Sicherheitsanforderungen für Vertrauensdienstkomponenten, die den Identitätsnachweis von Vertrauensdienstsubjekten erbringen»

Die Einhaltung dieser Anforderungen wurde von KPMG als Konformitätsbewertungsstelle geprüft und zertifiziert.

Die Konformitätsbewertungsstelle überprüft fidentity regelmässig sowie nach allen sicherheitsrelevanten Änderungen an diesem Dokument.

Swisscom verfügt über eine Haftpflichtversicherung mit einer für die Zwecke von [VZertES] ausreichenden Deckung.

Swisscom ITSF verfügt über eine Haftpflichtversicherung mit einer für die Zwecke der [eIDAS-VO] ausreichenden Deckung.

11. Streitigkeiten

Beschwerden sind an info@fidentity.ch zu richten.
Die Parteien werden sich bemühen, zu einer gütlichen Lösung zu kommen.
Soweit gesetzlich nicht anders vorgeschrieben, ist der Gerichtsstand Bern.