fidentity

Fidentity Practice statement

Version control

Version	Date	Author	Comment
1	1.10.2022	Thorsten Hau	First version
2	1.2.2023	Thorsten Hau	Added identity attributes in section 5

1. Referenced documents

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

1.2 Swisscom CP/CPS EIDAS (EU): PDF, and Timestamping: PDF

Swisscom T&C:

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

ETSI 119 461

2. Acronyms and Definitions

CPS = Certification practices statement.
The definitions used in the Swisscom CPS are used throughout this document.

3. General remarks

fidentity acts as the registration authority (RA partner) that identifies and authenticates applicants (natural persons that want to sign a document with a qualified signature), records and reviews applications for qualified signing services, archives the application documentation (documents, authorizations, etc.) and forwards the data to the certification authority. fidentity is obliged by contract to comply with the processes defined by Swisscom in its practice statement for registration, certificate issuance, revocation and archiving.

Swisscom Trust Services' standing as TSP under CH and EU law may be verified here:

- CH Trust list
- EU Trust list

fidentity endeavours to provide an availability of 99.9%.

4. Certificates

Qualified signatures that are created when using fidentity are created by using certificates issued by Swisscom trust services.

Applicants and/or relying parties can choose whether the signature is valid under EU law (EIDAS) or Swiss law (ZertES).

The DN is structured as follows:

Element	X.520 Attribute	Content
Display name	commonName	cn=<FName LName> (as per MRZ, no middle names)
Identity		
	Pseudonym	Pseudonym=<ID-document number> (as per MRZ)
Country	countryName	c=< 3-digit countrycode> Issuing country as per MRZ
Uniqueness	serialNumber	serialNumber=fid<Process ID> (fidentity process ID)
Organisation	organisation	o=<fidentity AG>
Organisational Unit	organizational Unit	ou=<Identity and Signing>

Test certificates must contain the expression "TEST" in the common name (CN) as well as in any organization description.
The issued certificates are short lived as per Swisscom policy (10 minutes) and can only be used for the signing operation at hand.

5. Identification

fidentity validates applicant identities according to Use case 9.2.3.4 “Use case for unattended remote identity proofing - automated operation” from ETSI norm 119 461.

Identity attributes are collected from the ID document that the user presents during the identification process. Data is collected from the images of the document as well as the NFC Chip embedded in the document. The attributes are:

- Document number
- Document expiration date
- Facial image
- Names (as per NFC and MRZ, possibly truncated)
- Nationality
- Issuing country
- Date of birth
- Gender

fidentity accepts identity documents that collectively fulfill the below requirements:

- electronics machine readable travel documents (eMRTDs) as per ICAO 9303.
- documents that are permissible to enter Switzerland.
- documents that are technically compatible with its service.
-

Accepted documents are conclusively listed in its published list of acceptable documents. The list may be updated from time to time.

6. Authentication

fidentity authenticates applicants for the identification and signing operation at hand (within the user session). Authentication happens through the session information and the identification process. Applicant does not receive access means to perform additional signing operations later.

7. Consent

All applicants must accept the following terms and conditions (T&C) when using the fidentity service:

- Swisscom trust services T&C in its capacity as TSP
- fidentity T&C as a delegate of Swisscom Trust Services TSP

8. Data protection

fidentity records data that is produced during the identification and signing process as it deems necessary.

The fidentity data privacy policy is laid out in the data privacy policy published on its website.

Data protection inquiries may be directed to info@fidentity.ch.

9. Physical, Procedural and Personnel Security Controls

9.1. Computing sites

The systems of fidentity are located in data centres. The important components are redundant and are located in Switzerland. The Trust Centres provide adequate protection and infrastructure protection measures and comply with legal requirements.
The data centres have an interruption-free power supply (no-break). In the event of a power
failure, electricity is produced by an emergency power unit.
In the Trust Centres redundant air conditioning systems ensure a suitable room temperature and
humidity.
The server rooms for the technical infrastructure have adequate protection against water damage.
There are fire protection regulations. In particular, the Trust Centres have a sufficient number of fire alarm systems and hand-held fire extinguishers.

Data storage devices are kept in locked rooms or cabinets. If data storage devices with sensitive data are not located in a Swisscom data centre, they are kept in a vault.
All data on electronic data storage devices or paper are destroyed in a professional manner and then disposed of.
Backups are kept on physically separated systems.

9.2. Procedural controls

Trusted roles must be taken over by persons who are subject to regular review. Such persons may be fidentity employees or contractors. They have access to the systems of fidentity and carry out operations which can have a significant effect on confidentiality, integrity, availability or compliance.
Reliable persons include, but are not limited to administrators, engineers, security officer, responsible managers.
The roles and responsibilities of people in trusted roles are distributed in such a way that a person cannot act alone to circumvent security measures and undermining the trustworthiness of RA operations.
The assignment of trusted roles to persons is reviewed annually.

Technical access to IT systems is realized by strong authentication or user ID and password.

fidentity stipulates a separation of the tasks to prevent the accumulation of incompatible roles on a person and thus to prevent conflicts of interest, to enforce the dual-control principle and to prevent harming behavior.

The employees of fidentity, who are responsible for the operation of the platform or the monitoring fulfil the legal requirements, in particular with regards to expertise, reliability, experience and qualifications.

All employees with access to fidentity's IT systems have to provide an extract from the criminal record and from the debt collection register.

Only qualified employees are employed by fidentity. An employee only receives authorization to perform a specific role after proof of the necessary technical qualification.
All employees receive regular training (at least every 12 months) on data privacy best practices.

Unauthorized actions that endanger the security of the IT systems or violate data protection regulations are subject to disciplinary action.

Employees have access to course material, operating documents and procedural Instructions.

9.3. Traceability

The following events are logged:

- Access, start-up and shutdown, crashes, errors, changes
- Changes to private keys
- Physical access to the infrastructure
- Changes to this document

Each event is time stamped and the person or process executing is specified.
The log data is transferred to a central log server and protected against access, deletion and manipulation.

9.4. 9.4 Archiving

fidentity archives legally required identification data for the legally required time:

- Swiss (ZertES) compliant QES: at least 11 years
- EU (EIDAS) compliant QES: at least 35 years

fidentity employs suitable measures to ensure that the data can neither be read or copied unauthorized, nor altered or deleted.

9.5. Compromise and disaster recovery

fidentity implements comprehensive and effective procedures for the detection and treatment of incidents and weaknesses.

The service is only resumed after a disaster, if security is ensured.

9.6. Service Termination

When the identification and signing services are terminated, the following measures are taken:

1. notification to the TSP (Swisscom) at least 30 days before business termination
2. transfer of the archived identification data to Swisscom
3. client organizations are immediately informed about the cessation of business
4. a notice of cessation of business is published on the website

9.7. Activation data

Activation data for signatures, the private keys of the subscribers remain within the Swisscom trust centers. The subscriber authorizes the use of his private key via the activation data, i.e. identification session information and eMRTD validation. Activation data meets the requirements of Sole Control Assurance Level 2.

9.8. IT Security controls

fidentity performs several types of security controls:

1. Ongoing external penetration testing to detect weak spots in its defense against unknown or novel attacks.
2. Yearly penetration-testing to scan the entirety of the service for well-known weaknesses.
3. A defined change process supported by software that ensures full transparency and testing of changes.
4. Ongoing automated and manual testing of changes
5. Code quality metrics

In addition, the following security measures are implemented:

- Restrictive access control
- User authentication and authorization is based on the "need-to-know" and "need-to-do" principles
- Perimeter protection: virus protection, use of firewall cascades and Web Application Firewall (WAF).
- Use of current software releases and timely installation of security-relevant software updates only after testing on a staging system

Security management covers the following aspects:

- Annual audits (compliance audit by an accredited conformity assessment body)
- Regular evaluation and development of the security concept (annually)

fidentity is composed of microservices that are separated into separate sub-networks and protected by a multi-layered firewall and WAF.

10. Compliance

Federal Act on Certification Services in the Field of Electronic Signatures and Other Applications of Digital Certificates (Federal Act on the Electronic Signature, [ZertES]), as of 1 January 2017

Regulation (EU) No 910/2014 on electronic identification and trust services for electronic
transactions in the internal market and repealing directive 1999/93/EC [eIDAS-VO], in the
version of 29.01.2015

Austrian Federal Law on electronic signatures and trust services for electronic transactions
(Signature- and Trust Services Law - [SVG]) as of 01.07.2016

Austrian Ordinance on electronic signatures and trust services for electronic transactions
(Signature- and Trust Services Ordinance - [SVV]) as of 02.08.2016

ETSI TS 119 461 V1.1.1 (2021-07) "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects"

Compliance with these requirements has been audited and certified by KPMG as a conformity assessment body.

The conformity assessment body reviews fidentity regularly as well as after any security-relevant changes to this document.

Swisscom holds liability insurance with coverage that is sufficient for the purposes of [VZertES].
Swisscom ITSF holds liability insurance with cover that is sufficient for the purposes of [eIDAS-VO].

11. Dispute

Complaints shall be direct to info@fidentity.ch.
The parties will endeavor to find an amicable solution.
Unless legally required otherwise, the place of jurisdiction is Bern.