DeepCloud
Trust Service Practice Statement

Version: 1.4
Date: 20.03.2024

DEEPCLOUD AG
Wittenbach
Classification level:
C1 - Public

DOCUMENT CONTROL SECTION

Date	Version	Status (draft/to be reviewed)	Author	Description
24.11.2022	0.1	draft	Markus Ilg / Florian Geldmacher	Initial Version
29.11.2022	0.2	To be reviewed	Florian Geldmacher	Incorporated review feedback
16.12.2022	0.3	To be reviewed	Florian Geldmacher	Add notification to participants Use cases of TSP Minor amendments
13.01.2023	1.0	To be approved	Florian Geldmacher	Add repository location for documentation Adapt overview section Adapt to CISO review
27.03.2023	1.1	To be approved	Florian Geldmacher	Add data retention
22.05.2023	1.2	To be approved	Florian Geldmacher	Add Hoop Corporate Services AG, Abacus Research AG and Swisscom AG as providers
07.07.2023	1.3	To be approved	Florian Geldmacher	Adapt location in 5.1.1
17.11.2023	1.4	To be reviewed	Florian Geldmacher	Add fully automated process description in 3.2.1

APPROVAL SECTION

Date	1st Approval by	2nd Approval by	Version
17.1.2023	Tom Roorda	Claudio Hintermann	1.0
28.03.2023	Tom Roorda	Claudio Hintermann	1.1
30.05.2023	Tom Roorda	Claudio Hintermann	1.2
07.07.2023	Tom Roorda	Claudio Hintermann	1.3
20.03.2024	Tom Roorda	Claudio Hintermann	1.4

Qualified Electronic Signature · EU (eIDAS)

Tom Roorda
20.03.2024
deepsign

X

Tom Roorda
CISO

Qualified Electronic Signature · EU (eIDAS)

Claudio Hintermann
20.03.2024
deepsign

X

Claudio Hintermann
CEO

TABLE OF CONTENTS

1. INTRODUCTION

This document sets out the Trust Service Practice Statement (TSPS) for DeepID as identity proofing and signature authorization system and DeepSign as electronic signature service of DeepCloud AG (hereinafter “DeepCloud”).

DeepCloud operates as a TSP in the role of registration authority partner for the identification of natural persons.

Identified persons can receive advanced and qualified signatures as well as qualified time-stamps based on certificates issued by Swisscom. [9.1]

The structure of this document is based on RFC7382. Subsections not applicable to the purpose of this service have the statement “not applicable”. If the sections are omitted, the whole section does not apply to the purpose of this service.

1.1. OVERVIEW

This TSPS describes:

- Participants
- Facility management (physical security, personnel, audit, etc.)
- Audit procedures
- Business and legal issues

This TSPS is applicable to all persons, including, without limitation, all Subjects, Subscribers, Relying Parties, Registration Authorities and any other persons that have a relationship with DeepCloud with respect to certificates of which the identity is proven or authenticated by this service. This TSPS also provides statements of the rights and obligations of DeepCloud, authorized Registration Authorities, Subjects, Subscribers, Relying Parties, and any other person, or organisation that may rely on proven identities by this service for certificates.

DeepCloud`s TSPS describes DeepCloud practices of providing the identity and registration process used for Qualified Trust Services in conformity with the Swiss Federal law ZertES, ETSI EN 319 401 and other related service-based standard requirements. The offered services are non-discriminatory.

1.2. DOCUMENT NAME AND IDENTIFICATION

The name of this document is "DeepCloud TSPS - Trust Services Practice Statement” as indicated on the cover page of this document.
This document and its versions are published at https://www.deepcloud.swiss/registry.

1.3. PARTICIPANTS

DeepCloud acts as a RA delegate for Swisscom (CA authority) for performing registration tasks and conforms to the obligations stated in the Swisscom RA delegation contract.
The subject of this contract is the delegation of the identification activity of the CA authority to DeepCloud within the meaning of the ZertES and other signature regulations.

1.4. CERTIFICATE USAGE

The usage of the certificates is described within the CPS of Swisscom, see [9.1].

1.5. Policy Administration

1.5.1. Organisation Administering the Document

This Trust Service Practice Statement is administered by DeepCloud.

DeepCloud AG

Abacus-Platz 1
9300 Wittenbach – St. Gallen
Schweiz
Tel: +41 58 854 14 14
Mail: info@deepcloud.swiss
Web: https://www.deepcloud.swiss/

1.5.2. Contact

DeepCloud AG

Abacus-Platz 1
9300 Wittenbach – St. Gallen
Schweiz
Tel: +41 58 854 14 14
Mail: info@deepcloud.swiss
Web: https://www.deepcloud.swiss/

1.5.3. Person Determining TSPS Suitability for the Policy

The Management Board of DeepCloud AG determines the suitability of this TSPS document.

1.5.4. TSPS Approval Procedures

This TSPS document and its related documentation are regularly reviewed by the CISO and approved by the CEO of DeepCloud. Following the approval by the CEO of DeepCloud, the TSPS and its relevant documentation are published as stated in clause [2.2] of this TSPS and communicated to employees of DeepCloud and external partners as relevant.

1.6. Definitions and Acronyms

In this TSPS, the service-related certificate policies, and the certification practice statements the following terms and acronyms with the described meaning/definition are being used:

Term	Acronym	Description
Advanced Electronic Signature	AES	A digital signature that can be associated with the owner and enables his identification. It is created using means that are under the sole control of the owner and makes any modification of the associated set of data obvious.
Algorithm		A process for completing a task. An encryption algorithm is merely the process, usually mathematical, to encrypt and decrypt messages.

Attribute		Information bound to an entity that specifies a characteristic of that entity, such as a group membership or a role, or other information associated with that entity.
Certificate		Information issued by a trusted third party, often published in a directory with public access. The certificate contains at least a subject, a public key, a unique serial number, an issuer and a validity period.
Certificate Authority	CA	An entity or trusted third party that issues, signs, revokes, and manages digital certificates.
Certification Practice Statement	CPS	Document that describes the implemented practices of the CA when providing the trust service.
Digital signature		A system allowing individuals and organisations to electronically certify features such as their identity or the authenticity of an electronic document.
eIDAS		European ordinance on “electronic Identification, Authentication and trust Services” or “REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC”. Compliance with the trust services part implies compliance with the following standards: ETSI EN 319 401, 319 411-1, 319 411-2
Electronic Signature		Digital Signature
General Terms and Conditions	GT & C	AB DeepID (General Terms and Conditions for DeepID)
International Civil Aviation Organization	ICAO	The **I**nternational **C**ivil **A**viation **O**rganization is a specialized agency of the United Nations that coordinates the principles and techniques of international air navigation, and fosters the planning and development of international air transport to ensure safe and orderly growth
Machine Readable Zone	MRZ	Machine Readable Zone on passport and ID documents, containing structured data which is represented by the document itself.
Qualified Certificate	QC	Certificate which meets the requirements of ETSI EN 319 411-1/2 and article 8 ZertES.
Qualified	QES	Qualified electronic signature means an advanced electronic signature that is

Electronic Signature		created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures, as defined in article 3 (12) of eIDAS and in ZertES article 2 e.
Registration Authority	RA	A registration authority verifies the identity of entities requesting their digital certificates and approves the CSR to the Certificate Authority (CA) to issue the leaf-certificate.
Relying Party		Individuals or organizations that use certificates of this CA to validate the signatures and verify the identity of Subscribers and/or to secure communication with these Subscribers. Relying Parties are allowed to use such certificates only in accordance with the terms and conditions set forth in the CP, CPS and this TSPS. It is in the sole responsibility of the Relying Party to verify revocation status, legal validity, transaction limits and applicable policies.
Revocation		Withdrawing the certificate status of a certificate.
Signature		Cryptographic element that is used to identify and authenticate the originator of the document and to verify the integrity of the document.
Subject		Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
Subscriber		Legal or natural person bound by agreement with a trust service provider to any subscriber obligations.
TAV-BAKOM		Amendment to VZertES, technical and administrative directives on the issuance of digital signatures, issued November 23, 2016. SR 943.032
Time-stamping Authority	TSA	Authority which issues time-stamp tokens.
Trust Service Provider	TSP	An organization that issues digital certificates and/or provides other signature and certification services.
Trust Services Pactive Statement	TSPS	This document: Statement of the practices that a TSP employs in providing a trust service.
Two-Factor Authentication	2FA	Two-factor authentication (also known as 2-Step Verification) is a method of confirming a user's claimed identity by utilizing a combination of two different components.
VZertES		Swiss ordinance for digital signatures, issued November 23, 2016. SR 943.032.
ZertES		Swiss Digital Signature Law. Issued March 18, 2016. SR 943.03. Compliance with this law always implies adherence to VZertES and TAV-BAKOM.

2. Publication and Repository Responsibilities

The TSP (DeepCloud) makes its certificates, TSPS, service-based Policy and/or Practice Statement, Subscriber Agreement with terms and conditions and related documents for this service publicly available.

2.1. Repositories

The TSP publishes all current documentation on https://www.deepcloud.swiss/registry (available 24h a day / 7 days a week).

2.2. Publication of Certification Information

The DeepCloud TSPS is reviewed at least once a year. A new version will be published in case of relevant changes for the following documents:

- Trust Service Practice Statement
- General Terms and Conditions (T&C)

The DeepCloud executive board can decide to amend this TSPS and respective amendments without notification for amendments that are non-material (i.e. with little or no impact).

Changes with material impact will be first submitted to the Audit Body to obtain the required approval, if applicable, and will be announced afterwards. DeepCloud will use the e-mail-address provided upon registration or make a notification available in the DeepID App to inform the applicant about a new version of the TSPS in case the validity period of the identification has not yet expired. Other participants will be notified using email or web page.

The DeepCloud executive board, at its sole discretion, decides whether amendments have any impact on the Subscriber and/or Relying Parties. All changes to the TSPS will be published after approval.

DeepCloud reserves the right to publish newer versions of the documentation without prior notice.

2.3. Time or Frequency of Publication

Refer to clause [2.2] above.

Information on certification status is published in accordance with the relevant service-based Policies and Practice Statements.

2.4. Access Controls on Repositories

This TSPS is provided as public information on the *deepcloud.swiss* web site. Management access requires a privileged account.

3. Identification and Authentication

3.1. Naming

The naming for the issued certificates follows the rules given by Swisscom (RA delegation).

3.2. Initial Identity Validation

The following is a high-level description of the identity proofing process in place at DeepCloud. Abacus owns the technology (former Yapeal ident SW) and DeepCloud is the licensee of the

technology/SW, which works according to the ETSI-Standard TS 119 461 V1.1.1 (2021-07).

Identity proofing is the process of proving with the required degree of reliability that the purported identity of an applicant is correct. It consists of several steps.

The process validates and evaluates evidence items and depending on the score either automatically identifies individuals or triggers a manual verification step by a DeepID agent.

First, the acceptable ID documents are determined based on the applicant's domicile and nationality from the ID documents catalogue. It contains descriptions and properties of the various attributes that can be extracted from identity documents and are stored as metadata in the document repository. Supported are all ordinary passports based on ICAO standard and identity cards from most European countries.

According to ETSI Standard TS 119 461, the entire identity proofing process consists of five steps as will be described next.

Initiation - during this step the kind of event triggering the process is being determined: Spontaneous, upon invitation, re-identification after loss of mobile, re-new to handle changes of personal data, and upgrade.

Attribute and Evidence Collection — The unattended remote Identification of natural persons is the main use case supported by the system. This step embraces a number of activities including scanning the ID document (including MRZ), reading the NFC chip, taking 3D selfie, matching person with information on ID document, completing ID document and personal details, email verification, collecting phone number, setting memorable photo for additional security, etc.

Attribute and Evidence Validation — During this part of the process the collected attributes are validated against the requirements as stated in ETSI TS 119 461. The gathered evidence is extensively analysed based on the information in the Identity Document Catalogue and using sophisticated image processing algorithms. After face matching with a 3D selfie a document authenticity scoring is calculated.

Binding the Applicant — During this processing step the presented document and the applicant are matched according to the requirements defined by the ETSI Standard. A liveness test with a challenge/response video is used to exclude fake photos.

In the last step — **Issuing of the Identity Proofing** result — the applicant’s device is enrolled using technology from Futurae after successful identification. Thereafter, the applicant's identity can be accessed and used in any context using DeepID as identification.

The entire process is highly automated under the monitoring of specialized DeepID agents who resolve identified issues and control manual additions made by the applicant.

3.2.1. Identification of Individual Participant

For all applications, the following requirements apply:

1. The applicant must present a valid passport or identity card, following the ICAO machine readable travel documents standard and belonging to the documents catalogue [9.1].
2. The applicant must have a legal age, see GT&C [9.1].
3. The presented documents must be valid at the time of the identification and registration.
4. The email address is checked to be existing and correct. The device is registered as legitimate authentication means for later adjustments of the user data and as a method for the release of remote signatures of DeepCloud services.

The applicant confirms his acknowledgement of the privacy policy and the acceptance of the DeepCloud GT&C.

For applications where the identification is used for signing with advanced signatures (AES) or qualified signatures (QES), the following additional requirements apply:

1. Qualifying documents
    a. Only documents which are allowed to cross borders into Switzerland are accepted for AES or QES according to ZertES.
    b. All global passports and ID cards issued in the EU/EEA are accepted for AES or QES according to eIDAS.
2. The document must be valid at the time of a signature request
3. The applicant's domicile must be within the EU, the EEA or Switzerland.
4. The applicant's identity must either
    a. be manually verified and accepted by a DeepID agent.
    b. Or be verified automatically in case of supported documents with NFC chip by
        i. availability of full name details on NFC chip
        ii. passing the identification process with a high degree of certainty of identity.
        iii. validating and matching data on the NFC chip with collected data.
        iv. verifying the integrity of the NFC chip.
5. The registration and the use of the device, used as registration means, must be carried out using a procedure corresponding to SCAL2 as described in [DIN EN 419 241-1:2018].

The proof of identity and the consent to the Terms and Conditions of Usage are archived according to the information in GT&C.
Applications for personal identification may only be made for oneself (no representation).

3.2.2. Authentication of Organization Identity

Not applicable

3.2.3. Authentication of Individual Identity

The authentication for the use of the identity validated through DeepCloud is done through Futurae [9.1] strong authentication, implemented in the DeepID application.

3.2.4. Non-verified Subscriber Information

Not applicable

3.2.5. Validation of Authority

Not applicable

3.2.6. Criteria for Interoperation

Not applicable

3.3. Identification and Authentication for Re-Identity Requests

The re-identity proofing request follows the process described in [3.2].
A re-identification for AES/QES is mandatory at least in the following scenarios

- The last identification took place more than 5 years ago
- The document used for identification is expired

3.4. Identification and Authentication for Revocation Request

Not applicable

4. Certificate Life Cycle Operational Requirements (OMITTED)

DeepCloud requests one certificate specific to the document to be signed from Swisscom AIS for each signing request. See [9.1]

5. Facility, Management, and Operational Controls

For the rendering of its services, DeepCloud relies on a number of external partners. They provide services in their respective areas of expertise as follows:

- Google Cloud EMEA Ltd.:
  The cloud infrastructure (including computing, storage, DB, Virtual Network) for the identification service has been outsourced to Google Cloud Services. Three completely separated environments are available for development, testing, and production with their own NAT Network, infrastructure, and own entitlements each. Google has been certified concerning information security and data protection multiple times.
- Futurae Technologies AG:
  Authentication
- YAPEAL AG:
  SW development, IT Operations, Support provider
- Abacus Research AG:
  SW development, IT Operations, Support provider
- Hoop Corporate Services AG
  Support provider
- Swisscom AG
  Trust Service Provider for certificates / signatures

DeepCloud retains the overall responsibility for conformance with the procedures described in the Information Security Policy even if the TSP's functionality is delivered by outsourcing partners. DeepCloud defines the outsourcers' liability and ensures that outsourcers are bound to implement any controls required by DeepCloud. DeepCloud has documented agreements and contracts with its subcontractors and outsourcing partners providing services to ensure that they are bound to implement any requirements and controls required by DeepCloud.

In the field of security management, DeepCloud guides itself by the generally recognised standards, e.g. ISO 27001.

DeepCloud carries out a regular risk assessment to identify, analyse and evaluate risks taking into account business and technical issues as well. Based on the risk assessment results, corresponding appropriate risk treatment measures commensurate to the degree of risk are selected and the necessary procedures are determined and documented regarding the implementation of these risk treatment measures in accordance with DeepCloud's Information Security Policy as well as this TSPS. A residual risk analysis is carried out and documented as well in which the residual risk is identified and, where appropriate, accepted. The risk assessment is carried out at least annually, based on the requirements of the ISO 27001 standard and released by DeepCloud management body.

DeepCloud management is responsible for defining, implementing and maintaining the Information Security Policy, which forms a basis for consistency and completeness of information security and management support.

The Information Security policy is reviewed annually or if significant changes occur, to ensure the continuing suitability, adequacy and effectiveness. DeepCloud Chief Information Security Officer approves policies and practices related to information security for the overall DeepCloud services. DeepCloud management communicates information security policies and procedures to employees and relevant external parties who are impacted by it.

DeepCloud has defined a detailed inventory of assets and has assigned a classification consistent with the risk assessment, which is reviewed regularly at planned intervals or if significant changes occur to ensure the continuing suitability, adequacy and effectiveness. The configurations of the TSPs systems are also regularly checked for changes which violate the TSP's security policies to ensure an appropriate level of protection of all assets including information assets. Controls are implemented to avoid loss, damage or compromise of assets or information and interruption to business activities.

5.1. Physical Controls

The physical controls, other than the DeepID agents' office locations, are implemented by the respective service providers.

5.1.1. Site Location and Construction

The DeepID agents are located in Switzerland (DeepCloud AG, Abacus Research AG, Yapeal AG and Hoop Corporate Services SA) and in dedicated cases in Italy (Hoop Corporate Services SA) or in a country with an adequate level of data protection. The requirements of ETSI EN 319 401 are fulfilled.

Server sites are handled by the respective providers, described in [5].

5.1.2. Physical Access

Handled by the respective providers, described in [5].

5.1.3. Power and Air Conditioning

Handled by the respective providers, described in [5].

5.1.4. Water Exposures

Handled by the respective providers, described in [5].

5.1.5. Fire Prevention and Protection

Handled by the respective providers, described in [5].

5.1.6. Media Storage

Handled by the respective providers, described in [5].

5.1.7. Waste Disposal

Handled by the respective providers, described in [5].

5.1.8. Off-Site Backup

Handled by the respective providers, described in [5].

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles must be taken over by persons who are subject to regular review. Such persons may be DeepCloud employees or contractors. They have access to the systems of the DeepCloud services and carry out identity checks which can have a significant effect on:

- Validation of information in identity verifying applications.
- The acceptance, rejection or other processing of identity verifying applications.
- The handling of the information or inquiries of the identity verifying applicant.
- Changes of personal data of the applicant (e.g. address, name)

Reliable persons include, but are not limited to:

- Lead DeepID agent
- COO
- DeepID agent
- System administrators
- Engineers
- Information security officer
- Responsible managers
- Auditor

The roles and responsibilities of people in trusted roles are distributed in such a way that a person cannot act alone, thus circumventing security measures and undermining the trustworthiness of DeepCloud's operations. The assignment of trusted roles to persons is reviewed annually.

5.2.2. Number of Persons Required per Task

For tasks being in conflict of interest or need segregation of duty the system enforces appropriate roles or number of persons to fulfil the tasks, respectively.

5.2.3. Identification and Authentication for Each Role

The technical access to the individual IT systems is realized by strong authentication.

5.2.4. Roles Requiring Separation of Duties

The Role Concept [9.1] 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 behaviour. The assignment of these trusted roles to individuals is reviewed annually.

5.3. Personnel Controls

The TSP fulfils the requirements for personnel from ETSI EN 319 401.

5.3.1. Qualifications, Experience, and Clearance Requirements

DeepCloud ensures to employ staff and subcontractors who possess the necessary expertise, reliability, experience, and qualifications to perform a service/job function and support the trustworthiness of the TSP's operations. Additionally, TSP staff and, if applicable, subcontractors, have received training regarding security and personal data protection rules as appropriate for the offered services and job function.

5.3.2. Background Check Procedures

The HR and its system providers verify the background of its employees during the interviewing process.

5.3.3. Training Requirements

The TSP ensures that the persons involved in the identification service have the necessary knowledge, experience, and required skills for their position. The identity, reliability, and professional knowledge of the personnel are checked before the start of work. Regular and event-related training ensure competence in the areas of activity as well as general information security. Training and performance records are documented. Training and tests are conducted using the OpenOlat training platform.

5.3.4. Retraining Frequency and Requirements

Retraining of employees is done as necessity arises, depending on the needs of the organisation or the needs of the individual, but at least once a year including updates on new threats and current security practices.

5.3.5. Job Rotation Frequency and Sequence

Job rotation of employees is done as necessity arises, depending on the needs of the organization, or by request of an individual employee. Role changes are documented.

5.3.6. Sanctions for Unauthorised Actions

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

5.3.7. Independent Contractor Requirements

Above and beyond regular documentation, contractors that are candidates for an Access, Operations or Audit role must provide proof of their qualifications in the same manner as internal personnel (see clause 5.3.1).

5.3.8. Documentation Supplied to Personnel

DeepCloud employees have access to course material, operating documents and procedural instructions on the DeepCloud Intranet and the Abacus internal training platform OpenOlat.

5.4. Audit Logging Procedures

Audit logging is provided on several levels for infrastructure and service.

5.4.1. Types of Events Recorded

The following events are logged:

- Server-related events such as access attempts, system start-up and shutdown, system crashes, hardware errors, and software and configuration changes.
- Access to the server rooms, technical alarms and intrusion alarms.
- Changes within application data.

Each logged event is time stamped and the person or process executing is specified.

5.4.2. Frequency of Processing Log

Audit logs are processed automatically and continuously.

5.4.3. Retention Period for Audit Log

Audit logs are retained according to the purpose of the log data. In detail, the retention periods are described in the retention policy.

Application audit data is retained according to the respective requirements defined within the RA delegation contract, which stipulates a retention period in connection with

- ZerteES/eIDAS FES of at least 13 years
- ZertES QES of at least 17 years
- eIDAS QES of at least 36 years

5.4.4. Protection of Audit Log

Audit log data can only be accessed by the specialized internal auditors. System logs can be accessed by system operators and auditors.

5.4.5. Audit Log Backup Procedures

Backups are handled by the respective providers, described in [5].

5.4.6. Audit Collection System (Internal vs. External)

Audit collections are handled by the respective providers, described in [5].

5.4.7. Notification to Event-Causing Subject

Notifications are handled by the respective providers described in [5].

5.4.8. Vulnerability Assessments

Vulnerability assessments are handled by the respective providers, described in [5].

5.5. Records Archival

5.5.1. Types of records archived

All data relevant to the identification process are archived.

5.5.2. Retention Policy

DeepCloud has a retention policy in place - inclusive handling the storage and archival of information (e.g. personal data, audit logs) in regards as its role as Trusted Service Provider:
In principle, such information is retained as long as there is a retention obligation for it or another purpose justifying the retention. This may involve legal or contractual retention obligations. Data regarding a DeepID that is related to an electronic signature is retained at least as long as the respective retention duty.

The following principles apply:

- Information which is no longer needed for a purpose is deleted after the respective retention period. The client can request to delete data which must not be retained anymore or informs DeepCloud to store or archive the information even longer.
- Information which must no longer be retained with regards to the purpose of the processing will be deleted

5.6. Key Changeover

Not applicable

5.7. Compromise and Disaster Recovery

Service recoveries are handled by the respective providers, described in [5].

5.8. RA Termination

When the RA services are terminated, the following measures are taken:

1. Notification without (undue) delay to Swisscom, the supervisory body and the conformity assessment body.
2. Preparation of logs and evidences used for identity proof of the subscribers to
    a. archive for further investigation after cessation of the business
    b. transfer to Swisscom.
3. The subscribers are informed about the cessation of the business as well as of the revocation, transfer or continuation.

6. Technical Security Controls

This section describes the security controls used by DeepCloud.

The certificates used for signing are only requested at signing time for the specific document. The certificates cannot be used for batch signatures.
Technical Security Controls are handled by the respective providers, described in Facility, Management, and Operational Controls.

6.1. Key Pair Generation and Installation

Not applicable

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Not applicable

6.3. Other Aspects of Key Pair Management

Not applicable

6.4. Activation Data

Not applicable

6.5. Computer Security Controls

Access to the DeepCloud service components is subject to a risk analysis and their risk potential is protected accordingly.

The following security measures are implemented:

- Strong user authentication (2FA / Futurae)
- Role-based user authorization
- Use of current software releases and timely installation of security-relevant software updates.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Software (proprietary or third-party) can only be used once it has been accepted, tested and released.

6.6.2. Security Management Controls

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)
- Checking the security during operation (see also chapter [5.4])
- Logging of all security related operations
- Implementation of upgrades and patches
- Implementation of upgrades or patches on a productive system only after release on a test system.

6.6.3. Life Cycle Security Controls

Life Cycle Security Controls are handled by the respective providers, described in [5].

6.7. Network Security Controls

The network infrastructures used for services of DeepCloud are handled by the suppliers [5]. All traffic is authenticated and encrypted.
The network is separated into environments to best segregate operational aspects like management versus operation, development versus production.
The networks are constantly monitored, and critical incidents are immediately pursued by the respective on-call organisation.

6.8. Time-Stamping

Clock synchronisation is guaranteed using the NTP protocol of the respective provider [5] for all systems in DeepCloud's infrastructure.

7. Certificate and CRL Profiles

Not applicable

8. Compliance Audit and Other Assessments

The services, processes, and security controls are based on the following laws and regulations:

- These TSPS and associated documents such as the security concept, the [role concept], etc.
- 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 January 1, 2017
- Regulation on certification services in the field of electronic signatures and other applications of digital certificates (Regulation on electronic signatures, [VZertES]), as of January 1, 2017
- Technical and administrative regulations on certification services in the field of electronic signatures and other digital certificate applications ([TAV]), as of January 1, 2017
- ETSI TS 119 461 V1.1.1 (2021-07) Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [ETSI EN 319 401] (2018-04)

- DIN EN 419 241:2018: Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements (SCAL1 und SCAL2)

Compliance with the requirements set out in this chapter has been audited and certified by KPMG as a conformity assessment body within the framework of the conformity assessment of DeepCloud as a certified Trust Service Provider.

The conformity assessment body reviews DeepCloud regularly as well as after any security-relevant changes to the TSPS.

The areas affected by an audit shall be defined by the responsible conformity assessment body. For risks that necessarily require a review, certain areas can be identified in advance.

Any deficiencies identified are rectified in consultation with the conformity assessment body and DeepCloud or the audited registration authority.

9. Other Business and Legal Matters

9.1. References

- CSP Swisscom “Diamant” “Saphir”) https://w3.swissdigicert.ch/CP_CPS_Diamant_Saphir_2_16_756_1_83_en.pdf
- Information Security Policy https://www.deepcloud.swiss/legal/Information_Security_Policy_EN.pdf
- Privacy Policy https://www.deepcloud.swiss/de/datenschutz/
- AB DeepID (General Terms and Conditions for DeepID)
- https://www.deepcloud.swiss/registry
  - Documents Catalogue
  - TSPS
- Role Concept [internal]
- Yapeal https://yapeal.ch/
- Futurae https://www.futurae.com/
- ICAO – Machine readable travel documents https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf

9.1.1. Yapeal

Yapeal AG which is FINMA regulated operates the DeepCloud infrastructure used for identity proofing in partial fulfilment of the licence for TSP.

9.2. Fees

Identification process DeepID is free of charge.
Fees for other DeepCloud services are published on the *deepcloud.swiss* webpage.

9.3. Financial Responsibility

DeepCloud holds liability insurance with coverage that is sufficient for the purposes of ZertES and VZertES.

9.4. Confidentiality of Business Information

Information collected during the registration process is regarded as confidential information.

DeepCloud is responsible for taking measures to uphold the confidential status of information. The data may

only be processed in connection with the provision of the service and may only be passed on to third parties who have been contractually obliged to maintain confidentiality.
Documents may be viewed for auditing and control purposes in the presence of the Information Security Officer or Information Security Manager of DeepCloud.

9.5. Privacy of Personal Information

DeepCloud processes (including collection, storing and deletion) data only to deliver its services for the identification process. DeepCloud and its providers process data on systems located in Switzerland.

DeepCloud follows these principles:

- Personal data may only be collected lawfully.
- Personal data may only be processed in good faith and processing must be proportionate.
- Personal data may only be processed for the purpose indicated when the data were acquired, that is apparent from the circumstances, the privacy policy, GT&C or that is specified by law.

Duties of disclosure and cooperation of DeepCloud towards courts and other authorities are regulated by contractual duties and the law and will not be affected by the terms of this TSPS. DeepCloud is in particular required to hand over data concerning the identity process to Swisscom and other authorities in accordance with contractual duties and applicable legislation.

9.6. Intellectual Property Rights

9.6.1. DeepCloud

DeepCloud holds copyright over the AB DeepID (GT&C DeepID) [9.1].

9.6.2. Certification

DeepCloud verifies that the use of certification documents, certificates and conformity designations are in accordance with the general terms and conditions of the certification bodies and respects the intellectual property rights therein.
This also includes an annual verification that these certification marks are not used illegally by DeepCloud. The COO and the Legal Counsel are responsible for this annual review.

9.7. Representations and Warranties

DeepCloud warrants to comply with the requirements stipulated in the RA delegation contract with Swisscom.
Further warranties are regulated in the relevant contracts concluded with DeepCloud.

9.8. Disclaimers of Warranties

Disclaimers of warranties for the services of DeepCloud towards an applicant are regulated in the GT&C DeepID accepted by the applicant while using the identification service.

9.9. Liability and Limitations of Liability

DeepCloud`s liability and limitations of its liability is determined in accordance with contractual agreements like the RA delegation contract with Swisscom and the GT&C DeepID with the applicant (Chapter 14).

9.10. Indemnities

Not applicable

9.11. Term and Termination

DeepCloud is entitled to terminate the relationship with the applicant at any time without giving reasons. The applicant can stop using DeepID at any time and delete the DeepID app from his means of authentication. Details of the termination and its effects are determined in the GT&C DeepID (Chapter 16).

9.12. Amendments

Any amendments to this TSPS will be announced in consultation with the conformity assessment body.

9.13. Resolution of Disputes

In the event of any dispute the participants will endeavour to resolve the dispute amicably.

9.14. Governing Law

All legal relations pertaining to the services of DeepCloud falling under this TSPS will be governed by the relevant provision set forth in the RA delegation contract with Swisscom and the GT&C DeepID with the applicant. If there are no special provisions in such contracts, the following applies:
All legal relationships in connection with the GT&C DeepID shall be governed by Swiss law, to the exclusion of international private law and the Vienna Sales Convention, irrespective of whether an applicant uses DeepID in his capacity as a consumer or for business reasons. If the applicant is a consumer habitually resident in the EU/EEA, the mandatory consumer protection law of the EU/EEA state in which the applicant is habitually resident in the EU/EEA shall otherwise apply in addition.

Subject to mandatory places of jurisdiction, the city of St. Gallen shall be the exclusive place of jurisdiction for all disputes arising from or in connection with the GT&C DeepID.

9.15. Compliance with Applicable Law

All participants will comply with the laws and regulations applicable to them.