WebID Solutions GmbH

Trust Service Practice Statement

Version 1.3
Date: 29.8.2019

Document History

Version	Date	Changes
1.0	21.09.2017	Initial version
1.1	02.01.2019	Minor changes and annual review
1.2	29.04.2019	Minor additions and refinement
1.3	29.08.2019	Changes and amendments in Chapters 1; 1.1; 1.3.5; 1.5.4; 2.3, 3.2.3; 5.1.8; 5.2.1; 5.5.2; 5.2.4; 5.4.1; 5.5.2; 5.7.1; 6.2; 6.5; 6.5.1; 6.6.1; 6.6.2; 6.6.4; 9.12.2 to address further ETSI EN 319-401 requirements

CONTENT

1 Introduction

WebID Solutions GmbH is a trust service provider offering online services for identity verification of persons in order to support WebID Solution's partners needing reliable identification of their customers.

In addition, in collaboration with certification service providers and contract partners WebID Solutions enables individual customers of the contract partners to electronically sign legally binding contracts using qualified electronic signatures according to the eIDAS regulation.

The identity verification services are compliant with the requirements of the German "Geldwäschegesetz" (prevention of money laundering act) and the Regulation 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 (eIDAS).

In particular, WebID Solutions verifies the identity of natural persons in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" recognized in Germany which provide equivalent assurance in terms of reliability to physical presence.

This document is the Trust Service Practice Statement (TSPS) of WebID Solutions GmbH. It is not a full Certification Practice Statement (CPS) according to RFC 3647 because WebID Solutions only provides identity verification services, but does not offer other certification services like issuing certificates or the provision of certificate validation services.

The purpose of this document is to serve as a base for compliance with eIDAS.

1.1 Overview

The services of WebID Solutions allow customers of contract partners to be reliably identified using online video conferencing for identification while the customer is at home or at his/her workplace. WebID Solutions delivers the results of identity verifications in electronic form to its contract partners and/or to certification service providers for the issuance of qualified electronic certificates. The qualified certificates may then be used to sign legally binding electronic contracts.

WebID Solutions offers its services to all customers of its contract partners without discrimination.

While the services cannot be provided for people with mutism and deafness, the service provided is accessible for persons with disabilities and can be used without any restrictions by persons with other disabilities.

The services of WebID Solutions conform to the German Geldwäschegesetz (prevention of money laundering act) and the eIDAS regulation on electronic identification and trust services.

The services of WebID Solutions have been assessed for compliance with the requirements of eIDAS according to the standards ETSI EN 319 401, ETSI EN 319 411-1, and ETSI EN 319 411-2 and the compliance with the requirements of eIDAS has been confirmed by an independent assessment body.

The video identification services offered by WebID Solutions can be used by TSPs for the issuance of QCP-n, QCP-n-qscd, QCP-l, and QCP-l-qscd certificates. For QCP-l and QCP-l-

qscd WebID can only identify the natural person representing the organization, the organization itself must be identified by the TSP.

The video identification is performed by trained and experienced identity verification specialists according to legally admitted procedures. The video conference replaces the personal (physical) presence of the person to be identified.

1.2 Document Name and Identification

This document is the “Trust Service Practice Statement of the WebID Solutions GmbH.

Name of the document	WebID Solutions GmbH – Trust Service Practice Statement
Version	1.33, 29.08.2019

1.3 PKI Participants

1.3.1 Certification Authorities

A Certification Authority (CA) is an entity authorized to issue public key certificates. A CA is also responsible for the distribution, publication, and revocation of certificates.

WebID Solutions does not operate a CA but offers identification services on behalf of CAs.

1.3.2 Registration Authorities

A Registration Authority (RA) acts on behalf of a CA. RAs are responsible for verifying both business information and personal data contained in a subscriber’s certificate.

An RA submits certificate requests to issuing CAs, approves applications for certificates, renewal, or re-keying, and handles revocation requests.

WebID Solutions does not operate an RA but offers identification services on behalf of a CAs RA.

1.3.3 Subscribers

Subscribers are the end-entities of certificates issued by a CA. Subscribers are individual persons.

WebID Solutions identifies the subscribers on behalf of contract partners or CAs.

1.3.4 Relying Parties

A Relying Party is an individual or entity that relies on a certificate. A Relying Party uses a Subscriber’s certificate to verify the integrity of a digitally signed document and to identify the signer of the document.

1.3.5 Supplier (Third Parties)

Where the provisioning of services involves subcontracting, outsourcing, or other third party arrangements, WebID Solutions has documented agreements and contractual relationships in place.

WebID Solutions uses a supplier for the operation of the datacenter. It provides managed dedicated servers for storing data. The operator of the external datacenter is obliged to protect the servers in the datacenter against physical and environmental threats and to maintain the security of the servers in the datacenter up to the operating system level.

The datacenter's conformance with the information security policy is ensured through regular audits performed by WebID personnel.

However, WebID Solutions does retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the specific functionality is undertaken by outsourcers.

1.4 Certificate Usage

Not applicable, WebID Solutions provides identity verification services and does not issue certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This TSPS is administered by:

WebID Solutions GmbH
Friedrichstraße 88
10117 Berlin

1.5.2 Contact Person

Compliance Officer
WebID Solutions GmbH
Friedrichstraße 88
10117 Berlin
Phone: +49 30 5557476 50
E-Mail: compliance@webid-solutions.de

1.5.3 Person Determining CPS Suitability for the Policy

WebID Solutions' Compliance Officer determines the suitability of this TSPS with the Policy.

1.5.4 TSPS Approval Procedures

This TSPS document has been prepared for compliance with the requirements of eIDAS on identity verification.

The TSPS document is approved by WebID Solutions' Management Board, published and communicated to all relevant employees and external parties.

The Management Board is also responsible for implementing the practices as specified in this document.

The TSPS and the Terms and Conditions are reviewed in regular intervals. Amendments to these documents must be approved by WebID Solutions' Management Board before becoming effective.

The Terms and Conditions are made available to all subscribers and relying parties through durable means of communication.

1.6 Definitions and Acronyms

1.6.1 Definitions

Not required.

1.6.2 Acronyms

Not required.

1.6.3 References

ETSI EN 319 401	ETSI EN 319 401, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI EN 319 411-1	ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI EN 319 411-2	ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
eIDAS	Regulation 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

2 Publication and Repository Responsibilities

2.1 Repositories

WebID Solutions publishes this TSPS and other relevant documents like General Terms and Conditions (AGB) and the Data Protection Statement on its website www.webid-solutions.de.

2.2 Publication of Certificate Information

Not applicable. WebID Solutions does not issue certificates.

2.3 Time or Frequency of Publication

This TSPS and any subsequent amendments are immediately made publicly available after approval.

The websites of WebID Solutions are publicly available 24 hours per day, 7 days per week. Upon system failure or other kind of outages WebID Solutions will restore proper functionality without delay.

2.4 Access Controls on Repositories

The repository is publicly and internationally available. Read only access is unrestricted.

WebID Solutions protects the integrity and authenticity of all documents in the repository. The repository is subject to access control mechanisms to protect its availability and prevent unauthorized persons from adding, deleting, or modifying information in the repository.

3 Identification and Authentication

3.1 Naming

Not applicable. WebID Solutions does not issue certificates.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Not applicable. WebID Solutions does not issue certificates.

3.2.2 Authentication of Organization Entity

Not applicable. WebID Solutions does not issue certificates.

3.2.3 Authentication of Individual Identity

The customer's identity is checked against an official, valid, government-issued photo ID document that fulfills legal and regulatory requirements.

The customer has to be present in a video conference call and screenshots and a voice protocol are recorded as evidence.

The information collected during the identification include at the full name (surname and given name(s)) of the applicant, the date and place of birth, the current address, the type, validity period, issuing authority, and the reference number of the identity document presented. The current address is either part of the data of the ID document (if contained) or is filled out by the customer before the beginning of the identification process.

WebID Solutions also verifies the customer's mobile phone number for authentication purposes when the customer applies for a qualified certificate at a cooperating CA.

All data exchanged electronically with the customer is protected through encryption.

After performing the video identification WebID Solutions transfers the collected identification data to the CA. All data included in this transmission is encrypted and digitally signed.

3.2.4 Non-verified Subscriber Information

Not applicable. WebID Solutions offers only identity validation services.

3.2.5 Validation of Authority

Not applicable. WebID Solutions offers only identity validation services.

WebID Solutions does not validate the customer's authority to apply for a certificate; this must be performed by the CA issuing the certificate.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

Not applicable. WebID Solutions does not issue certificates.

Therefore, WebID Solutions does not differentiate between identifications for initial certificate issuance or re-key requests.

3.4 Identification and Authentication for Revocation Requests

Not applicable. WebID Solutions does not issue certificates and does not handle revocation requests.

4 Certificate Life-Cycle Operational Requirements

Not applicable.

WebID Solutions performs identification services according to chapter 3.2.3. WebID Solutions does not issue certificates, does not process certificate applications, and does not provide certificate status validation services.

5 Facility, Management, and Operational Controls

WebID Solutions carries out regular risk assessments to identify, analyze, and evaluate risks related to its services taking into account business and technical issues.

WebID Solutions then selects appropriate risk treatment measures taking into account the results of the risk assessment.

The risk treatment measures chosen ensure that the level of security is commensurate with the degree of risk.

The risk assessment is approved by WebID Solutions management who accepts the residual risks identified in the risk assessment with this approval.

5.1 Physical Controls

WebID Solutions has implemented a general security policy which supports the security requirements of the services, processes, and procedures covered by this TSPS.

These security mechanisms are commensurate with the level of threat in the identity validation environment.

5.1.1 Site Location and Construction

For redundancy purposes, WebID Solutions operates two facilities at two different locations. Both of them are capable to provide all services required for identity verification.

At both locations the systems of WebID Solutions are located in secure rooms with biometric access control and CCTV surveillance. For data protection reasons the CCTV system is configured in such a way that it does not record the video conferencing screens of the identity validation specialists.

WebID Solutions' servers are located in a secure data center and managed and operated (at the operating system level) by data center staff. WebID Solutions' applications and data are stored encrypted and not accessible for data center personnel.

All operations related to identity verification are conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

Several layers of physical security controls restrict access to the sensitive hardware and software systems used for performing operations. The systems used for identity validation services are physically separated from other systems so that only authorized employees can access them.

5.1.2 Physical Access

WebID Solutions protects its relevant systems, especially database servers and the systems used by the identity validation specialists for video conferencing, with physical security mechanisms to:

- permit no unauthorized access to the hardware;
- store all identity validation data in encrypted form;
- monitor, either manually or electronically, for unauthorized intrusion at all times;
- maintain and periodically inspect an access log.

WebID Solutions has implemented physical access controls to reduce the risk of unauthorized persons being able to access WebID Solution's premises. This includes the workplaces of identity validation specialists as well as database servers, routing and switching components, and firewalls.

Physical access to systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided access. The access control system is always functional and uses biometrics in combination with access chips.

Access to WebID Solutions' premises requires multi-factor authentication with chip and biometrics.

Visitors to WebID's premises cannot enter those without support of authorized employees. All visitors must be identified by their personal ID document, which is to be documented by the WebID personell. In all relevant security areas, visitors must be accompanied by authorized employees.

5.1.3 Power and Air Conditioning

All systems at the location where identity verification takes place and all systems in the secure data center have industry standard power and air conditioning systems to provide a suitable operating environment.

Furthermore, all relevant systems are provided with an uninterruptable power supply sufficient for a short period of operation in the absence of commercial power, to support either a smooth shutdown or to re-establish commercial power.

5.1.4 Water Exposure

All systems have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire Prevention and Protection

All systems have industry standard fire prevention and protection mechanisms in place.

5.1.6 Media Storage

Media is stored in safes to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit data, archive data, or backup information is duplicated and stored securely in a location separate from the main location.

5.1.7 Waste Disposal

Sensitive documents and materials occur only in electronic form. Media used to collect or transmit sensitive information are securely erased before disposal. Paper-based media is disposed according to DIN 66399 category P-5. Other waste is disposed of in accordance with normal waste disposal requirements.

5.1.8 Off-site backup

WebID Solutions performs regular routine backups of critical system data, audit log data, and other sensitive information.

WebID Solutions is not obliged to keep identity verification data for a long period of time because all relevant identity verification data is sent to the CA for the purpose of issuing a qualified certificate immediately after being collected. The CA is then obliged to archive these data according to the regulations made in eIDAS.

The copy of all identity data stored on WebID Solutions' systems can be viewed as secondary backup stored off-site.

5.2 Procedural Controls

5.2.1 Trusted Roles

WebID's management appoints Trusted Roles with job duties considered critical for the trustworthy provision of the Trusted Services. As such all employees that have access to or control video identification data are appointed to Trusted Roles. For the services provided by WebID Solutions these roles are Identity Verification Specialists (or Identity Verification Agents), System Administrators, Security Officers, System Operators, Developers, and Auditors.

5.2.2 Number of Persons Required per Task

No stipulation.

5.2.3 Identification and Authentication for Each Role

Initially, the identity of all personnel in Trusted Roles is verified through personal, physical presence and the check of an official photo ID document. Identity is further confirmed through the background checking procedures in section 5.3.2.

Personnel in Trusted Roles is named and approved by senior management of WebID Solutions before being permitted to access CA relevant systems.

Identification and authentication during operations for each role is based on individual passwords and individual access tokens and PINs.

5.2.4 Roles Requiring Separation of Duties

All personnel performing sensitive operations are assigned a Trusted Role. A segregation of conflicting duties and areas of responsibility is implemented to reduce opportunities for modification and misues to its minimum. Sufficient computer security controls for the separation of identified Trusted Roles, including the separation of security administration and operation functions, are in place. Access Management is designed on a need-to-know basis.

5.3 Personnel Controls

5.3.1 Qualification, Experience, and Clearance Requirements

All employees involved in the operation of WebID Solutions' systems and all Identity Verification Specialists have appropriate knowledge and experience related to their duties. They must have demonstrated security consciousness and awareness regarding their duties and receive appropriate training in organizational policies and procedures.

Employees involved in identity verification services have signed a confidentiality (non-disclosure) agreement as part of their initial terms and conditions of employment.

Managerial personnel possess professional experience with the services provided and are familiar with security procedures for personnel with security responsibilities.

Personnel in trusted roles are held free from conflict of interest that might prejudice the impartiality of operations.

5.3.2 Background Check Procedures

All WebID Solutions' employees involved in identity verification services have must undergo a background check which, at a minimum, covers the following areas:

- Employment;
- Education;
- Place of residence;
- Criminal background check; and
- References (if available).

The extent to which these investigations are performed is restricted by the applicable local legislation.

Criminal background checks consist of presenting a criminal record (Führungszeugnis) according to § 30 Bundeszentralregistergesetz. The checks must be clear of records related to trustworthiness.

Regular periodic reviews are performed to verify the continuous trustworthiness of all personnel.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the WebID Solutions systems and services receives comprehensive training. Training is conducted in the following areas:

- security principles and mechanisms,
- use and operation of identity verification equipment and applications,
- job responsibilities including training about validity and authenticity of ID documents,
- incident handling and reporting especially regarding fraudulent attempts during identifications,
- disaster recovery procedures.

WebID Solutions maintains records of all trainings performed.

5.3.4 Re-Training Frequency and Requirements

Retraining is performed to the extent and frequency required to ensure that the required level of proficiency is maintained.

In addition, the identity verification specialists and other staff are trained appropriately if any significant change to systems or processes occurs.

5.3.5 Job Rotation Frequency and Sequence
No stipulation.

5.3.6 Sanctions for Unauthorized Actions
Appropriate administrative and disciplinary actions are taken in case of unauthorized actions (i.e., not permitted by this TSPS or other policies).

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures.

5.3.7 Independent Contractor Requirements
WebID Solutions has not planned to employ independent contractor personnel to perform identity verifications.

If independent contractors are required to support the regular employees they must fulfill the same requirements as regular employees.

5.3.8 Documentation Supplied to Personnel
This TSPS, applicable system operations documents, operations procedures documents, and any relevant other documents required to perform their jobs shall be made available to WebID Solutions' employees.

5.4 Audit Logging Procedures

5.4.1 Types of Events Logged
WebID Solutions keeps audit trails and system log files that document actions taken as part of the identity verification services. All relevant events related to the services provided are logged.

Log entries include the following elements:

- date and time of the entry
- serial or sequence number of entry, for automatic journal entries
- identity of the entity making the journal entry
- description/kind of entry.

The identity verification logs include:

- kind of identification document presented by the customer,
- record of unique identification data of identification document (e.g. ID document serial number)
- identity of the identity verification specialist performing the identity proofing.

Further, all security events will be logged. Such security events might include changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities, and PKI system access attempts. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism is used.

5.4.2 Frequency of Processing Log
WebID Solutions' system and its components are continuously monitored and can provide real time alerts if unusual security and operational events occur and allow an immediate review by system security administrators.

Quality management measures require regular reviews of the audit logs including verification that the logs have not been tampered with and an investigation of any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log
Records are archived for at least ten years.

5.4.4 Protection of Audit Log
Procedures are implemented to protect archived data and audit data from destruction or modification prior to the end of the audit log retention period. Audit logs are moved to a safe, secure storage location separate from the component which produced the log.

Access to audit logs is restricted to authorized personnel.

5.4.5 Audit Log Backup Procedures
Audit logs are synchronized to a separate location.

5.4.6 Audit Collection System (Internal vs. External)
Audit data is generated and recorded automatically at the application, network, and operating system level.

Where this is not possible audit data is generated manually and recorded by personnel.

5.4.7 Notification to Event-Causing Subject
No stipulation.

5.4.8 Vulnerability Assessments
Based on events in the log files the Security Officer initiates vulnerability assessments.

5.5 Records Archival

5.5.1 Types of Records Archived
At a minimum, WebID Solutions records the following data for archival:

- this TSPS
- contractual obligations
- system and equipment configuration
- modifications and updates to systems or configurations
- all evidences collected during identifications (photos of ID documents and voice recording) including supporting documentation
- audit logs mentioned in section 5.4
- documentation required by compliance auditors.

5.5.2 Retention Period for Archive
All records except for evidences collected during video identifications and supporting information are archived for at least ten years.

Long term archival of evidences collected during video identifications and supporting information, i.e. identification data according to the requirements of eIDAS, is regulated by contractual agreements with the CAs.

Currently the CA is responsible for archival of identification data and contractually agrees with WebID Solutions on a shorter archive period specified in the contractual agreements.

In this case all person related data is deleted from WebID Solutions' systems after the archive period has expired.

5.5.3 Protection of Archive

WebID Solutions protects the archive so that only authorized persons in trusted roles are able to access the archive. The archive is stored in a trustworthy system protecting it against unauthorized viewing, modification, deletion, or other tampering. The media holding the archive data and the applications required to process the archive data is maintained to ensure that the archive data can be accessed for the time period defined above.

5.5.4 Archive Backup Procedures

WebID Solutions performs daily database backups. Full system backups are performed regularly. Once per day an additional backup is written to external media.

5.5.5 Requirements for Time-Stamping of Records

No stipulaton.

5.5.6 Archive Collection System (Internal or External)

The archive collection systems are internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Access to the archive is restricted to personnel in trusted roles.

Information in the archive is verified in regular intervals as described in section 5.4.2.

5.6 Key Changeover

Not applicable. WebID Solutions does not handle CA keys.

5.7 Compromise and Disaster Recovery

WebID Solutions has implemented a disaster recovery and business continuity plan intended to allow restoration of business operations in a reasonably timely manner following interruption to, or failure of, critical business processes.

A secondary location with all equipment required to perform identity verifications is available for emergency and disaster recovery purposes.

5.7.1 Incident and Compromise Handling Procedures

Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions is minimized.

Backups of essential business information are performed on a regular basis. WebID Solutions tests internal disaster recovery procedures regularly.

Incidents affecting the security or the integrity of WebID's services are reported to the relevant CA(s) and to the supervising authority, and, if applicable, to affected subscribers and third parties, without unnecessary delay (in any case within 24 hours) after WebID Solutions has become aware of the incident by the required means of communication.

Functions, availability and utilization of relevant services and systems are monitored for immediate recognition of system failures and incidents.

Start-ups and shutdowns of the logging functions and availability and utilization of needed services are monitored for immediate recognition of system failures and incidents.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

WebID Solutions maintains backup copies of its databases and software in order to be able to rebuild business capabilities in case of software and/or data corruption.

In the event of corruption of computing resources, software, and/or data employees immediately report such an occurrence to the Security Officer. The Security Officer invokes the emergency plan if required.

If software or data has been corrupted the affected system is completely wiped to remove any possible remaining causes for the corruption. The system is then restored from a clean image.

5.7.3 Entity Private Key Compromise Procedures

Not applicable. Key compromise must be handled by the CA.

5.7.4 Business Continuity Capabilities after a Disaster

WebID Solutions has created and maintains a business continuity plan so that in the event of a business disruption critical business functions may be resumed.

WebID Solutions maintains a secondary call center location geographically separate from the primary location which serves as a disaster recovery facility (see section 5.1.1).

In the event of a disaster requiring permanent cessation of operations from the primary facility, WebID Solutions' management will assess the situation and formally declare a disaster situation, if required.

Once a disaster situation is declared, the restoration of services functionality at the secondary site will be initiated.

The recovery time objective is no greater than 24 hours.

WebID Solutions conducts at least one disaster recovery test per calendar year to ensure functionality of services at the secondary site. Formal business continuity exercises are also conducted yearly.

5.8 CA or RA Termination

Not applicable. WebID Solutions does not operate a CA or RA.

5.8.1 Termination of Identification Service

WebID Solutions has implemented a termination plan which defines which actions must be taken in case of termination of services. Among others, the termination plan covers the aspects

which entities must be informed about the termination, to whom remaining obligations will be transferred, and who will store relevant data that needs to be retained.

As after termination of services no systems are required to be operational for a longer period of time WebID Solutions will bear the costs for the execution of the termination plan.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Not applicable. WebID Solutions does not generate keys.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Not applicable for cryptographic module engineering controls because WebID Solutions does not operate crytograpgic modules.

WebID Solutions manages only private keys for its own purposes, in particular for encrypting the applications and data stored on the servers in the third party datacenter.

For encrypting the communication with the TSP, the TSP has provided an 4096 bit encryption key. Identification data is encrypted with a randomly chosen AES key, the AES key is then encrypted with the public part of the 4096 bit encryption key. Encrypted key and and encrypted data is then sent to the TSP.

WebID Solutions keeps the number of personnel authorized to use these keys to a minimum. Unauthorized use is prohibited. The passphrases for these keys are kept secret.

6.3 Other Aspects of Key Pair Management

Not applicable. WebID Solutions does not generate and manage keys.

6.4 Activation Data

Not applicable. WebID Solutions does not generate and manage keys.

6.5 Computer Security Controls

A general information security policy document (security policy) is available and has been approved by management. It is published, and communicated, as appropriate, to all employees affected by it. This policy may be supplemented by detailed policies and procedures for personnel involved in identity verification.

The information security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing. It contains a statement of management intent, supporting the goals and principles of information security, and gives an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization.

The information security policy lists general and specific responsibilities for information security management, including reporting security incidents, and contains references to documentation

which supports the policy. Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined. An authorization process for new information processing facilities exists and is followed.

WebID Solutions' management ensures that there is clear direction and visible management support for security initiatives. WebID Solutions' management is responsible for maintaining the security policy and coordinates the implementation of information security measures. This includes regular reviews (at least yearly) of the information security policy and associated documents like the risk assessment, the inventory of assets, and the TSPS.

The risk assessment is approved by WebID Solutions' management, reviewed regularly and revised if necessary. The management accepts with this approval the residual risks identified in the risk assessment.

6.5.1 Specific Computer Security Technical Requirements

WebID Solutions ensures that the systems storing and processing software and data are trustworthy systems protected against unauthorized access.

All systems are protected against viruses, malicious, and unauthorized software.

Patches or updates for network security software components or operating system components are applied within a reasonable time after their relevance and applicability has been verified. Reasons for not applying security patches are documented.

All systems are hardened, i.e. all unnecessary user accounts, applications, protocols, and ports are removed or disabled.

Access to systems is restricted to individuals with a valid business reason for such access. General application users have no accounts on production systems.

User and account management has been implemented. Access rights are granted based on the role concept. Rights are immediately removed if no longer required. In addition, user accounts, roles, and access rights are regularly reviewed. Particularly, use of system utility programs are restricted and controlled.

All data is stored in encrypted form to protect it against manipulations and unauthorized access.

The network with systems for identity verification is logically separated from other components. This separation prevents network access to critical systems except through defined application processes and network paths. Firewalls are installed to protect the production and management network from internal and external intrusion or other forms of attacks.

Direct access to databases supporting identity verifications and storing customer's identity data is limited to persons in trusted roles having a valid business reason for such access.

The workplaces of the identity verification specialists must be physically separated from each other in such a way that the video cameras and microphones of one workplace cannot capture screen images or voices of video conferences at other workplaces. Workplaces are created with minimum application set-up and user account access rights necessary for operating the identification process.

Bringing personal belongings to the workplaces is prohibited.

6.5.2 Computer Security Rating
No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls
Development systems are separated from production systems.

Within the system development projects for the identification services of WebID Solutions security requirements are reviewed and analysed to ensure security of WebID Soloutions' IT systems for the service.

New software or new applications, releases, modifications and emergency software fixes are installed on production systems only after they have been successfully tested according to the change control policy. Installation of new software or applications prior to approval is not permitted.

6.6.2 Security Management Controls

The configuration of WebID Solutions' systems and any modifications and upgrades is documented and controlled.

The integrity of video conferencing software and database applications are under permanent control through automatic integrity checking mechanisms for detecting unauthorized modification to the software or configuration. Critical vulnerabilities are addressed within a maximum period of 48 hours after their discovery.

6.6.3 Life Cycle Security Controls
No stipulation.

6.6.4 Network security controls
WebID Solutions has installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, etc.).

Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy.

Configurations of servers, clients, and all network routing systems including firewalls are regularly checked for compliance with the requirements of this TSPS.

Access to all servers is subject to authentication.

Communication of sensitive information, especially the video conference stream and the identification data submitted to the CA, is always protected through encryption.

Regular vulnerability scans and penetrations test are performed by an independent third party for all of WebID Solutions network components and systems.

Any vulnerability assessed during such scans are fully reviewed and mitigation actions are taken according to the determined impact of the assessed vulnerability, or, in case it is determined that the vulnerability does not require remediation, the factual basis for such decision is documented.

WebID has separated its network into different zones. It uses separate dedicated networks for the administraton of its operational IT systems (e.g. databases) and the video identification clients.

Systems used for administration of the security policy implementation are not used for other purposes.

6.7 Time-Stamping

Cryptographic time-stamps are not required.

However, database entries about identification sessions contain time and date information. File names of protocols and other relevant records like log files must include at least the date of creation.

Systems synchronize their internal time via ntp protocol. WebID Solutions' ntp server synchronizes with Physikalisch-Technische Bundesanstalt UTC(PDB) once per hour.

7 Certificate, CRL, and OCSP Profiles

Not applicable. WebID Solutions does not issue certificates or CRLs and does not operate OCSP responders.

8 Compliance Audit and Other Assessments

WebID Solutions is subject to regular external audits. These include audits pursuant to ETSI EN 319 411-1 and ETSI EN 319 411-2 which are required to prove conformity with the regulations made in eIDAS.

These audits require demonstration of a maximum level of security and conformity to well-recognized policies and practices.

In addition, WebID Solutions performs internal self-audits. Topics covered by these audits include checks of proper implementation of applicable policies and extensive checks on the quality of identifications performed and on the quality of collected evidences collected during identifications.

The results of these compliance audits are documented and archived. They may be released at the discretion of WebID Solutions management to compliance auditors and if required by government authorities for the purpose of legal proceedings.

8.1 Frequency and Circumstances of Assessment

According to eIDAS, article 20 (1) compliance audits according to section 8 must be performed at least every 24 months.

Additional assessments are required if substantial changes are made to WebID Solutions' systems, configurations, or processes that might affect the overall security if the services.

8.2 Identity/Qualifications of Assessor

The conformity assessment required by eIDAS is performed by an accredited assessment body.

8.3 Assessor's Relationship to Assessed Entity

Compliance audits must be performed by a public firm that is independent of WebID Solutions.

8.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that WebID Solutions' components comply with the statements of this TSPS, with the eIDAS regulation, and with the requirements specified in the audit standard under consideration.

Thus, all applicable aspects of this TSPS and all the standards mentioned in section 8 are covered by the compliance audits.

The scope of the ETSI audit includes (but is not limited to) environmental controls, infrastructure and administrative CA controls, network controls, and identity verification processes and procedures.

8.5 Actions Taken as a Result of Deficiency

If significant exceptions or deficiencies are identified during the compliance audit as defined in section 8 this will result in a determination of actions to be taken. This determination will be made by WebID Solutions' management in cooperation with the auditor. WebID Solutions' management is responsible for developing and implementing a corrective action plan.

If it is determined that such exceptions or deficiencies pose an immediate threat identity verification services a corrective action plan must be developed within a period of time agreed upon with the auditor and implemented within a reasonable period of time. For less serious exceptions or deficiencies, the management evaluates the significance of such issues and determines the appropriate actions.

8.6 Communications of Results

No stipulation.

9 Other Business and Legal Matters

9.1 Fees

Fees for the identity verification services are subject to contractual agreements between WebID Solutions and its business partners.

WebID Solutions does not charge a fee for access to this TSPS. Any use other than viewing, such as reproduction, redistribution, modification, or creating derivatives is not permitted.

9.2 Financial Responsibility

For both contractual and non-contractual customers and business partners the regulations of indemnification of German law are binding.

WebID Solutions undergoes regular financial assessments to verify that it has the financial stability and resources required to operate in conformity with this TSPS and the requirements of eIDAS.

9.2.1 Insurance Coverage
WebID Solutions maintains a Professional Liability insurance coverage.

9.2.2 Other Assets
No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Confidential information includes any information provided by customers for purposes of identity verification.

9.3.2 Information Not Within the Scope of Confidential Information
Documents and other information in the repository are not considered confidential/private information.

9.3.3 Responsibility to Protect Confidential Information

All of WebID Solutions' personnel are responsible for protecting the confidential information in their possession in accordance with this TSPS, in accordance with contractual agreements, and in accordance with the German data protection regulations.

9.4 Privacy of personal information

9.4.1 Privacy Plan
All information that allows the identification of customers is protected from unauthorized disclosure.

9.4.2 Information Treated as Private
German statutory data privacy law defines which information must be treated as private.

Further information to be treated as private can be contractually agreed upon.

9.4.3 Information not Deemed Private
Information included in the certificates that are issued by a CA based on identity verifications performed by WebID Solutions is considered not to be private.

9.4.4 Responsibility to Protect Private Information
All employees of WebID Solutions receiving private information are obliged to protect it from compromise and disclosure to third parties.

All employees must adhere to German privacy laws.

9.4.5 Notice and Consent to Use Private Information
Unless otherwise stated in this TSPS WebID Solutions will not use private information without the owner's consent.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process
If disclosure of private information about customers is necessary in response to judicial, administrative, or other legal proceedings the information shall be given only to the requesting authority or the customers themselves.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Not applicable.

9.6.2 RA Representations and Warranties

WebID Solutions has overall responsibility for all technical and organizational processes and procedures of its video-ident services.

WebID Solutions warrants that it performs identity verification functions as described in this TSPS.

WebID Solutions forwards complete, accurate, and verified data about subjects for further processing to the CA.

Retention, archiving, and protection of data are performed according to the stipulations of this TSPS.

Archived subscriber data is protected in compliance with German data protection legislation, All data is stored in encrypted form and accessible only for employees in trusted roles.

All services related to identity verification and all handling of customer data described in this TSPS are performed by WebID Solution’s employees. WebID Solutions does not delegate such tasks to third parties.

Technical services may be performed by reliable third party data center personnel. Data center personnel have no access to customer data.

9.6.3 Subscriber Representations and Warranties

Customers warrant that all representations made in the video conference are true,

9.6.4 Relying Party Representations and Warranties

Not applicable. WebID Solutions does not issue certificates and has no contact with relying parties.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liability

Limitations of Liability are subject to contractual agreements between WebID Solutions and its business partners. In any case, limitations of liability contained in WebID Solutions' General Terms and Conditions (available at https://www.webid-solutions.de/de/standard-terms-of-business.html) shall apply. Limitations of Liability as specifically agreed on in each individual case, where applicable, remain unaffected.

9.9 Indemnities

The regulations of indemnification of German law are binding.

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, customers and CAs issuing qualified certificates based on the identity verification performed by WebID Solutions may be required to indemnify WebID Solutions for:

- submitting false facts or misrepresenting facts on the customer's identity,
- failure to disclose a material fact on the identity verification with intent to deceive any party,
- failure to protect the customer's private data, use of an untrusted system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the customer's private data.

9.10 Term and Termination

9.10.1 Term

The TSPS becomes effective upon publication on WebID Solutions' web site. Amendments to this TSPS become effective upon publication.

9.10.2 Termination

This TSPS as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Despite the fact that this TSPS may eventually no longer be in effect, the following obligations and limitations of this TSPS shall survive: section 9.6 (Representations and Warranties), section 9.2 (Financial Responsibility), and section 9.3 (Confidentiality of Business Information).

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this TSPS may be made by WebID Solutions' management. Amendments shall either be in the form of a document containing an amended form of the TSPS or an update. Amended versions or updates shall be published in the repository.

9.12.2 Notification Mechanism and Period

When relevant changes are intended to be made to this TSPS, WebID Solutions will inform the CAs for which WebID acts as subcontractor, WebID's customers (e.g.banks), if required, and the assessment body (see section 8.2). If required also the supervisory authority will be informed.

There is no need to inform certificate applicants and relying parties. Certificate applicants must accept the (new) TSPS during the identification process. Relying parties have no relationship with WebID Solutions; for relying parties only the CA's TSPS is relevant.

9.12.3 Circumstances under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

WebID Solutions only provides identity verification services in order to support the registration authorities of the CAs that issue the certificates. WebID Solutions has no contractual agreements with end-users or relying parties.

For disputes with end-users and relying parties the dispute resolution procedures of the issuing CAs apply.

Complaints regarding WebID Solutions' services can be submitted to datenschutz@webid-solutions.de.

9.14 Governing Law

Applicable law is the law of the Federal Republic of Germany.

9.15 Compliance with Applicable Law

This TSPS is subject to applicable national law, in particular the eIDAS regulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If parts of any of the provisions in this TSPS are incorrect or invalid, this shall not affect the validity of the remaining provisions until the TSPS is updated. The process for updating this CP is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The WebID Solution GmbH shall not be responsible for any breach of warranty, delay, or failure in performance under this TSPS that result from events beyond its control, such as strike, acts of war, riots, epidemics, power outages, fire, earthquakes, and other disasters.

9.17 Other provisions

No stipulation.