Verimi Trust Services Practice Statement

Title: Verimi Trust Services Practice Statement

Date: 25.04.2024

Name: Dr. Dirk Woywod, Verimi GmbH

Classification: Public

Version: V4.5

Contents

1 Introduction

Verimi GmbH is an identity service provider offering online services for identity verification of natural persons and legal entities (in the following “users”) in order to support Verimi’s partners needing reliable identification of their users.

In addition, in collaboration with qualified trust service providers and contract partners Verimi enables individual users of the contracted partners (in the following “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 Anti-Money Laundering Regulation 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, Verimi verifies the identity of natural persons amongst other methods 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.

The technical specifications and procedures implemented by Verimi fulfil the requirements of assurance level “high” or “substantial” as defined in eIDAS, Article 8 and in the Implementing Regulation (EU) 2015/1502 of 8 September 2015.

Conformance with eIDAS at assurance level “high” and “substantial” allows certification service providers to use these services for identity verification in their processes of issuing qualified certificates.

This document is the Trust Service Practice Statement (TSPS) of Verimi GmbH. It is not a full Certification Practice Statement (CPS) according to RFC 3647 because Verimi only provides identity verification services but does currently 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 Verimi allow users of partners to be reliably identified using a variety of identification methods while the user is not physically present, i.e., at home or at his/her workplace. Verimi delivers the results of identity verifications in electronic form to its 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 documents, e.g., contracts.

The Verimi platform consists of three core frontend applications, each offering full functionality for identification of natural persons:

(1) The Web application, which is accessible via the Internet and can be used via any browser independent of the operating system.
(2) The native iOS app for an enhanced user experience on Apple devices
(3) The native Android app for an enhanced user experience on Android OS devices

In addition, for the identification/registration of legal entities, Verimi offers a frontend application to be used only by trained Point-of-Sales (PoS) agents

(4) The native iOS or Android Verimi-for-Business App for use on tablets and mobile phones

All frontend applications are continuously being further developed. In addition to testing for possible security vulnerabilities, the security improvements of the respective operating systems are integrated.

Verimi services are offered to all users of its contract partners without discrimination to the public. Verimi takes the relevant standards such as ETSI EN 301 549 - Accessibility requirements for ICT products and services - or W3C Web Accessibility Initiative WAI into account to provide services accessible for persons with disabilities without avoidable restrictions.

For specific identification methods, methodology-inherent restriction exists:

- eID-Ident requires the person to have a German ID Card or electronic Residence Permit Card (eAT).
- Video-Ident services cannot be provided for people with mutism and deafness.
- GwG-Ident requires the person to have an active and suitable bank account at one of the supported financial institutions.

The services of Verimi conform to the German Anti-Money Laundering law and the eIDAS regulation on electronic identification and trust services.

The services of Verimi have been assessed for compliance with the relevant 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 relevant requirements of eIDAS has been confirmed by an accredited conformity assessment body (CAB).

This TSPS applies to Identification Services for the following trust service policies: EN 319411-1 LCP, NCP and EN 319411-2 QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd.

The identification services offered on the platform are either performed by trained and experienced identity verification specialists or provided via secure IT-systems and are all in accordance with legally admitted procedures. They replace the personal (physical) presence of the person to be identified.

The Usage of the Verimi services is defined by the Terms of Usage: https://verimi.de/en/terms-of-use-for-customers/.

Verimi cooperates with external service provider and subcontractor to offer the services, please see Chapter 9.8 for liability and 9.17 for other obligations.

1.2 Document Name and Identification

This document is the “Trust Service Practice Statement” of the Verimi GmbH.

Name of the document	Verimi GmbH – Trust Service Practice Statement

Version	4.5 25.04.2024

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.

Verimi 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.

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

In most of the cases Verimi does not operate a RA but offers identification services on behalf of a CAs RA. Only in case of Local-Ident (Point of Sale) for legal entities (see 3.2.3, Section IV) Verimi operates its own RA.

1.3.3 Subscribers

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

Verimi identifies the subscribers on behalf of contracted 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.

1.4 Certificate Usage

Verimi provides identity verification services and does not issue certificates. The certificate usage is restricted to the usage defined in the certificate policy of the relevant Trust Service Provider.

This TSPS applies to Identification Services for the following trust service policies EN 319411-1 LCP, NCP and EN 319411-2 QCP-n, QCP-l, QCP-n-qscd and QCP-l-qscd.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This TSPS is administered by:

Verimi GmbH, Oranienstraße 91, 10969 Berlin

1.5.2 Contact Person

Compliance Officer, Verimi GmbH, Oranienstraße 91, 10969 Berlin

E-Mail: compliance@verimi.com

1.5.3 Person Determining CPS Suitability for the Policy

Verimi's 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 Chapter III on identity verification for Trust Services.

TSPS document is approved by Verimi's Senior Management and published and communicated to all relevant employees and external parties immediately.

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

The Terms and Conditions are made available to all subscribers and relying parties through durable means of communication. Amended versions or updates of this TSPS, the PKI Disclosure Statement (PDS) and the Terms and Conditions are published immediately at the website. Please see www.verimi.de for details.

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

Verimi publishes this TSPS and other relevant documents such as General Terms and Conditions (AGB) and the Data Protection Statement on its website www.verimi.de.

2.2 Publication of Certificate Information

Not applicable. Verimi does not issue certificates.

2.3 Time or Frequency of Publication

This TSPS and any subsequent amendments are made immediately publicly available after approval. Verimi develops, implements, enforces, and annually updates this TSPS to meet the compliance standards of the documents listed in Section 1.6.3.

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

2.4 Access Controls on Repositories

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

Verimi 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. Verimi does not issue certificates.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Not applicable. Verimi does not issue certificates.

3.2.2 Authentication of Organization Entity

Not applicable. Verimi does not issue certificates.

3.2.3 Authentication of Individual Identity

The authentication of the individual identity is checked in different ways. Original individual identification methods include:

I. eID-Ident

Verimi sources the transmission of personal identification data via the eID function of the German identity card via an identity service provider (Identifizierungsdiensteanbieter) certified in accordance with the Technical Guideline BSI-TR-03128 and with an information security management certified according to the international standard ISO 27001. Verimi regularly checks the existence of valid conformity certificates as part of a compliance audit.

The information collected during the identification include the full name (surname and given name(s)) of the applicant, the doctoral degree, the date and place of birth, the current address, and nationality as well as the type, and the last day of validity of the identity document presented.

eID-Ident relies on the infrastructure of the German eID functions which is notified by the member states of the European Union at eIDAS level “high”.

II. Video-Ident

The Video-Ident procedure is carried out for Verimi by a **Video-Ident-service provider**. The procedure is certified to meet all requirements of the Federal Financial Supervisory Authority (BaFin)[1] as well as all requirements of the Regulation (EU) No. 910/2014 (eIDAS) for the identification of natural persons for qualified trust services.

The information collected during the identification include the full name (surname and given name(s)) of the applicant, the date and place of birth, the current address, the

[1] BaFin Rundschreiben 3/2017 (GW) – Videoidentifizierungsverfahren, Geschäftszeichen GZ: GW 1-GW 2002-2009/0002, 10. April 2017: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2017/rs_1703_gw_videoident.html.

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 user before the beginning of the identification process.

III. GwG-Ident

GwG-Ident is a procedure for the transfer of identity attributes from identities which have already been collected earlier by **GwG-compliant service providers** (e.g., financial service providers, banks). Verimi is a regulated Payment Service Provider (ZAG) licensed and supervised by the German Federal Financial Supervisory Authority BaFin.

The establishment of a business relationship (e.g., the opening of an bank account) with a service provider who complies with the GwG already requires the identification of the contract partner by the service provider following the general duty of care in accordance with § 10 GwG. As part of the GwG's general duty of care in identifying the contractual partner, strict requirements are placed on the reliable collection of identity data in accordance with the Know Your Customer Principle (KYC). Compliance with the statutory provisions of the GwG is monitored by the BaFin in Germany.

In accordance with § 11 (4) GwG, the following information must be collected, checked, and recorded during identification: First name and surname, place and date of birth, nationality and address. The verification of the identity attributes is generally carried out in accordance with § 13 (1) No. 1 GwG in conjunction with the following. § 12 (1) sentence 1 No. 1 GwG on the basis of a valid official identity document. In this context, further data relating to the initial identification procedure will be collected in accordance with GwG § 8 (2): Type of identity document (e.g. identity card or passport), identity card number and issuing authority.

In addition to the personal presentation of an Official Photo ID on site, an inspection can also be carried out by means of another suitable procedure whose security level is equivalent to the presentation of the document on site, § 13 (1) No. 2 GwG.

GwG § 12 (1) sentence 1 No. 1-5 specifies which proof of identity may be used to verify identity. GwG § 13 specifies the procedures that may be used for this purpose. This results in the following permissible initial identification procedures within the framework of GwG Identification Procedure

- **GwG-Ident-Video**: according to § 13 (1) No. 2 GwG in connection with § 12 (1) sentence 1 No. 1 GwG and taking into account Circular 3/2017 of BaFin[2] on the basis of a valid official identity document which contains a photograph of the holder and which fulfils the passport and identification requirements in Germany (in operation).
- **GwG-Ident-QES:** according to § 12 (1) sentence 1 No. 3 GwG by the use of a qualified electronic signature (planned).
- **GwG-Ident-eIDAS-High (e.g., eID function):** according to an electronic identification system referred to in § 12 (1) sentence 1 No. 4 GwG and notified as "high" pursuant to Article 8 (2) letter c in conjunction with Article 9 of Regulation (EU) No

[2] BaFin, Circular 3/2017 (GW) - video identification procedures. Link: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/2017/rs_1703_gw_videoident_en.html. Last check 06.11.2018.

910/2014. Including the electronic proof of identity mentioned in § 12 (1) sentence 1 No. 2 GwG (planned).

In accordance with the GwG, further procedures are possible with regard to the identification of the business partner, e.g., on the basis of further documents in accordance with § 12 (1) sentence 1 No. 5 or in accordance with simplified due diligence obligations in accordance with §14 GwG. In addition to identity attributes, the date of validity of the ID document, ID card number and type of ID card are transferred with regard to the initial identification procedure. Verimi uses this data to check whether the identity attributes originate from a permitted initial identification procedure.

Identity attributes from the GwG identification procedure are attributes of an identity which have already been collected at an earlier point in time by a GwG-compliant service provider. Verimi therefore checks whether the evidence used within the scope of the initial identification is still valid at the time of the takeover before the adoption of identity attributes on the basis of the date of validity of the identity document. Only identity attributes are transferred where the evidence used in the initial identification is valid at the time of transfer.

Please see for Details: „Prüfbericht – Durchführungsverordnung (EU) 2015/1502, TU-VIT.97127.Ident“, Version 1.4 vom 24.01.2019“. (available on request).

IV. Local-Ident (Point of Sale) for legal entities

Verimi offers an identification of legal entities. Specifically, the objective of this identification method is to identify a natural person representing a legal entity. The identification is done in a 3-step-process by a trained Point-of-Sale (PoS) agent. The trained PoS agent is obliged to hand over collect correct and complete data. This is done by means of a signed declaration of commitment by the PoS agent.

- Identification of the natural person
  The identification is done by a PoS agent based for a natural person present at the PoS with a valid identity document. The information collected during the identification include the full name (surname and given name(s)) of the applicant, the doctoral degree, the date and place of birth, the current address, and nationality as well as the type, and the last day of validity of the identity document presented.
- Identification of the legal entity
  Next, the natural person is asked to provide information on the legal entity (official name and address). The information is then validated by the PoS agent.
  Matching of the natural person to the legal entity. The PoS agent matches the natural person to the legal entity either via information provided by the natural person or by information from the public register.

  It should be noted that currently only the following legal forms are active:

  - Limited liability company (Gesellschaft mit beschränkter Haftung) - GmbH
  - Entrepreneurial company (Unternehmergesellschaft) - UG (haftungsbeschränkt)
  - Public limited company (Aktiengesellschaft) - AG
  - Societas Europae (European public limited company) - SE
  - Registered association (Eingetragener Verein) - e.V.

  The identification of legal entities of other legal forms or of mixed forms are not possible. The identification of companies that are still in the formation stage is also excluded.

V. Wallet-Ident

Wallet ident enables the user to re-use a previous identification stored with Verimi. As such, it is not an original identification method itself but rather relies on the identification methods I. – IV. as listed above. The accessible attributes depend on the original identification method used to determine the attributes. The reliability of the process is derived from

- the reliability of the original identification service used
  The appropriate description is given under sections I. – IV.
- the reliability of the identity data storage
  The data is stored in certified data centers (see section 5.1) using cryptographic algorithms according to BSI TR-02102 to ensure integrity and confidentiality
- the reliability of the authentication mechanism when accessing and retrieving the stored identity data
  A 2-factor authentication is used to secure the data access. The authentication method with the Verimi App and the Verimi PIN has been assessed against the requirements of BSI TR-03107 and shown to exhibit the level substantial.

3.2.4 Non-verified Subscriber Information

Not applicable. Verimi offers only identity validation services.

3.2.5 Validation of Authority

Not applicable. Verimi offers only identity validation services.

Verimi does not validate the user'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. Verimi does not issue certificates.

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

3.4 Identification and Authentication for Revocation Requests

Not applicable. Verimi does not issue certificates and does not handle revocation requests.

4 Certificate Life-Cycle Operational Requirements

Not applicable.

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

5 Facility, Management, and Operational Controls

Verimi carries out regular risk assessments to identify, analyse, and evaluate risks related to its services considering business and technical issues.

Verimi then selects appropriate risk treatment measures considering the results of the risk assessment. The chosen risk treatment measures ensure that the level of security is commensurate with the degree of risk.

The risk assessment is approved by Verimi's management who accepts the residual risks identified in the risk assessment with this approval.

Verimi's information security management system is ISO 27001 certified. It ensures that proper security controls adequate to manage the risks are taken.

In addition to Verimi, the requirements from chapter 5.1 also apply to external service providers and the outsourcing partner.

5.1 Physical Controls

Verimi 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

Verimi operates the Verimi platform exclusively in the Open Telekom Cloud (OTC), hosted by Deutsche Telekom AG, but fully administered by Verimi.

For redundancy purposes, Verimi operates its platform in different facilities at different availability zones. All of them can provide the part of the Verimi platform services required for identity verification.

Verimi's servers are located in secure data centers and managed and operated (at the operating system level) by data center staff. The security of the data centers is demonstrated via a suitable certification the existence and validity of which Verimi regularly checks as part of a compliance audit.

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 placed so that only authorized employees can access them. Verimi's applications and data are stored encrypted and not accessible for data center personnel. The environment is physically protected and deters, prevents and detects unauthorized use of, access to, or disclosure of sensitive information.

5.1.2 Physical Access

Verimi ensures that its relevant systems, especially the relevant database servers and the systems used for the identity services, are operated 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.

Verimi has implemented physical access controls to reduce the risk of unauthorized persons being able to access Verimi's premises. In addition, Verimi ensures that the physical access to its data centers incl. database servers, routing and switching components, and firewalls is sufficiently restricted.

All IT components (servers, databases) required for the implementation of the Verimi service are located in specially secured locations. Only administrators have access to the premises in accordance with the principle of dual control, i.e. two persons must authenticate themselves to the secured access points using personalized chip cards and PINs in order to gain access. Every access is logged in a revision-proof manner and regularly analysed by the Verimi security team.

Visitors to Verimi's premises cannot enter those without support of authorized employees. In all relevant security areas, visitors must be accompanied by authorized employees.

5.1.3 Power and Air Conditioning

The secure data centers have industry standard power and air conditioning systems to provide a suitable operating environment.

Furthermore, the data centers 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

The secure data centers have reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire Prevention and Protection

The secure data centers have industry standard fire prevention and protection mechanisms in place.

5.1.6 Media Storage

Sensitive physical media is stored in a safe to protect it from accidental damage (such as water, fire, electromagnetic fields, etc.). Media that contains audit data, archive data, or backup information is duplicated and stored securely as described in section 5.1.2..

All data carriers used are encrypted before data is stored. Only Verimi is in possession of the keys. Paper-based information is securely destroyed via a service provider."

5.1.7 Waste Disposal

Most 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 with critical information is disposed in such a way, that the restoration of the information is prevented. Other waste is disposed of in accordance with normal waste disposal requirements.

5.1.8 Off-site backup

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

Verimi is not obliged to keep identity verification data for a long period of time because all relevant identity verification data is sent to the Qualified Trust Service Provider (QTSP) for the purpose of issuing a qualified certificate immediately after being collected. The QTSP is then obliged to archive these data according to the regulations made in eIDAS.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted persons include all employees that have access to the source code or administer the Verimi platform. Special roles include:

Security Team

The security team consists of a Chief Information Security Officer (CISO) and several security experts like System Auditors, checking archives and audit logs.

In addition to developing personnel, organizational, technical and infrastructural security measures, the security team is also responsible for implementing these measures and maintaining them during ongoing operations. This requires not only regular training of all Verimi employees, but also adjustments to the current security situation in order to be able to react to any security incidents that may occur.

System Administration Team

Verimi has appointed an Administration Team which consists of System Administrators (install, configure, maintain and recover systems) and System Operators (operate the systems and perform system backups of it).

PoS-Agent

PoS-agents conduct the identification in the name of Verimi in person. They are specifically trained for this task.

Data Protection Officer (DSB)

In line with the European Commission's new basic data protection regulation, Verimi has appointed a Data Protection Officer. The data protection officer is not only supported by a team of qualified employees, but also by renowned scientific institutions. With respect to data security, the Privacy Team works closely with the Verimi Security Team.

Chief Information Security Officer

Verimi has appointed a Chief Information Security Officer (CISO). Its main tasks include:

- Coordination of information security goals with the company management
- Coordination and planning of information security in cooperation with the Information Security Team (IST)
- Creation and maintenance of guidelines and regulations for information security in the company
- Advising management on information security issues
- Documentation of information security measures
- Information security training for employees
- Planning and design of incident management ("Incidents") and emergency precautions (incl. emergency plan/manual)

Compliance Officer

Verimi has appointed a Compliance Officer. The Compliance Officer implements the compliance regulations of Verimi in the corporate structure and business processes by setting up a compliance management system. With his knowledge of the corporate structure as well as the operational processes and products, he determines the company-specific risks for legal violations in a systematic risk analysis.

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.

The person who takes over a trusted role must agree to this before approval.

Personnel have no access to the trusted functions until the necessary checks are completed.

Personnel in trusted roles is named and approved by senior management of Verimi before being permitted to access relevant systems requiring the principle of "least privilege" when accessing or when configuring access privileges.

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 misuse to its minimum.

5.3 Personnel Controls

In addition to Verimi, the requirements from chapter 5.3 also apply to external service provider and the outsourcing partner.

5.3.1 Qualification, Experience, and Clearance Requirements

All employees involved in the operation of Verimi's systems 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 employees of Verimi are thoroughly checked for their qualifications for the tasks for which they are responsible before being hired. Training and previous employment are examined based on training and work certificates.

In addition, new employees undergo a criminal background check. This consists 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 Verimi systems and services receive comprehensive training. Training is conducted in the following areas:

- Information Security,
- Compliance,
- Data Protection,
- relevant norms and standards,
- security principles and mechanisms,
- use and operation of the Verimi platform,
- incident handling and reporting,
- disaster recovery procedures.

Verimi conducts regular security training sessions to raise awareness of Information Security and Data Protection. Training is mandatory not only for Verimi's technical staff (e.g. system administrators and developers), but also for administrative staff and for the respective target groups. The courses cover all relevant topics of Information Security and Data Protection, from current threats to attacker procedures (including social engineering) to the consequences of successful attacks and methods for risk minimization.

It is ensured, that PoS-agents are trained in validating identities based on identification documents.

In addition, renowned researchers are invited to present current topics from their work and discuss their results at internal knowledge days. The insight into innovative technologies allows the continuous improvement of Verimi.

Verimi maintains records of compliance, Data Privacy and security trainings performed.

5.3.4 Re-Training Frequency and Requirements

Re-Training is performed to the extent and frequency required to ensure that the required level of proficiency is maintained. It takes place at least once a year.

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

Independent contractors who support the regular employees are required to fulfil 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 have been made available to Verimi employees.

5.4 Audit Logging Procedures

In addition to Verimi, the requirements of chapter 5.4 also apply to external service providers and the outsourcing partner.

5.4.1 Types of Events Logged

Verimi 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, including 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.

Security log entries include in particular the following elements:

- date and time of the entry
- description/kind of entry.

The security logs are automatically collected.

The identity verification audit logs in particular include:

- kind of identification methods used,
- record of identification presented,
- identity of service requesting / providing the identity.

These audit logs are automatically created, integrity protected and immediately encrypted. They can only be accessed in case of a special audit using a distinct auditor decryption key.

5.4.2 Frequency of Processing Log

Verimi's 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.

The security logs are regularly reviewed 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 security log reviews are documented.

5.4.3 Retention Period for Audit Log

Event logs are stored for 10 years in minimum. Records are archived for as long as required by the respective legislation and specific regulations.

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 stored within the data center which provides sufficient redundancy via its availability zone concept and the geographically distinct locations.

5.4.6 Audit Collection System (Internal vs. External)

Audit data is generated and recorded automatically at the application, network, and operating system level.

5.4.7 Notification to Event-Causing Subject

No stipulation

5.4.8 Vulnerability Assessments

Software may have errors. Some of these errors can lead to security vulnerabilities. The same applies to the security measures implemented, be they of a personal, organizational, technical, or infrastructural nature. Despite evaluation of these measures regarding security, security gaps may arise which were not identified in the evaluation.

The security team therefore regularly checks the effectiveness of the implemented measures, also by simulating its own attacks (hacking, but also e.g., phishing attacks), and thus tests the effectiveness of the security measures and security training courses. In addition, based on events in the log files the security team initiates vulnerability assessments.

For any vulnerability, given the potential impact, Verimi

- creates and implements a plan to mitigate the vulnerability; or
- documents the factual basis that the vulnerability does not require remediation.

5.5 Records Archival

In addition to Verimi, the requirements of chapter 5.5 also apply to external service providers and outsourcing partner.

5.5.1 Types of Records Archived

At a minimum, Verimi records the following data for archival:

- this TSPS
- contractual obligations
- system and equipment configuration
- modifications and updates to systems or configurations
- audit logs mentioned in section 5.4
- documentation required by compliance auditors.

5.5.2 Retention Period for Archive

All records are archived in accordance with legal or regulatory requirements. For supporting information, this is usually for at least ten years.

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

Either the QTSP is responsible for archival of identification data and contractually agrees with Verimi on a shorter archive period specified in the contractual agreements or the QTSP contractually agrees with Verimi that long-time archival is in the responsibility of Verimi. In this case the archival period is specified in the contracts with the QTSP.

In any case, in accordance with data protection regulation all person-related data is deleted from Verimi's systems after the archive period has expired.

5.5.3 Protection of Archive

Verimi 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 archived data is maintained to ensure that the archive data can be accessed for the time period defined above.

5.5.4 Archive Backup Procedures

Verimi performs regular database backups according to Verimi's backup concept. This concept takes into account the criticality of the data and defines the minimum backup cycles and backup methods.

The backups are performed by the administrators. The CISO is responsible for the correct execution of the backup.

5.5.5 Requirements for Time Stamping of Records

No stipulation.

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. Verimi does not handle CA keys.

5.7 Compromise and Disaster Recovery

Verimi 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.

Based on mobile communication and VPN-based use of internal IT-systems and data, Verimi employees can work in a decentralized manner from different locations and even from home until the availability of the primary location is restored or a contingent location ready for use.

In addition to Verimi, the requirements from chapter 5.7 also apply to external service provider and the outsourcing partner.

5.7.1 Incident and Compromise Handling Procedures

Should security gaps become apparent, e.g., due to own observations or actual attacks, the security team has already conducted possible attack scenarios and prepared appropriate countermeasures. These can range from the short-term shutdown of security-critical services to the shutdown of the entire platform until security is restored.

In addition, the current security situation is regularly monitored. Other sources, e.g., the Computer Emergency Response Team of the Federal Office for Information Security, provide information on current security gaps and attacks to initiate appropriate countermeasures.

The regular internal procedures of the departments and internally responsible contact persons are used to deal with security incidents. The CISO, ISB and DSB are informed and involved in a supportive manner if necessary.

Verimi addresses any critical vulnerability not previously addressed, within 48 hours of its discovery.

Incidents affecting the security or the integrity of Verimi'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 Verimi has become aware of the incident by the required means of communication.

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

Verimi 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 team. The security team 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 in a clean manner.

5.7.3 Entity Private Key Compromise Procedures

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

5.7.4 Business Continuity Capabilities after a Disaster

Business Continuity Management (BCM) protects Verimi in an emergency from serious damage or losses threatening its existence. In addition to Verimi, it also applies to external service providers. It describes the content, personnel and organizational specifications and procedures for emergency management to

- ensure the continuation of time-critical activities and processes should an emergency occur
- take appropriate measures to avoid damage as far as possible
- to reduce the impact of damage that has occurred
- support a fast and orderly restoration of normal operation

The person responsible for Verimi in case of emergencies is named, the definition of the terms as well as the processes according to Plan - Do - Check - Act takes place. The emergency manual describes the emergency strategies taking into account defined emergency scenarios and their criticality. Specifications and details are described in the "Business Continuity Management" guideline.

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

In the event of a disaster requiring permanent cessation of operations from the primary facility, Verimi's 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 a secondary site will be initiated. The Operator of the Verimi IT Services made a commitment to make the services in less than 12 hours after a disaster available at a secondary site.

After a disaster has been dealt with, the CISO analyses the causes and takes measures within the ISO 27001-certified process to prevent a recurrence of the incident.

Verimi conducts regular disaster recovery and business continuity tests to ensure functionality of services in the case of a disaster.

5.8 CA or RA Termination

Not applicable. Verimi does not operate a CA or RA Services.

5.8.1 Termination of Identification Service

Verimi has implemented a termination plan that 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 Verimi will bear the costs for the execution of the termination plan.

6 Technical Security Controls

Verimi has implemented and operates a number of security controls in order to protect user's data and the application.

In addition to Verimi, the requirements of chapter 6 also apply to external service providers and the outsourcing partner.

6.1 Key Pair Generation and Installation

Not applicable. Verimi does not generate keys.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Not applicable. Verimi does not generate and manage keys.

6.3 Other Aspects of Key Pair Management

Not applicable. Verimi does not generate and manage keys.

6.4 Activation Data

Not applicable. Verimi 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 applicable, to all employees, subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies affected by it. This policy may be supplemented by detailed policies and procedures for personnel involved in identity verification.

Changes to the information security are communicated in Confluence and docs.verimi.

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 explains 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.

Verimi's management ensures that there is clear direction and visible management support for security initiatives. Verimi's 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 Verimi's management, reviewed regularly, and revised if necessary. The management accepts with this approval the residual risks identified in the risk assessment.

The security of Verimi is constantly being improved. The Fraunhofer Institute AISEC and the Identity Management Working Group of Freie Universität Berlin are supporting the project.

6.5.1 Specific Computer Security Technical Requirements

All Verimi systems were designed from the outset with a view to the secure implementation of the Verimi service (Security by Design). These include not only the cryptographic methods used, but also the technical infrastructural, software-side and overarching elements for securing the platform. Consequently, 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. Verimi uses virus scanners and firewalls from various vendors to protect itself from external attacks. Virus signatures and firewall configurations are regularly updated and adapted to the current security situation.

These measures alone are not sufficient to protect the platform. For example, so-called zero day exploits (security gaps that were previously unknown) are not detected. In order to be able to react to current attacks, various intrusion detection and intrusion prevention systems were implemented within the Verimi platform, which detect attacks by anomaly detection and can initiate appropriate countermeasures.

In addition, all activities are recorded, stored and regularly checked for anomalies by the security experts, so that a manual check of the security of the system is also guaranteed:

Patches or updates for network security software components or operating system components are applied after their relevance and applicability has been verified.

All systems are hardened, i.e., all unnecessary user accounts, applications, protocols, network connections and ports are removed or disabled. The platform's operating system is a Linux derivative in which all unneeded functions are deactivated and all security enhancing features are enabled. This includes in particular the configuration groups file system, software updates and integrity checks.

The configuration of the systems is checked regularly for changes which violate the Verimi security policies. The maximum interval between two checks is one year.

The Verimi apps for Android and iOS are also hardened with the help of a tool: The Trusted Application Kit (TAK) from Build38 (a spin-off of Giesecke+Devrient) includes white box crypto for obfuscation of keys and crypto functions, two-way TLS, secure memory, hook and root detection and device fingerprinting for binding to the smartphone.

Access to systems administration, development environment and code repository is restricted to individuals with a valid business reason for such access. General application users/Verimi employees have no access to these systems and applications.

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.

All data is stored in encrypted form to protect it against manipulations and unauthorized access. All user data managed by Verimi is protected at all times, within the Verimi platform, on the transmission path and with the application partner. Only cryptographic methods recommended by the Federal Office for Information Security (BSI) are used to protect identity data. The Technical Guidelines[3,4] published by the BSI are observed. In addition, the cryptographic methods used in Verimi are described. If security gaps should arise in the future when cryptographic methods are used, an immediate switch to other methods must be ensured. A migration concept exists for this purpose.

A two-zone model is implemented. Servers and databases for the secure operation of Verimi are located in Zone 1. Key management services (random number generator, storage of user-specific keys for encryption of identity attributes, keys for encryption of username and password and keys for signature of ID and access tokens) in Zone 2, also called Secure Zone. Access to these IT components is additionally secured via virus scanners, firewalls and intrusion detection/intrusion prevention systems and is logged and analysed separately from Zone 1.

[3] BSI: TR 02102-1, Cryptographic procedures: Recommendations and lengths, Version 2016-01, 15 February 2016, Federal Office for Information Security.

[4] [4] BSI: TR 02102-2, Cryptographic procedures: Recommendations and key lengths, Part 2 - Use of Transport Layer Security (TLS), Version 2016-01, Bundesamt für Sicherheit in der Informationstechnik

System maintenance can also be performed online by Verimi administrators. This access to the Verimi platform is secured via VPN. Administrators receive individual credentials for this purpose. Here, too, a four-eyes principle has been implemented.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

In addition to Verimi, the requirements of chapter 6.6 also apply to external service provider and outsourcing partner.

6.6.1 System Development Controls

Development systems are separated from production systems.

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 Verimi's systems and any modifications and upgrades must be documented and controlled.

Verimi's information security management system is ISO 27001 certified. It ensures that proper security controls adequate to manage the risks are taken.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network security controls

All security relevant keys are securely stored in a separate environment, the Zone, hosted by OTC and administered by Verimi. [5]

All network zones of the Verimi Platform are administrated by Verimi via VPN, which allows connections to special computers within the Verimi platform. These hosts are used exclusively for the purpose of administration, a connection is only allowed for Verimi administrators with Verimi equipment. Logins to sensitive software require an additional second factor in form of a TOTP; this applies to all allowed users, not only administrators. The administration hosts of the Secure Zone are additionally protected by a 3 factor authentication, including the possession of a FIPS 140-2 certified Yubikey, which will be given only to specially trusted members of the Verimi staff.

[5] See Chapter 9.6 for liability and 9.17 for obligations of external service provider.

Verimi uses a separate dedicated network for administration of IT systems and an operational network for other purposes.

The availability and utilization of required services within the Verimi network is monitored constantly.

Local network components (e.g., routers) configurations are periodically checked for compliance with the requirements specified by this document. The maximum interval between two checks is four weeks.

Network connections on the Verimi platform require strong authentication based on digital certificates. This includes the authentication of Verimi internal communication of services, external communication with application partners and administrator access to the log and monitoring system. Verimi has installed adequate protection from both inside and outside attacks (firewalls, intrusion detection mechanisms, etc.).

The Verimi platform uses two different PKIs: one for production and one for testing purposes.

Access to all servers is subject to authentication. All communication channels are secured by Transport Layer Security (TLS 1.2). These are:

- Communication path between user (App or web browser) and application partner
- Communication path between user (App or web browser) and Verimi
- Communication path between Verimi and application partner

All data is transmitted both encrypted and authenticated. Only cipher suites recommended by the BSI[6] are used.

The respective communication partners must authenticate themselves during the establishment of the TLS connection. Verimi and its application partners use X.509 certificates issued by trusted Certification Authorities (CA). Verimi only accepts TLS certificates of the following CAs:

- GlobalSign, https://www.globalsign.com
- DigiCert, https://www.digicert.com
- D-Trust, https://www.d-trust.de/
- T-Systems, https://www.telesec.de/

Users authenticate themselves to Verimi using one of the available authentication procedures.

Communication of sensitive information, especially the ident services provided to the Verimi platform, the communication between Verimi platform and Verimi App and the identification data submitted to the CA/TSP, is always protected through encryption and

[6] BSI: TR 02102-2, Cryptographic procedures: Recommendations and key lengths, Part 2 - Use of Transport Layer Security (TLS), Version 2016-01, Bundesamt für Sicherheit in der Informationstechnik.

authentication via mutual TLS. Trust Service Provider connected to the Verimi platform describe the relevant security measures in their Trust Service Practise Statement.

Communication between Verimi GmbH and the Verimi platform takes place via a VPN-secured connection.

Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy. Regular penetration tests are performed by an independent third party for Verimi network components and systems, once a year at minimum.

6.8 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.

In addition, Verimi signs all incoming and outgoing payloads to 3rd party service providers if the payload is not yet signed. So, Verimi is able to prove the integrity and time of receiving or sending.

Systems synchronize their internal time via NTP protocol. Verimi's NTP daemon synchronizes with the public services of the Open Telekom Cloud (OTC) and is installed on the production machines.

7 Certificate, CRL, and OCSP Profiles

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

8 Compliance Audit and Other Assessments

Verimi is subject to regular external audits. These include audits pursuant to ETSI EN 319 401; 319 411-1 and 319 411-2 which are required to prove conformity with the regulations made in eIDAS Chapter III.

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

In addition, Verimi 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 evidence collected during identifications.

The results of these compliance audits are documented and archived. They may be released at the discretion of Verimi 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. Surveillance audits are made 12 months after each full audit.

Additional assessments are required if substantial changes are made to Verimi's 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 Conformity Assessment Body (CAB) that is accredited to operate under eIDAS and that is independent of Verimi.

8.4 Topics Covered by Assessment

The purpose of a compliance audit is to verify that Verimi's 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 Verimi's management in cooperation with the auditor. Verimi's management is responsible for developing and implementing a corrective action plan.

If it is determined that such exceptions or deficiencies pose an immediate threat to 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 Verimi and its business partners.

Verimi 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 users and business partners the regulations of indemnification of German law are binding.

Verimi 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

Verimi maintains a Professional Liability insurance coverage.

9.2.2 Other Assets

No stipulation.

9.3 Confidentiality of Business Information

In addition to Verimi, the requirements of chapter 9.3 also apply to external service provider and outsourcing partner.

9.3.1 Scope of Confidential Information

In the framework of the established, ISO 27001 certified information security management system (ISMS), the level of confidentiality of information is determined. Four levels of confidentiality are distinguished: public, internal, confidential, and strictly confidential. (Strictly) confidential information include in particular any information provided by user for purposes of identity verification.

9.3.2 Information Not Within the Scope of Confidential Information

Documents and other information classified within the ISMS classification scheme as public are not considered confidential/private information.

9.3.3 Responsibility to Protect Confidential Information

All of Verimi's 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 users 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 Verimi is considered not to be private.

9.4.4 Responsibility to Protect Private Information

All employees of Verimi receiving private information are obliged to protect it from compromise and disclosure to third parties.

All employees must adhere to German and European privacy laws.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this TSPS Verimi 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 users is necessary in response to judicial, administrative, or other legal proceedings the information shall be given only to the requesting authority or the users 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

Verimi has overall responsibility for all technical and organizational processes and procedures of its identification services.

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

Verimi 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 and European data protection legislation, all data is stored in encrypted form.

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

9.6.3 Subscriber Representations and Warranties

User warrant that all representations made by Verimi on its website and on its platform are true.

9.6.4 Relying Party Representations and Warranties

Not applicable. Verimi 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 Verimi and its business partners. In any case, limitations of liability contained in Verimi's General Terms of Use (available at https://verimi.de/en/terms-of-use-for-customers/) shall apply. Limitations of Liability as specifically agreed on in each individual case, where applicable, remain unaffected.

Verimi is legally liable for all vicarious agents and subcontractors as for its own actions. Furthermore, Verimi ensures that all vicarious agents and subcontractors used are sufficiently liable to Verimi in accordance with the risk involved. In accordance with the Supplier and Service Provider Policy, it is mandatory to include certain contents or security clauses for the contracts with the provider. The contracts must also take into account the results of risk assessments. Furthermore, the following aspects must be specified:
Definition of the information to be protected; measures and obligations to protect the information (e.g. e-mail encryption) and dealing with security incidents and breaches of the agreement.

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, users and CAs issuing qualified certificates based on the identity verification performed by Verimi may be required to indemnify Verimi for:

- submitting false facts or misrepresenting facts on the user's identity,
- failure to disclose a material fact on the identity verification with intent to deceive any party,
- failure to protect the user'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 user's private data.

9.10 Term and Termination

9.10.1 Term

The TSPS becomes effective upon publication on Verimi's 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 Verimi's 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

No stipulation.

9.12.3 Circumstances under Which OID Must be Changed

Not applicable.

9.13 Dispute Resolution Provisions

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

Complaints regarding Verimi's services can be submitted to service@verimi.com.

As a licensed payment service provider, Verimi is obliged to maintain a complaint management process for consumers according to the guidelines JC 2014 43 27 of the Joint Committee of the European Supervision Authorities. Verimi has extended the scope of this complaint process also to all customer complaints under the field of application of this TSPS.

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 "Vertrauensdienstegesetz" (VDG) implementing the eIDAS regulation in Germany.

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 TSPS is described in section 9.12.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The Verimi 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: Obligation of Service Provider

According to Verimi's policy for suppliers and service providers, the obligations and responsibilities of the service providers and subcontractors used must be precisely defined. Furthermore, all service contracts must contain the following content:

- Rules on the confidential handling and exchange of data and information.
- Return of company assets.
- Rules on the admissibility of subcontracting.
- Reliable delivery of products.
- Service level (SLA).
- Dealing with security incidents and breaches of agreement.
- Ownership of assets
- Measures to protect information.
- Definition of the information to be protected.
- Audit rights of Verimi.
- The service provider shall establish and maintain a set of rules for their task.
- The service provider is organizationally and technically capable of performing their tasks on the basis of the set of rules.
- All applicable BSI Technical Reports, guidelines and relevant standards are complied with by the body. This applies in particular to compliance with the requirements of ISO 27001 and BSI IT-Grundschutz. The certification covers all systems and components relevant for the activity in your authentication process.
- The service provider has sufficient resources to perform its tasks and, if necessary, to assume the liability arising from the tasks.
- If the service provider uses external third parties (subcontractors) to perform the assigned tasks, these third parties must be known to Verimi and must have at least the same level of trust as the body.
- If a licence is required to provide the service, this must be verified.

10 Document Maintenance

Document Name:	Verimi Trust Services Practice Statement
Language:	Englisch
English Title:	Verimi Trust Services Practice Statement
Translation:	
Classification:	Public
Categorie (Level):	
Author:	Dirk Woywod, Verimi GmbH
Contact:	Dirk Woywod
Date of entry into force:	25.04.2024
Last Review:	25.04.2024
Next Review:	25.04.2025

11 Document History

Version	Date	Responsible	Reason for Change
0.1	31.07.2019	Timo Neumann	Document created
0.5	29.08.2019	Timo Neumann	Initial Draft
0.7	01.10.2019	Timo Neumann	Completion of initial draft
0.71	02.10.2019	Arno Fiedler	Review
0.9	10.10.2019	Timo Neumann	Quality Assurance
1.0	14.10.2019	Timo Neumann	Release Version
1.1	14.01.2020	Arno Fiedler	Update based on auditor feedback
1.2	17.01.2020	Arno Fiedler	Editorial changes
2.0	16.03.2020	Andreas Schmidt	Update based on auditor feedback
3.0	15.10.2020	Bernd Löffeld	Change of the Trusted Zone
3.1	28.02.2022	Dirk Woywod	Update Time Stamping
3.2	29.03.2022	André Petzold	Update Ident Methods and White Paper
3.2	30.05.2022	Dirk Woywod	Clarification Certificate Usage
4.0	24.03.2023	Timo Neumann, Dirk Woywod	Inclusion of Ident for Legal Entities
4.1	30.05.2023, 19.06.2023, 22.06.2023	Dirk Woywod, Markus Kässer	Update based on Auditor Feedback
4.2	02.08.2023	Markus Kässer	Update 3.2.3. IV. and 6.5.1 to current conditions
4.3	18.10.2023	Markus Kässer	Update 3.2.3. IV. and 1.3.2 for Go-Live of Legal Entities

4.4	28.03.2024	Markus Kässer	Update 5.3.4, 6.5 and 6.5.1. based on Auditor Feedback
4.5	25.04.2024	Markus Kässer	Update 1.1, 6. and deleted 10 based on Auditor Feedback