Identity Proofing Service Practice Statement - IPSPS

POS Solutions GmbH

v1.0

SIGNATURINFORMATION	**Unterzeichner**	BERNT VOSSEBEIN
	Datum/Zeit-UTC	2026-02-18T08:55:35+01:00
	Prüfung	Siehe http://www.signaturpruefung.gv.at
Hinweis	Diese Unterschrift ist gemäß EU Verordnung Nr. 910/2014 (eIDAS) der handschriftlichen Unterschrift grundsätzlich rechtlich gleichgestellt.	

General Information

Designation	Identity Proofing Service Practice Statement (IPSPS) of POS Solutions GmbH for the POSident module of the "Trusted Platform Services (TPS)" platform

Version	1.0
Date	February 16, 2026
Status	Approved
Next scheduled review	February 15, 2027

Document versions

Date	Version	Editor	Comment
February 16, 2026	1.0	Bruno Reisinger Bernt Vossebein	Initial document

CONTENTS

1 Purpose, scope, and target audience

1.1 Purpose of the document

This Identity Proofing Service Practice Statement (hereinafter IPSPS) describes the organizational and technical procedures used by POS Solutions GmbH (hereinafter IPSP) to perform identity checks on natural persons on behalf of Trust Service Providers/Qualified Trust Service Providers (hereinafter TSP/QTSP) or other clients using the POSident module of the "Trusted Platform Services (TPS)" platform on behalf of Trust Service Providers/Qualified Trust Service Providers (hereinafter referred to as TSP/QTSP) or other clients.

The document serves as proof and description of the implementation of the requirements of Art. 24(1)c eIDAS2 2024/1183, the relevant implementing acts, and the relevant ETSI specifications, in particular ETSI 119 461 v2.1.1 (2025-02) and

ETSI EN 319 401 V3.1.1 (2024-06). It forms the basis for conformity assessments by a Conformity Assessment Body (hereinafter CAB).

1.2 Scope

This IPSPS applies to all IPSP identity proofing processes used for identity verification prior to the issuance of qualified certificates or comparable services. The procedures are designed to achieve a Level of Identity Proofing (LoIP) "Extended" in accordance with ETSI 119 461 v2.1.1 (2025-02).

The following use cases according to ETSI 119 461 v2.1.1 (2025-02) are covered:

- UC1: 9.2.2 Use cases using an identity document for attended remote identity proofing
  - POSident VIDEOIDENT
- UC2: 9.2.3 Use cases using an identity document for unattended remote identity proofing
  - POSident FOTOIDENT chip
- UC3: 9.2.4 Use case for identity proofing by authentication using eID
  - POSident eIDENT – ID Austria
  - POSident eIDENT – German eID – Online ID function

1.3 Target groups

The target groups for this document are in particular:

- Management, information security, data protection, and compliance at the IPSP.
- Customers and partners of the IPSP.

- Clients (TSP/QTSP and other service providers) who use the identity proofing service.
- CAB and supervisory authorities.
- Where applicable, relying parties and end users, insofar as excerpts from the Practice Statement are published.

2 Legal basis , and standards

2.1 EU legal framework

The identity proofing service is based in particular on the following legal acts of the European Union:

• Regulation (EU) No. 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183 ("eIDAS2"), in particular Art. 24(1)c.

• Implementing Act (EU) 2025/1566 on Article 24(1)(c) eIDAS2, including Annex (reference standards for identity proofing).

• General Data Protection Regulation (EU) 2016/679 (GDPR) and ePrivacy Directive 2002/58/EC.

2.2 Standards and specifications

The IPSP implements the following standards in particular:

- ETSI 119 461 v2.1.1 (2025-02): Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI EN 319 401 V3.1.1 (2024-06): Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ISO/IEC 30107-3 Presentation Attack Detection (PAD)
- Injection Attack Detection (IAD) based on the CEN TS 18099 standard - Biometric data injection attack detection

2.3 ENISA methods and implementation guidelines

- ENISA "Methodology for Sectoral Cyber Security Assessments" EU Cyber Security Certification Framework, Sept-2021
- ENISA Implementing Guidance on Commission Implementing Regulation (EU) 2024/2690 of October 17, 2024

3 Roles, actors, and responsibilities

3.1 Identity Proofing Service Provider (IPSP)

Name/company: POS Solutions GmbH

Headquarters: Industriezeile 54, 5280 Braunau am Inn, Austria

Commercial register number: FN 329918 z

Responsible person: Bernt Vossebein, Managing Director

Contact: Email:office@pos.ag , Telephone: +43 7722 67350 8118

Website: https://pos.ag/

3.2 Other relevant roles

3.2.1 /Conformity Assessment Body (CAB)

Name / Company: A-SIT Center for Secure Information Technology – Austria

Headquarters: Seidlgasse 22 / Top 9, 1030 Vienna, Austria

Commercial register number:

Contact: Email:office@a-sit.at , Telephone: +43–1–50319 63–0

Website: https://www.a-sit.at/en/secure-information-technology-center-austria/

3.2.2 National Regulatory Authority – Competent Authority /Policy Authority (PA)

Name/company: Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)

Headquarters: Mariahilfer Straße 77-79, 1060 Vienna, Austria

Commercial register number: 208312t

Contact: Email:rtr@rtr.at Telephone: +43 1 58058-0

Website: https://www.rtr.at/rtr/startseite.de.html

4 Policy management

4.1 Organization that manages the document

This document is published and maintained by the IPSP and must be reviewed annually as part of the ISMS management review and in the event of significant changes (e.g., regulatory requirements, process adjustments) and updated if necessary.

Changes are approved by management and documented with version numbers. Responsibilities for review, approval, and communication are stored in the IPSP's central document control system.

The guideline is stored in the central document management system of POS Solutions GmbH and made available to the relevant stakeholders. Changes are communicated through internal and external communication measures.

4.2 Contact

If you have any questions about this document or other topics, please contact the IPSP at +43 7722 67350 8118 oroffice@pos.ag .

4.3 Suitability of the IPSP for the guideline

The PA (see3.2.2) decides on the suitability of this IPSPS in relation to the certification policy (CP).

4.4 IPSPS Approval Process

The final decision on the approval of the IPSPS rests with the management of the TSP.

5 Conformity assessment and certificate validity period

5.1 Applicable assessment basis

The identity proofing service is subject to conformity assessment by an accredited CAB. The assessment bases are the underlying EU legal framework (see2.1), the underlying standards and specifications (see2.2), and the relevant ENISA methods and implementation guides (see2.3).

5.2 Conformity assessment body

The conformity assessment of the IPSPS is carried out by the CAB (see3.2.1).

5.3 Audit and monitoring cycle

- Initial certification audit: February 9, 2026 (completion of the first full audit).
- Surveillance audit: No later than 12 months after the actual audit date, in this case by February 9, 2027
- Recertification/full audit: No later than 24 months after the last full audit or in the event of significant changes to the service.

5.4 Validity, suspension, and withdrawal

The validity of the confirmation of conformity is a maximum of 24 months or until revoked by the CAB. The IPSP informs the clients concerned and, if necessary, the competent supervisory authorities.

6 General description of the identity proofing service

6.1 Operation of the identity proofing service

6.1.1 Trusted Platform Services (TPS)

The services listed in the Practice Statement are provided by the POSident module of the TPS platform.

This service platform is a highly flexible platform for implementing point-of-sale services. Applications (both native and web-based) running on tablets, smartphones, tablet PCs, shop PCs, or terminals use its services to efficiently implement sales processes. It is aimed at companies that are striving for an electronic end-to-end (e2e) process because they want to eliminate their paper-based processes.

Basic architecture

The TPS platform is multi-tenant capable and based on a strict layer architecture. The required functions and services are implemented via corresponding modules and specific workflows. These modules and services can be combined and connected in series via a workflow engine. Other important basic functions of the TPS platform are:

- Monitoring and logging functions at various levels for tracking processes and procedures on the server.
- Support for high-availability solutions (load balancing, clustering, etc.).
- Administration and configuration of the entire TPS platform and its modules via the Admin Web UI.

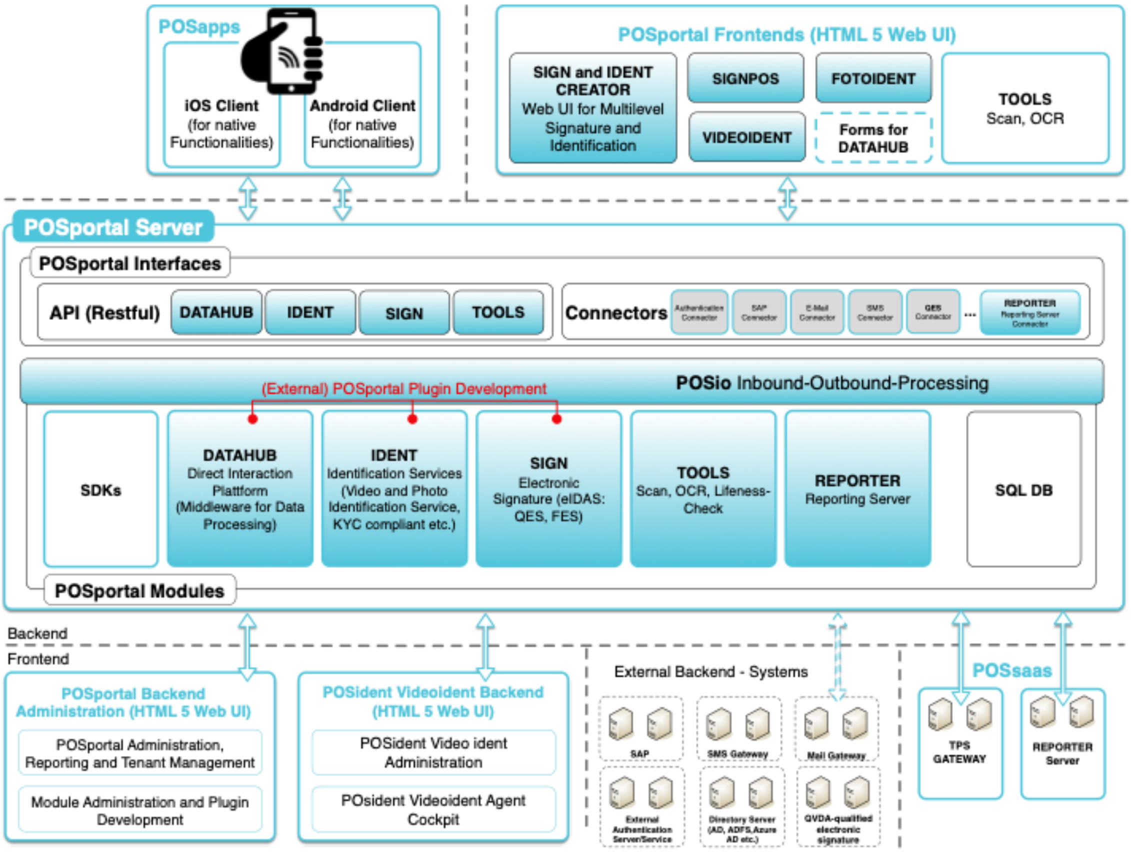
POSapps
iOS Client (for native Functionalities)
Android Client (for native Functionalities)
POSportal Frontends (HTML 5 Web UI)
SIGN and IDENT CREATOR
Web UI for Multilevel Signature and Identification
SIGNPOS
FOTOIDENT
VIDEOIDENT
Forms for DATAHUB
TOOLS
Scan, OCR
POSportal Server
POSportal Interfaces
API (Restful)
DATAHUB
IDENT
SIGN
TOOLS
Connectors
Authentication Connector
SAP Connector
E-Mail Connector
SMS Connector
QES Connector
...
REPORTER
Reporting Server Connector
(External) POSportal Plugin Development
POSio Inbound-Outbound-Processing
SDKs
DATAHUB
Direct Interaction Plattform (Middleware for Data Processing)
IDENT
Identification Services (Video and Photo Identification Service, KYC compliant etc.)
SIGN
Electronic Signature (eIDAS: QES, FES)
TOOLS
Scan, OCR, Lifeness-Check
REPORTER
Reporting Server
SQL DB
POSportal Modules
Backend
Frontend
POSportal Backend Administration (HTML 5 Web UI)
POSportal Administration, Reporting and Tenant Management
Module Administration and Plugin Development
POSident Videoident Backend (HTML 5 Web UI)
POSident Video ident Administration
POsident Videoident Agent Cockpit
External Backend - Systems
SAP
SMS Gateway
Mail Gateway
External Authentication Server/Service
Directory Server (AD, ADFS,Azure AD etc.)
QVDA-qualified electronic signature
POSsaas
TPS GATEWAY
REPORTER Server

Figure1: Architecture diagram of the TPS platform

Trusted Platform Services (TPS) platform – modules

Building on the basic framework, the TPS platform offers a range of modules that can also be combined depending on customer requirements:

- POSdatahub – Data processing platform
  Interface hub for structured data collection and data distribution
- POSident – Online identification
  - VIDEOIDENT: Online remote identification via video chat
  - FOTOIDENT – Systemic auto-identification
    - FOTOIDENT basic – Systemic auto-identification via photo
    - FOTOIDENT plus – Systemic auto-identification via photo and manual verification by an agent
    - FOTOIDENT chip – Systemic auto-identification via photo and ID chip
  - BANKIDENT – Identification via bank account
  - eIDENT – Identification via electronic ID

        - POSident eIDENT – ID Austria
        - POSident eIDENT – German eID – Online ID function
        - POSident eIDENT – ich.app
    - AML – Identification via FOTOIDENT basic and subsequent PSD2 (Payment Services Directive) registration/identity verification.
- POSsign – Module for electronic signatures
- POStools – Integration of useful additional functions
- POStx – Live reporting

6.2 Operation of the POSportal server in the POS Solutions GmbH data center

6.2.1 Operation

The operation of the TPS platform in a certified data center within the EU ensures the secure operation of the POSident identification platform.

The data center is ISO/IEC 27001:2022 certified. This ensures that the requirements for the planning, implementation, monitoring, and improvement of information security management (ISMS) in the data center are implemented in accordance with the secure operation of the platform.

6.2.2 Security analyses of the data center

6.2.2.1 Procedure

To ensure secure operation, an infrastructure pentest and an application pentest are carried out once a year by an external certified testing laboratory. In addition, a security scan is carried out once a quarter by an external service provider.

The penetration tests reveal vulnerabilities within the environment and the application and demonstrate the effects and consequences of an attack. The test verifies whether the existing security controls are effective and adequately meet the requirements of a system in terms of CIA (confidentiality, integrity, availability). The testing process involves actively analyzing the environment for vulnerabilities. The specific test cases vary depending on the scenario and the associated permissions.

6.2.2.2 Categories of security analysis

The security analysis focuses on the following categories.

Authentication and authorization problems

In the worst case, critical services may not require any authentication at all, or the authentication scheme used may be circumvented. This can result in critical data or functions being accessible to attackers without any further preventive security controls. On the other hand, services may not check, or may only inadequately check, a user's authorization to access or modify resources. As a result, users can bypass the authorization scheme and least privilege principles and either increase their privileges (vertical privilege escalation) or pretend to be someone else (horizontal privilege escalation, spoofing).

Misconfiguration

A security misconfiguration is often the result of services that are not adequately adapted to a specific environment, that have not been explicitly hardened, or of services that are not suitable for productive use. For example, services that should only be accessible via special interfaces, such as from a management LAN, can often be found and used. An example of a lack of hardening would be a network share that does not require SMB signing, or the use of a protocol that cannot guarantee the confidentiality and integrity of a service (e.g., Telnet). Standard passwords for a component that have not been changed before production use are another example. Such vulnerabilities are usually easy for attackers to discover and exploit.

Outdated components with known vulnerabilities

Services and applications that have not been patched are often affected by known security vulnerabilities. They can often be easily exploited, either because no exploit is required for exploitation or because exploits have already been made public. Vulnerabilities in this category are usually a symptom of ineffective patch and vulnerability management and an incomplete or inaccurate asset inventory. Sometimes components have already reached the end of their support lifecycle (EoL) and there may be no (security) updates available at all

available at all. Although exploits for certain vulnerabilities may not be publicly available, attackers may have already developed or acquired them.

Information Disclosure

Information systems and services sometimes provide information that is helpful to an attacker.

Although information disclosure is often the result of another vulnerability, it can also be a vulnerability category in its own right. For example, a web service may be programmed to return more data than is necessary and expected. Another example would be an LDAP service that returns passwords stored in a description field. The information gained helps attackers increase their privileges, access other systems, or improve their knowledge of a system and carry out further attacks even more effectively.

Inadequate network segmentation

Segmentation tests ensure that the controls separating different network zones from each other are effective and functioning as intended. For example, environments may be vulnerable to VLAN hopping attacks. Sometimes they can even be bypassed directly, e.g., if VLANs are routed or components that have interfaces in multiple zones (e.g., NAS or time servers) can be misused as gateways or pivoting systems.

7 Supported identity proofing use cases

7.1 General

According to section1.2 , the following use cases are covered in IPSPS according to ETSI 119 461 v2.1.1 (2025-02):

- UC1: 9.2.2 Use cases using an identity document for attended remote identity proofing
  - POSident VIDEOIDENT
- UC2: 9.2.3 Use cases using an identity document for unattended remote identity proofing
  - POSident FOTOIDENT chip
- UC3: 9.2.4 Use case for identity proofing by authentication using eID
  - POSident eIDENT – ID Austria
  - POSident eIDENT – German eID – Online ID function

7.2 Types of data

7.2.1 Basic data

During the identity verification process, the following basic personal data is collected and verified for all use cases listed.

The following data is either read from the ID document (UC1, UC2) or returned by the eID authentication (UC3):

- First name
- Last name
- Nationality
- Date of birth
- Mobile number

7.2.2 Additional data UC 1, UC2

For these two use cases, the following data is also read from the ID card and checked:

- ID type
- ID card number
- Expiration date
- Date of issue

- Issuing authority
- Place of birth
- ID images (depending on the ID, front or front + back)
- Live image from video stream (UC1) or live image from liveness detection (UC2)
- Portrait photo taken during the identity verification process

7.2.3 Additional data UC 3

The following additional data is collected for eID authentication:

- Type of eID (ID Austria or German eID)
- eIDAS Level of Assurance/Required security level (only permissible valuehttp://eidas.europa.eu/LoA/high
- Unique personal identification number in the context of the respective eID (see7.7)
- Process-specific eID assertion in the context of the respective eID (see7.7)

7.3 Supported identification documents

The identity verification services from UC1 and UC2 generally accept passports or identity cards that comply with the International Civil Aviation Organization (ICAO 9303) standard regarding the use of NFC and visual inspection zones. Driver's licenses are excluded with the exception of Austrian driver's licenses (UC1 only).

List of supported ID documents depending on the use case:

- UC1: according to SLA.
- UC2: UC2 only supports passports and ID cards with chips that comply with ICAO specification "Doc 9303 - Machine Readable Travel Documents - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)".
- UC3 - POSident eIDENT German eID – German identity card with online function and EUDI wallet, if available.

7.4 Availability of services

The availability of the identity verification service for UC1 is regulated in the Service Level Agreement (SLA) in the partner agreement. According to the current agreement, the service is available between 7:00 a.m. and 10:00 p.m.

The identity verification services for UC2 and UC3 are not restricted to any specific time. They are available around the clock.

7.5 UC1 - Use cases using an identity document for attended remote identity proofing

In the context of use case UC1, the identity verification process is carried out using the TPS procedure "POSident VIDEOIDENT" with a certified third-party provider.

The video identification provider offers a certified "eIDAS2"-compliant process for identifying natural persons for the issuance of qualified certificates, which is used in the POSident VIDEOIDENT module.

The IPSP has a corresponding partner agreement with the video identification provider, which ensures the proper execution of video identifications in accordance with Regulation (EU) No. 910/2014, as amended by (EU) 2024/1183.

For this procedure, the corresponding software components, standard interfaces, and standard integration scenarios of the third-party provider are used for identification. This means:

- Video identification is carried out in the third-party provider's call center.
- The AML-trained agents use the third-party provider's agent cockpit.
- The identification process is carried out in accordance with the third-party provider's certified process.
- The third-party provider's components are used to identify the person.
- Use of a third-party identification app or web-based solution.
- Integration of the third-party process into POSident's own video identification app using the third-party SDK for iOS and Android.

The identification process is started by selecting the "VIDEOIDENT" method in the POSident selection menu. The natural person to be identified is then forwarded to the video identification process. After completion of the process, a redirect to the POSident module takes place.

The rest of the process, in particular the transmission of data to the QTSP for the issuance of the qualified certificate, is carried out as described in the section "8 ."

The third-party provider is listed as permitted in the RA contract with the QTSP provider.

7.6 UC2 - Use cases using an identity document for unattended remote identity proofing POSident

The "POSident FOTOIDENT chip" procedure is used for use case UC2.

In this procedure, the ID data is read from the chip of the ID document during the photo identification process.

In the case of an ID document with a chip, the personal data is stored on the chip of the ID document in accordance with ICAO specification "Doc 9303 - Machine Readable Travel Documents - Part 10: Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)".

In the "POSident FOTOIDENT chip" process, data groups DG1, DG11, DG12, and DG14 are read.

To ensure that there has been no manipulation, a check is performed to verify that the data has been signed with the corresponding Country Signing Certification Authority (CSCA) certificate, which is set up by each country that issues e-ID cards.

The entire process is described in the "POSident FOTOIDENT chip" end-user documentation (see section13 References).

For facial comparison and liveness detection, a platform certified according to "ISO/IEC 30107-3 Presentation Attack Detection (PAD)" is used, which is installed in the IPSP's data center.

The relevant certificates and evidence are available to the CAB.

Systematic tests on the values

- APCER - Attack Presentation Classification Error Rate
- BPCER - Bona Fide Presentation Classification Error Rate
- FAR - False Acceptance Rate
- FRR - False Rejection Rate

were carried out in accordance with ISO/IEC 30107-3 and ISO/IEC 19795-1. The relevant evidence is available to the conformity assessment body.

The following values are defined as target values:

- APCER: 0.5%
- BPCER: 0.1%
- FRR: 2%
- FAR: 0.5%

In December 2025, a penetration test was carried out as part of the regular penetration tests, in which the CEN/TS 18099-2024 standard for injection attack detection (IAD) was also included in the scope of the test. The corresponding test report is also available to the conformity assessment body.

An injection attack detection test carried out by a CEN TS 18099-accredited laboratory will be submitted by the end of 2026 at the latest.

7.7 UC 3 - Use case for identity proofing by authentication using eID

For use case UC3, the "POSident eIDENT ID Austria" and "POSident eIDENT German eID - Online ID function" procedures are used.

According to the current eIDAS Regulation (EU) No. 910/2014 (eIDAS), as amended by (EU) 2024/1183, "electronic identity - e-ID" meets the requirements for issuing a qualified certificate if the assurance level of identification is "high" (see Articles 6–12 and Art. 24(1)c).

After identification by means of eID, the relevant data listed in the section7.2 is transmitted to the QTSP for the issuance of the qualified certificate (see section8).Types of data

7.7.1 POSident eIDENT ID Austria

The POSident module uses the central eIDAS node of the Republic of Austria (see https://www.id-austria.gv.at/de/developer/anbinden/anbindung-mit-openid-connect) to identify the person via ID Austria.

After identification has been carried out, the security level is checked in the response structure, which is then also transmitted to the QTSP for the issuance of the qualified certificate. The return of the security level is defined in the specification https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html.

Communication with the central eIDAS accounts takes place via SSL/TLS using the OpenID Connect (OIDC) authentication protocol.

The IPSP has the appropriate accreditation, which allows it to use ID Austria as identification for natural persons for the issuance of qualified certificates.

7.7.2 POSident eIDENT German eID – online ID function

For this procedure, identity verification is carried out using the certified solution "Online ID function with eID". This identification method meets the relevant security level requirements (Assurance Level) and is certified by the BSI (German Federal Office for Information Security) in accordance with BSI TR-03128, meaning that a qualified certificate may be issued on the basis of the identification.

Identification via the German ID card with online function is carried out via an iOS or Android app.

8 Issuance of the qualified certificate by a qualified trust service provider ( ) – QTSP

For the use cases UC1, UC2, and UC3 described above, the qualified certificates are issued by an eIDAS-compliant QTSP. As part of the integrated QTSP signature dialog (native to the respective QTSP), the user enters into a direct contractual relationship with the respective QTSP.

The standard "ETSI EN 319 411-2 v.2.3.1 (2021-05) - 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" defines the relevant requirements for qualified certificates for electronic signatures.

All data required for issuing a qualified certificate is transferred via a secure interface provided by the QTSP. To ensure the authenticity and integrity of all identification data transmitted to the QTSP, it is packaged in a JSON structure defined by the QTSP and signed with a certificate stored on the TPS platform. By storing the associated public key on the QTSP server, both the origin and authenticity of the data can be ensured.

The certificate to be used here is based on the ECC-256 procedure and is provided by the QTSP.

The respective data transferred for the individual use cases UC1, UC2, and UC3 are listed in the section "7.2 ."

The following graphic shows the certificate issuance process using the example of the eIDAS-compliant QTSP Primesign/CRYPTAS it-Security GmbH.

The certificate itself is then issued using the process specified by the QTSP.

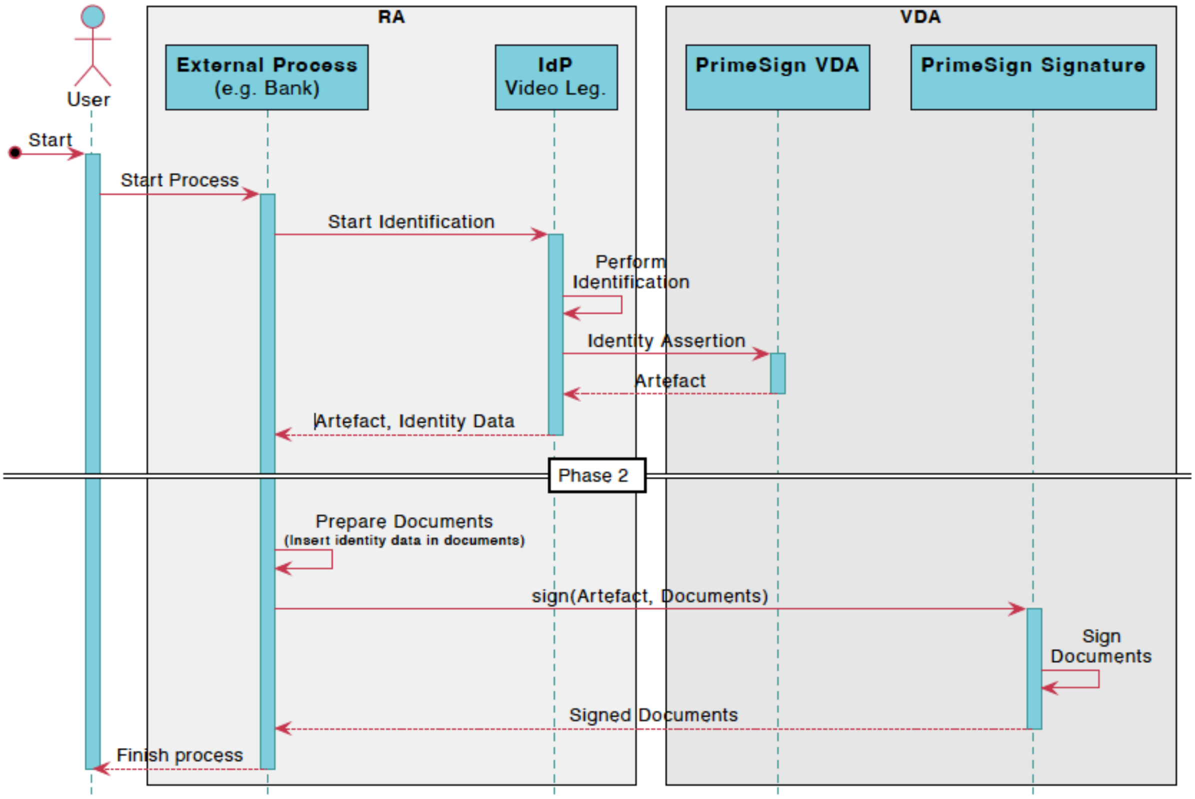

Figure2: Example of the PrimeSign OneTime certificate issuance process (simplified).

9 Obligations

9.1 Acting in accordance with the IPSPS

The IPSP and all third-party providers are obliged to act in accordance with the IPSPS and to undergo internal and external audits to verify and ensure compliance with regulations or policies.

For service providers, this means, in particular, compliance with the relevant requirements of Regulation (EU) No. 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183 ("eIDAS2").

Controls A.5.19 and A.5.34 of Annex A to ISO/IEC 27001:2022 ensure that information security risks arising from supplier relationships are systematically identified, assessed, addressed contractually, monitored, and controlled.

9.2 Announcement of termination of identification activities

The IPSP has established procedures to ensure the orderly, transparent, and traceable termination of identification activities.

The termination of the provision of identification services shall be based exclusively on a formal decision by the IPSP and shall be notified in writing to all affected contractual partners, supervisory authorities, and other relevant bodies **at least three (3) months in advance**. The notification shall include at least the planned termination date, the scope of the identification services affected, and information on transition and settlement measures.

10 Security requirements

POS Solutions GmbH operates an information security management system covering information security, business continuity, cybersecurity, data protection, etc., which is certified according to the ISO/IEC 27001:2022 standard.

For further information, see https://pos.ag/media/342p12e4/isms-policy_web.pdf.

Further information on the ISO/IEC 27001:2022 certification of POS Solutions GmbH: https://pos.ag/plattform/pos-solutions-gmbh/iso27001-zertifizierung/.

The following section documents the implementation of the individual security requirements by referring to the corresponding points of the "ISO/IEC 27001:2022" standard as well as the respective controls from Annex A.

All controls are applicable and fully implemented. The implementation of the controls is documented in the SoA document (Statement of Applicability) of the ISO/IEC 27001-ISMS. The SoA document "POS_Solutions_GmbH_SoA_ISO27001_2025.pdf" is referenced in the section13 .

10.1 Organizational measures

Within the framework of the information security management system (ISMS), the "Organizational measures" (A.5.1–A.5.37) of ISO/IEC 27001:2022 Annex A are implemented. These controls address, among other things, the classification of information (document control), access rights, supplier management, handling of information security incidents, control of legal requirements, and documented operating procedures.

10.2 Physical security requirements

Within the framework of the information security management system (ISMS), the physical security requirements are implemented in accordance with the "Physical Measures" (A.7.1–A.7.14) of ISO/IEC 27001:2022 Annex A. These controls address physical perimeters, access controls, monitoring, protection against environmental hazards, equipment placement, media storage, and secure disposal.

10.3 Procedures/Processes/Workflows

As part of our ISMS, we implement the requirements for documented processes and procedures in accordance with ISO/IEC 27001:2022 Annex A Control "A.5.37 – Documented operational procedures". In addition, other Annex A controls (e.g., A.5.1, A.5.2, A.5.24–A.5.27, A.5.36) address organizational and operational security-related process elements that are relevant for the consistent and secure execution of services.

10.4 Personnel security

Personnel security requirements are implemented in accordance with ISO/IEC 27001:2022 Annex A Controls "Personnel Measures" (A.6.1 – A.6.8). These controls cover the areas of security screening, employment and contract terms, information security awareness, education, training, disciplinary process, responsibilities upon termination or change of employment, confidentiality or non-disclosure agreements, remote work, and reporting of information security incidents.

10.5 Audit Logging

As part of our ISMS, we implement the ISO/IEC 27001:2022 Annex "A 8.15 – Logging" control to log, store, protect, and analyze security-related events, system activities, and exceptions.

In addition, controls "A.8.16 – Monitoring of Activities" and "A.8.17 – Clock Synchronization" are taken into account to ensure the integrity, consistency, and monitorability of the logs.

As part of the identity verification service, the following events are recorded in the audit log:

- Unique internal identification GUID and optional external identification number
- Start of the identity verification process – timestamp
- Data processed depending on the identity proofing use case
- Events relevant to identity verification, including timestamp
- Verification of data and evidence
- Acceptance or rejection of the identity verification

An audit log is recorded for each identification process in accordance with Section7 . Among other things, this log also serves as proof of the contractual activities vis-à-vis the QTSP. The audit log and the associated logs are retained for three months as evidence for internal and external audits.

According to the Austrian Signature and Trust Services Act (SVG) – § 10, the QTSP is obliged to keep the documentation for certificate issuance for 30 years.

11 Other business and legal matters

11.1 Applicable general terms and conditions

The IPSP's general terms and conditions are published on the website at https://pos.ag/media/nyhndidt/pos_solutions_gmbh_agb_webseite_de.pdf.

11.2 Data protection

As part of our ISMS, we base data protection and the protection of personal data on the relevant controls in ISO/IEC 27001:2022 Annex A. Measures implemented include control "A.5.34 - Data protection and protection of personal data - PII" and supplementary controls A.5.12 – A.5.18 for the classification and labeling of information, information control, information transmission, access control, identity management, authentication information, and access rights, as well as controls A.8.10 – A.8.12, which cover the areas of data deletion, data masking, and the prevention of data leaks.

The current IPSP privacy policy is referenced on the website –https://pos.ag/datenschutz/.

11.3 Limitations of liability

The limitations of liability are contained in the General Terms and Conditions published on the website (see11.1).

11.4 Dispute resolution

In the event of a dispute between IPSP and a customer or between IPSP and a third party, the management of IPSP shall decide after hearing all parties involved and taking all interests into account. The decision shall be recorded in writing and communicated within a reasonable period of time. This procedure does not restrict the possibility of settling disputes in court.

Complaint management is regulated in the General Terms and Conditions published on the website (see11.1).

11.5 Applicable law

The activities of the IPSP are subject to Austrian law and Regulation (EU) No. 910/2014 (eIDAS), as amended by Regulation (EU) 2024/1183 ("eIDAS2").

12 Definitions and abbreviations

Abbreviation	Definition
CAB	Conformity Assessment Body
CP	Certificate Policy
IPSP	Identity Proofing Service Provider
IPSPS	Identity Proofing Service Practice Statement
PA	Policy Authority
QTSP	Qualified Trust Service Provider
TPS	Trusted Platform Services
TSP	Trust Service Provider

13 References

List of current references:

- Further information on the ISO/IEC 27001:2022 certification of POS Solutions GmbH: https://pos.ag/plattform/pos-solutions-gmbh/iso27001-zertifizierung/.
- ISMS Policy: https://pos.ag/media/342p12e4/isms-policy_web.pdf.
- SoA document of the ISO/IEC 27001-ISMS
  POS_Solutions_GmbH_SoA_ISO27001_2025.pdf
- End User Documentation POSident FOTOIDENT chip
  End User Documentation POSident FOTOIDENT chip for Android v1.1
  End User Documentation POSident FOTOIDENT chip for iOS v1.1
  End User Documentation POSident FOTOIDENT chip for PC v1.1