Identity Proofing Service Practice Statement - IPSPS

POS Solutions GmbH

v1.0

SIGNATURINFORMATION	**Unterzeichner**	BERNT VOSSEBEIN
	Datum/Zeit-UTC	2026-02-18T08:54:43+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.	

POS Solutions GmbH - Industriezeile 54 - A-5280 Braunau (Inn)
office@pos.ag - www.pos.ag

Allgemeine Angaben

Bezeichnung	Identity Proofing Service Practice Statement (IPSPS) der POS Solutions GmbH für das POSident Modul der „Trusted Platform Services (TPS)“ Plattform

Version	1.0
Datum	16.02.2026
Status	Freigegeben
Nächste planmäßige Überprüfung	15.02.2027

Dokumenten Versionen

Datum	Version	Bearbeiter	Kommentar
16.02.2026	1.0	Bruno Reisinger Bernt Vossebein	Initialdokument

INHALT

1 Zweck, Geltungsbereich und Zielgruppe

1.1 Zweck des Dokumentes

Dieses Identity Proofing Service Practice Statement (nachfolgend IPSPS) beschreibt die organisatorischen und technischen Verfahren, mit denen die POS Solutions GmbH (nachfolgend IPSP) mit dem POSident Modul der „Trusted Platform Services (TPS)“ Plattform Identitätsprüfungen von natürlichen Personen im Auftrag von Trust Service Providern/Qualified Trust Service Providern (nachfolgend TSP/QTSP) oder anderen Auftraggebern durchführt.

Das Dokument dient als Nachweis und Beschreibung der Umsetzung der Anforderungen aus Art. 24(1)c eIDAS2 2024/1183, der einschlägigen Durchführungsrechtsakte sowie der einschlägigen ETSI-Spezifikationen, insbesondere ETSI 119 461 v2.1.1 (2025-02) und

ETSI EN 319 401 V3.1.1 (2024-06). Es bildet die Grundlage für Konformitätsbewertungen durch eine Konformitätsbewertungsstelle/Conformity Assessment Body (nachfolgend CAB).

1.2 Geltungsbereich

Dieses IPSPS gilt für alle Identity-Proofing-Prozesse des IPSP, die zur Identitätsprüfung vor Ausstellung von qualifizierten Zertifikaten oder vergleichbaren Diensten eingesetzt werden. Die Verfahren sind so ausgelegt, dass sie ein Level of Identity Proofing (LoIP) „Extended“ nach ETSI 119 461 v2.1.1 (2025-02) erreichen.

Folgende Use Cases nach ETSI 119 461 v2.1.1 (2025-02) werden abgedeckt:

- 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 Ausweisfunktion

1.3 Zielgruppen

Die Zielgruppen dieses Dokuments sind insbesondere:

- Management, Informationssicherheit, Datenschutz und Compliance des IPSPs.
- Kunden und Partner des IPSPs.

- Auftraggeber (TSP/QTSP und andere Dienstanbieter), die den Identity-Proofing-Dienst nutzen.
- CAB und Aufsichtsbehörden.
- Ggf. „Relying Parties“ und Endnutzer, soweit Auszüge des Practice Statements veröffentlicht werden.

2 Rechtsgrundlagen und Standards

2.1 EU-Rechtsrahmen

Der Identity-Proofing-Dienst orientiert sich insbesondere an folgenden Rechtsakten der Europäischen Union:

• Verordnung (EU) Nr. 910/2014 (eIDAS), in der Fassung der Verordnung (EU) 2024/1183 („eIDAS2"), insbesondere Art. 24(1)c.

• Durchführungsrechtsakt (EU) 2025/1566 zu Art. 24(1)c eIDAS2 einschließlich Anhang (Referenzstandards für Identity Proofing).

• Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) und ePrivacy-Richtlinie 2002/58/EG.

2.2 Standards und Spezifikationen

Der IPSP setzt insbesondere folgende Standards um:

- 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) auf Basis des Standard CEN TS 18099 - Biometric data injection attack detection

2.3 ENISA Methoden und Implementierungsleitfäden

- 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 17.10.2024

3 Rollen, Akteure und Verantwortlichkeiten

3.1 Identitätsprüfungsdienstleister/Identity Proofing Service Provider (IPSP)

Name / Firma: POS Solutions GmbH

Sitz: Industriezeile 54, 5280 Braunau am Inn, Österreich

Firmenbuch-/Handelsregisternummer: FN 329918 z

Verantwortlicher: Bernt Vossebein, Geschäftsführer

Kontakt: E-Mail: office@pos.ag, Telefon: +43 7722 67350 8118

Website: https://pos.ag/

3.2 Weitere relevante Rollen

3.2.1 Konformitätsbewertungsstelle/Conformity Assessment Body (CAB)

Name / Firma: A-SIT Zentrum für sichere Informationstechnologie – Austria

Sitz: Seidlgasse 22 / Top 9, 1030 Wien, Österreich

Firmenbuch-/Handelsregisternummer:

Kontakt: E-Mail: office@a-sit.at, Telefon: +43–1–50319 63–0

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

3.2.2 Nationale Aufsichtsstelle – Zuständige Behörde/Policy Authority (PA)

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

Sitz: Mariahilfer Straße 77-79, 1060 Wien, Österreich

Firmenbuch-/Handelsregisternummer: 208312t

Kontakt: E-Mail: rtr@rtr.at Telefon: +43 1 58058-0

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

4 Verwaltung von Richtlinien

4.1 Organisation, die das Dokument verwaltet

Dieses Dokument wird vom IPSP veröffentlicht und gepflegt und ist jährlich im Rahmen des ISMS-Management Reviews sowie bei signifikanten Änderungen (z. B. regulatorische Anforderungen, Prozessanpassungen) zu überprüfen und ggf. zu aktualisieren.

Änderungen werden von der Geschäftsführung freigegeben und versioniert dokumentiert. Die Zuständigkeiten für Überprüfung, Freigabe und Kommunikation sind in der zentralen Dokumentenlenkung des IPSPs hinterlegt.

Die Richtlinie wird im zentralen Dokumentenmanagementsystem der POS Solutions GmbH abgelegt sowie den relevanten Stakeholdern zur Verfügung gestellt. Änderungen werden durch interne und externe Kommunikationsmaßnahmen kommuniziert.

4.2 Ansprechpartner

Bei Fragen zu diesem Dokument oder anderen Themen kann der IPSP unter +43 7722 67350 8118 oder office@pos.ag kontaktiert werden.

4.3 Eignung des IPSPS für die Richtlinie

Die PA (siehe 3.2.2) entscheidet über die Eignung dieses IPSPS in Bezug auf die Zertifizierungsrichtlinie (CP).

4.4 IPSPS-Genehmigungsverfahren

Die endgültige Entscheidungsgewalt über die Genehmigung des IPSPS liegt bei der Geschäftsführung des TSP.

5 Konformitätsbewertung und Zertifikatslaufzeit

5.1 Anwendbare Bewertungsgrundlage

Der Identity-Proofing-Dienst unterliegt einer Konformitätsbewertung durch einen akkreditierten CAB. Bewertungsgrundlagen sind der zu Grunde liegende EU-Rechtsrahmen (siehe 2.1), die zu Grunde liegenden Standards und Spezifikationen (siehe 2.2) sowie die relevanten ENISA Methoden und Implementierungsleitfäden (siehe 2.3).

5.2 Konformitätsbewertungsstelle

Die Konformitätsbewertung des IPSPS wird durch den CAB vorgenommen (siehe 3.2.1).

5.3 Audit- und Überwachungszyklus

- Initiales Zertifizierungsaudit: 09.02.2026 (Abschluss des ersten Vollaudits).
- Überwachungsaudit: Spätestens 12 Monate nach dem tatsächlichen Audit-Termin, hier bis 09.02.2027
- Re-Zertifizierung / Vollaudit: Spätestens 24 Monate nach dem letzten Vollaudit oder bei wesentlichen Änderungen des Dienstes.

5.4 Gültigkeit, Aussetzung und Entzug

Die Gültigkeit der Konformitätsbestätigung beträgt maximal 24 Monate oder bis zum Widerruf durch den CAB. Der IPSP informiert die betroffenen Auftraggeber und – sofern erforderlich – zuständige Aufsichtsbehörden.

6 Allgemeine Beschreibung des Identity-Proofing-Dienstes

6.1 Betrieb des Identity-Proofing-Dienstes

6.1.1 Trusted Platform Services (TPS)

Die im Practice Statement angeführten Dienste werden durch das POSident Modul der TPS-Plattform zur Verfügung gestellt.

Diese Services-Plattform ist eine hoch flexible Plattform zur Implementierung von “Point of Sale” Diensten. Applikationen (native als auch web-basierte), die auf Tablets, Smartphones, Tablet-PCs, Shop-PCs oder Terminals laufen, nutzen dessen Dienste zur effizienten Umsetzung von Sales Prozessen. Es werden damit Unternehmen adressiert, die einen elektronischen End-to-Endprozess (e2e) anstreben, weil sie ihre papierbasierten Prozesse eliminieren wollen.

Basis Architektur

Die TPS-Plattform ist mandantenfähig und basiert auf einer strikten Layer Architektur. Die erforderlichen Funktionen und Dienste werden über entsprechende Module und spezifische Workflows realisiert. Über eine Workflow Engine können diese Module und Dienste kombiniert und hintereinandergeschaltet werden. Weitere wichtige Basisfunktionen der TPS-Plattform sind:

- Monitoring und Logging-Funktionen auf verschiedenen Ebenen zum Nachvollziehen der Prozesse und Abläufe am Server.
- Unterstützung von Hochverfügbarkeitslösungen (Load-Balancing, Clustering etc.).
- Administration und Konfiguration der gesamten TPS-Plattform und dessen Module über das Admin-Web-UI.

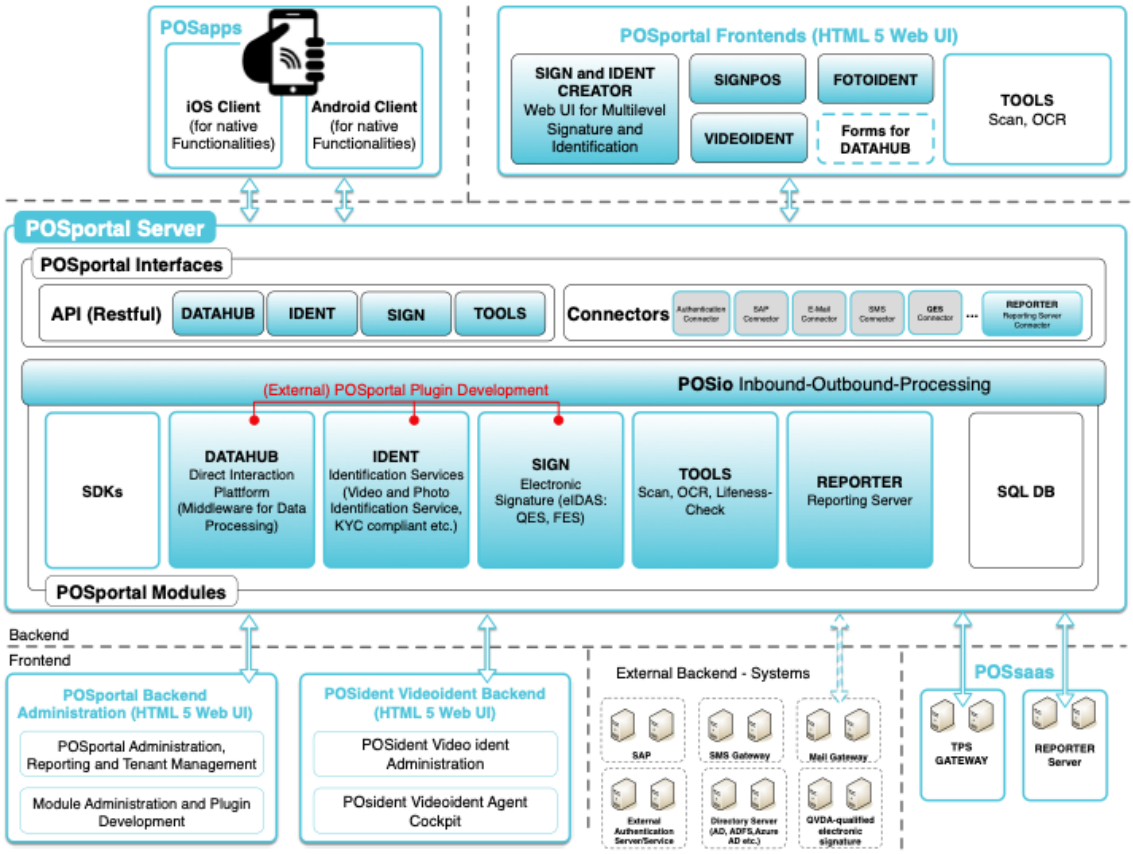

Abbildung 1: Architekturdiagramm der TPS-Plattform

„Trusted Platform Services (TPS)“ Plattform – Module

Aufbauend auf dem Basis Framework bietet die TPS-Plattform eine Reihe von Modulen, die je nach Kundenanforderung auch kombiniert werden können:

- POSdatahub - Data-Processing-Platform
  Schnittstellendrehscheibe zur strukturierten Datenerfassung und Datenverteilung
- POSident - Online Identifikation
  - VIDEOIDENT: Online-Remote-Identifizierung per Video-Chat
  - FOTOIDENT – Systemische Autoidentifikation
    - FOTOIDENT basic – Systemische Autoidentifikation per Foto
    - FOTOIDENT plus – Systemische Autoidentifikation per Foto und manueller Nachkontrolle durch einen Agenten
    - FOTOIDENT chip – Systemische Autoidentifikation per Foto und Ausweischip
  - BANKIDENT - Identifizierung über den Bank-Account
  - eIDENT - Identifikation mittels elektronischer ID

        - POSident eIDENT – ID Austria
        - POSident eIDENT – German eID – Onlineausweisfunktion
        - POSident eIDENT – ich.app
    - AML – Identifizierung mittels FOTOIDENT basic und nachfolgender PSD2 (Payment Services Directive) Anmeldung / Identitätsprüfung.
- POSsign – Modul zur elektronischen Signatur
- POStools – Einbindung von nützlichen Zusatzfunktionen
- POStx – Live Reporting

6.2 Betrieb des POSportal Servers im Rechenzentrum der POS Solutions GmbH

6.2.1 Betrieb

Durch den Betrieb der TPS-Plattform im zertifizierten Rechenzentrum innerhalb der EU ist ein sicherer Betrieb der Identifizierungsplattform POSident gewährleistet.

Das Rechenzentrum ist ISO/IEC 27001:2022 zertifiziert. Dies gewährleistet, dass die Anforderungen für die Planung, Implementierung, Überwachung und Verbesserung des Informationssicherheitsmanagements (ISMS) im Rechenzentrum zum sicheren Betrieb der Plattform entsprechend umgesetzt sind.

6.2.2 Sicherheitsanalysen des Rechenzentrums

6.2.2.1 Vorgehen

Zur Gewährleistung des sicheren Betriebs wird einmal jährlich durch ein externes zertifiziertes Prüflabor ein Infrastruktur-Pentest sowie ein Applikations-Pentest durchgeführt. Zusätzlich wird einmal im Quartal von einem externen Dienstleister ein Sicherheits-Scan durchgeführt.

Die Pentests decken Schwachstellen innerhalb der Umgebung und der Applikation auf und demonstrieren die Auswirkungen und Konsequenzen eines Angriffs. Die Überprüfung verifiziert, ob die vorhandenen Sicherheitskontrollen wirksam sind und die Anforderungen eines Systems hinsichtlich CIA (Confidentiality, Integrity, Availability) angemessen erfüllen. Der Testprozess beinhaltet eine aktive Analyse der Umgebung auf Schwachstellen. Die spezifischen Testfälle variieren je nach Szenario und der zugehörigen Berechtigungen.

6.2.2.2 Kategorien der Sicherheitsanalyse

Im Zuge der Sicherheitsanalyse wird der Fokus auf folgende Kategorien gelegt.

Authentifizierungs- und Autorisierungsprobleme

Im schlimmsten Fall erfordern einerseits kritische Dienste möglicherweise überhaupt keine Authentifizierung oder das eingesetzte Authentifizierungsschema kann umgangen werden. Das kann dazu führen, dass kritische Daten oder Funktionen ohne weitere präventive Sicherheitskontrolle für Angreifer zugänglich sind. Andererseits überprüfen Dienste möglicherweise nicht oder nur unzureichend die Berechtigung eines Benutzers für den Zugriff auf Ressourcen bzw. deren Änderung. Folglich können Benutzer das Autorisierungsschema und die Least- Privilege-Prinzipien umgehen und entweder ihre Berechtigungen erhöhen (vertikale Privilegieneskalation) oder vorgeben, jemand anderes zu sein (horizontale Privilegieneskalation, Spoofing).

Fehlkonfiguration

Eine Sicherheits-Fehlkonfiguration ist oft das Ergebnis von Diensten, die nicht angemessen an eine bestimmte Umgebung angepasst sind, die nicht explizit gehärtet wurden oder von Diensten, die nicht für einen Produktiv-Einsatz geeignet sind. So können oft z. B. Dienste aufgefunden und benutzt werden, die nur über spezielle Schnittstellen erreichbar sein sollen, zum Beispiel nur von einem Management LAN aus. Ein Beispiel für fehlende Härtung wäre eine Netzwerkfreigabe, die keine SMB-Signierung erfordert, oder die Verwendung eines Protokolls, das die Vertraulichkeit und Integrität eines Dienstes nicht gewährleisten kann (z. B. Telnet). Standardpasswörter einer Komponente, die vor dem Produktionseinsatz nicht geändert wurden, sind ein weiteres Beispiel. Solche Schwachstellen sind in der Regel für Angreifer leicht zu entdecken und auszunutzen.

Veraltete Komponenten mit bekannten Schwachstellen

Dienste und Anwendungen, die nicht gepatcht wurden, sind oft von bekannten Sicherheitslücken betroffen. Sie können oft leicht ausgenutzt werden, entweder weil für die Ausnutzung kein Exploit erforderlich ist oder weil Exploits bereits öffentlich gemacht wurden. Schwachstellen dieser Kategorie sind in der Regel ein Symptom für ein ineffektives Patch- und Schwachstellenmanagement sowie eines unvollständigen bzw. ungenauen Asset Inventory. Manchmal haben Komponenten bereits das Ende ihres Support-Lebenszyklus (EoL) erreicht und es sind möglicherweise überhaupt keine (Sicherheits)-Updates mehr verfügbar. Obwohl Exploits für bestimmte Schwachstellen möglicherweise nicht öffentlich verfügbar sind, können Angreifer trotzdem bereits welche entwickelt oder erworben haben.

Information Disclosure

Informationssysteme und -dienste liefern manchmal Informationen, die hilfreich für einen Angreifer sind.

Obwohl Information Disclosure oft die Folge einer anderen Sicherheitslücke ist, kann es auch eine eigene Schwachstellenkategorie sein. Zum Beispiel kann ein Webservice so programmiert sein, dass er mehr Daten als erforderlich und erwartet zurückgibt. Ein anderes Beispiel wäre ein LDAP-Dienst, der Passwörter zurückgibt, die in einem Beschreibungsfeld gespeichert wurden. Die gewonnenen Informationen helfen Angreifern ihre Privilegien zu erhöhen, auf weitere Systeme zuzugreifen oder das Wissen über ein System zu verbessern und weitere Angriffe noch effektiver auszuführen.

Unzureichende Netzwerksegmentierung

Segmentierungstests stellen sicher, dass die Kontrollen, die verschiedene Netzwerkzonen von einander trennen, effektiv sind und wie vorgesehen funktionieren. Beispielsweise können Umgebungen für VLAN-Hopping- Angriffe anfällig sein. Manchmal können sie sogar direkt umgangen werden z.B. wenn VLANs geroutet werden oder Komponenten, die Schnittstellen in mehreren Zonen haben (z. B. NAS oder Zeitserver), als Gateway oder Pivoting-Systeme missbraucht werden können.

7 Unterstützte Identity-Proofing Use Cases

7.1 Allgemeines

Laut Abschnitt 1.2 werden im IPSPS folgende Use Cases nach ETSI 119 461 v2.1.1 (2025-02) abgedeckt:

- 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 Ausweisfunktion

7.2 Arten von Daten

7.2.1 Basisdaten

Während des Identitätsprüfungsprozesses werden für alle angeführten Use Cases die folgenden personenbezogenen Basisdaten erfasst und überprüft.

Die folgenden Daten werden entweder vom Ausweisdokument ausgelesen (UC1, UC2) oder von der eID-Authentifizierung zurückgeliefert (UC3):

- Vorname
- Nachname
- Nationalität
- Geburtsdatum
- Mobilnummer

7.2.2 Zusatzdaten UC 1, UC2

Für diese beiden Use Cases werden noch folgenden Daten aus dem Ausweis ausgelesen und überprüft:

- Ausweisart
- Ausweisnummer
- Ablaufdatum
- Ausstellungsdatum
- Ausstellende Behörde
- Geburtsort

- Ausweisbilder (In Abhängigkeit des Ausweis Vorderseite oder Vorderseite+Rückseite)
- Livebild aus Videostream (UC1) oder Livebild aus Liveness-Detection (UC2)
- Während des Identitätsprüfungsprozesses erfasstes Portraitfoto

7.2.3 Zusatzdaten UC 3

Für die eID-Authentifizierung werden folgende Zusatzdaten erfasst:

- Art der eID (ID Austria oder German eID)
- eIDAS Level of Assurance/Notwendiges Sicherheitsniveau (einzig zulässiger Wert http://eidas.europa.eu/LoA/high)
- Eindeutiges Personenkennzeichen im Kontext der jeweiligen eID (siehe 7.7)
- Prozessspezifische eID-Assertion im Kontext der jeweiligen eID (siehe 7.7)

7.3 Unterstützte Ausweisdokumente

Die Identitätsprüfungsdienste aus UC1 und UC2 akzeptieren grundsätzlich Reisepässe oder Personalausweise, die dem Standard der internationalen Zivilluftfahrt Organisation (ICAO 9303) hinsichtlich der Verwendung von NFC und Sichtungsprüfungszonen entsprechen. Führerscheine sind mit Ausnahme des österreichischen Führerscheins (nur UC1) ausgeschlossen.

Liste der unterstützten Ausweisdokumente in Abhängigkeit des Use Cases:

- UC1: gemäß SLA.
- UC2: Im UC2 werden nur Reisepässe sowie Personalausweise mit Chip laut ICAO Spezifikation ICAO Spezifikation „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)" unterstützt.
- UC3 - POSident eIDENT German eID – Deutscher Personalausweis mit Onlinefunktion und EUDI Wallet, wenn verfügbar.

7.4 Verfügbarkeit der Dienste

Die Verfügbarkeit des Identitätsprüfungsdienstes für UC1 ist im Service-Level-Agreement (SLA) im Partnervertrag geregelt. Laut derzeitigem Vertrag ist der Dienst zwischen 07:00 und 22:00 verfügbar.

Die Identitätsprüfungsdienste für UC2 und UC3 sind auf keine bestimmte Zeit eingeschränkt. Sie sind rund um die Uhr verfügbar.

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

Im Kontext des Use Case UC1 wird der Identitätsprüfungsprozess über das TPS-Verfahren „POSident VIDEOIDENT“ mit einem zertifizierten Drittanbieter durchgeführt.

Der Videoidentanbieter bietet einen zertifizierten „eIDAS2“ konformen Prozess zur Identifizierung von natürlichen Personen zur Ausstellung von qualifizierten Zertifikaten, welcher im POSident VIDEOIDENT Modul zur Anwendung kommt.

Der IPSP besitzt einen entsprechen Partnervertrag mit dem Videoidentanbieter, der die ordnungsgemäße Durchführung der Videoidentifizierungen nach Verordnung (EU) Nr. 910/2014 in der Fassung (EU) 2024/1183 sicherstellt.

Für dieses Verfahren werden zur Identifizierung die entsprechenden Softwarekomponenten, Standardschnittstellen und Standardintegrationsszenarien des Drittanbieters verwendet. Das heißt:

- Die Videoidentifizierung wird im Callcenter des Drittanbieters durchgeführt.
- Die AML geschulten Agenten verwenden das Agentencockpit des Drittanbieters.
- Der Identifizierungsprozess erfolgt nach dem zertifizierten Prozess des Drittanbieters.
- Zur Identifizierung der Person werden die Komponenten des Drittanbieters verwendet.
- Verwendung einer Identifizierungs-App oder einer Web-basierten Lösung des Drittanbieters.
- Integration des Drittanbieterprozesses mittels des Drittanbieter SDKs für iOS und Android in die POSident eigene Videoident App.

Der Start des Identifikationsprozesses erfolgt durch Auswahl der Methode „VIDEOIDENT“ im POSident Auswahlmenü. Anschließend wird die zu identifizierende natürliche Person zum Videoident-Prozess weitergeleitet. Nach Abschluss des Prozesses erfolgt ein Redirect zum POSident Modul.

Der weitere Prozess, insbesondere die Übermittlung der Daten an den QTSP zur Ausstellung des qualifizierten Zertifikates erfolgt wie im Abschnitt 8 beschrieben.

Der Drittanbieter ist im RA Vertrag mit dem QTSP-Anbieter als zulässig vermerkt.

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

Für den Use Case UC2 kommt das Verfahren „POSident FOTOIDENT chip“ zum Einsatz.

Bei diesem Verfahren werden die Ausweisdaten im Zuge des Fotoident-Prozesses aus dem Chip des Ausweisdokumentes ausgelesen.

Bei einem Ausweisdokument mit Chip sind die persönlichen Daten laut laut ICAO Spezifikation ICAO Spezifikation „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)” auf dem Chip des Ausweises gespeichert.

Beim Verfahren „POSident FOTOIDENT chip“ werden die Datengruppen DG1, DG11, DG12 und DG14 ausgelesen.

Zur Sicherstellung, dass keine Manipulation vorliegt, wird überprüft, ob die Daten mit dem entsprechenden Country Signing Certification Authority (CSCA) Zertifikat signiert wurden, welches von jedem Land, welches e-Ausweise ausstellt, eingerichtet wird.

Der gesamte Prozess ist in der „Endbenutzerdokumentation „POSident FOTOIDENT chip“ beschrieben (siehe Abschnitt 13 Referenzen).

Zum Gesichtsabgleich und zur Liveness Detection wird eine nach „ISO/IEC 30107-3 Presentation Attack Detection (PAD)“ zertifizierte Plattform verwendet, welche im Rechenzentrum des IPSPs installiert ist.

Die entsprechenden Zertifikate und Nachweise liegen dem CAB vor.

Systematische Tests zu den Werten

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

wurden gemäß ISO/IEC 30107-3 bzw. gemäß ISO/IEC 19795-1 durchgeführt. Entsprechende Nachweise liegen der Konformitätsbewertungsstelle vor.

Als Zielwerte sind folgende Werte definiert:

- APCER: 0,5%
- BPCER: 0,1%
- FRR: 2%

- FAR: 0,5%

Im Dezember 2025 wurde im Zuge der regelmäßigen Penetration-Tests ein Penetration-Test durchgeführt, in dem auch der Standard CEN/TS 18099-2024 für den Bereich Injection Attack Detection (IAD) in den Scope des Tests mitaufgenommen wurde. Der entsprechende Testreport liegt der Konformitätsstelle ebenfalls vor.

Ein durch ein CEN TS 18099 akkreditiertes Labor durchgeführter Injection Attack Detection Test wird bis spätestens Ende 2026 nachgereicht.

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

Für den Use Case UC3 kommen die Verfahren „POSident eIDENT ID Austria“ und das „Verfahren „POSident eIDENT German eID - Online Ausweisfunktion zur Anwendung.

Laut aktueller eIDAS Verordnung (EU) Nr. 910/2014 (eIDAS), in der Fassung (EU) 2024/1183 erfüllt die „Elektronische Identität - e-ID“ die Anforderungen zur Ausstellung eines qualifizierten Zertifikates, wenn das Sicherheitsniveau (Assurance Level) der Identifizierung das Niveau „hoch“ hat (siehe dazu Artikel 6 – 12, sowie Art. 24(1)c).

Nach der Identifizierung mittels eID werden die entsprechenden im Abschnitt 7.2 angeführten Daten an den QTSP zur Ausstellung des qualifizierten Zertifikates übermittelt (siehe Abschnitt 8).Arten von Daten

7.7.1 POSident eIDENT ID Austria

Das POSident Modul verwendet zur Identifizierung der Person via ID Austria den zentraler eIDAS-Knoten der Republik Österreich (siehe https://www.id-austria.gv.at/de/developer/anbinden/anbindung-mit-openid-connect).

Nach Durchführung der Identifizierung wird in der Response Struktur das Sicherheitsniveau geprüft, welches dann auch an den QTSP zur Ausstellung des qualifizierten Zertifikates übermittelt wird. Die Rückgabe des Sicherheitsniveaus ist in der Spezifikation https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html definiert.

Die Kommunikation mit dem zentralen eIDAS Konten erfolgt via SSL/TLS unter Verwendung des OpenID Connect (OIDC) Authentifizierungsprotokolls.

Der IPSP besitzt eine entsprechende Akkreditierung, die es ihm erlaubt, die ID Austria als Identifikation von natürlichen Personen zur Ausstellung von qualifizierten Zertifikaten zu verwenden.

7.7.2 POSident eIDENT German eID – Onlineausweisfunktion

Für dieses Verfahren wird die Identitätsprüfung mit der zertifizierten Lösung „Online-Ausweisfunktion mit eID“ durchgeführt. Diese Identifizierungsmethode erfüllt die entsprechenden Anforderungen an das Sicherheitsniveau (Assurance Level) ist vom BSI (Deutsches Bundesamt für Sicherheit in der Informationstechnik) zertifiziert nach BSI TR-03128, sodass auf Basis der Identifizierung ein qualifiziertes Zertifikat ausgestellt werden darf.

Der Identifizierung über den deutschen Personalausweis mit Onlinefunktion erfolgt über eine iOS oder Android App.

8 Ausstellung des qualifizierten Zertifikates durch den qualifizierten Vertrauensdiensteanbieter - QTSP

Für die beschriebenen Use Cases UC1, UC2 und UC3 werden die qualifizierten Zertifikate eines eIDAS konformen QTSP ausgestellt. Im Rahmen des integrierten QTSP eignen Signaturdialogs (nativ vom jeweiligen QTSP) schließt der Nutzer eine direkte Vertragsbeziehung mit dem jeweiligen QTSP.

Die Norm „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“ definiert die entsprechenden Anforderungen an qualifizierte Zertifikate für elektronische Signaturen.

Die Übergabe sämtlicher zur Ausstellung eines qualifizierten Zertifikates benötigter Daten erfolgt über eine vom QTSP bereitgestellte sichere Schnittstelle. Zur Sicherstellung der Authentizität und Integrität sämtlicher an den QTSP übermittelten Identifizierungsdaten werden diese in einer vom QTSP definierten JSON-Struktur verpackt und mit einem auf der TPS-Plattform hinterlegten Zertifikat signiert. Durch die Hinterlegung des zugehörigen Public Keys am QTSP-Server kann sowohl die Herkunft als auch die Authentizität der Daten sichergestellt werden.

Das hier zu verwendende Zertifikat basiert auf dem ECC-256 Verfahren und wird vom QTSP zur Verfügung gestellt.

Die jeweiligen Daten, die für die einzelnen Use Cases UC1, UC2 und UC3 übergeben werden, sind im Abschnitt 7.2 angeführt.

Die folgende Graphik zeigt den Ablauf der Zertifikatsausstellung am Beispiel des eIDAS konformen QTSPs Primesign/CRYPTAS it-Security GmbH.

Die Ausstellung des Zertifikates selbst erfolgt im Anschluss über den vom QTSP vorgegebenen Prozess.

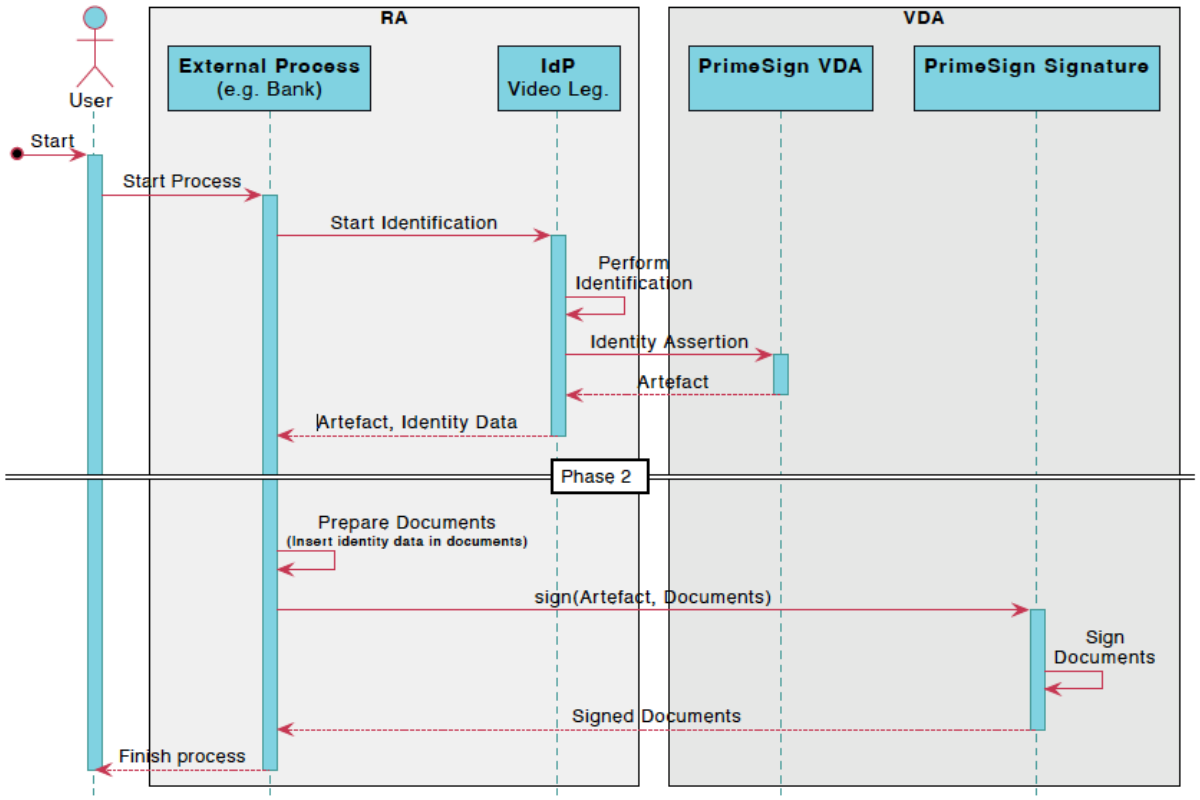

Abbildung 2: Beispiel Ablauf Zertifikatsausstellung PrimeSign OneTime Zertifikat (simplified).

9 Verpflichtungen

9.1 Handlung in Übereinstimmung mit dem IPSPS

Der IPSP und alle Drittanbieter sind verpflichtet in Übereinstimmung mit dem IPSPS zu handeln und sich internen und externen Audits zu unterziehen, um die Einhaltung der Vorschriften oder Policies zu prüfen bzw. zu gewährleisten.

Bei den Dienstleistern sind dies insbesondere die Einhaltung der relevanten Anforderungen der Verordnung (EU) Nr. 910/2014 (eIDAS), in der Fassung der Verordnung (EU) 2024/1183 („eIDAS2“).

Durch die Controls A.5.19 und A.5.34 des Anhangs A gemäß ISO/IEC 27001:2022 ist gewährleistet, dass Informationssicherheitsrisiken durch Lieferantenbeziehungen systematisch identifiziert, bewertet, vertraglich adressiert, überwacht und gesteuert werden.

9.2 Ankündigung Beendigung der Tätigkeit der Identifizierung

Der IPSP hat Verfahren etabliert, die eine geordnete, transparente und nachvollziehbare Beendigung der Tätigkeit der Identifizierung sicherstellen.

Die Beendigung der Erbringung von Identifizierungsdiensten erfolgt ausschließlich auf Basis einer formellen Entscheidung des IPSP und wird allen betroffenen Vertragspartnern, Aufsichtsbehörden sowie anderen relevanten Stellen **mindestens drei (3) Monate im Voraus** schriftlich angezeigt. Die Mitteilung enthält mindestens den geplanten Beendigungszeitpunkt, den Umfang der betroffenen Identifizierungsdienste sowie Informationen zu Übergangs- und Abwicklungsmaßnahmen.

10 Sicherheitsanforderungen

Die POS Solutions GmbH betreibt ein Informationssicherheitsmanagementsystem betreffend Informationssicherheit, Business Continuity, Cybersicherheit, Datenschutz etc., das nach der Norm ISO/IEC 27001:2022 zertifiziert ist.

Weiter Informationen dazu siehe https://pos.ag/media/342p12e4/isms-policy_web.pdf.

Weitere Informationen zur ISO/IEC 27001:2022 Zertifizierung der POS Solutions GmbH: https://pos.ag/plattform/pos-solutions-gmbh/iso27001-zertifizierung/.

Im folgenden Abschnitt wird die Umsetzung der einzelnen Sicherheitsanforderungen durch Verweise auf die entsprechenden Punkte der „ISO/IEC 27001:2022“ Norm als auch der jeweiligen Controls aus dem Anhang A dokumentiert.

Alle Controls sind anwendbar und vollständig umgesetzt. Die Umsetzung der Controls ist im SoA-Dokument (Statement of Applicabilty) des ISO/IEC 27001-ISMS dokumentiert. Das SoA Dokument „POS_Solutions_GmbH_SoA_ISO27001_2025.pdf“ ist im Abschnitt 13 referenziert.

10.1 Organisatorische Maßnahmen

Im Rahmen des Informationssicherheits-Managementsystems (ISMS) werden die „Organisatorischen Maßnahmen“ (A.5.1–A.5.37) des ISO/IEC 27001:2022 Annex A umgesetzt. Diese Controls adressieren u.a. die Klassifizierung von Informationen (Dokumentenlenkung), Zugangsrechten, Lieferantenmanagement, Behandlung von Informationssicherheitsvorfällen, Kontrolle der rechtlichen Anforderungen sowie dokumentierte Bedienabläufe.

10.2 Physische Sicherheitsanforderungen

Im Rahmen des Informationssicherheits-Managementsystems (ISMS) werden die physischen Sicherheitsanforderungen gemäß den „Physischen Maßnahmen“ (A.7.1–A.7.14) des ISO/IEC 27001:2022 Annex A umgesetzt. Diese Controls adressieren physische Perimeter, Zutrittskontrollen, Überwachung, Schutz vor Umweltgefahren, Geräteplatzierung, Medienlagerung sowie sichere Entsorgung.

10.3 Prozeduren/Prozesse /Abläufe

Im Rahmen unseres ISMS setzen wir die Anforderungen an dokumentierte Prozesse und Abläufe gemäß ISO/IEC 27001:2022 Annex A Control „A.5.37 – Dokumentierte Betriebsabläufe“ um. Darüber hinaus adressieren weitere Annex A-Controls (z. B. A.5.1, A.5.2, A.5.24–A.5.27, A.5.36) organisatorische und

sicherheitsrelevante Prozess-Elemente, die für die konsistente und sichere Durchführung der Services relevant sind.

10.4 Personalsicherheit

Die Anforderungen an die Personalsicherheit werden gemäß den ISO/IEC 27001:2022 Annex A Controls „Personenbezogene Maßnahmen“ (A.6.1 – A.6.8) umgesetzt. Diese Controls umfassen die Bereiche Sicherheitsüberprüfung, Beschäftigung und Vertragsbedingungen, Informationssicherheitsbewusstsein, Ausbildung, Schulung, Maßregelungsprozess, Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung, Vertraulichkeit – oder Geheimhaltungsvereinbarungen, Remote-Arbeit und Meldung von Informationssicherheitsereignissen.

10.5 Audit Logging

Im Rahmen unseres ISMS setzen wir das Control ISO/IEC 27001:2022 Annex „A 8.15 – Protokollierung“ um, um sicherheitsrelevante Ereignisse, Systemaktivitäten und Ausnahmen zu protokollieren, zu speichern, zu schützen und zu analysieren.

Ergänzend werden die Controls „A.8.16 – Überwachung von Aktivitäten“ und „A.8.17 – Uhrensynchronisation“ berücksichtigt, um die Integrität, Konsistenz und Überwachbarkeit der Logs sicherzustellen.

Im Zuge des Identitätsprüfungsdienstes werden die folgenden Ereignisse im Auditprotokoll aufgezeichnet:

- Eindeutige interne Identifikations-Guid sowie optionale externe Identifikationsnummer
- Beginn des Identitätsprüfungsprozesses – Timestamp
- Die in Abhängigkeit des Identity-Proofing Use Cases verarbeiteten Daten
- Im Zuge der Identitätsprüfung relevante Ereignisse inkl. Timestamp
- Überprüfung der Daten und Nachweise
- Annahme oder Ablehnung der Identitätsprüfung

Es wird für jeden Identifizierungsprozess laut Abschnitt 7 ein Auditprotokoll erfasst. Dieses Protokoll dient u.a. auch als Nachweis der vertragsgegenständlichen Tätigkeiten gegenüber des QTSP. Das Auditprotokoll und die zugehörigen Logs werden zum Nachweis für interne und externe Audits drei Monate aufbewahrt.

Der QTSP ist laut Österreichischem Signatur- und Vertrauensdienstegesetz (SVG) – § 10 verplichtet die Dokumentation zur Zertifikatsausstellung 30 Jahre aufzubewahren.

11 Sonstige geschäftliche und rechtliche Angelegenheiten

11.1 Anwendbare allgemeine Geschäftsbedingungen

Die allgemeinen Geschäftsbedingungen des IPSP sind auf der Webseite unter dem Link https://pos.ag/media/nyhndidt/pos_solutions_gmbh_agb_webseite_de.pdf veröffentlicht.

11.2 Datenschutz

Im Rahmen unseres ISMS stützen wir den Datenschutz und Schutz personenbezogener Daten auf entsprechende Controls des ISO/IEC 27001:2022 Annex A. Implementierte Maßnahmen umfassen das Control „A.5.34 - Datenschutz und Schutz von personenbezogenen Daten – PII“ sowie ergänzende Controls A.5.12 – A.5.18 zur Klassifikation und Kennzeichnung von Informationen, Informationssteuerung, Informationsübermittlung, Zugangssteuerung, Identitätsmanagement, Authentifizierungsinformationen und Zugangsrechte sowie die Controls A.8.10 – A.8.12, welche die Bereiche Datenlöschung, Datenmaskierung und den Bereich Verhinderung von Datenlecks umfassen.

Die aktuelle Datenschutzerklärung des IPSP ist auf der Webseite referenziert -https://pos.ag/datenschutz/.

11.3 Haftungsbeschränkungen

Die Haftungsbeschränkungen sind in auf der Webseite veröffentlichen AGBs enthalten (siehe 11.1)

11.4 Streitbeilegung

Wenn es zu einer Streitigkeit zwischen dem IPSP und einem Kunden oder zwischen dem IPSP und einem Dritten kommt, entscheidet die Geschäftsführung des IPSP nach Anhörung aller Beteiligten und unter Berücksichtigung aller Interessen. Die Entscheidung wird schriftlich festgehalten und innerhalb einer angemessenen Frist mitgeteilt. Dieses Verfahren schränkt die Möglichkeit die Streitigkeiten gerichtlich zu regeln nicht ein.

Das Beschwerdemanagement ist in den in auf der Webseite veröffentlichen AGBs geregelt (siehe 11.1)

11.5 Anwendbares Recht

Die Aktivitäten des IPSP unterliegen in Verbindung mit dem österreichischen Recht der Verordnung (EU) Nr. 910/2014 (eIDAS), in der Fassung der Verordnung (EU) 2024/1183 („eIDAS2“).

12 Definitionen und Abkürzungen

Abkürzung	Definition
CAB	Conformity Assessment Body - Konformitätsbewertungsstelle
CP	Certificate Policy – Zertifizierungsrichtlinie
IPSP	Identity Proofing Service Provider - Identitätsprüfungsdienstleister
IPSPS	Identity Proofing Service Practice Statement - Erklärung zur Praxis der Identitätsprüfung
PA	Policy Authority - Zuständige Behörde
QTSP	Qualified Trust Service Provider - Qualifizierter Vertrauensdiensteanbieter
TPS	Trusted Plattform Services
TSP	Trust Service Provider - Vertrauensdiensteanbieter

13 Referenzen

Liste der aktuell angeführten Referenzen:

- Weitere Informationen zur ISO/IEC 27001:2022 Zertifizierung der POS Solutions GmbH: https://pos.ag/plattform/pos-solutions-gmbh/iso27001-zertifizierung/.
- ISMS Policy: https://pos.ag/media/342p12e4/isms-policy_web.pdf.
- SoA-Dokument des ISO/IEC 27001-ISMS
  POS_Solutions_GmbH_SoA_ISO27001_2025.pdf
- Endbenutzerdokumentation POSident FOTOIDENT chip
  Endbenutzerdokumentation POSident FOTOIDENT chip für Android v1.1
  Endbenutzerdokumentation POSident FOTOIDENT chip für iOS v1.1
  Endbenutzerdokumentation POSident FOTOIDENT chip für PC v1.1