360core AG
Schützengasse 25 · 8001 Zürich · Tel +41 44 700 28 88
solutions@360core.ch · www.360core.ch · CHE-414.534.215 VAT

Identity Proofing Practice Statement

Document properties - Policy administration

Responsibility	Senior Management
Review cycle	Yearly
Document ID	ETSI-POL-001
ETSI TS 119 461 mapping	Clause 6.1
ETSI EN 319 401 mapping	REQ 6.1

Document history and approvals

Version	Date	Comments	Author	Approved by
1.0	01/06/2026	First version	Lukas Wissner	Marcel van der Sanden Lukas Wissner

360core AG
Schützengasse 25 · 8001 Zürich · Tel +41 44 700 28 88
solutions@360core.ch · www.360core.ch · CHE-414.534.215 VAT

TABLE OF CONTENTS

360core AG
Schützengasse 25 · 8001 Zürich · Tel +41 44 700 28 88
solutions@360core.ch · www.360core.ch · CHE-414.534.215 VAT

1 Introduction, scope, publication, repository, participants

1.1 This document is 360core's public declaration of its identity proofing practices as mandated by Requirement 6.1 ETSI EN 319 401 ("Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers") to enhance trust and confidence in its digital identification platform. The statement provides information relevant for users and stakeholders of our identity proofing service. Information relevant to other participants in a given Public Key Infrastructure (PKI) ecosystem can be found in those participants' respective public practice statements.

1.2 Important and recurring key terms with specific meanings in this document are defined in Section 11, while certain acronyms are clarified when they first appear in the text body.

1.3 Recognizing the complexity of the subject matter and the applicability of laws, standards, industry best practices, and guidance at multiple levels, this text is intended to provide the general public with a brief and easy-to-understand overview, explaining in detail how 360core identifies individuals remotely and with which level of assurance, who can use the service and in which circumstances, what security measures are in place, what types of personal data about applicants are processed, where and how long such data is stored, in addition to other business, legal, and technical matters.

1.4 360core AG is a Swiss identity proofing service provider (IPSP) first certified in 2026, and to be recertified on a yearly basis, by KPMG AG (for ZertEs in Switzerland) and KPMG (Liechtenstein) AG (for eIDAS in the EU) that offers, as its single supported use case for which compliance is claimed, and as a subcontractor to Swisscom Trust Services AG, fully automated, that is, unattended remote identity verification of individuals (also called "applicants", "subjects", or "subscribers") in an identity proofing context where identity attributes are collected by means of a digital identity document, or put differently, where applicants hold, and electronically present, a government-issued NFC-enabled passport, identity card, or driving license - also known as ePassport, biometric passport, digital identity document, or electronic machine-readable travel document (eMRTD).

1.5 To collect authoritative, reliable, and quality evidence from such digital identity documents through the Near Field Communication (NFC) protocol support present in virtually all modern smartphones, 360core has developed a mobile identity verification app ("360 Identities") that anyone can download without restrictions as an Android app from Google Play (360 Identities supports Android 7 and higher) or as an iOS app from the App Store (360 Identities supports iOS 14 and higher).

1.6 As a mobile app, 360 Identities is supported by a cloud-based network located in Switzerland and in the EU responsible for process orchestration, evidence evaluation, process logging, and process observation ("Evidence Processing Server"), in addition to a cloud-based network provided by the same cloud-based data processor which is responsible for liveness detection ("Biometric Verification Server").

1.7 In its function as a subcontractor to 360core, the cloud service provider (CSP) hosting the Evidence Processing Server and the Biometric Verification Server must abide by all applicable requirements that apply to 360core, and which are outlined in this IPSP Practice Statement (*see* Art. 1.9), to ensure uniform information security (ISO 27001:2022 conformance) and data privacy standards (FADP, GDPR) across the cloud supply chain including in terms of applicable service level agreements (SLA), the right to audit, business continuity management (BCM), and disaster recovery plans (DRP).

1.8 General information about 360core, available support channels, an email address to file complaints, the commercial pricing for 360 Identities, its Terms of Use, Privacy Policy, and our practices for identity proofing in general (this statement) can be downloaded in the "Compliance Hub" section of the public repository on our website at **www.360core.ch/software-solutions/digital-identities**.

1.9 In its role as a trust service component in conjunction with a trust service provider (TSP) or Certification Authority (CA) - where 360core takes on all or core parts of the so-called registration service or registration authority (RA) component - 360 Identities demonstrates continual conformance with the following standards, laws, and requirements:

- ETSI TS 119 461 (for the use case reflected in Clause 9.2.3.4)
- ETSI EN 319 401
- RFC 3647 (Internet 509 Public Key Infrastructure Certificate Policy and Certification Framework)
- ICAO Doc 9303 - Machine Readable Travel Documents
- Swiss law on electronic signatures, ZertES
- Swiss ordinance on electronic signatures, VZertES
- Swiss Federal Act on Data Protection (FADP)
- Regulation (EU) 2016/679 (GDPR)
- Regulation (EU) No 910/2014 (eIDAS)
- FINMA Circular 2016/7 Margins 32 - 39 ("Online Identification")
- RTS on Customer Due Diligence under Article 28(1) of Regulation (EU) 2024/1624 (AMLR)

2 Identity proofing description and right of access to data

2.1 Typically, the identity proofing process with 360 Identities is initiated (INI) by an API call from 360core's Evidence Processing Server to Swisscom Trust Service's Multiple Authentication Broker (MAB), a certified TSP platform that manages identity verifications, KYC processes, and two-factor signature approvals. In other words, applicant authentication is performed through Swisscom Trust Services whereby the following data is collected and disclosed:

- Mobile number

2.2 The business context for the identity proofing initiation could be the need to conduct an electronic transaction that requires strong customer authentication, such as when an applicant wishes to generate a qualified electronic signature (QES) for repetitive signing on a digital signature platform like 360 Signatures, also operated by 360core, in order to sign a contract with a signature equivalent to the handwritten signature, or open a bank account digitally. In general, 360 Identities can be integrated into customer user journeys, business processes and workflows in several ways:

- Deeplink or QR code in a web or mobile application: The applicant is presented with a deeplink or QR code starting the identity proofing process including guidance for downloading 360 Identities on a common marketplace
- App-to-App: if already installed, 360 Identities can be launched via a relying party's own app

2.3 Once a session ID and a timestamp have been generated by the identity proofing party (360core) and the relying party (Swisscom Trust Services), 360core's Evidence Processing Server screens the applicant's mobile device for session metadata (device fingerprinting, checks making sure the device is not jail-broken or rooted) and initializes in conjunction with 360 Identities - and upon acceptance of all relevant terms of use - identity attribute and evidence collection (COL) whereby (i) physical identity attributes are captured from the visual inspection zone (VIZ) and machine-readable zone (MRZ) of the physical identity document by the camera functionality of 360 Identities and passed to the Evidence Processing Server for optical character recognition (OCR) and (ii) digital identity attributes are captured by 360 Identities through the NFC technology embedded in the applicant's smartphone from the digital identity document, that is, from the biometric chip embedded in the physical identity document.

2.4 During the validation stage (VAL), 360core's Evidence Processing Server validates the eMRTD's country-signing certificate through the International Civil Aviation Association's (ICAO) Public Key Database (PKD) and a chip clone detection is performed. In addition, it determines the freshness, reliability, and

consistency of the collected identity attributes including, where available, the validity of the supporting identity document.

2.5 For the following textual digital identity attributes captured from the electronic identity document - as extracted from ICAO fields DG1 or DG10 (DG stands for Data Group) - a 100% linguistic match is required when compared to, and cross validated against, identity attributes extracted from the MRZ of the physical identity document:

- First name
- Middle name
- Last name
- Document number

2.6 By only evaluating datapoints sitting in the MRZ of a physical identity document and matching them against the corresponding datapoints stored in the document's electronic chip, error-prone data normalization is unnecessary, allowing 360core's Evidence Processing Server to bypass the handling of differences in encoding of identity attributes (that is, differences in name attributes such as diacritics and other special characters) between different evidence types (*see* VAL-8.3.1-04X). At the same time, data truncation in the MRZ and DG1 is reliably detected and can be escalated if necessary.

2.7 The textual fields sitting the MRZ and ICAO DG1 of international passport (TD3 format) are limited to 44 characters and do not allow for applicant name notations with diacritics and other special characters, but where DG11 (containing the full applicant names with diacritics and no character limitations) is present in the biometric chip of international passports (as is the case in Switzerland and many other countries), such full names (including in non-Latin alphabets) will equally be available in the Export Payload for downstream processing by relying parties where required.

2.8 In the last step, and still during the same session, liveness detection performed by 360core's Liveness Verification Server binds (BIN) the collected authoritative identity attributes to real-live human beings (applicants) by means of having applicants record a video selfie of their face with the front-facing color camera in their mobile device in order to verify that the applicant is the legitimate passport holder and not a bad actor using spoofs presented to the camera. This last step yields a binary PASS/FAIL determination depending on a set confidence score threshold with a face liveness confidence score between 0 and 100 using machine learning algorithms, which are probabilistic.

2.9 The mobile device, camera, and connection requirements for 360core's liveness detection are as follows:

- The mobile device must not be jail-broken or rooted
- The minimum refresh rate of the device display must be 60 Hz
- The minimum display or screen size must be 4 inches
- The mobile device must have a front-facing camera able to record colors
- There must be no virtual camera or camera software
- The minimum camera recording capability must be 15 frames per second
- The minimum bandwidth (internet connection) must be 100 kbps (= modest)

2.10 Additionally, during the face-match check, 360core's Evidence Processing Server compares 4 high-quality reference images ("source images") as extracted from the liveness selfie video with the applicant's high-resolution passport photo ("target image") as extracted from the digital identity document. Again, this step yields a binary PASS/FAIL determination depending on the set similarity threshold with a face match confidence score between 0 and 100 using machine learning algorithms, which are probabilistic.

2.11 The probabilistic nature of machine learning algorithms employed in liveness detection and face matching allows for the calculation of a confidence score that may not meet 360core's quality goals and security objectives (as outlined in Article 4.1) and may therefore result in genuine applicants being incorrectly classified as illegitimate, fraudulent, or as threat actors ("false negatives").

2.12 360core mitigates the risks arising where such automated individual decision-making impacts on an applicant's rights, privacy, or access to services by implementing suitable measures to safeguard the applicant's rights, freedoms, and legitimate interests via a customer support channel in the footer of its website, where applicants can present their case, challenge 360core's fully automated liveness and face matching decision, and request human intervention (*see* GDPR Art. 22 "Automated individual decision making, including profiling").

2.13 The *output* of 360core's identity proofing process ("Export Payload") or, in data protection terminology, the full scope of its personal data processing activity - which never goes beyond the explicitly agreed identity proofing context in accordance with the principle of data minimization - and the categories of personal data involved, thus comprises the following collected and validated identity attributes of online applicants, derived from the *input* of their identity document and the selfie liveness video, both of which are transmitted remotely via the mobile application by applicants themselves, and are processed on the server side to yield an aggregate binary PASS/FAIL determination:

- IP address, VPN signals

- Mobile device information
- Web browser information
- Image of the physical identity document
- First name (transmitted to the TSP where applicable)
- Middle name (transmitted to the TSP where applicable)
- Last name (transmitted to the TSP where applicable)
- Gender
- Date of birth (transmitted to the TSP where applicable)
- Nationality
- Issue country (transmitted to the TSP where applicable)
- Issue date
- Expiry date (transmitted to the TSP where applicable)
- Document type (transmitted to the TSP where applicable)
- Document number (transmitted to the TSP where applicable)
- NFC chip data (textual): DG1, DG11 (if available)
- NFC chip data (images): DG2, DG5 (if available)
- Selfie liveness video
- 4 audit images from the selfie liveness video

2.14 These above data points are used by 360core ("data processor") for automated decision-making through biometric means based on the data subject's explicit consent in the context of establishing the identity of the applicant in settings as described above.

2.15 The recipients to whom this personal data as described above is disclosed through a secure backend communication channel as required are (i) Swisscom Trust Services in Switzerland ("data controller") in its quality of TSP or CA in the context of the issuance of a QES under ZertES or eIDAS (ii) you as our corporate customer - where we act as your data processor for identity proofing - and you act as the data controller for your own customers and optionally (iii) the user of 360 Identities through its UI.

2.16 Accordingly, data subjects access requests (DSAR), such as the right to information, the right to rectification, the right to erasure, the right to restriction of processing, and the right to data portability under the Swiss Federal Act on Data Protection (FADP) and the EU's General Data Protection Regulation (GDPR), in addition to certificate revocation or suspension requests (for example, if the applicant's name or employment has changed, or in case of the certificate's suspected compromise) must be exercised with the data controller (outlined above in Art. 2.15) directly.

2.17 The data output from Art. 2.13 gives auditable and actionable proof to TSPs such as Swisscom Trust Service and other potential consumer organizations (depending on other contractually agreed contexts as the case may be) that the identity of an individual is proven beyond doubt and that the individual is a living subject present at the point of capture.

2.18 This assurance can then be used by TSPs and other certificate users and relying parties (that is, relying on the accuracy of the identity information) to issue qualified electronic signatures under ZertES or eIDAS or generate other certificates such as electronic seals (typically used to certify the integrity of emails, digital documents, or submissions to authorities) or for other online transactions where a digital identity is associated with a web form, email, electronic document, or other mission-critical data exchanges such as customer authentication, financial institution onboarding and KYC workflows, ongoing due diligence in the financial and corporate sectors, the management of signatories, transaction authentication for online banking, age verification for eCommerce and many more.

3 Data protection and recordkeeping practice

3.1 Throughout the entire identity proofing process, 360core does not physically store any of the data points enumerated under Art. 2.13 or supporting images and videos beyond its processing activities for the duration of the respective short-lived identity proofing session, which typically lasts less than one minute. Instead, once the identity proofing process is successfully completed and a positive determination has been made, 360core merely transmits the collected identity attributes to the relying party (scope as required by the relying party) for audit-proof archival by the relying party.

3.2 However, first-hand session audit logs generated the Evidence Processing Server during the identity proofing process are archived by 360core and backed up in unalterable form using WORM (Write-Once Read-Many) object locking technology in ISO 27001 certified data centers located exclusively in Switzerland across multiple locations (also called availability zones) in compliance with FINMA requirements.

3.3 Those logs are stored in entirely anonymized format for the duration of (i) the Swiss legal retention period of 11 years starting from the respective qualified certificate's expiry in accordance with Art. 11 para. 1 and 2 VZertES ("Activity logs") and (ii) the Austrian legal retention period of 30 years (eIDAS flows) starting from the respective qualified certificate's expiry pursuant to Article 10.3 of the Austrian Digital Signature and Trust Services Act ("Access rights and retention period").

3.4 Given that qualified electronic signatures under ZertES and eIDAS have a maximum lifespan of 5 years, the aggregate legal retention period for identification proofing data is thus (i) 17 years for identity proofing audit logs generated under Swiss law and (ii) 36 years for such audit logs generated under Union law. We note that both scenarios provide for a safety buffer of one year to calculate uniform disposal schedule offsets.

3.5 For the sake of completeness, we also note that the involved trust service providers must apply the same retention periods to plain text identity proofing evidence as transmitted by 360core in its export payload.

4 Goals for quality and security practices

4.1 When providing identity proofing, 360core strives to correctly identify applicants while preventing fraud such as spoofing, presentation attacks, and impersonation by bad actors. In line with industry best practice, 360core has the following objectives in terms of resilience to the false acceptance ("false negatives") and the false rejection ("false positives") of applicants during liveness detection:

- Risk tolerance for False Acceptance Rate (FAR): **0%**
- Risk tolerance for False Rejection Rate (FRR): **< 0.2%**

4.2 360core has liveness detection and automated ID-matching algorithms tested by an accredited European laboratory at least every second year and adapts security measures to new species of threats to harden its anti-fraud posture against novel presentation attacks and achieve the objectives outlined above under Art. 4.1, ensure industry-standard resilience, and strike a balance between user-friendliness and security.

4.3 In addition, 360 Identities and its underlying server-side network infrastructure (the Evidence Processing Server and the Liveness Verification Server) undergo yearly penetration testing by an established and recognized German provider of penetration testing services.

4.4 As a fully automated solution, 360 Identities is available for identity proofing 24/7/365. To this effect, 360core deploys Tier III compute and high-performance databases with multi-zone availability and stives to guarantee an uptime of 99.99% SLA, allowing for a maximum downtime of just 52.56 minutes per year.

4.5 In general, the configuration of 360core's relevant systems is checked for changes violating 360core's security goals at planned intervals: the maximum interval between two checks cannot exceed one year (REQ-6.3-09).

5 ISO 27002:2022 - Summary of organizational controls

5.1 Information on organizational controls is indicated in the respective policy qualifier.

6 ISO 27002:2022 - Summary of people controls

6.1 Public digital trust services and digital identities are provided by decentralized computer networks designed, configured, operated, and maintained by humans, particularly those holding trusted roles with regard to the technical side of the identity proofing network infrastructure. Such trusted roles form an integral part of the PKI and include in particular:

- Senior Management (C-Level)
- System Administrators (cloud engineers and DevOps)
- Information Security Officers (CISOs)
- Compliance Officers
- Data Protection Officers
- Internal Auditors
- Product Owners

6.2 360 core runs background verification checks (such as the collection of references, confirmation of claimed academic and professional qualifications, job experience, identity proofing, etc.) on all trusted roles at onboarding and by means of ongoing screening via data sets of established date vendors (such as LSEG World-Check, Dow Jones Risk & Compliance Database, LexisNexis WorldCompliance Data, Moody's GRID) against sanctions, enforcements, negative news, conflicts of interest to ensure all personnel of 360core are eligible and suitable for the trusted roles for which they are considered and remain eligible and suitable during their employment.

6.3 Where trusted roles are contracted through suppliers of services, screening requirements are included in the contractual agreements between 360core and such suppliers.

6.4 Access to 360core server infrastructure is granted only after multi-factor authentication has been completed and in accordance with the need-to-know principle, whereby access is strictly limited to policies necessary for the performance of the respective function, in line with the principles of separation of duties and avoidance of conflicts of interests. Passwords are renewed on an ongoing basis and enforced by the system administrator.

6.5 Also, in accordance with the principle of separation of duties, an employee of 360core is never allowed to approve of their own actions (e.g., code changes,

the publication of new software versions, or the inspection of log files in production environments, etc.).

6.6 In addition, an employee of 360core holding a trusted role is always backed up by a deputy to ensure business continuity and avoid single points of failure. Senior management, system administrators, and CISO's must *at all times* have a deputy who is capable of fully replacing the absent individual in every respect.

6.7 360core promotes continuous learning and a culture of self-improvement. All staff of 360core receive appropriate information security awareness, education and training in relevant fields. Trusted roles have access to complimentary training programs tailored to their specific role in the field of information security, cloud engineering, compliance and other areas relevant to their work in the field of identity proofing.

6.8 360core has recourse to drastic sanctions including termination against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of computer networks.

6.9 For smaller violations, a disciplinary process has been formalized and communicated to take action against personnel and other counterparties who have committed an information security policy violation.

6.10 Information security responsibilities and duties remain valid after termination or change of employment and are contractually enforced, in particular through confidentiality and non-competition clauses and non-disclosure agreements with regard to intellectual property and other knowledge obtained. This includes the removal and cleaning up of network permissions no longer required.

6.11 360core implements and enforces security measures when personnel are working remotely to protect information accessed, processed or stored outside 360core's network security perimeter. This is done through the provision of suitable equipment and storage furniture (e.g., exclusive storage of sensitive information on password-protected external hard drives) with the objective that the loss of a privately-owned device that is not under the control of a 360core does not lead to the disclosure of sensitive information.

7 ISO 27002:2022 - Summary of physical controls

7.1 360core does not host its own server infrastructure but has recourse to a public cloud service provider certified against ISO 27002:2022.

7.2 However, the use of cloud services involves shared responsibility for information security and collaborative effort between the CSP and 360core ensuring that the respective responsibilities are clearly defined and implemented appropriately.

7.3 Information on physical controls is indicated in the respective policy qualifier.

8 ISO 27002:2022 - Summary of technical controls

8.1 Information is an asset that, like other business assets, is essential to an organization's business and, consequently, needs to be suitably protected.

8.2 When configuring its cloud infrastructure, 360core practices security by design and privacy by design through appropriate cryptographic methods for data in transit and data at rest to prevent unauthorized access.

8.3 Visibility into network traffic is guaranteed through appropriate cloud observability tools to detect suspicious activities or the presence of threat actors at an early stage. Security events are analyzed and, if found to be incidents, escalated and resolved by taking appropriate countermeasures.

8.4 Changes to software follow strict change management procedures including testing on isolated development environments and the publication of new releases in line with the 4-eyes principle.

8.5 Further Information on detailed physical controls is indicated in the respective policy qualifier.

9 Provisions for termination of service

9.1 In case 360core discontinues, for whatever reason, its identity proofing practice, it notifies Swisscom Trust Services and other relevant relying parties and stakeholders such as its accredited conformity assessment body directly without delay, but no later than 30 days in advance and arranges at its own cost for the archived session audit log data to be securely transferred to the TSP.

9.2 Other stakeholders may be informed through an appropriate notification on 360core public website.

360core AG
Schützengasse 25 · 8001 Zürich · Tel +41 44 700 28 88
solutions@360core.ch · www.360core.ch · CHE-414.534.215 VAT

10 List of accepted identity documents

360 Identities accepts all Electronic Machine-Readable Travel Documents (eMRTD) equipped with a Radio Frequency Identification (RFID) chip that can be read via the Near Field Communication (NFC) protocol and comply with the requirements of ICAO Doc 9303, as per the following list:

COUNTRY	PASSPORT	ID
Afghanistan	Accepted	Accepted
Åland Islands		
Albania	Accepted	Accepted
Algeria	Accepted	
American Samoa	Accepted	
Andorra	Accepted	
Angola	Accepted	
Anguilla	Accepted	
Antarctica		
Antigua and Barbuda	Accepted	
Argentina	Accepted	Accepted
Armenia	Accepted	Accepted
Aruba	Accepted	
Australia	Accepted	
Austria	Accepted	Accepted
Azerbaijan	Accepted	Accepted
Bahamas	Accepted	
Bahrain	Accepted	
Bangladesh	Accepted	
Barbados	Accepted	Accepted
Belarus	Accepted	
Belgium	Accepted	Accepted
Belize	Accepted	
Benin	Accepted	
Bermuda	Accepted	
Bhutan		
Bolivia		
Bonaire, Sint Eustatius and Saba	Accepted	
Bosnia-Herzegovina	Accepted	Accepted
Botswana	Accepted	
Bouvet Island	Accepted	
Brazil	Accepted	Accepted
British Indian Ocean Territory	Accepted	
British Virgin Islands	Accepted	
Brunei Darussalam		
Bulgaria	Accepted	Accepted
Burkina Faso		

Burundi		
Cabo Verde		
Cambodia		
Cameroon	Accepted	
Canada	Accepted	
Cayman Islands	Accepted	
Central African Republic		
Chad		
Chile	Accepted	Accepted
China	Accepted	
Christmas Island	Accepted	
Cocos (Keeling) Islands	Accepted	
Colombia	Accepted	
Comoros		
Congo-Brazzaville		
Congo-Kinshasa		
Cook Islands	Accepted	Accepted
Costa Rica	Accepted	Accepted
Côte d'Ivoire	Accepted	Accepted
Croatia	Accepted	Accepted
Cuba		
Curaçao	Accepted	Accepted
Cyprus	Accepted	Accepted
Czechia	Accepted	Accepted
Denmark	Accepted	
Djibouti		
Dominica	Accepted	
Dominican Republic	Accepted	Accepted
Ecuador	Accepted	
Egypt	Accepted	
El Salvador		
Equatorial Guinea		
Eritrea		
Estonia	Accepted	Accepted
Eswatini		
Ethiopia	Accepted	Accepted
Falkland Islands	Accepted	
Faroe Islands	Accepted	
Fiji	Accepted	
Finland	Accepted	Accepted
France	Accepted	Accepted
French Guiana	Accepted	
French Polynesia	Accepted	
French Southern and Antarctic Lands	Accepted	
Gabon		

Gambia		
Georgia	Accepted	Accepted
Germany	Accepted	Accepted
Ghana	Accepted	
Gibraltar	Accepted	
Greece	Accepted	Accepted
Greenland	Accepted	
Grenada		
Guadeloupe	Accepted	
Guam	Accepted	
Guatemala		
Guernsey	Accepted	
Guinea		
Guinea-Bissau		
Guyana		
Haiti		
Heard Island and McDonald Islands	Accepted	
Honduras		
Hong Kong		
Hungary	Accepted	Accepted
Iceland	Accepted	Accepted
India	Accepted	
Indonesia	Accepted	
Iran	Accepted	
Iraq	Accepted	
Ireland	Accepted	
Isle of Man	Accepted	
Israel	Accepted	Accepted
Italy	Accepted	Accepted
Jamaica	Accepted	
Japan	Accepted	
Jersey	Accepted	
Jordan	Accepted (01.09.2025-)	
Kazakhstan	Accepted	Accepted
Kenya	Accepted	
Kiribati		
Kosovo	Accepted	Accepted
Kuwait	Accepted	
Kyrgyzstan	Accepted	Accepted
Laos		
Latvia	Accepted	Accepted
Lebanon	Accepted	
Lesotho		
Liberia		
Libya		

Liechtenstein	Accepted	Accepted
Lithuania	Accepted	Accepted
Luxembourg	Accepted	Accepted
Macao		
Madagascar		
Malawi		
Malaysia	Accepted	
Maldives	Accepted	Accepted
Mali		
Malta	Accepted	Accepted
Marshall Islands		
Martinique	Accepted	
Mauritania		
Mauritius		
Mayotte	Accepted	
Mexico	Accepted	
Micronesia		
Moldova	Accepted	Accepted
Monaco	Accepted	Accepted
Mongolia	Accepted	Accepted
Montenegro	Accepted	Accepted
Montserrat	Accepted	
Morocco	Accepted	Accepted
Mozambique		
Myanmar		
Namibia	Accepted	
Nauru		
Nepal	Accepted	
Netherlands	Accepted	Accepted
New Caledonia	Accepted	
New Zealand	Accepted	
Nicaragua		
Niger		
Nigeria	Accepted	
Niue	Accepted	
Norfolk Island	Accepted	
North Korea		
North Macedonia	Accepted	
Northern Mariana Islands	Accepted	
Norway	Accepted	Accepted
Oman	Accepted	
Pakistan	Accepted	
Palau		
Palestine	Accepted	
Panama	Accepted	

Papua New Guinea		
Paraguay	Accepted	
Peru	Accepted	Accepted
Philippines	Accepted	
Pitcairn	Accepted	
Poland	Accepted	Accepted
Portugal	Accepted	Accepted
Puerto Rico	Accepted	
Qatar	Accepted	
Réunion	Accepted	
Romania	Accepted	Accepted
Russia	Accepted	
Rwanda	Accepted	
Sahrawi Arab Democratic Republic		
Saint Barthélemy	Accepted	
Saint Helena, Ascension and Tristan da Cunha	Accepted	
Saint Kitts and Nevis	Accepted	
Saint Lucia		
Saint Martin	Accepted	
Saint Pierre and Miquelon	Accepted	
Saint Vincent and the Grenadines	Accepted	
Samoa		
San Marino	Accepted	Accepted
Sao Tome and Principe		
Saudi Arabia	Accepted	
Senegal	Accepted	
Serbia	Accepted	Accepted
Seychelles	Accepted	
Sierra Leone		
Singapore	Accepted	
Sint Maarten	Accepted	
Slovakia	Accepted	Accepted
Slovenia	Accepted	Accepted
Solomon Islands		
Somalia		
South Africa		
South Georgia and the South Sandwich Islands	Accepted	
South Korea	Accepted	
South Sudan		
Spain	Accepted	Accepted
Sri Lanka		
Sudan		
Suriname		
Svalbard and Jan Mayen	Accepted	
Sweden	Accepted	Accepted

Switzerland	Accepted	Accepted (01.12.2026-)
Syria	Accepted	
Taiwan	Accepted	
Tajikistan	Accepted	Accepted
Tanzania	Accepted	
Thailand	Accepted	
Timor-Leste	Accepted	
Togo	Accepted	
Tokelau	Accepted	
Tonga	Accepted	
Trinidad and Tobago		
Tunisia		
Türkiye	Accepted	Accepted
Turkmenistan	Accepted	
Turks and Caicos Islands	Accepted	
Tuvalu		
Uganda	Accepted	
Ukraine	Accepted	Accepted
United Arab Emirates	Accepted	Accepted (08.08.2021-)
United Kingdom of Great Britain	Accepted	
United States Minor Outlying Islands	Accepted	
United States of America	Accepted	
United States Virgin Islands	Accepted	
Uruguay	Accepted	
Uzbekistan	Accepted	Accepted
Vanuatu		
Vatican City	Accepted	Accepted
Venezuela		
Viet Nam	Accepted	
Wallis and Futuna	Accepted	
Yemen	Accepted	
Zambia		
Zimbabwe	Accepted	

360core AG
Schützengasse 25 · 8001 Zürich · Tel +41 44 700 28 88
solutions@360core.ch · www.360core.ch · CHE-414.534.215 VAT

11 Key terms used in the identity proofing context

360 Identities 360 identities is a mobile app designed by 360core used for *identity proofing* and *liveness detection* of online customers making digital fraud practically impossible

Applicant Person (legal or natural) whose *identity* is to be proven

Attack potential *Measure* of the effort needed to exploit a *vulnerability* in a Target of Evaluation (TOE)

Attack Presentation Classification Error Rate (APCER) Proportion of attack presentations using the same presentation attack instrument species incorrectly classified as bona fide presentations in a specific scenario

Authentic source Repository or system, held under the responsibility of a public sector body or private entity, that contains and provides *attributes* about a natural or legal person or object and that is considered to be a primary source of that information or recognized as authentic in accordance with Union or national law, including administrative practice

Authoritative evidence Evidence that is presented by the *applicant*, holds identifying *attribute(s)* of the *identity*, and is trusted for the binding of these attributes to the applicant

Authoritative source Any source irrespective of its form that can be relied upon to provide accurate data, information and/or *evidence* that can be used to prove *identity*

(Identity) attribute Characteristic, quality, right or permission of a natural or legal person or of an object

Binding to applicant Part of an *identity proofing process* that verifies that the *applicant* is the person identified by the presented *evidence*

Bona fide Presentation Classification Error Rate (BPCER) Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

Digital identity document *Identity document* that is issued in a machine-processable form, that is digitally signed by the issuer, and that is in purely digital form

Evidence Processing Server Subcomponent of *360 Identities* hosted in a cloud-based network located in Switzerland and the EU responsible for *identity proofing process* orchestration, *authoritative evidence* evaluation, identity proofing process logging, and observation

eMRTD Electronic Machine-Readable Travel Document

False Acceptance Rate (FAR) Proportion of verification transactions with false biometric claims erroneously accepted

False Rejection Rate (FRR) Proportion of verification transactions with true biometric claims erroneously rejected

Freshness Time between time of issuance of an *evidence* and time of use/validation of the evidence

High attack potential *Measure* of the effort needed by a highly skilled adversary with significant resources and an opportunity to exploit a *vulnerability* in a Target of Evaluation (TOE)

Identity *Attribute* or set of attributes that uniquely identify a person within a given context

Identity document Physical or digital *identity* document issued by an authoritative source and attesting to the *applicant's* identity

Identity proofing context External *requirements* affecting the *identity proofing process*, given by the purpose of the identity proofing, the related regulatory *requirements*, and any resulting restrictions on the selection of *attributes* and *evidence* and on the identity proofing process itself

Identity proofing (process) *Process* by which the *identity*, and possibly additional *attributes*, of an *applicant* is verified by the use of *evidence* attesting to the required identity attributes

Injection attack Attack consisting of injecting content controlled by the attacker into the data capture *process*

Legitimate evidence holder Person for whom the *evidence* is issued

Liveness detection *Measurement* and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture

Liveness verification server Subcomponent of *360 Identities* hosted in a cloud-based network located in the EU used for *liveness detection* of online customers

Measure Variable to which a value is assigned as the result of *measurement*

Measurement *Process* to determine a value

Moderate attack potential *Measure* of the effort needed by a skilled adversary with significant resources and opportunity to exploit a *vulnerability* in a Target of Evaluation (TOE)

Physical identity document *Identity document* issued in physical and human-readable form

(IPSP) practice statement Statement of the practices that an IPSP employs in providing the *identity proofing* trust service component

Presentation attack Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Presentation attack detection (PAD) Automated determination of a *presentation attack*

Process Set of interrelated or interacting activities which transforms inputs into outputs

Pseudonym Fictitious *identity* that a person assumes for a particular

purpose, which differs from their original or true identity

Relying party A recipient of an identification assurance who acts in reliance on that assurance

Remote identity proofing *Identity proofing process* where the *applicant* is physically distant from the location of the identity proofing

Requirement Need or expectation that is stated, generally implied or obligatory

Subject Legal or natural person that is enrolled to a trust service

Threat Potential cause of an unwanted incident, which can result in harm to a system or organization

Trusted register Public register, database, or other source that is an authoritative source for the conveyance of *identity attributes* in the *identity proofing context*

Trust service Electronic service that enhances trust and confidence in electronic transactions

Trust service component One part of the overall service of a *trust service provider (TSP)*

Trust service provider (TSP) Entity which provides one or more *trust service*

Unattended remote identity proofing *Identity proofing process* by remote use of identity document where the capture of the identity document (physical or *digital document*) and the face video of the *applicant* are performed in an automated, interactive session without human supervision

Validation Part of an identity proofing process that determines whether or not *attributes* are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid

Vulnerability Weakness of an asset or control that can be exploited by one or more *threats*