

Remote Identity Verification Policy

QuickSign, 19-21 rue Poissonnière 75002 Paris - RCS: Paris B 450 439 963

Phone: +33 1 825 20 500 – www.quicksign.with

Document history

Version	Description	Date	Validated by
1.0	First version of the document	09/06/2026	Ahmed Boussadia
1.1	Description of hybrid and NFC pathways and decision rules; verification of the validity of identity documents; evidence file; retention periods; GDPR qualification; accessibility; reference corrections.	22/10/2026	Ahmed Boussadia

©QuickSign – PUBLIC

Table of Contents

Document history **2**

Table of Contents **3**

1 Introduction **9**

1.1 General presentation 9

1.2 Document identification 9

1.3 Entities involved in remote identification 9

1.3.1 Remote identification provider *9*

1.3.2 Sponsor *9*

1.3.3 Users *10*

1.4 Use of remote identity verification 10

1.4.1 Applicable areas of use *10*

1.4.2 Prohibited areas of use *10*

1.5 Policy Management 10

1.5.1 Entity managing the policy *10*

1.5.2 Contact point *10*

1.5.3 Entity determining the conformity of a statement of practices with this document *10*

1.5.4 Procedures for approving compliance of the statement of practices *11*

1.6 Definitions and acronyms 11

1.6.1 Acronyms *11*

1.6.2 Definitions *13*

2 Responsibilities regarding the provision of information to be published **17**

2.1 Entities responsible for providing information 17

2.2 Information to be published 17

2.3 Publication deadlines and frequencies 17

2.4 Access control for published information 17

3 Identification and authentication **18**

3.1 Identity attributes 18

3.1.1 Uniqueness of people *18*

3.2 Identity verification 18

3.2.1 Identification method *18*

3.2.2 Fraud *20*

3.2.2.1 Indicators for detecting identity theft attempts 20

3.2.2.2 Technical means implemented to measure the indicators 20

3.2.2.3 Organizational means implemented to measure the indicators 20

3.2.2.4 Actions taken in the event of suspected or confirmed identity theft 20

3.2.2.5 Notification of the nature of the operation to the user and prevention of entrapment risks 20

3.2.2.6 Appeals procedures 20

3.2.3 Data acquisition *21*

3.2.3.1 Terminal 21

©QuickSign – PUBLIC

3.2.3.2 Identity document 21
3.2.3.3 Acquisition of the user's face 22
3.2.4 Validation of an organization's identity *22*
3.2.5 Identity verification of a bearer *22*
3.2.5.1 Terminal 22
3.2.5.2 Identity document 22
3.2.5.2.1 Titles accepted 22
3.2.5.2.2 Checks carried out 22
3.2.5.2.3 Verdict of the verification 24
3.2.5.2.4 Measures applicable to certain types of users 24
3.2.5.2.5 Measures against recurring attacks 24
3.2.5.2.6 Minimum resolution 24
3.2.5.3.1 Minimum resolution 24
3.2.5.3.2 Checks carried out 24
3.2.5.3.3 Verdict of the verification 25
3.2.5.4.1 Minimum resolution 25
3.2.5.4.2 Checks carried out 25
3.2.5.4.3 Verdict of the verification 25
3.2.6 Unverified information from the user *25*
3.3 TRANSMISSION OF THE RESULT TO THE BUSINESS SERVICE 25
3.3.1 Elements included in the transmitted result *25*
3.3.2 Excluded items *26*
4 NON-TECHNICAL SECURITY MEASURES **27**
4.1 PHYSICAL SECURITY MEASURES 27
4.1.1 Geographical location and construction of the sites *27*
4.1.2 Physical access *28*
4.1.3 Power supply and air conditioning *28*
4.1.4 Exposure to water damage *28*
4.1.5 Fire prevention and protection *29*
4.1.6 Preservation of media *29*
4.1.7 Media decommissioning *29*
4.1.8 Offsite backup *29*
4.2 PROCEDURAL SECURITY MEASURES 29
4.2.1 Trusted roles *29*
4.2.1.1 Administrator 30
4.2.1.2 Operator 30
4.2.1.2.1 Mission 30
4.2.1.2.2 Skills and knowledge 30
4.2.1.3 Expertise and Quality Referent – missions related to biometrics 31
4.2.1.3.1 Mission 31
4.2.1.3.2 Skills and knowledge 31
4.2.1.4 Expertise and Quality Referent – missions related to identity documents 32
4.2.1.4.1 Mission 32
4.2.1.4.2 Skills and knowledge 32
4.2.1.5 Security officer 32
4.2.2 Number of people required per task *33*

4.2.3 Identification and authentication for each role 33
4.2.4 Roles requiring a separation of responsibilities 33
4.3 Personnel security measures 33
4.3.1 Qualifications, skills, and authorizations required 33
4.3.1.1 Arrival and departure procedure 33
4.3.2 Background check procedures 34
4.3.3 Initial training requirements 34
4.3.3.1 Awareness 34
4.3.3.2 Training 34
4.3.4 Continuing education requirements and training frequencies 35
4.3.5 Frequency and sequence of rotations between different assignments 35
4.3.6 Penalties for unauthorized actions 35
4.3.6.1 Code of Ethics 35
4.3.7 Requirements for external service provider staff 36
4.3.8 Documentation provided to staff 36
4.4 Audit data compilation procedures 36
4.4.1 Type of event to record 36
4.4.2 Frequency of event log processing 37
4.4.3 Event log retention period 37
4.4.4 Protection of event logs 37
4.4.5 Event log backup procedure 37
4.4.6 Event log collection system 37
4.4.7 Notification of event registration to the event manager 37
4.4.8 Vulnerability assessment 37
4.5 Data archiving and creation of the evidence file 38
4.5.1 Types of data to archive in the evidence file 38
4.5.2 Archive retention period 39
4.5.3 Archive protection 39
4.5.4 Archive backup procedure 40
4.5.5 Data timestamping requirements 40
4.5.6 Archive Collection System 40
4.5.7 Procedure for retrieving and verifying archives 40
4.6 Termination of service 40
5 Technical security measures **41**
5.1 Computer system security measures 41
5.1.1 Terminal-specific technical security requirements 41
5.1.1.1 Integrity of components 41
5.1.1.2 Security of flows 41
5.1.1.3 Identification and authentication 41
5.1.1.4 Supervision and control 41
5.1.2 Specific technical security requirements for computer systems 41
5.1.2.1 Identification and authentication 41
5.1.2.1.1 Use of named accounts 41
5.1.2.1.2 Choosing and sizing passwords 42

©QuickSign – PUBLIC

5.1.2.1.3 Strong authentication 42
5.1.2.1.4 Default accounts 42
5.1.2.1.5 Privileged accounts 42
5.1.2.1.6 Identification and authentication of business services 42
5.1.2.1.7 Administrator identification and authentication 42
5.1.2.1.8 Operator identification and authentication 42
5.1.2.2.1 Access control policy 43
5.1.2.2.2 Periodic review of accounts 43
5.1.2.3 Administration and operation 43
5.1.2.4 Integrity of components 43
5.1.2.4.1 Security of sensitive assets 43
5.1.2.4.2 IT infrastructure security 44
5.1.2.5 Security of flows 45
5.1.2.5.1 Flow matrix and filtering policy 45
5.1.2.5.2 Interconnections of the service's information system 45
5.1.2.5.3 Data stream encryption 46
5.1.2.6 Logging and auditing 46
5.1.2.7 Supervision and control 46
5.1.2.7.1 Security incident management 46
5.1.2.7.2 Operational bulletins 46
5.1.2.7.3 Quality and level of service 47
5.1.2.7.4 Test plan for the effectiveness of the measures 47
5.1.2.8 Awareness 47
5.1.3 Computer system security assessment level *48*
5.2 Security measures related to system development 48
5.2.1 Security management measures *48*
5.2.1.1 Secure development 48
5.2.1.2 Password protection 48
5.2.2 System lifecycle security assessment level *48*
5.3 Network security measures 48
5.3.1 Terminal connection *48*
5.3.2 Segmentation and compartmentalization *49*
5.3.3 Services visible from the internet *49*
5.3.4 Internet gateway *49*
5.4 Timestamping / dating system 49
6 Compliance audit and other assessments **50**
6.1 Frequency and/or circumstances of assessments 50
6.2 Identity and qualifications of assessors 50
6.3 Relationships between evaluators and evaluated entities 50
6.4 Scope of assessments 50
6.5 Actions taken following the conclusions of the evaluations 50
6.6 Communication of results 50
7 Other business and legal issues **51**
7.1 Prices 51
7.2 Financial responsibility 51

7.2.1 Insurance coverage 51
7.2.2 Other resources 51
7.2.3 Coverage and warranty for user entities 51
7.3 Confidentiality of professional data 51
7.3.1 Scope of confidential information 51
7.3.2 Information outside the scope of confidential information 51
7.3.3 Responsibilities regarding the protection of confidential information 52
7.4 Protection of personal data 52
7.4.1 Alternative to remote identity verification 52
7.4.2 Personal Data Protection Policy 52
7.4.3 Personal information 52
7.4.3.1 Non-biometric personal data and raw biometric data 53
7.4.3.2 Biometric personal data 53
7.4.4 Non-personal information 54
7.4.5 Responsibility in terms of personal data protection 54
7.4.6 Notification and consent to the use of personal data 54
7.4.7 Conditions for disclosing personal information to judicial or administrative authorities 54
7.4.8 Other circumstances of disclosure of personal information 54
7.4.9 Accessibility 54
7.5 Intellectual and industrial property rights 54
7.6 Contractual interpretations and guarantees 54
7.7 Warranty limitations 55
7.8 Limitation of liability 55
7.9 Compensation 55
7.10 Duration and early termination of this policy 55
7.10.1 Validity period 55
7.10.2 Early termination of validity 55
7.10.3 Effects of expiry and clauses remaining applicable 55
7.11 Individual notifications and communications between participants 55
7.12 Amendments to the Policy 55
7.12.1 Amendment procedures 55
7.12.2 Mechanism and period for providing information on amendments 56
7.12.3 Circumstances under which the OID needs to be changed 56
7.12.4 User information 56
7.13 Provisions concerning conflict resolution 56
7.14 Competent jurisdictions 56
7.15 Compliance with laws and regulations 56
7.16 Miscellaneous provisions 56
7.16.1 Entire agreement 56
7.16.2 Transfer of activities 56
7.16.3 Consequences of an invalid clause 56
7.16.4 Application and waiver 57
7.16.5 Force majeure 57

7.17 OTHER PROVISIONS 57
APPENDIX 1:List of authorized identity documents 58

1 Introduction

1.1 General presentation

This document is QuickSign's Remote Identity Verification Policy. It outlines all the commitments made by QuickSign within the framework of its remote identity verification service to achieve Extended LoIP certification, in accordance with Implementing Regulation (EU) 2025/1566 and in particular with the ETSI TS 119 461 standard.

1.2 Document identification

This document is uniquely identified by the following OID:1.2.250.1.546.1.1.1.1
This OID is broken down as follows:

QuickSign root	Service PVID	Extended LoIP level offer	Document type: policy	Document version
1.2.250.1.546	1	1	1	1

1.3 Entities involved in remote identification

1.3.1 Remote identification provider

QuickSign is the service provider operating the remote identity verification service. It is responsible for carrying out the following four steps:

- the acquisition of identification data;
- verification of identification data;
- the preparation of the evidence file;
- the transmission of results to the sponsor.

1.3.2 Sponsor

Within the framework of this policy, the sponsor is a QuickSign customer, an organization subject to anti-money laundering and counter-terrorist financing regulations that uses the QuickSign service for business onboarding in accordance with Regulation (EU) 2024/1624. It may also be a Qualified Trust Service Provider (QTSP) as defined by eIDAS using the QuickSign service for the issuance of qualified certificates.

1.3.3 Users

Users are natural persons, clients of the sponsor, who use the QuickSign service to identify themselves remotely.

1.4 Use of remote identity verification

1.4.1 Applicable areas of use

The remote identification service is designed to enable:

- Establishing secure remote business relationships.
- Remote identification for the purpose of issuing qualified certificates under the eIDAS Regulation.

1.4.2 Prohibited areas of use

The service described in this policy is not intended to be used for any regulated identification service other than that described in the previous section.
Future versions of this policy may include extensions applicable to other areas.

1.5 Policy Management

1.5.1 Entity managing the policy

The policy is managed by the Steering Committee for the QuickSign remote identification service.

1.5.2 Contact point

QuickSign can be contacted at the following address:

QuickSign, 19-21 rue Poissonnière 75002 Paris - RCS: Paris B 450 439 963

plainte-pvid@QuickSign.com

1.5.3 Entity determining the conformity of a statement of practices with this document

The entity defined in 1.5.1 determines the conformity of the statement of practices with this policy.

1.5.4 Procedures for approving compliance of the statement of practices

The entity defined in 1.5.1 determines the conformity of the statement of practices to this document through an internal approval process. This approval process includes a review of completed audits.

1.6 Definitions and acronyms

1.6.1 Acronyms

Acronym	Meaning
ANSSI	National Cybersecurity Agency
CGU	General Terms of Use
CNI	National identity card
CNIe	National electronic identity card
CNIL	National Commission for Information Technology and Freedoms
CSCA	Country Signing Certification Authority
ETSI	European Telecommunications Standards Institute
FMR / FNMR	False Match Rate / False Non-Match Rate
HTTP	Hypertext Transfer Protocol
IAD	Injection Attack Detection
ICAO	International Civil Aviation Organization (OACI)
IP	Internet Protocol
LDFM	Liveness Detection and Face Matching
LoIP	Level of Identity Proofing
MRZ	Machine Readable Zone
NFC	Near Field Communication

NTP	Network Time Protocol
OID	Object Identifier
PA	Passive Authentication (verification of the chip data signature)
PAD	Presentation Attack Detection
SAP	Security Assurance Plan
PRADO	Public Register of Authentic travel and identity Documents Online
PVID	Remote Identity Verification Provider
QTSP	Qualified Trusted Service Provider
GDPR	General Data Protection Regulation (EU) 2016/679
IS	Information system
SSI	Information systems security
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier (Wi-Fi network name)
TDS	Residence permit
TLS	Transport Layer Security
TS	Technical Specification (ETSI technical specification)
EU	European Union
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WCAG	Web Content Accessibility Guidelines

©QuickSign – PUBLIC

1.6.2 Definitions

Identity attributes – subset of identification data transmitted by the remote identity verification service to the business service

Sponsor – entity responsible for a business service that uses a remote identity verification service

Component of the information system – any software or hardware component of the information system involved in providing the remote identity verification service.

Consent – any freely given, specific, informed and unambiguous indication of the user's wishes by which he or she, by a statement or by a clear affirmative action, agrees to the processing of personal data relating to him or her.

Interim findings on remote identity verification – information generated by the remote identity verification service as part of analyses carried out by automated processes or by operators, and necessary for the development of the remote identity verification verdict. Several interim findings may contribute to the same verdict.

Service Agreement – a written agreement or contract between a remote identity verification provider and a client for the performance of the service. If the provider is a private organization, the service agreement includes the contract.

Declaration of remote identity verification practices – A set of practices (organization, operational procedures, technical and human resources, etc.) that the remote identity verification provider applies in the context of providing its service and in accordance with the remote identity verification policy it has committed to respecting. The declaration of remote identity verification practices is confidential and is made available only to those individuals who have a need to know.

Liveness detection – the detection of the "live" nature of the user aims to authenticate the video of the user's face, to verify that it has not been subject to physical or digital alteration.

Identification data – a set of personal data acquired and verified by the service in order to verify the identity of a natural person. Within the framework of this reference document, identification data may be the video of the user's face, the video of the identity document

presented by the user, or data relating to the user (including the photograph of the user's face) stored in the security component of the identity document.

Personal data – any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Biometric data – personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm his or her unique identification.

Evidence file – an element retained by the service provider containing relevant information to be produced for the resolution of disputes, or in the event of an investigation, and in particular to provide evidence in court. This framework specifies the minimum data to be retained. The data contained in the evidence file is not retained for biometric processing.

State of the art – a collection of best practices, technologies, and reference documents relating to information systems security or identity verification that are publicly accessible, and the information that clearly derives from them. These documents may be made available online by the information systems security community, disseminated by reference bodies, or originate from legislative, regulatory, or normative sources.

Extended LoIP – "Extended" identity verification level as defined by ETSI TS 119 461. This is the level required for identity verification prior to the issuance of qualified certificates as defined in Implementing Regulation (EU) 2025/1566.

Legitimate holder of the identity document – person to whom the identity document was issued by the issuing country, and whose identity is represented by that identity document.

Reason for failure – Cause of a “failure” verdict for remote identity verification. The reason for the failure is transmitted by the remote identity verification service to the business service or the user and allows, in particular, for differentiation between a failure

related to suspected fraud and a failure for technical reasons (insufficient terminal camera resolution, insufficient lighting, focusing problem, etc.). In the case of suspected fraud, the reason does not include any information about the checks performed or the type of fraud suspected.

Electronic identification means – a tangible and/or intangible element containing personal identification data and used to authenticate oneself for an online service.

Remote Identity Verification Policy – A set of rules, identified by a unique identifier (OID), defining the requirements that a remote identity verification service provider must meet in setting up and delivering its service. A remote identity verification policy may also, if necessary, identify the obligations and requirements of other stakeholders, including users and sponsors. The remote identity verification policy is made available to users.

Provider – legal entity that provides a remote identity verification service.

Service provision – provision of remote identity verification services to a client, within the framework of the service agreement established between the provider and the client.

Result of remote identity verification – a set of information transmitted by the remote identity verification service to the business service, including the verdict (success or failure) of the remote identity verification, the reason for failure where applicable, and the identity attributes relating to the users required by the business service and verified by the provider.

Subcontracting – operation by which the service provider entrusts, under its responsibility, to an entity all or part of the execution of the service agreement (and where applicable the contract) concluded with the client.

Remote Identity Verification Service – service subject to this reference document, responsible for acquiring and verifying user identification data in order to identify them, for compiling the evidence file and for transmitting the result of the remote identity verification to the business service.

Asynchronous remote identity verification service – a remote identity verification service is said to be asynchronous when the verification phase of identification data is carried out at a later date than the acquisition phase of identification data.

Hybrid remote identity verification service – A remote identity verification service is considered hybrid when the verdict “success” of the remote identity verification result can

©QuickSign – PUBLIC

only be pronounced by an operator after the latter has validated the results of the verifications carried out by automated processes and performed their own verification of the identification data.

Business service – service with which the user wishes to identify themselves, which is the responsibility of the sponsor, using the remote identity verification service.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Identity document – an official document certifying a person's identity.

User – natural person whose identity is verified by the remote identity verification service.

Identity theft – the act of fraudulently using the identification data of a third party. Within the framework of this reference document, the concept of identity theft also encompasses identity alteration, which consists of using fraudulent identification data that does not belong to an existing person.

2 Responsibilities regarding the provision of information to be published

2.1 Entities responsible for providing information

QuickSign is responsible for publishing the information listed in §2.2.

2.2 Information to be published

QuickSign undertakes to provide the following information to users and the sponsor:

- This remote identity verification policy;
- The General Terms of Use (CGU) of the remote identity verification service.

This information is publicly available on the publication website at the following address:https://www.QuickSign.com/fr/conformite/

2.3 Publication deadlines and frequencies

The documents listed in §2.2 are published after each update.

2.4 Access control for published information

The published information is made available to the public in accordance with the requirements of this Chapter 2. It is freely accessible for reading. Additions, deletions, and modifications to this information are limited to persons authorized by the entity responsible for the published information.

3 Identification and authentication

3.1 Identity attributes

3.1.1 Uniqueness of people

The uniqueness of the identified person is ensured by the following set of attributes of the identity document:

- Name(s);
- First name(s);
- Date of birth;
- Place of birth.

This set of attributes is considered to uniquely characterize a person.

3.2 Identity verification

3.2.1 Identification method

QuickSign implements two remote identity verification workflows, without operator assistance during capture. Both fall under Annex C.3.4 of the ETSI TS 119 461 V2.1.1 (2025-02) standard:

(a) a hybrid process, combining automated controls and the decision of a trained operator:
   (i) the user films their physical identity document (VideoID brick), under anti-injection control (IAD);
   (ii) the user completes a liveness detection (PAD) and injection detection (IAD) session, and their face is compared with the photograph on the identity document;
   (iii) A trained operator examines the videos and the results of the automated processing, then pronounces the verdict.

(b) an NFC process, known as the automatic method, with automatic validation, for identity documents equipped with a chip conforming to the ICAO 9303 standard and for which Appendix 1 indicates "NFC eligibility: yes" (in particular identity cards conforming to Council Regulation (EU) 2025/1208 of 12 June 2025 and passports):
   (i) the user films their identity document (VideoID brick), under anti-injection control (IAD);

(ii) the chip of the identity document is read by NFC and the electronic signature of the data is verified up to the issuing State's Country Signing Certification Authority (CSCA);
(iii) access to the chip requires the CAN or MRZ band data of the document; the identity data retained is that of the chip, authenticated up to the CSCA;
(iv) A liveness detection, injection detection and face comparison session compares the user's face to the photograph stored in the chip.

Option (a) falls under use case 9.2.3.3 of the ETSI TS 119 461 V2.1.1 (2025-02) standard. It is referred to as a “hybrid method” in the remainder of this document. It applies to identity documents not equipped with a chip, or when chip reading is impossible. Binding the identity document to the individual uses alternative (b) of requirement USE-9.2.3.3-05X (automated biometrics, with fallback to manual verification).
Process (b) falls under use case 9.2.3.4 of the ETSI TS 119 461 V2.1.1 (2025-02) standard. It is referred to as the “automatic method” in the remainder of this document. When all checks are successful, the identity is automatically validated. Records reviewed by an operator following a biometric failure fall under use case 9.2.3.3, alternative b) (biometrics with fallback to manual verification).

An identity document whose expiry date has passed is rejected in both methods. In the automatic method, the expiry date read from the chip (DG1) is compared to the verification date; an expired document results in an automatic "failure" verdict, without switching to the hybrid method.
The following decision rules apply to both methods:

Situation	Decision
Invalid chip data signature (NFC scan)	**Automatic rejection**, without human review
Attempted injection detected (IAD) or failure of liveness detection (PAD)	**Automatic rejection**, without human review
Face comparison failed	Human review by an operator, according to the file review procedure. The operator can lift the failure if they establish a false rejection; the reason is recorded in the evidence file. The files thus validated are subject to ex-post control by sampling of

	the FEB (§3.2.5.3.3 and §3.2.5.4.3)
Chip reading not possible for an NFC-enabled document	The case can be redirected to the hybrid method

The list of eligible identity documents is available in APPENDIX 1 of this document.

3.2.2 Fraud

3.2.2.1 Indicators for detecting identity theft attempts

The identification process is based on the following indicators:

- Indicators for detecting inconsistencies in the identity document;
- Resemblance rate between the user and the photo on the identity document;
- Liveness detection indicators;
- Assessment by a trained operator.

The details of each indicator are confidential and are described in the remote identification practices statement.

3.2.2.2 Technical means implemented to measure the indicators

The technical means implemented are confidential and are described in the remote identification practices statement.

3.2.2.3 Organizational means implemented to measure the indicators

The organizational measures implemented are confidential and are described in the remote identification practices statement.

3.2.2.4 Actions taken in the event of suspected or confirmed identity theft

In the event of identity theft, whether proven or suspected, whether detected by the service provider or communicated by the client's business service, an alert is raised.

The procedures for managing and reporting alerts are confidential and are described in the remote identification practices statement. These procedures include systematically informing the Expertise and Quality Referent depending on the nature of the fraud.

3.2.2.5 Notification of the nature of the operation to the user and prevention of entrapment risks

The methods used are confidential and are described in the remote identification practices statement.

3.2.2.6 Appeals procedures

The user can contact the service provider at the contact point defined in §1.5.2, or contact the client directly, in particular:

- For the purpose of cancelling a fraudulent identity.
- In the event of refusal to authenticate the user when the user is acting in good faith.
- In the event of a proven malfunction of the remote identity verification service.

In the event of an appeal, the request will be handled and monitored by QuickSign's support service, as follows:

- In the event of identity fraud reported by the user, an incident ticket is created and the sponsor is notified.
- In the event of problems of technical origin, the quality teams are informed.

Any claim related to alleged or proven identity theft will be presented to the Expertise and Quality Referent, who will rule on the veracity and seriousness of the situation.

3.2.3 Data acquisition

3.2.3.1 Terminal

The acquisition of user identification data is carried out by the user's terminal.
Within the framework of the hybrid method, the installation of an application provided by QuickSign on the user's mobile device is not necessary: the service is entirely web-based.
As part of the automatic method, the installation of a native application including a QuickSign module that allows access to the NFC component of the terminal is required.
It should be noted that the application in question is not provided directly by QuickSign but is integrated within a service of the sponsor (for example, mobile banking application), which may be required to access the service.
The process is offered in French only.

3.2.3.2 Identity document

Within the framework of the hybrid method, to ensure correct capture of the identity document, the user will be asked to ensure:

- an adequate light level for capture;
- Ensure that the focus is effective to guarantee that the capture is not blurry;
- that no reflection is permanently present on the document, preventing it from being read;
- To be in a quiet place with no background noise;
- That nothing obstructs the reading of the identity document;
- that they hold the identity document by the edges to optimize its readability.

The acquisition of the identity document is unpredictable, so that it cannot be replayed by an attacker. The mechanisms used are confidential and detailed in the associated practices statement.

In the context of the automatic method, the user needs to have (a) a terminal equipped with an NFC reader and (b) an identity document equipped with an NFC chip (see APPENDIX 1 for a complete list of eligible documents).

3.2.3.3 Acquisition of the user's face

To ensure proper capture of their face, the user may be asked to:

- ensure an adequate level of brightness for capture;
- Ensure that the focus is effective to guarantee that the capture is not blurry;
- To be in a quiet place with no background noise;
- ensure that nothing obstructs the capture of the face.

A random control mechanism makes the face acquisition phase unpredictable so that it cannot be replayed by an attacker.

3.2.4 Validation of an organization's identity

Not applicable.

3.2.5 Identity verification of a bearer

3.2.5.1 Terminal

No processing, even partial, relating to the authenticity of the document presented or to the correspondence of the user's face extracted from the identity document or to liveness detection is carried out on the terminal.

3.2.5.2 Identity document

3.2.5.2.1 Titles accepted

The forms of identification accepted under this policy are identified in APPENDIX 1 of this document.

3.2.5.2.2 Checks carried out

In the automated method, following the reading of information on the NFC chip of the identity document, the cryptographic signature of the extracted data is verified, and the root certificate that signed the extracted data is checked to ensure it corresponds to an approved issuing authority (CSCA). Access to the chip requires the CAN or MRZ data from the document; the retained identity data is that of the chip, authenticated up to the CSCA. CSCA certificates are retrieved from the official websites of the issuing countries (generally government ministries). A document whose CSCA is not known to QuickSign is directed to the hybrid method if its design meets the graphical acceptability threshold; otherwise, it is rejected.

Within the framework of the hybrid method, the remote identity verification practices statement associated with this policy:

- identifies, for each accepted identity document, the security features verified by QuickSign. QuickSign relies on the online public register of authentic identity and travel documents (PRADO);
- for each verified security feature of accepted identity documents:
    - describes all the checks carried out;
    - specifies for each check whether it is carried out automatically or by a human operator, and whether it is carried out systematically or only under certain conditions;
- identifies, for each accepted identity document, the unverified security features of the identity document among those referenced in the online public register of authentic identity and travel documents (PRADO) and, for each unverified security feature, a justification is provided where applicable.

QuickSign has a team of Expertise and Quality referents, competent for all accepted identity documents; these referents are designated in the inventory of trusted roles.

The declaration of remote identity verification practices identifies, for each accepted identity document, whether a validity check of the identity document is carried out via a service provided by the issuing State, and if so:

- identifies the validity verification service;
- specifies whether this validity check is carried out automatically or by a human operator;
- specifies whether this validity check is carried out systematically or only under certain conditions, and if so, describes these conditions;
- specifies the consequences if the validity verification service is unavailable.

QuickSign identifies validity verification services from the list published by the Council of the European Union in the PRADO register ("Check the validity of document numbers"). When a service of the issuing state is accessible to QuickSign, the operator consults it during the review of the file within the framework of the hybrid method.
Under the automated method, the authenticity and integrity of the document data are established by cryptographic verification of the chip; this verification alone cannot determine whether the document has been reported lost, stolen, or revoked. No validity verification services are consulted in this method: these services exist only for some issuing states, access is often restricted or limited to manual consultation, and they are not practically usable in an automated process covering many states (ETSI TS 119 461, VAL-8.3.2-03, notes 4 and 5). The residual risk of a reported lost or stolen document that goes undetected is addressed in the risk analysis: it is reduced by comparing the user's

face, under liveness and injection detection, with the chip photograph, and essentially remains only for an imposter who closely resembles the cardholder. It is considered acceptable.
National services reserved for government agencies, including the French service DocVerif, are not accessible to QuickSign.

Furthermore, identity documents showing physical damage (torn or damaged identity document, etc.) are subject to a "failure" verdict in accordance with the limits defined in the statement of practices.

3.2.5.2.3 Verdict of the verification

If a validity check of the identity document is carried out and it concludes that the identity document is invalid, then the verdict of the remote identity verification is systematically "failure".

The user only receives a “success” or “failure” response from the service, but does not receive details of the checks, nor the cause of the failure.

3.2.5.2.4 Measures applicable to certain types of users

The remote identity verification practices statement specifies whether particular security measures are applied to certain types of users to strengthen controls designed to prevent identity theft. If so, the remote identity verification practices statement details these measures.

3.2.5.2.5 Measures against recurring attacks

The remote identity verification practices statement details the measures implemented to limit repeated attack attempts. Users have a limited number of attempts, set at 3, to complete their identity verification.

3.2.5.2.6 Minimum resolution

The service recommends, if possible, a capture of at least 720p (1280×720, 25 frames per second) for optimal processing.
In general, the better the quality and smoother the video collected, the better the quality of the control operations and the lower the rejection rate due to poor video quality.

3.2.5.3 Face comparison

3.2.5.3.1 Minimum resolution

See previous section.

3.2.5.3.2 Checks carried out

The Remote Identity Verification Practices Statement associated with this policy describes all the checks performed when comparing the user's face to the photograph on their identity document. The Remote Identity Verification Practices Statement specifies for each

check whether it is performed automatically or by a human operator, and whether it is performed systematically or only under certain conditions. Where applicable, these conditions are described in the Remote Identity Verification Practices Statement.

3.2.5.3.3 Verdict of the verification

The declaration of remote identity verification practices specifies the procedures applied when an operator pronounces a verdict of "success" when the results of automated processing relating to the comparison of the user's face suggest a verdict of "failure". These files are part of the population controlled a posteriori by the FEB's sampling review procedure ("picking") (random sampling, 95% confidence, margin of error of 3 to 5%), which verifies the correct application of the review procedures.
An injection attempt detected by automated processing results in an automatic "failure" verdict. In this case, review by an operator is not possible.

3.2.5.4 Liveness detection

3.2.5.4.1 Minimum resolution

See previous section

3.2.5.4.2 Checks carried out

The remote identity verification practices statement associated with this policy describes all checks performed as part of the liveness detection process. The remote identity verification practices statement specifies for each check whether it is performed automatically or by a human operator, and whether it is performed systematically or only under certain conditions. Where applicable, these conditions are described in the remote identity verification practices statement.

3.2.5.4.3 Verdict of the verification

A failure to detect liveness results in a "failure" verdict: review by an operator cannot overturn this verdict. Only a failure of face comparison can be overturned by an operator (§3.2.5.3.3).
An injection attempt detected by automated processing results in an automatic "failure" verdict. In this case, review by an operator is not possible.

3.2.6 Unverified information from the user

Not applicable

3.3 Transmission of the result to the business service

3.3.1 Elements included in the transmitted result

The result is transmitted to the client for each verification, regardless of the verdict.
It includes:

- the verdict (success or failure);

- for a "success" verdict, the level of verification achieved: Extended LoIP as defined by the ETSI TS 119 461 standard;
- in case of failure, a generic reason (technical failure, or refusal due to suspicion of fraud), without details of the checks carried out;
- verified identity attributes (list below);

- the image of the identity document extracted from the video.

These identity attributes are as follows (in the automatic method, an attribute absent from the chip is not transmitted):

- birth name(s) or married name(s) if applicable;
- first name(s);
- sex;
- date of birth;
- Place of birth;
- identity document number;
- type of identity document;
- issuing authority of the identity document.

3.3.2 Excluded items

The videos of the identity document and face are not transmitted to the sponsor.
The result contains no score or details of the checks carried out, beyond the verdict and the generic reason.

4 Non-technical security measures

Risk analysis

QuickSign conducted a risk analysis covering two areas:

- An information systems security risk analysis, enabling the definition of security measures to be implemented by the service;
- A risk analysis specific to identity theft.

Risk analysis and risk treatment plans are reviewed annually and validated by QuickSign Management, represented by the Deputy General Manager.

In accordance with the claimed Extended LoIP level, the risk analysis considers at a minimum attackers with a high attack potential (as defined in ETSI TS 119 461), particularly for presentation attacks, injection attacks and identity document attacks.

QuickSign applies a documented threat intelligence procedure, which covers information system threats and identity fraud ([POL] Cyber and Regulatory Intelligence Policy; [PRS] Cyber Intelligence Processing Procedure). Its findings inform risk analysis, testing plans, and operator training.

Information System Security Policy

QuickSign defines and implements an information systems security policy based on the risk assessment and the risk treatment plan.

QuickSign reviews the information systems security policy at least annually, and in the event of a change in the risk assessment or risk treatment plan.

QuickSign has its information systems security policy formally validated in writing by its management.

4.1 Physical security measures

QuickSign identifies appropriate physical security measures and continually raises user awareness of the risks involved in circumventing the rules (see 4.3.3.1).

4.1.1 Geographical location and construction of the sites

QuickSign hosts and processes data relating to the remote identity verification service exclusively within the territory of a Member State of the European Union.

QuickSign operates and administers the remote identity verification service exclusively from the territory of a Member State of the European Union.

Staff can remotely access the service's information system only via a VPN with two-factor authentication, from workstations managed by QuickSign, and from the territory of a Member State of the European Union.

4.1.2 Physical access

QuickSign's solution is hosted by cloud service providers within the European Union. The physical machines provided by these providers are dedicated to QuickSign.
The service contract includes requirements for the physical security of access to the servers.
The hosting providers of the QuickSign solution implement mechanisms to ensure that only authorized persons can access the premises housing the remote identity verification service information system.
In particular, access to server rooms and technical areas is controlled using locks or badge access control systems. Unaccompanied access by external service providers to server rooms and technical areas is prohibited, unless it is possible to strictly track access and restrict it according to time slots. A review of access rights is conducted regularly to identify unauthorized access.
When an employee leaves or a service provider changes, it is necessary to withdraw access rights or change access codes.
Finally, network ports located in areas open to the public (meeting rooms, reception areas, corridors, closets, etc.) should be restricted or disabled to prevent an attacker from easily gaining access to the company network.
The hosting providers of the QuickSign solution implement mechanisms to log access to premises hosting the remote identity verification service information system.
The hosting providers of the QuickSign solution define and implement measures to ensure the confidentiality and integrity of access logs to the premises hosting the remote identity verification service.

4.1.3 Power supply and air conditioning

Contingency measures are in place to ensure that an interruption of power supply service, or an air conditioning failure, does not affect QuickSign's availability commitments.

4.1.4 Exposure to water damage

QuickSign takes into account the risks inherent in water damage. Protective measures are implemented by hosting providers to mitigate residual risks.

4.1.5 Fire prevention and protection

Secure areas are subject to appropriate fire prevention and protection measures.

4.1.6 Preservation of media

The media are stored securely.

4.1.7 Media decommissioning

Media considered sensitive in terms of confidentiality are subject to destruction measures, or can be reused in an operational context of an identical level of sensitivity.

4.1.8 Offsite backup

QuickSign develops and implements a backup and recovery plan for the remote identity verification service devices. This backup plan includes the following components:

- system backup;
- configuration backup;
- data backup.

QuickSign tests the backup and restore plan at least once a year.
QuickSign defines and implements measures to ensure the confidentiality and integrity of backups performed, at the same level as that required by this policy for the verification system.
QuickSign complies with all the measures and recommendations on securing backups of the [ISO27002] standard.
The backup plan includes the following elements:

- the list of data deemed vital for the organization and the servers concerned;
- the different types of backup;
- the frequency of backups;
- the procedure for administering and executing backups;
- storage information and access restrictions to backups;
- restoration testing procedures;
- the destruction of the media that contained the backups.

4.2 Procedural security measures

4.2.1 Trusted roles

QuickSign has defined the following trusted roles:

- Administrator;
- Operator;
- Expertise and Quality Referent (single role; its missions relate to biometrics and identity documents);
- Security officer;

- Internal auditor: consults the archives and logs of the service to check their compliance; this role is incompatible with those of administrator and operator within the audited scope.

All staff in trusted roles are based in metropolitan France.

4.2.1.1 Administrator

The administrator is responsible for the administration and configuration of all technical components of the service, as well as its day-to-day operation. The administrator is authorized to perform backups and restores.

4.2.1.2 Operator

4.2.1.2.1 Mission

The operator performs the following tasks:

a) verify, in accordance with this identity verification policy, the identity of users based on the user identification data acquired, and the results of automated processing carried out on this identification data;
b) pronounce the verdict “success” or “failure” relating to the remote identity verification and generate an alert whenever identity theft or alteration is suspected or detected.

4.2.1.2.2 Skills and knowledge

The operator possesses the following skills:

a) Know and apply the remote identity verification policy;
b) Know and apply the information systems security policy;
c) Know the current threat landscape related to identity theft;
d) Know and apply the legislation and regulations in force relating to the protection of personal data, and in particular the [GDPR];
e) Understand the attackers' methods of operation that lead to the risk scenarios identified in the risk assessment, and in particular those relating to identity documents and biometrics;
f) Be a physiognomist, able to recognize and compare faces on photo and video media;
g) Know the security features of identity documents and the checks to be carried out to identify fake or altered identity documents;

h) Know and master the use of the PRADO register.

4.2.1.3 Expertise and Quality Referent – missions related to biometrics

4.2.1.3.1 Mission

The Expertise and Quality Referent role is a single role. Their missions and skills are presented below by area.
The Expertise and Quality Referent is responsible for the following tasks:

a) Process alerts generated by operators when they suspect or detect an occurrence of a risk scenario identified in the risk assessment and related to biometrics;
b) Examine, within the framework of the review by the referents (PVIDQS-TS119461-0010), the files invalidated by the picking, in particular those validated by an operator after a failure of the face comparison, and derive training or procedural actions from them;
c) Provide training for operators in biometric verification, including verification of biometric identification data and face comparison;
d) Provide training for operators on the attackers' methods of operation used to carry out the risk scenarios identified in the assessment of identity theft risks related to biometrics;
e) Verify that operators have the expected skills related to biometrics;
f) Formally validate changes to the remote identity verification policy when these changes relate to biometrics;
g) Validate the design and implementation of biometric verifications performed by automated processing.

4.2.1.3.2 Skills and knowledge

The Expertise and Quality Referent possesses the following skills:

a) Know and apply the remote identity verification policy;
b) Know and apply the information systems security policy;
c) Know the current threat landscape related to identity theft;
d) Master the threat landscape related to biometrics;
e) Know and apply the legislation and regulations in force relating to the protection of personal data, and in particular [GDPR];
f) Master the attackers' methods of operation used to carry out the risk scenarios identified in the risk assessment and related to biometrics;
g) Master the checks to be carried out to identify the occurrences of the risk scenarios identified in the risk assessment and related to biometrics;
h) Know and apply the procedures relating to alerts generated by an operator when they suspect or detect an occurrence of a risk scenario identified in the risk assessment and relating to biometrics;

©QuickSign – PUBLIC

i) Know and apply the picking and review procedure by the referents (PVIDQS-TS119461-0010).

4.2.1.4 Expertise and Quality Referent – missions related to identity documents

4.2.1.4.1 Mission

The Expertise and Quality Referent carries out the following missions:

a) Formally validate changes to the remote identity verification policy when these changes relate to identity documents;
b) Process alerts generated by operators when they suspect or detect a risk scenario identified in the risk assessment and related to the identity document;
c) Examine, within the framework of the review by the referents (PVIDQS-TS119461-0010), the files invalidated by the picking which relate to identity documents, and derive training or procedural actions from them;
d) Provide training for operators in identity document verification, and in particular in checking the security features of identity documents in order to identify fake or altered identity documents;
e) Provide training for operators on the attackers' methods of operation used to carry out the risk scenarios identified in the assessment of identity theft risks related to identity documents;
f) Verify that operators possess the expected skills related to identity documents

4.2.1.4.2 Skills and knowledge

The Expertise and Quality Referent possesses the following skills:

a) Know and apply the remote identity verification policy;
b) Know and apply the information systems security policy;
c) Master the threat landscape related to counterfeit identity documents;
d) Know and apply the legislation and regulations in force relating to the protection of personal data, and in particular the [GDPR].

4.2.1.5 Security officer

Under this policy, the security officer is responsible for liaising with the relevant state services in the event of fraud or attack.

The security officer is also an information systems security expert, supported by management. This contact person is known to all users and is the first point of contact for all questions relating to information systems security:

- definition of the rules to be applied according to the context;
- verification of the application of the rules;
- raising user awareness and defining a training plan for IT professionals;

- centralization and processing of security incidents observed or reported by users.

This designated contact person is trained in information systems security and crisis management.

4.2.2 Number of people required per task

QuickSign employs a sufficient number of operators and Expertise and Quality Referents, who carry out the defined missions and have the identified skills, to fully and comprehensively provide the remote identity verification service.

4.2.3 Identification and authentication for each role

See §5.1.2.1 (Identification and authentication) and §5.1.2.2.1 (Access control policy).

4.2.4 Roles requiring a separation of responsibilities

The roles of operators and Expertise and Quality Referents are exclusive.

4.3 Personnel security measures

4.3.1 Qualifications, skills, and authorizations required

QuickSign verifies the training, qualifications, and professional references of candidates for the remote identity verification service. It also verifies the accuracy of their resumes prior to hiring them.
QuickSign develops and implements a regular control plan to verify that operators and Expertise and Quality Referents possess the identified skills.

4.3.1.1 Arrival and departure procedure

All rights granted to an individual are revoked upon their departure or in the event of a change of position. Onboarding and offboarding procedures are defined in conjunction with the human resources department. They take into account:

- the creation and deletion of computer accounts and associated mailboxes;
- the rights and access to be granted and withdrawn from a person whose role changes;
- the management of physical access to the premises (allocation, return of badges and keys, etc.);
- the allocation of mobile equipment (laptop, USB key, hard drive, smartphone, etc.);
- the management of sensitive documents and information (transfer of passwords, changing passwords or codes on existing systems).

4.3.2 Background check procedures

QuickSign asks candidates to provide proof that they are not subject to an entry in Bulletin No. 3 of their criminal record that would be inconsistent with their duties.

4.3.3 Initial training requirements

Upon arrival at the entity, the new employee is informed of the security issues, the rules to be respected and the good practices to adopt in terms of information systems security through awareness and training actions.

4.3.3.1 Awareness

After recruitment, operators must undergo awareness training on the specific risks related to their function and be informed of their duty of discretion.
They cover at least the following topics:

- the objectives and challenges faced by the entity in terms of information systems security;
- information considered sensitive;
- regulations and legal obligations;
- the rules and security guidelines governing daily activity: compliance with the security policy, no connection of personal equipment to the entity's network, no disclosure of passwords to a third party, no reuse of professional passwords in the private sphere and vice versa, reporting of suspicious events, etc.;
- the available means that contribute to system security: systematic session locking when the user leaves their workstation, password protection tools, etc.;
- the rules for choosing and sizing passwords;
- the risks caused by circumventing physical security rules;
- the risks associated with mobile devices.

4.3.3.2 Training

To ensure they are at the forefront of information systems security, operational teams undergo training upon taking up their posts on:

- the legislation in force;
- the main risks and threats;
- maintaining systems in a secure condition;
- authentication and access control;
- fine-tuning and hardening of systems;
- network segmentation;
- logging.

This general training plan is complemented by a training plan specific to each trusted role (see 4.2.1).

QuickSign ensures that, prior to performing the service, each operator and Expertise and Quality Referent has successfully completed the training plan and passed the control plan.

4.3.4 Continuing education requirements and training frequencies

QuickSign develops and implements a regular training plan for operators and Expertise and Quality Referents in line with the identified missions and skills.
In particular, in accordance with the FEB operator training plan (PVIDQS-TS119461-0009), teams undergo continuous training of at least one day per month and formal refresher training at least once a year, followed by an assessment of acquired skills, on the topics mentioned in §4.3.3.2. A supplementary session is organised for each change in the threat, accepted identity documents or decision rules.
These training courses are complemented by regular awareness-raising activities, tailored to the target users and which can take various forms (emails, display, meetings, dedicated intranet space, etc.).

4.3.5 Frequency and sequence of rotations between different assignments

Not applicable

4.3.6 Penalties for unauthorized actions

4.3.6.1 Code of Ethics

QuickSign has a code of ethics integrated into its internal regulations, stipulating in particular that:

- The services are performed with integrity, discretion and impartiality;
- staff only use methods, tools and techniques validated by QuickSign;
- Staff members undertake not to disclose any information to a third party, even anonymized and decontextualized, obtained or generated within the framework of the service, except with formal, written and authenticated authorization from the client;
- Staff members undertake to report to the service provider any illegal content discovered during the service;
- Staff members commit to respecting applicable national legislation and regulations and best practices related to their activities.

QuickSign requires all its staff to sign a document indicating that the person has read the code of ethics prior to performing the service.
QuickSign ensures compliance with the code of ethics and provides for disciplinary sanctions for operators, administrators and experts of the verification service who have violated the security rules or the code of ethics.

4.3.7 Requirements for external service provider staff

In the event of outsourcing all or part of its IT system or data, QuickSign assesses upstream the specific risks of IT outsourcing (control of the information system, remote actions, shared hosting, etc.) in order to take into account, from the drafting of the requirements applicable to the future provider, the appropriate security needs and measures.
The operators and the Expertise and Quality Referents are contractually bound with QuickSign or with one of its subcontractors in the case of subcontracting part of its activity.
To formalize these commitments, the service provider provides QuickSign a security assurance plan (SAP) or any equivalent document. This is a contractual document describing all the specific measures that the subcontractor undertakes to implement to guarantee compliance with the security requirements specified by QuickSign.
The service contracts include specific clauses to guarantee regular training in information systems security for external staff, particularly IT service providers.

4.3.8 Documentation provided to staff

QuickSign makes available to operators and Expertise and Quality Referents all the training and technical resources that enable them to fulfill the missions entrusted to them.

4.4 Audit data compilation procedures

QuickSign maintains relevant logs to detect potential malfunctions and attempts at unauthorized access to information system components.
In particular, QuickSign has determined the critical components of its information system and defined the list of events to be recorded.

4.4.1 Type of event to record

Security-related events are logged.
In particular, QuickSign logs:

- all automated processes and actions performed by human operators as part of a remote identity verification;
- all physical access to the premises housing the remote identity verification service's information system;
- Firewall: packets blocked;
- systems and applications: authentication and authorization (failures and successes), unexpected shutdowns;

- services: protocol errors (e.g., 403, 404, and 500 errors for HTTP services), traceability of application flows to interconnections (URLs on an HTTP relay, message headers on an SMTP relay, etc.).

4.4.2 Frequency of event log processing

QuickSign performs a correlation of logs between the different components of the remote identity verification service information system.
QuickSign conducts a sampling review of logs, and in particular of operations carried out by operators.

4.4.3 Event log retention period

QuickSign has defined an event log retention policy, which sets out their retention periods.
Security-critical events are kept for at least 365 days.

4.4.4 Protection of event logs

Event logs are subject to protection measures to ensure their integrity, availability and confidentiality.

4.4.5 Event log backup procedure

Event logs are collected to ensure their backup.

4.4.6 Event log collection system

All automated processing and actions performed by human operators as part of a remote identity verification are centralized on a component of the information system to which the operators do not have access rights.

4.4.7 Notification of event registration to the event manager

Not applicable.

4.4.8 Vulnerability assessment

QuickSign conducts vulnerability monitoring and applies security patchesapplies security patches on all system components within one month of their release by the publisher.
QuickSign has defined a system update policy that describes:

- the way in which the inventory of information system components is carried out;
- sources of information relating to the publication of updates;
- the tools to deploy the patches across the fleet;

- the potential qualification of the fixes and their gradual deployment across the fleet.

Obsolete components that are no longer supported by their manufacturers are isolated from the rest of the system. To anticipate this obsolescence, a number of precautions are put in place, if necessary, by QuickSign:

- establish and maintain an inventory of the information system's systems and applications;
- choose solutions whose support is guaranteed for a duration corresponding to their use;
- monitor software updates and end-of-support dates;
- maintain a homogeneous software portfolio (the coexistence of different versions of the same product multiplies the risks and complicates monitoring);
- limit software dependencies, that is, the dependencies of operation of one software program on another, particularly when support for the latter comes to an end;
- include in contracts with service providers and suppliers clauses guaranteeing the monitoring of security patches and the management of obsolescence;
- identify the time and resources needed (material, human, budgetary) for the migration of each software application at the end of its life (non-regression tests, backup procedure, data migration procedure, etc.).

4.5 Data archiving and creation of the evidence file

Each identity check, whether it results in a "success" or a "failure" verdict, leads to the creation of an evidence file.

4.5.1 Types of data to archive in the evidence file

The minimum required elements of the evidence file are as follows:

- the user's photograph extracted from the video of their face;

- for the automatic method, the photograph stored in the chip (DG2);
- the photograph of the identity document;
- the user's first and last names;
- the user's date and place of birth;
- the unique identity document number;
- the issuing authority of the identity document;
- the type of identity document;
- the date of issue and expiry of the identity document;
- the date of acquisition of identification data;

- the identifier of the operator or the Expertise and Quality Referent who verified the identification data and pronounced the verdict;
- the date of verification of identification data;
- the date on which the verdict was pronounced;
- all checks carried out on the identification data, as well as the result of the remote identity verification transmitted to the business service, in particular:
    - the nature of the verification
    - the interim findings produced by automated processing, the operator or the Expertise and Quality Referent following the verification
    - the verdict of the remote identity verification (success or failure)
    - the reasons given by the operator or the Expertise and Quality Referent in the event of a "failure" verdict, or in the event of a "success" verdict contrary to the result of the automated processing

- the type of method used to verify the user's identity;
- for the automatic method, the result of the verification of the chip data signature;
- the results of liveness detection (PAD) and injection detection (IAD);
- the level of verification achieved (Extended LoIP) in the event of a "success" verdict;
- where applicable, the record of the consultation of a document validity verification service (service, date, result);
- identification of the sponsor (legal entity).

These elements provide all the information necessary for resolving disputes.
The evidence file does not contain any data intended for biometric processing.

4.5.2 Archive retention period

Evidence files are kept for at least 7 years, whether or not the identity verification service is used to generate a qualified certificate; this minimum period notably covers the requirement of the ETSI EN 319 411-2 standard. A longer period applies when required by the sponsor or by regulations, in particular to align it with the duration of the contract for which identification was required, in compliance with the GDPR.

4.5.3 Archive protection

The evidence file is generated by QuickSign, then sealed with a QuickSign electronic seal (entity seal) including a timestamp, which guarantees its integrity and origin. It is then encrypted and transmitted to a legal archivist, Docapost Arkhinéo, for preservation, access traceability, and integrity guarantee.
The data contained in the evidence file is not subject to any biometric processing except in the case of a judicial request, in compliance with applicable regulatory requirements.
Evidence files are automatically destroyed at the end of the retention period.

4.5.4 Archive backup procedure

The archives are backed up to ensure their availability.

4.5.5 Data timestamping requirements

In order to correlate events between different components, their time synchronization source (using the NTP protocol) must be identical.
The acquisition date of identification data is obtained from the service servers and is synchronized at least once every 24 hours via NTP with a reliable time source.

4.5.6 Archive Collection System

QuickSign sets up an archive collection system in order to centralize the data in an evidence file.

4.5.7 Procedure for retrieving and verifying archives

Evidence files can be retrieved in the event of a court order. Furthermore, the user has the right to access the data in the evidence file, as well as the processing carried out by QuickSign on this data.

However, access to certain data will not be permitted (details of checks) due to QuickSign's legitimate interest in keeping the details of the security measures implemented confidential;

Furthermore, given the need to maintain the integrity of the evidence file to preserve its legal validity, the user may not modify the evidence file but may request that the sponsor correct their data. The correction will require a level of verification at least equivalent to the initial level of verification.

4.6 Termination of service

QuickSign maintains a business cessation plan (PVIDQS-TS119461-0008), reviewed annually, to minimize the impact of a service interruption and ensure the availability of evidence. In the event of a service interruption, QuickSign notifies the sponsors, the supervisory body, and the conformity assessment body at least three months in advance; terminates subcontractor authorizations; maintains access to evidence files for the entire retention period, either directly or by transferring this responsibility to a third party; and destroys or revokes the service's private keys.

5 Technical security measures

5.1 Computer system security measures

5.1.1 Terminal-specific technical security requirements

5.1.1.1 Integrity of components

For the hybrid method, the service does not require the installation of a specific application on the user's device. It is a service that can be called from an application of the client.
For the automatic method, it is necessary for the user to install a native application from the sponsor including the QuickSign component for identity verification via the NFC chip.

The service uses technologies that allow for the direct capture of necessary video streams without interruption. Any transmission of a video stream or part of a video stream under the user's control is prohibited.

The client monitors the availability of fraudulent applications designed to replace its application calling the QuickSign service, on official application stores.

5.1.1.2 Security of flows

QuickSign protects the confidentiality and authenticity of the identification data exchanged between the user's terminal and the remote identity verification service.

5.1.1.3 Identification and authentication

QuickSign authenticates the terminal when it is under its responsibility or that of the business service (authentication by certificate for example).

5.1.1.4 Supervision and control

QuickSign carries out monitoring to detect the availability of fraudulent applications aimed at replacing the service, on official application stores.

5.1.2 Specific technical security requirements for computer systems

5.1.2.1 Identification and authentication

5.1.2.1.1 Use of named accounts

QuickSign uses named user accounts whenever possible. The use of generic or service accounts is minimal and strictly limited to a small number of staff. Generic and service accounts are managed according to a policy at least as strict as that for named user accounts. Furthermore, a named administrative account, separate from the user account, is assigned to each administrator. The login credentials and authentication secrets are different. This administrative account, which has greater privileges, is dedicated

exclusively to administrative tasks. Moreover, it is used in environments dedicated to administration to avoid leaving connection logs or password hashes in a more exposed environment.

5.1.2.1.2 Choosing and sizing passwords

QuickSign defines rules for choosing and sizing passwords.
QuickSign oversees and verifies the application of these rules, in particular through awareness actions (see 4.3.3 and 4.3.4).

5.1.2.1.3 Strong authentication

Whenever possible, QuickSign implements two-factor authentication.

5.1.2.1.4 Default accounts

The default authentication elements of the system components are modified upon installation. When it comes to passwords, they are chosen according to recommendations regarding selection, sizing, and storage.

5.1.2.1.5 Privileged accounts

In particular, accounts with specific rights, such as privileged accounts, receive special attention. QuickSign keeps an inventory of these accounts, updates it regularly and records the following information:

- users with an administrator account or rights greater than those of a standard user on the information system;
- users with sufficient rights to access the working directories of managers or all users;
- users using a workstation not administered by the IT department and which is not subject to security measures dictated by the entity's general security policy.

QuickSign defines and uses a simple and clear nomenclature to identify service accounts and administration accounts.

5.1.2.1.6 Identification and authentication of business services

The service performs mutual authentication with the business service when it transmits the results. The protocol used guarantees the integrity, confidentiality, and anti-replay protection of the transmitted data.

5.1.2.1.7 Administrator identification and authentication

Administrators use, whenever possible, named accounts with two-factor authentication.

5.1.2.1.8 Operator identification and authentication

Operators use named accounts with two-factor authentication.

5.1.2.2 Access control

QuickSign restricts operators' access to the remote identity verification service's information system to what is strictly necessary for the performance of their duties.

5.1.2.2.1 Access control policy

QuickSign establishes a precise list of sensitive resources (see 5.1.2.4). For each of these, QuickSign:

- defines which population can have access to it;
- strictly controls access, ensuring that users are authenticated and belong to the targeted population;
- avoids its dispersion and duplication in uncontrolled locations or areas subject to less strict access control.

5.1.2.2.2 Periodic review of accounts

QuickSign conducts periodic reviews of these accounts to ensure that access to sensitive elements (particularly work directories and managers' email accounts) is controlled. These reviews also allow for the removal of access that has become obsolete, for example, following a user's departure.
A regular review of access rights is also carried out in order to identify unauthorized access.

5.1.2.3 Administration and operation

The workstations of administrators, operators and Expertise and Quality Referents are connected exclusively to the remote identity verification service's information system. In particular, a workstation or server used for administrative actions must under no circumstances have access to the Internet.
If access to the internet or other information systems is required, administrators and operators must have a workstation separate from their administration workstation, deployed in an area external to the remote identity verification service's information system.
The administration network is specifically segmented, particularly from the users' office network, to protect against any compromise through forwarding from a user workstation to an administration resource (at a minimum, cryptographic logical compartmentalization based on VPN tunnels and VLANs).

5.1.2.4 Integrity of components

5.1.2.4.1 Security of sensitive assets

QuickSign identifies the list of sensitive data in order to protect it effectively. From this list of sensitive data, QuickSign determines which components of the information system they are located on (databases, file shares, workstations, etc.). These components correspond to the critical servers and workstations for QuickSign. In this capacity, they are subject to specific security measures, which may relate to backup, logging and access.

5.1.2.4.2 IT infrastructure security

Workstation security

QuickSign establishes a minimum level of security across the entire IT infrastructure of the entity (user workstations, servers, printers, telephones, USB devices, etc.) by implementing the following measures:

- limit installed applications and optional web browser modules to only those that are necessary;
- equip user workstations with a local firewall and antivirus software;
- encrypt the partitions where user data is stored;
- disable automatic executions (autorun).

In the event of a necessary derogation from the overall security rules applicable to workstations, these must be isolated from the system (if it is impossible to update certain applications for compatibility reasons, for example).

Local firewalls on workstations are enabled.

To standardize security policies, QuickSign relies, whenever possible, on centralized management including as many IT devices as possible.

Removable media

QuickSign protects itself against threats related to the use of removable media, particularly the connection of unknown USB drives. Furthermore, QuickSign minimizes the use of uncontrolled USB drives on the information system by having their contents inspected by the workstation's antivirus software.

Messaging

Users are made aware of email security (see 4.3.3.1). Furthermore, forwarding work emails to personal email accounts is prohibited.

QuickSign has an upstream antivirus scanning system for users' mailboxes to prevent the receipt of infected files and enables TLS encryption of exchanges between mail servers (of the entity or public) as well as between user workstations and the servers hosting the mailboxes.

Workstation administration

An IT system user, regardless of their hierarchical position or responsibilities, does not have administrative privileges on their workstation. Only administrators specifically tasked with workstation administration should have these rights when performing their tasks. If a delegation of privileges on a workstation is truly necessary to meet a specific user need, it is documented, time-limited, and revoked upon expiration.

Wi-Fi

Network architecture segmentation helps limit the impact of a radio intrusion to a specific area of the information system. Traffic from devices connected to the Wi-Fi access network is filtered and restricted to only the necessary traffic. Furthermore, QuickSign uses robust

encryption and centralized authentication, ideally via client certificates on the machines. Protecting the Wi-Fi network with a single, shared password is discouraged. If a password is necessary, it must be complex and its renewal scheduled, but it must never be shared with unauthorized third parties. Access points must also be managed securely (e.g., dedicated interface, change of the default administrator password). Finally, all Wi-Fi connections from personal or visitor devices (laptops, smartphones) are kept separate from the entity's Wi-Fi connections (e.g., separate SSIDs and VLANs, dedicated internet access).

Mobile terminals

QuickSign has implemented a mobile device security policy. Users are made aware of mobile device security (see 4.3.3.1). QuickSign implements information protection measures for mobile use, such as:

- the positioning of a privacy filter,
- the widespread adoption of mobile phones,
- the encryption of the disk's contents,
- securing the network connection of workstations used in mobile environments.

5.1.2.5 Security of flows

QuickSign creates and maintains a simplified network diagram (or map) representing the different IP zones and their associated addressing scheme, routing and security equipment (firewalls, application relays, etc.), and interconnections with external systems (the Internet, private networks, etc.) and partners. This diagram also allows for the location of servers holding sensitive information about the entity.

5.1.2.5.1 Flow matrix and filtering policy

QuickSign develops and maintains an up-to-date detailed description of the information system architecture of the remote identity verification service.

The information system is dedicated exclusively to QuickSign's trust services, which include the remote identity verification service. Any other service that does not involve a component of a trust service is performed on an information system physically isolated from the service's information system.

QuickSign develops and maintains the flow matrix for the remote identity verification system, as well as the associated filtering policy. This policy only allows flows strictly necessary for the operation of the remote identity verification service.

The flow matrix (incoming and outgoing) is reduced to the precise operational need, maintained over time, and the equipment configuration conforms to it.

5.1.2.5.2 Interconnections of the service's information system

QuickSign identifies, in the detailed description of the information system architecture of the remote identity verification service, the set of interconnections of the information

system of the identity verification service with third-party information systems, including the information system of the business service.
This interconnection takes place directly over the Internet. To ensure information security, QuickSign establishes a site-to-site tunnel in compliance with ANSSI recommendations.
QuickSign filters all traffic at the interconnections of the remote identity verification service's information system. In particular, IP filtering is performed by a firewall located as close as possible to the point where traffic enters the QuickSign network.

5.1.2.5.3 Data stream encryption

Secure network protocols should be used whenever possible, whether on public networks (the Internet, for example) or on the internal network of QuickSign.
All sensitive data transmitted over the Internet is systematically encrypted using appropriate protocols.

5.1.2.6 Logging and auditing

See 4.4.

5.1.2.7 Supervision and control

5.1.2.7.1 Security incident management

QuickSign has a security incident management procedure in place. This procedure includes:

- Notification of the security officer;
- Recording the incident in an incident log.

5.1.2.7.2 Operational bulletins

QuickSign includes in the operational bulletins, at a minimum:

- the operational indicators of the service (see next section);
- a review of complaints received, being processed or closed;
- a review of the list of occurrences of the risk scenarios identified in the risk analysis;
- a review of security incidents detected on the remote identity verification service's information system;
- a review of alerts generated by the remote identity verification service;
- the changes made to the remote identity verification service;
- changes to the remote identity verification policy;
- changes to the risk analysis, in particular if the list of risk scenarios is modified.

QuickSign transmits to the sponsor, at the frequency defined in the service agreement (quarterly by default), the operational bulletins relating to the remote identity verification service.
QuickSign protects operational bulletins, especially in terms of confidentiality.

5.1.2.7.3 Quality and level of service

QuickSign develops and implements a process for learning from detected incidents and fraud in order to continuously improve the effectiveness of its remote identity verification service.

QuickSign defines the operational indicators for the remote identity verification service with the client. These indicators include, at a minimum:

- The average waiting time for users;
- The number of remote identity checks carried out, regardless of the results of these checks;
- The number of remote identity checks based on the results of these checks (success or failure).

QuickSign develops and maintains a process for measuring indicators describing, for each of the operational indicators, the methods and means implemented by the provider to measure the indicator.

5.1.2.7.4 Test plan for the effectiveness of the measures

QuickSign develops and maintains a test plan to assess the effectiveness of measures aimed at evaluating the service's ability to detect identity theft attempts. This plan covers the following areas:

- authenticity of the identity document
- liveness detection
- face comparison
- risks related to influencing user behavior.

The test plan is validated by the Expertise and Quality Referents for each of the parts concerning them.

The test plan is executed by QuickSign annually and with each major change to the service, update to the risk assessments, or to the risk treatment plan. The results of the execution are recorded in a report and validated by the Expertise and Quality Referents.

If the rates measured during the execution of the test plan are lower than the target rates defined in the statement of practices:

- The designated contacts are informed without delay.
- An incident is created and then a remediation plan is defined to address the deviations.

5.1.2.8 Awareness

See 4.3.3.1

5.1.3 Computer system security assessment level

Not applicable.

5.2 Security measures related to system development

5.2.1 Security management measures

5.2.1.1 Secure development

QuickSign implements measures for the secure development of the software used, in particular:

- The software undergoes regular code reviews by another developer;
- The software must undergo non-regression testing before a new version is put into production;
- The software must undergo a documented acceptance testing process for each version to be put into production;
- The software generates suitable recording logs for correlating records between different processes in the service;
- The software developer is aware of the specific risks associated with the field of identity verification, and is bound by an obligation of confidentiality;
- Software development must be carried out under conditions allowing the actions of each developer to be audited;
- Each software vendor is required to inform the service provider of any internal fraud or attack aimed at altering the software provided;
- Each software supplier is considered a subcontractor of the service provider for the general application of information protection measures.

5.2.1.2 Password protection

The stored passwords are protected using secure solutions such as encryption or hashing mechanisms.

5.2.2 System lifecycle security assessment level

Not applicable.

5.3 Network security measures

5.3.1 Terminal connection

Only connections from terminals controlled by the entity are permitted on its various access networks, whether wired or wireless.

5.3.2 Segmentation and compartmentalization

The network architecture design incorporates segmentation into zones composed of systems with homogeneous security requirements. A zone is characterized by dedicated VLANs and IP subnets, or even dedicated infrastructure depending on its criticality. Segmentation measures, such as IP filtering using a firewall, are implemented between the different zones. In particular, equipment and data flows associated with administrative tasks are segmented as much as possible.

5.3.3 Services visible from the internet

Internet hosting infrastructure is physically isolated from all other information system infrastructure that is not intended to be visible from the internet. QuickSign implements an infrastructure to interconnect these services with the internet, allowing traffic related to these services to be filtered separately from other traffic within the organization. It also involves requiring incoming traffic to pass through a reverse proxy server incorporating various security mechanisms.

5.3.4 Internet gateway

QuickSign implements a secure internet access gateway comprising at least a firewall as close as possible to the internet access point to filter connections and a proxy server incorporating various security mechanisms. This proxy notably ensures user authentication and request logging.

5.4 Timestamping / dating system

See 4.5.5.

6 Compliance audit and other assessments

6.1 Frequency and/or circumstances of assessments

QuickSign has the following audits carried out:

- An internal audit carried out by external service providers specializing in the field;
- A certification audit carried out at least every 2 years.

6.2 Identity and qualifications of assessors

The assessors have proven expertise in information systems security and are specialists in the field of activity of the controlled component.

6.3 Relationships between evaluators and evaluated entities

QuickSign guarantees the independence and impartiality of the evaluator.

6.4 Scope of assessments

QuickSign develops and implements a control plan covering the entire scope of the remote identity verification service. This control plan aims to ensure that the information systems security policy and the identity verification policy are applied.
QuickSign reviews the control plan at least annually and

- in the event of a structural change to the information system of the remote identity verification service, particularly those concerning:
  - its hosting,
  - its infrastructure and
  - its architecture, or
- in the event of a structural change to the risk assessment, the risk treatment plan, the information systems security policy or the remote identity verification policy

6.5 Actions taken following the conclusions of the evaluations

Following an evaluation, QuickSign:

- updates the risk treatment plan to incorporate the results of the controls;
- has the results of the controls formally validated in writing by its management.

6.6 Communication of results

The results of the checks are confidential and are not made public.

7 Other business and legal issues

7.1 Prices

The price is contractually agreed upon between the client and QuickSign. There is no charge for the service between QuickSign and the user.

7.2 Financial responsibility

7.2.1 Insurance coverage

QuickSign has taken out civil liability and cyber insurance of an appropriate amount to cover the risks associated with the use of the service it provides.

7.2.2 Other resources

QuickSign has the necessary financial resources to fulfill the obligations defined in this policy.

7.2.3 Coverage and warranty for user entities

Not applicable.

7.3 Confidentiality of professional data

7.3.1 Scope of confidential information

The following information is considered confidential:

- Videos and identity data captured by the service;
- The biometric data calculated by the service;
- The results of the various checks, both human and automated, carried out by the service;
- Evidence files;
- Event logs;
- Audit reports;
- Declarations of practices associated with this document;
- The documentary corpus associated with this document.

7.3.2 Information outside the scope of confidential information

This document, the Terms and Conditions and more generally all data on the publication site are public.

7.3.3 Responsibilities regarding the protection of confidential information

QuickSign ensures the protection of confidential information.

7.4 Protection of personal data

7.4.1 Alternative to remote identity verification

In accordance with CNIL requirements regarding biometric processes, QuickSign systematically offers an alternative process. The implementation of the alternative process is the responsibility of the sponsor, and the arrangements may vary depending on the sponsor (for example, a face-to-face process). The user can also use the eID connectors or the European Digital Identity Wallet (EUDI Wallet) offered by QuickSign.

7.4.2 Personal Data Protection Policy

QuickSign applies a data protection policy that complies with applicable regulatory requirements, in particular the GDPR, the revised French Data Protection Act, and the guidelines of the CNIL (French Data Protection Authority). As such, the service provider adheres to the principle of data minimization for the data collected and stored.

7.4.3 Personal information

The personal data of users processed by the remote verification service are as follows:

Personal data	Biometric processing
User video capture	Yes (raw data)
Biometric measurements taken from the user's video capture	Yes (generated data)
Video capture of the identity document	Yes (raw data)
Data extracted from the video of the user's identity document:	N/A
• User's birth name and, if applicable, married name	No
• First name(s)	No
• Date of birth	No
• Place of birth	No
• Identity document number	No
• Sex	No

• Contents of the machine-readable zone (MRZ) of the document	No
• Photo on the identity document	Yes (raw data)
Biometric measurements taken from the photograph extracted from the identity document	Yes (generated data)

7.4.3.1 Non-biometric personal data and raw biometric data

The conditions are similar for each of the data points.

Retention period	at least 7 years for all evidence records, whether a qualified certificate is generated or not; a longer period applies where required by the sponsor (e.g. in line with the duration of the contract requiring video identification) or by regulation.
Storage method	The data is kept for 90 days after receipt in an active database of the remote identity verification provider.
Method of destruction	Automatic destruction of the file by a reliable erasure method at the end of the retention period.
Access method	This file is accessible only to QuickSign operators during the verification process, and then only to: - By judicial order - Upon request from the person concerned to exercise their right of access.
Retention purposes	Legal basis: - Preservation for evidentiary purposes in case of litigation - Retention for the purpose of legal compliance with the obligations imposed by the ETSI TS 119 461 standard.

7.4.3.2 Biometric personal data

The conditions are similar for each of the data points.

Retention period	A few moments, the time it takes to execute the algorithm.
Storage method	Not retained. Biometric templates exist only in RAM during the verification session and are never saved.
Method of destruction	Automatic memory erasure after algorithm execution.
Access method	Not accessible outside the application (the data is created, used by the application to establish the verdict, and then immediately deleted).

7.4.4 Non-personal information

Not applicable.

7.4.5 Responsibility in terms of personal data protection

QuickSign complies with current regulations, in particular the GDPR and the CNIL guidelines regarding biometrics.
For the processing necessary for identity verification and the creation of the evidence file, QuickSign acts as an independent data controller.

7.4.6 Notification and consent to the use of personal data

QuickSign collects explicit consent to use personal data, in particular biometric data.

7.4.7 Conditions for disclosing personal information to judicial or administrative authorities

Personal information may be made available to judicial or administrative authorities under the conditions provided for by the regulations.

7.4.8 Other circumstances of disclosure of personal information

Users can exercise their right to access their personal data, in accordance with the GDPR.

7.4.9 Accessibility

QuickSign designs its service to make it accessible to people with disabilities, in accordance with the requirements of Article 15 of Regulation (EU) No 910/2014 and Directive (EU) 2019/882.
The process is subject to accessibility audits against the WCAG standard. Corrective measures are tracked in QuickSign's action plan.
QuickSign aims for compliance with level AA of WCAG 2.1, as adopted by the EN 301 549 standard.
When a user cannot complete the process, the sponsor provides an alternative process (§7.4.1).

7.5 Intellectual and industrial property rights

Not applicable.

7.6 Contractual interpretations and guarantees

Not applicable.

7.7 Warranty limitations

Warranty limitations are outlined in the Terms and Conditions.

7.8 Limitation of liability

QuickSign is not responsible for misuse of its service.
QuickSign cannot be held liable for indirect damages related to the use of its service, in particular in the event of inability to establish remote identification of a user, even if this request is legitimate.

7.9 Compensation

Not applicable.

7.10 Duration and early termination of this policy

7.10.1 Validity period

This policy comes into effect upon its being made available on the publication site and is valid until replaced by a new version.

7.10.2 Early termination of validity

This policy remains in effect until a new version is published.

7.10.3 Effects of expiry and clauses remaining applicable

The clauses relating to the retention of evidence files remain applicable.

7.11 Individual notifications and communications between participants

Communications between QuickSign, sponsors and users are made by means provided for in the service agreement, and by the point of contact defined in §1.5.2.

7.12 Amendments to the Policy

QuickSign may amend this policy.

7.12.1 Amendment procedures

The amendment procedure takes the form of publishing a new version. Any change relating to biometrics or identity documents must be validated by the relevant Expertise and Quality Referent before publication.

7.12.2 Mechanism and period for providing information on amendments

QuickSign notifies sponsors of any new version at least 90 days before it comes into effect, unless changes are required by regulations or service security.

7.12.3 Circumstances under which the OID needs to be changed

In the event of a major change, the OID will be changed.

7.12.4 User information

QuickSign notifies the sponsor of the publication of a new version.

7.13 Provisions concerning conflict resolution

In case of conflict, an amicable solution may be found by contacting the point defined in §1.5.2.

7.14 Competent jurisdictions

Unless otherwise agreed between the parties, exclusive jurisdiction is granted to the competent courts within the jurisdiction of the Court of Appeal of Paris.

7.15 Compliance with laws and regulations

The provisions of this policy comply with French law.

7.16 Miscellaneous provisions

7.16.1 Entire agreement

Not applicable.

7.16.2 Transfer of activities

See §4.6: in the event of cessation or transfer of activity, the obligations to retain evidence files are maintained or transferred to a third party, in accordance with the business cessation plan (PVIDQS-TS119461-0008).

7.16.3 Consequences of an invalid clause

In the event that any clause of this policy is deemed unwritten or held void, the other clauses shall remain valid.

7.16.4 Application and waiver

Not applicable.

7.16.5 Force majeure

QuickSign cannot be held responsible for any damage resulting from a situation of force majeure.

7.17 Other provisions

Not applicable.

APPENDIX 1:List of authorized identity documents

The following list details the identity documents eligible for the QuickSign authentication process. All documents listed below are eligible for the hybrid authentication method. Documents eligible for the automated authentication method are identified by the “NFC Eligibility” column. Documents accepted for the hybrid method must have at least three security features, including at least two optically variable features that can be verified remotely.

Country code	Country name	Document type	NFC eligibility	PRADO code
AFG	Afghanistan	passport	Yes	AFG-AO-01001
AFG	Afghanistan	passport	Yes	AFG-AO-01002
AFG	Afghanistan	passport	Yes	AFG-AO-04001
AGO	Angola	passport	No	AGO-AO-01001
AIA	Anguilla	passport	No	AIA-AO-01001
ALB	Albania	identity card	No	ALB-BO-01001
ALB	Albania	passport	Yes	ALB-AO-02001
AND	Andorra	passport	No	AND-AO-02001
AND	Andorra	passport	Yes	AND-AO-01001
AND	Andorra	passport	Yes	AND-AO-03001
ARE	United Arab Emirates	passport	Yes	ARE-AO-02001
ARE	United Arab Emirates	passport	Yes	ARE-AO-03001
ARG	Argentina	passport	Yes	ARG-AO-02001
ARG	Argentina	passport	Yes	ARG-AO-03001
ARG	Argentina	passport	Yes	ARG-AO-04001
ARM	Armenia	passport	Yes	ARM-AO-01001
ARM	Armenia	passport	Yes	ARM-AO-02001
AUS	Australia	passport	No	AUS-AO-01001
AUS	Australia	passport	No	AUS-AO-02002
AUS	Australia	passport	No	AUS-AO-03001
AUS	Australia	passport	Yes	AUS-AO-04001
AUS	Australia	passport	Yes	AUS-AO-05001
AUS	Australia	passport	Yes	AUS-AO-06001

©QuickSign – PUBLIC

AUT	Austria	identity card	No	AUT-BO-02001
AUT	Austria	identity card	No	AUT-BO-02002
AUT	Austria	identity card	No	AUT-BO-02003
AUT	Austria	identity card	Yes	AUT-BO-03001
AUT	Austria	passport	Yes	AUT-AO-02001
AUT	Austria	passport	Yes	AUT-AO-02002
AUT	Austria	passport	Yes	AUT-AO-03001
AZE	Azerbaijan	passport	Yes	AZE-AO-02002
AZE	Azerbaijan	passport	Yes	AZE-AO-03001
BDI	Burundi	passport	No	BDI-AO-01001
BDI	Burundi	passport	Yes	BDI-AO-02001
BEL	Belgium	identity card	No	BEL-BO-08001
BEL	Belgium	identity card	No	BEL-BO-09001
BEL	Belgium	identity card	No	BEL-BO-09002
BEL	Belgium	identity card	No	BEL-BO-09003
BEL	Belgium	identity card	Yes	BEL-BO-10001
BEL	Belgium	identity card	Yes	BEL-BO-10002
BEL	Belgium	identity card	Yes	BEL-BO-10003
BEL	Belgium	identity card	Yes	BEL-BO-11004
BEL	Belgium	identity card	Yes	BEL-BO-11005
BEL	Belgium	passport	Yes	BEL-AO-09003
BEL	Belgium	passport	Yes	BEL-AO-10003
BEL	Belgium	passport	Yes	BEL-AO-11001
BEL	Belgium	passport	Yes	BEL-AO-11002
BEL	Belgium	passport	Yes	BEL-AO-11003
BEN	Benin	passport	No	BEN-AO-01001
BEN	Benin	passport	Yes	BEN-AO-02001
BEN	Benin	passport	Yes	BEN-AO-03001
BFA	Burkina Faso	passport	Yes	BFA-AO-03001
BFA	Burkina Faso	passport	Yes	BFA-AO-04001
BGD	Bangladesh	passport	No	BGD-AO-01001
BGD	Bangladesh	passport	Yes	BGD-AO-02001
BGD	Bangladesh	passport	Yes	BGD-AO-03001
BGD	Bangladesh	passport	Yes	BGD-AO-04001

©QuickSign – PUBLIC

BGR	Bulgaria	identity card	No	BGR-BO-02001
BGR	Bulgaria	identity card	Yes	BGR-BO-03001
BGR	Bulgaria	passport	Yes	BGR-AO-02001
BHR	Bahrain	passport	No	BHR-AO-01001
BIH	Bosnia and Herzegovina	identity card	No	BIH-BO-02001
BIH	Bosnia and Herzegovina	identity card	No	BIH-BO-03001
BIH	Bosnia and Herzegovina	passport	No	BIH-AO-01001
BIH	Bosnia and Herzegovina	passport	Yes	BIH-AO-02001
BIH	Bosnia and Herzegovina	passport	Yes	BIH-AO-03001
BLR	Belarus	passport	Yes	BLR-AO-02001
BLR	Belarus	passport	Yes	BLR-AO-03001
BLZ	Belize	passport	Yes	BLZ-AO-03001
BLZ	Belize	passport	Yes	BLZ-AO-05001
BMU	Bermuda	passport	No	BMU-AO-01001
BRA	Brazil	passport	No	BRA-AO-01001
BRA	Brazil	passport	Yes	BRA-AO-02001
BRA	Brazil	passport	Yes	BRA-AO-05001
BRA	Brazil	passport	Yes	BRA-AO-06001
BRN	Brunei	passport	No	BRN-AO-01001
BRN	Brunei	passport	Yes	BRN-AO-02001
BTN	Bhutan	passport	Yes	BTN-AO-01001
BWA	Botswana	passport	Yes	BWA-AO-02001
CAN	Canada	passport	Yes	CAN-AO-04001
CAN	Canada	passport	Yes	CAN-AO-05001
CHE	Switzerland	identity card	No	CHE-BO-01002
CHE	Switzerland	identity card	No	CHE-BO-01003
CHE	Switzerland	identity card	Yes	CHE-BO-02001
CHE	Switzerland	passport	Yes	CHE-AO-03002
CHE	Switzerland	passport	Yes	CHE-AO-04001
CHL	Chile	passport	No	CHL-AO-01001
CHN	China	passport	No	CHN-AO-01001

©QuickSign – PUBLIC

CHN	China	passport	No	CHN-AO-03001
CHN	China	passport	No	CHN-AO-04002
CHN	China	passport	Yes	CHN-AO-02001
CHN	China	passport	Yes	CHN-AO-03003
CHN	China	passport	Yes	CHN-AO-03004
CHN	China	passport	Yes	CHN-AO-04003
CHN	China	passport	Yes	CHN-AO-05001
CIV	Ivory Coast	passport	Yes	CIV-AO-02001
CMR	Cameroon	passport	Yes	CMR-AO-02001
CMR	Cameroon	passport	Yes	CMR-AO-03001
COD	Congo (Democratic Republic)	passport	Yes	COD-AO-01001
COD	Congo (Democratic Republic)	passport	Yes	COD-AO-02001
COG	Congo	passport	No	COG-AO-01001
COG	Congo	passport	Yes	COG-AO-02001
COL	Colombia	passport	No	COL-AO-01001
COL	Colombia	passport	Yes	COL-AO-02001
COL	Colombia	passport	Yes	COL-AO-04001
COM	Comoros	passport	Yes	COM-AO-01001
CPV	Cape Verde	passport	No	CPV-AO-01001
CRI	Costa Rica	passport	Yes	CRI-AO-01001
CUB	Cuba	passport	No	CUB-AO-01001
CYP	Cyprus	passport	No	CYP-AO-03001
CYP	Cyprus	passport	Yes	CYP-AO-04001
CYP	Cyprus	passport	Yes	CYP-AO-04002
CZE	Czech Republic	identity card	No	CZE-BO-01002
CZE	Czech Republic	identity card	No	CZE-BO-01003
CZE	Czech Republic	identity card	No	CZE-BO-01004
CZE	Czech Republic	identity card	No	CZE-BO-02001
CZE	Czech Republic	identity card	No	CZE-BO-03001
CZE	Czech Republic	identity card	No	CZE-BO-04001
CZE	Czech Republic	identity card	No	CZE-BO-04002
CZE	Czech Republic	identity card	Yes	CZE-BO-04003
CZE	Czech Republic	identity card	Yes	CZE-BO-04004

©QuickSign – PUBLIC

CZE	Czech Republic	passport	Yes	CZE-AO-04001
CZE	Czech Republic	passport	Yes	CZE-AO-04002
DEU	Germany	identity card	Yes	DEU-BO-02001
DEU	Germany	identity card	Yes	DEU-BO-02004
DEU	Germany	passport	Yes	DEU-AO-01007
DEU	Germany	passport	Yes	DEU-AO-02002
DEU	Germany	passport	Yes	DEU-AO-04001
DEU	Germany	passport	Yes	DEU-AO-04004
DJI	Djibouti	passport	Yes	DJI-AO-02001
DMA	Dominica	passport	Yes	DMA-AO-02001
DMA	Dominica	passport	Yes	DMA-AO-03001
DNK	Denmark	passport	No	DNK-AO-03001
DNK	Denmark	passport	No	DNK-AO-03002
DNK	Denmark	passport	No	DNK-AO-03003
DNK	Denmark	passport	Yes	DNK-AO-04001
DNK	Denmark	passport	Yes	DNK-AO-04002
DNK	Denmark	passport	Yes	DNK-AO-04003
DNK	Denmark	passport	Yes	DNK-AO-05001
DNK	Denmark	passport	Yes	DNK-AO-05002
DNK	Denmark	passport	Yes	DNK-AO-05003
DNK	Denmark	passport	Yes	DNK-AO-06001
DOM	Dominican Republic	passport	No	DOM-AO-01001
DOM	Dominican Republic	passport	Yes	DOM-AO-02001
DZA	Algeria	passport	Yes	DZA-AO-01001
ECU	Ecuador	passport	No	ECU-AO-01001
EGY	Egypt	passport	Yes	EGY-AO-01001
ERI	Eritrea	passport	Yes	ERI-AO-02001
ESP	Spain	identity card	Yes	ESP-BO-03001
ESP	Spain	identity card	Yes	ESP-BO-05001
ESP	Spain	identity card	Yes	ESP-BO-06001
ESP	Spain	passport	No	ESP-AO-01002
ESP	Spain	passport	No	ESP-AO-01003
ESP	Spain	passport	No	ESP-AO-02001

©QuickSign – PUBLIC

ESP	Spain	passport	No	ESP-AO-03001
ESP	Spain	passport	Yes	ESP-AO-04001
ESP	Spain	passport	Yes	ESP-AO-05001
EST	Estonia	identity card	No	EST-BO-03001
EST	Estonia	identity card	No	EST-BO-04001
EST	Estonia	identity card	Yes	EST-BO-04002
EST	Estonia	passport	Yes	EST-AO-03005
EST	Estonia	passport	Yes	EST-AO-06001
ETH	Ethiopia	passport	No	ETH-AO-01001
ETH	Ethiopia	passport	No	ETH-AO-02001
FIN	Finland	identity card	No	FIN-BO-10001
FIN	Finland	identity card	Yes	FIN-BO-11001
FIN	Finland	identity card	Yes	FIN-BO-12001
FIN	Finland	identity card	Yes	FIN-BO-12002
FIN	Finland	identity card	Yes	FIN-BO-12003
FIN	Finland	identity card	Yes	FIN-BO-12004
FIN	Finland	passport	Yes	FIN-AO-06001
FIN	Finland	passport	Yes	FIN-AO-06002
FIN	Finland	passport	Yes	FIN-AO-07001
FIN	Finland	passport	Yes	FIN-AO-07002
FRA	France	identity card	No	FRA-BO-02002
FRA	France	identity card	Yes	FRA-BO-03001
FRA	France	passport	No	FRA-AO-01001
FRA	France	passport	No	FRA-AO-01002
FRA	France	passport	No	FRA-AO-02001
FRA	France	passport	No	FRA-AO-02002
FRA	France	passport	Yes	FRA-AO-03001
FRA	France	passport	Yes	FRA-AO-03002
FRA	France	passport	Yes	FRA-AO-03003
FRA	France	passport	Yes	FRA-AO-03004
FRA	France	residence permit	Yes	FRA-HO-09001
FRA	France	residence permit	Yes	FRA-HO-12001
GAB	Gabon	passport	Yes	GAB-AO-02001
GAB	Gabon	passport	Yes	GAB-AO-03001

©QuickSign – PUBLIC

GBR	United Kingdom	passport	No	GBR-AO-01001
GBR	United Kingdom	passport	No	GBR-AO-01002
GBR	United Kingdom	passport	No	GBR-AO-01003
GBR	United Kingdom	passport	No	GBR-AO-01004
GBR	United Kingdom	passport	No	GBR-AO-01005
GBR	United Kingdom	passport	Yes	GBR-AO-02001
GBR	United Kingdom	passport	Yes	GBR-AO-02002
GBR	United Kingdom	passport	Yes	GBR-AO-02003
GBR	United Kingdom	passport	Yes	GBR-AO-02004
GBR	United Kingdom	passport	Yes	GBR-AO-02005
GBR	United Kingdom	passport	Yes	GBR-AO-02006
GBR	United Kingdom	passport	Yes	GBR-AO-02007
GBR	United Kingdom	passport	Yes	GBR-AO-02008
GBR	United Kingdom	passport	Yes	GBR-AO-04001
GBR	United Kingdom	passport	Yes	GBR-AO-04002
GBR	United Kingdom	passport	Yes	GBR-AO-05001
GBR	United Kingdom	passport	Yes	GBR-AO-05002
GBR	United Kingdom	passport	Yes	GBR-AO-06001
GBR	United Kingdom	passport	Yes	GBR-AO-07001
GEO	Georgia	passport	No	GEO-AO-01001
GEO	Georgia	passport	No	GEO-AO-02001
GEO	Georgia	passport	Yes	GEO-AO-03001
GEO	Georgia	passport	Yes	GEO-AO-03002
GEO	Georgia	passport	Yes	GEO-AO-04001
GHA	Ghana	passport	No	GHA-AO-01001
GHA	Ghana	passport	Yes	GHA-AO-02001
GIN	Guinea	passport	Yes	GIN-AO-02001
GIN	Guinea	passport	Yes	GIN-AO-03001
GMB	Gambia	passport	No	GMB-AO-01001
GNQ	Equatorial Guinea	passport	Yes	GNQ-AO-02001
GRC	Greece	identity card	Yes	GRC-BO-02001
GRC	Greece	identity card	Yes	GRC-BS-02001
GRC	Greece	passport	Yes	GRC-AO-03009
GRC	Greece	passport	Yes	GRC-AO-04001

©QuickSign – PUBLIC

GRD	Grenada	passport	No	GRD-AO-01001
GUY	Guyana	passport	Yes	GUY-AO-02001
HND	Honduras	passport	No	HND-AO-01001
HND	Honduras	passport	Yes	HND-AO-03001
HRV	Croatia	identity card	No	HRV-BO-02001
HRV	Croatia	identity card	No	HRV-BO-03002
HRV	Croatia	identity card	Yes	HRV-BO-04001
HRV	Croatia	passport	No	HRV-AO-01002
HRV	Croatia	passport	Yes	HRV-AO-03001
HTI	Haiti	passport	No	HTI-AO-02001
HTI	Haiti	passport	Yes	HTI-AO-02002
HUN	Hungary	identity card	No	HUN-BO-03001
HUN	Hungary	identity card	No	HUN-BO-03002
HUN	Hungary	identity card	No	HUN-BO-03005
HUN	Hungary	identity card	No	HUN-BO-04001
HUN	Hungary	identity card	No	HUN-BO-04002
HUN	Hungary	identity card	No	HUN-BO-05001
HUN	Hungary	identity card	No	HUN-BO-05002
HUN	Hungary	identity card	No	HUN-BO-05003
HUN	Hungary	identity card	No	HUN-BO-05004
HUN	Hungary	identity card	Yes	HUN-BO-06001
HUN	Hungary	passport	Yes	HUN-AO-03001
IND	India	passport	No	IND-AO-01001
IRL	Ireland	passport	Yes	IRL-AO-04001
IRL	Ireland	passport	Yes	IRL-AO-04002
IRL	Ireland	passport	Yes	IRL-AO-05001
IRN	Iran	passport	Yes	IRN-AO-03001
IRN	Iran	passport	Yes	IRN-AO-04001
IRQ	Iraq	passport	No	IRQ-AO-02001
IRQ	Iraq	passport	Yes	IRQ-AO-01001
IRQ	Iraq	passport	Yes	IRQ-AO-03001
IRQ	Iraq	passport	Yes	IRQ-AO-04001
ISL	Iceland	passport	Yes	ISL-AO-03001
ISL	Iceland	passport	Yes	ISL-AO-05001

©QuickSign – PUBLIC

ISR	Israel	passport	No	ISR-AO-01001
ISR	Israel	passport	Yes	ISR-AO-02001
ISR	Israel	passport	Yes	ISR-AO-03001
ITA	Italy	identity card	No	ITA-BO-04004
ITA	Italy	identity card	Yes	ITA-BO-04005
ITA	Italy	passport	No	ITA-AO-02001
ITA	Italy	passport	No	ITA-AO-02002
ITA	Italy	passport	Yes	ITA-AO-02003
ITA	Italy	passport	Yes	ITA-AO-02004
ITA	Italy	passport	Yes	ITA-AO-02005
ITA	Italy	driving license	No	ITA-FO-06001
JAM	Jamaica	passport	No	JAM-AO-02001
JOR	Jordan	passport	Yes	JOR-AO-01001
JOR	Jordan	passport	Yes	JOR-AO-01002
JPN	Japan	passport	No	JPN-AO-01002
JPN	Japan	passport	Yes	JPN-AO-02001
JPN	Japan	passport	Yes	JPN-AO-02002
JPN	Japan	passport	Yes	JPN-AO-02003
JPN	Japan	passport	Yes	JPN-AO-02004
JPN	Japan	passport	Yes	JPN-AO-09001
JPN	Japan	passport	Yes	JPN-AO-09002
KAZ	Kazakhstan	passport	Yes	KAZ-AO-02001
KEN	Kenya	passport	Yes	KEN-AO-02001
KEN	Kenya	passport	Yes	KEN-AO-03001
KGZ	Kyrgyzstan	passport	Yes	KGZ-AO-01001
KGZ	Kyrgyzstan	passport	Yes	KGZ-AO-02001
KNA	Saint Kitts and Nevis	passport	Yes	KNA-AO-01001
KOR	South Korea	passport	No	KOR-AO-02001
KOR	South Korea	passport	Yes	KOR-AO-03002
KOR	South Korea	passport	Yes	KOR-AO-04001
KWT	Kuwait	passport	Yes	KWT-AO-01001
LAO	Laos	passport	Yes	LAO-AO-02001
LBN	Lebanon	passport	No	LBN-AO-01001

©QuickSign – PUBLIC

LBN	Lebanon	passport	Yes	LBN-AO-02001
LBR	Liberia	passport	Yes	LBR-AO-02001
LBR	Liberia	passport	Yes	LBR-AO-04001
LBY	Libya	passport	Yes	LBY-AO-02001
LIE	Liechtenstein	identity card	No	LIE-BO-01001
LIE	Liechtenstein	identity card	No	LIE-BO-02001
LIE	Liechtenstein	passport	No	LIE-AO-01003
LIE	Liechtenstein	passport	Yes	LIE-AO-02001
LIE	Liechtenstein	passport	Yes	LIE-AO-03001
LSO	Lesotho	passport	No	LSO-AO-01001
LSO	Lesotho	passport	Yes	LSO-AO-01002
LSO	Lesotho	passport	Yes	LSO-AO-02001
LTU	Lithuania	identity card	No	LTU-BO-02001
LTU	Lithuania	identity card	No	LTU-BO-02002
LTU	Lithuania	identity card	Yes	LTU-BO-03001
LTU	Lithuania	identity card	Yes	LTU-BO-03002
LTU	Lithuania	passport	Yes	LTU-AO-04001
LTU	Lithuania	passport	Yes	LTU-AO-04002
LTU	Lithuania	passport	Yes	LTU-AO-04003
LTU	Lithuania	passport	Yes	LTU-AO-04004
LTU	Lithuania	passport	Yes	LTU-AO-04005
LTU	Lithuania	passport	Yes	LTU-AO-04006
LTU	Lithuania	passport	Yes	LTU-AO-04007
LUX	Luxembourg	identity card	No	LUX-BO-02002
LUX	Luxembourg	identity card	No	LUX-BO-02003
LUX	Luxembourg	identity card	No	LUX-BO-02004
LUX	Luxembourg	identity card	No	LUX-BO-02005
LUX	Luxembourg	identity card	Yes	LUX-BO-03001
LUX	Luxembourg	passport	No	LUX-AO-01001
LUX	Luxembourg	passport	Yes	LUX-AO-02005
LVA	Latvia	identity card	No	LVA-BO-02001
LVA	Latvia	identity card	Yes	LVA-BO-03001
LVA	Latvia	passport	No	LVA-AO-01002
LVA	Latvia	passport	Yes	LVA-AO-01004

©QuickSign – PUBLIC

LVA	Latvia	passport	Yes	LVA-AO-01005
MAR	Morocco	passport	Yes	MAR-AO-02001
MCO	Monaco	passport	No	MCO-AO-01001
MCO	Monaco	passport	Yes	MCO-AO-02001
MDA	Moldova	identity card	No	MDA-BO-01001
MDA	Moldova	identity card	No	MDA-BO-01002
MDA	Moldova	identity card	No	MDA-BO-02001
MDA	Moldova	identity card	No	MDA-BO-02002
MDA	Moldova	passport	Yes	MDA-AO-01003
MDA	Moldova	passport	Yes	MDA-AO-01004
MDA	Moldova	passport	Yes	MDA-AO-05001
MDA	Moldova	passport	Yes	MDA-AO-06001
MDV	Maldives	passport	Yes	MDV-AO-03001
MDV	Maldives	passport	Yes	MDV-AO-04001
MEX	Mexico	passport	Yes	MEX-AO-02003
MEX	Mexico	passport	Yes	MEX-AO-02004
MEX	Mexico	passport	Yes	MEX-AO-03001
MKD	North Macedonia	passport	Yes	MKD-AO-03001
MLI	Mali	passport	Yes	MLI-AO-02001
MLI	Mali	passport	Yes	MLI-AO-03002
MLI	Mali	passport	Yes	MLI-AO-04001
MLT	Malta	identity card	No	MLT-BO-02001
MLT	Malta	identity card	No	MLT-BO-03001
MLT	Malta	identity card	No	MLT-BO-04001
MLT	Malta	passport	Yes	MLT-AO-04001
MLT	Malta	passport	Yes	MLT-AO-05001
MNE	Montenegro	passport	Yes	MNE-AO-02001
MNE	Montenegro	passport	Yes	MNE-AO-03001
MNG	Mongolia	passport	Yes	MNG-AO-01001
MOZ	Mozambique	passport	No	MOZ-AO-01001
MOZ	Mozambique	passport	Yes	MOZ-AO-02001
MRT	Mauritania	passport	Yes	MRT-AO-01001
MSR	Montserrat	passport	Yes	MSR-AO-01001
MWI	Malawi	passport	Yes	MWI-AO-02001

©QuickSign – PUBLIC

MYS	Malaysia	passport	Yes	MYS-AO-01001
MYS	Malaysia	passport	Yes	MYS-AO-02001
MYS	Malaysia	passport	Yes	MYS-AO-03001
NAM	Namibia	passport	No	NAM-AO-01001
NGA	Nigeria	passport	No	NGA-AO-01001
NGA	Nigeria	passport	No	NGA-AO-01002
NGA	Nigeria	passport	Yes	NGA-AO-02001
NGA	Nigeria	passport	Yes	NGA-AO-03001
NIC	Nicaragua	passport	No	NIC-AO-01001
NIC	Nicaragua	passport	Yes	NIC-AO-03001
NLD	The Netherlands	passport	Yes	NLD-AO-04001
NLD	The Netherlands	passport	Yes	NLD-AO-04002
NLD	The Netherlands	passport	Yes	NLD-AO-05001
NLD	The Netherlands	passport	Yes	NLD-AO-06001
NOR	Norway	identity card	No	NOR-BO-01001
NOR	Norway	identity card	No	NOR-BO-01002
NOR	Norway	identity card	Yes	NOR-BO-02001
NOR	Norway	identity card	Yes	NOR-BO-02002
NOR	Norway	passport	No	NOR-AO-01001
NOR	Norway	passport	No	NOR-AO-02001
NOR	Norway	passport	No	NOR-AO-03001
NOR	Norway	passport	Yes	NOR-AO-04001
NOR	Norway	passport	Yes	NOR-AO-05001
NOR	Norway	passport	Yes	NOR-AO-06001
NPL	Nepal	passport	Yes	NPL-AO-01001
NPL	Nepal	passport	Yes	NPL-AO-02001
NZL	New Zealand	passport	No	NZL-AO-01001
NZL	New Zealand	passport	No	NZL-AO-01002
NZL	New Zealand	passport	No	NZL-AO-03001
NZL	New Zealand	passport	Yes	NZL-AO-03002
NZL	New Zealand	passport	Yes	NZL-AO-03003
NZL	New Zealand	passport	Yes	NZL-AO-04001
OMN	Oman	passport	No	OMN-AO-01001
OMN	Oman	passport	No	OMN-AO-01002

©QuickSign – PUBLIC

OMN	Oman	passport	Yes	OMN-AO-01003
PAK	Pakistan	passport	No	PAK-AO-02001
PAK	Pakistan	passport	Yes	PAK-AO-02002
PAK	Pakistan	passport	Yes	PAK-AO-02003
PAK	Pakistan	passport	Yes	PAK-AO-02004
PAK	Pakistan	passport	Yes	PAK-AO-02005
PAN	Panama	passport	No	PAN-AO-01001
PAN	Panama	passport	Yes	PAN-AO-02001
PER	Peru	passport	Yes	PER-AO-01003
PER	Peru	passport	Yes	PER-AO-02001
PHL	Philippines	passport	Yes	PHL-AO-02001
PHL	Philippines	passport	Yes	PHL-AO-03001
PHL	Philippines	passport	Yes	PHL-AO-04001
PLW	Palau	passport	Yes	PLW-AO-02001
POL	Poland	identity card	No	POL-BO-02001
POL	Poland	identity card	No	POL-BO-02002
POL	Poland	identity card	No	POL-BO-02003
POL	Poland	identity card	No	POL-BO-03001
POL	Poland	identity card	No	POL-BO-04001
POL	Poland	identity card	Yes	POL-BO-05001
POL	Poland	passport	No	POL-AO-01001
POL	Poland	passport	No	POL-AO-02001
POL	Poland	passport	Yes	POL-AO-05002
POL	Poland	passport	Yes	POL-AO-06001
POL	Poland	passport	Yes	POL-AO-07001
PRK	North Korea	passport	No	PRK-AO-01001
PRT	Portugal	identity card	No	PRT-BO-01001
PRT	Portugal	identity card	No	PRT-BO-02004
PRT	Portugal	identity card	No	PRT-BO-03001
PRT	Portugal	identity card	No	PRT-BO-03002
PRT	Portugal	identity card	No	PRT-BO-03003
PRT	Portugal	identity card	No	PRT-BO-03004
PRT	Portugal	identity card	No	PRT-BO-03005
PRT	Portugal	identity card	Yes	PRT-BO-04001

©QuickSign – PUBLIC

PRT	Portugal	passport	Yes	PRT-AO-01002
PRT	Portugal	passport	Yes	PRT-AO-01003
PRT	Portugal	passport	Yes	PRT-AO-04001
PRY	Paraguay	passport	Yes	PRY-AO-03001
QAT	Qatar	passport	No	QAT-AO-01001
QAT	Qatar	passport	Yes	QAT-AO-02001
QAT	Qatar	passport	Yes	QAT-AO-03001
ROU	Romania	identity card	Yes	ROU-BO-05001
ROU	Romania	identity card	Yes	ROU-BO-05002
ROU	Romania	identity card	Yes	ROU-BO-06001
ROU	Romania	passport	Yes	ROU-AO-03001
ROU	Romania	passport	Yes	ROU-AO-04001
RUS	Russia	passport	No	RUS-AO-02001
RUS	Russia	passport	No	RUS-AO-02002
RUS	Russia	passport	No	RUS-AO-02003
RUS	Russia	passport	No	RUS-AO-02004
RUS	Russia	passport	No	RUS-AO-02005
RUS	Russia	passport	Yes	RUS-AO-03001
RUS	Russia	passport	Yes	RUS-AO-03002
RUS	Russia	passport	Yes	RUS-AO-03003
RWA	Rwanda	passport	Yes	RWA-AO-02001
SAU	Saudi Arabia	passport	Yes	SAU-AO-02001
SEN	Senegal	passport	Yes	SEN-AO-03001
SGP	Singapore	passport	No	SGP-AO-03001
SGP	Singapore	passport	Yes	SGP-AO-04001
SGP	Singapore	passport	Yes	SGP-AO-05001
SHN	Saint Helena	passport	No	SHN-AO-01001
SHN	Saint Helena	passport	Yes	SHN-AO-02001
SLE	Sierra Leone	passport	No	SLE-AO-01001
SLV	El Salvador	passport	Yes	SLV-AO-02001
SLV	El Salvador	passport	Yes	SLV-AO-02002
SMR	San Marino	identity card	No	SMR-BO-02001
SMR	San Marino	passport	No	SMR-AO-01001
SMR	San Marino	passport	Yes	SMR-AO-02001

©QuickSign – PUBLIC

SMR	San Marino	passport	Yes	SMR-AO-03001
SOM	Somalia	passport	Yes	SOM-AO-01002
SOM	Somalia	passport	Yes	SOM-AO-02001
SOM	Somalia	passport	Yes	SOM-AO-04001
SOM	Somalia	passport	Yes	SOM-AO-05001
SRB	Serbia	identity card	No	SRB-BO-01001
SRB	Serbia	passport	Yes	SRB-AO-01001
SSD	South Sudan	passport	Yes	SSD-AO-01001
STP	Sao Tome and Principe	passport	Yes	STP-AO-01001
SVK	Slovakia	identity card	No	SVK-BO-03001
SVK	Slovakia	identity card	No	SVK-BO-04001
SVK	Slovakia	identity card	No	SVK-BO-05001
SVK	Slovakia	identity card	No	SVK-BO-05002
SVK	Slovakia	identity card	Yes	SVK-BO-06001
SVK	Slovakia	identity card	Yes	SVK-BO-07001
SVK	Slovakia	passport	Yes	SVK-AO-03001
SVK	Slovakia	passport	Yes	SVK-AO-04001
SVK	Slovakia	passport	Yes	SVK-AO-05001
SVN	Slovenia	identity card	No	SVN-BO-02001
SVN	Slovenia	identity card	Yes	SVN-BO-03001
SVN	Slovenia	passport	Yes	SVN-AO-02001
SVN	Slovenia	passport	Yes	SVN-AO-02002
SVN	Slovenia	passport	Yes	SVN-AO-02003
SVN	Slovenia	passport	Yes	SVN-AO-02004
SWE	Sweden	identity card	No	SWE-BO-03001
SWE	Sweden	identity card	Yes	SWE-BO-03002
SWE	Sweden	identity card	Yes	SWE-BO-04001
SWE	Sweden	passport	Yes	SWE-AO-04001
SWE	Sweden	passport	Yes	SWE-AO-05001
SYC	Seychelles	passport	No	SYC-AO-01001
SYR	Syria	passport	No	SYR-AO-01001
SYR	Syria	passport	Yes	SYR-AO-01002
SYR	Syria	passport	Yes	SYR-AO-01003

©QuickSign – PUBLIC

SYR	Syria	passport	Yes	SYR-AO-01004
TCA	Turks and Caicos Islands	passport	No	TCA-AO-01001
TGO	Togo	passport	No	TGO-AO-02001
TGO	Togo	passport	Yes	TGO-AO-03001
TGO	Togo	passport	Yes	TGO-AO-04001
THA	Thailand	passport	No	THA-AO-02001
THA	Thailand	passport	Yes	THA-AO-02002
THA	Thailand	passport	Yes	THA-AO-06001
TKM	Turkmenistan	passport	Yes	TKM-AO-01001
TLS	Timor-Leste	passport	Yes	TLS-AO-02001
TUN	Tunisia	passport	No	TUN-AO-01001
TUR	Türkiye	passport	Yes	TUR-AO-02001
TUR	Türkiye	passport	Yes	TUR-AO-03001
TUR	Türkiye	passport	Yes	TUR-AO-04001
TUV	Tuvalu	passport	Yes	TUV-AO-02001
TWN	Taiwan	passport	No	TWN-AO-02001
TWN	Taiwan	passport	Yes	TWN-AO-03001
TWN	Taiwan	passport	Yes	TWN-AO-04001
TWN	Taiwan	passport	Yes	TWN-AO-04002
TZA	Tanzania	passport	Yes	TZA-AO-02001
UGA	Uganda	passport	No	UGA-AO-01001
UGA	Uganda	passport	Yes	UGA-AO-03001
UKR	Ukraine	passport	No	UKR-AO-01001
UKR	Ukraine	passport	No	UKR-AO-01002
UKR	Ukraine	passport	Yes	UKR-AO-02001
UKR	Ukraine	passport	Yes	UKR-AO-02002
UKR	Ukraine	passport	Yes	UKR-AO-03001
UKR	Ukraine	passport	Yes	UKR-AO-03002
UKR	Ukraine	passport	Yes	UKR-AO-03003
URY	Uruguay	passport	Yes	URY-AO-01001
USA	United States	passport	Yes	USA-AO-04001
USA	United States	passport	Yes	USA-AO-05001
UZB	Uzbekistan	passport	Yes	UZB-AO-02001

©QuickSign – PUBLIC

VAT	Holy See	passport	Yes	VAT-AO-01003
VAT	Holy See	passport	Yes	VAT-AO-01004
VAT	Holy See	passport	Yes	VAT-AO-01005
VEN	Venezuela	passport	Yes	VEN-AO-02001
VGB	British Virgin Islands	passport	No	VGB-AO-01001
VGB	British Virgin Islands	passport	Yes	VGB-AO-02001
VNM	Vietnam	passport	No	VNM-AO-01002
VNM	Vietnam	passport	Yes	VNM-AO-01001
VNM	Vietnam	passport	Yes	VNM-AO-03001
YEM	Yemen	passport	Yes	YEM-AO-02001
YEM	Yemen	passport	Yes	YEM-AO-03001
ZAF	South Africa	passport	No	ZAF-AO-01001
ZAF	South Africa	passport	No	ZAF-AO-01002
ZAF	South Africa	passport	Yes	ZAF-AO-02001
ZMB	Zambia	passport	Yes	ZMB-AO-01001
ZWE	Zimbabwe	passport	No	ZWE-AO-01001
ZWE	Zimbabwe	passport	Yes	ZWE-AO-01002

©QuickSign – PUBLIC