Identity Proofing Service Provider (IPSP) policy and practice statement for products "VideoID High" and "Signicat Verify"

Version 1.2

Effective from 24 September 2026

Contents

1. Change history 3

2. Introduction 3

3. Legal and standards references 6

4. IPSP identification 7

5. Service architecture 7

6. IPSP applicable roles and their relationships 8

7. Definitions and abbreviations 8

8. Policies and Practices, Documentation 11

9. IPSP management and operation 14

10. Initiation of identity proofing 19

11. Attribute and evidence collection 19

12. Attribute and evidence validation 20

13. Binding to applicant 22

14. Issuing of proof 22

1. Change history

Date	Version	Approved by:	Description of change
24/09/2026	0.1	Trust Service Director	Initial draft based on Policy and Practice Statement for Identity Proofing for Qualified and Non-Qualified Certificates and Qualified and Non-Qualified Electronic Attestations of Attributes, with modifications to: • replace ID proofing via eIDs with ID proofing via ID document and biometric verification. • replace Signicat AS (Norway) with Signicat SLU (Spain). • remove any non-applicable TSP-related items (e.g. non-supported policies). • changed collection of evidence to default 30 days. • added FRR and FAR rates. • moved responsibility to assess IPSP process as failed in case required attributes were not collected. • used the term end user consistently according to the definition.
29/10/2026	1.0	Trust Service Director	• Added sex as an optional attribute (11.1). • Updated the biometric comparison operating point for Extended LoIP and its basis (8.5.3). • Added the accepted identity evidence for each use case, physical and digital identity documents (11.2). • Renamed the product “XID” to “Signicat Verify” (title, 2, 2.2, 5.1). • Corrected the reference to the use case for automated operation (2.2.1). • Editorial corrections.
02/11/2026	1.1	Trust Service Director	• Editorial corrections.
17/11/2026	1.2	Trust Service Director	• Added section 12.1. Basis for relying on attributes from a valid accepted document. • Defined the Practice Statement review schedule and recordkeeping requirements. Assigned Policy Owner and revision approval responsibilities to the Trust Service Director, while retaining the ISB's final approval authority.

2. Introduction

This document describes the practices applied by Signicat in providing an identity proofing trust service component called “VideoID High” and “Signicat Verify” which fulfil ETSI 119 461 v.2.1.1 LoIP level extended, hence can be used for issuing of qualified or non-qualified certificates or qualified or non-qualified electronic attestations of attributes. According the terminology used in the pre-mentioned ETSI standard, we call Signicat hereafter the IPSP (Identity Proofing Service Provider).

Functionally, the IPSP service is provided by Signicat’s Identity Proofing API (IPA), VideoID API or Assure API. The IPSP service is defined as a separate service only because of its use to serve (qualified) trust service providers with resulting compliance requirements that do not apply for other actors using the 3 pre-mentioned APIs.

The IPSP provides identity for 1 policy, which complies with a use case from clause C.3 of ETSI TS 119 461 v2.1.1 and with the eIDAS Regulation. This level can be used to issue qualified certificates under a QCP policy defined in ETSI EN 319 411-2 and qualified electronic attestations of attributes according to ETSI TS 119 471.

NOTE: Identity proofing for qualified policy must additionally comply with the eIDAS implementing act CIR (EU) 2025/1566 latest by 17 August 2027.

2.1. The VideoID service component

2.1.1. Overview

The VideoID High service component (hereinafter referred to as "VideoID") is a method compliant to the Use case for hybrid manual and automated operation as defined in section 9.2.3.3 of ETSI 119 461 v2.1.1.

It records the entire registration process of a person and allows for the remote validation of identity documents, by means of a video recording that captures and validates the identity document in real-time and in an automated manner, which is carried out by Signicat SLU through its verification operators.

The process consists of two parts:

- an automatic module in which multiple controls of security elements of the document shown during the video recording are carried out,
- as well as a biometric facial comparison between the bearer of the document, the end user, and the photo of the same, carrying out a proof of life and accurate data extraction by turns.

All this information serves as a decision support element for a human agent of the registration authority, who will review the complete video recording later (asynchronously), determining whether or not an identity can be granted on the basis of the evidence shown.

The technology verifies the authenticity of identity documents, including real-time security checks, such as the detection of holograms, badges, patterns and other document security features.

2.1.2. Description of the identification process

The identification process is developed on the basis of the following elements:

- Voice and text guidance during the video-identification process.
- Automated control of the elements of the environment (lighting conditions, network, camera quality) to obtain an optimal recording of the video identification and its evidence.
- Comparison of images with original documents through pattern matching technology to verify the authenticity of the document.
- Data extraction (OCR) from the MRZ or other parts of the document and possibility to call up credentials in real time.
- Verification that the front and back (if applicable) are from the same document.
- Biometric enrolment of the person and real-time comparison with the image of the identity document.
- Registration Authority Verification Tool, for review of the process by a qualified human being previously groomed by specific training.

In this sense, once the end user selects the document to be used to carry out the process, a streaming video recording controlled by the application will be made in which the process is initiated and in which the end user will show the front and back of his/her document for identification and validation in real time. In addition, the end user will also be asked to show his face for a facial recognition process based on automatic biometric scoring, including life detection, asking the end user to interact with a movement and data extraction of the document by OCR.

For the asynchronous review by a human agent, there is a security protocol based on EU good practices that relies on the tool offered to the human agent in which the evidence obtained during the process is shown, as well as the flags or notifications of those not obtained. The whole process is tracked with a time stamp at each step.

Therefore, the system ensures the chain of custody of the verification from the evidence collected by the automatic video process to the traces that link the identification to the qualified agent of the registration authority. The result is a verified identity with technical security equivalent to that performed in the presence of the subject.

2.1.3. End user obligations in relation to the video-identification process

The end user, throughout the process, undertakes to

- ensure that the document used in the process is an authentic, legally valid document and, furthermore
  - Is neither a photocopy nor a printed card.
  - Is not in digital format (mobile, tablet or computer).
  - It is not inside a cover.
  - It is complete and uncompromised by deterioration, containing all security elements.
- and throughout the process and while recording the video, to avoid rejection:
  - That lighting conditions in the video allow a clear view of both the identified person’s face and the document.
  - The video must have a constant flow with no interruptions or delays.
  - A living person must show the identification.
  - Should someone other than the person subject to identification be carrying out the process, then identification will be rejected.
  - Should someone else be present in the video but is obviously not acting in concert with the person to be identified, then the identification may still be valid, in the same way that it is supposed that a certain person is helping a disabled person to carry out the identification.
  - All areas of what is captured by the document must be clearly seen, from the rear, from the front as well as the person’s face.
  - The end user may not be asleep or otherwise display signs which may be interpreted as being under the influence of drugs or alcohol.

2.2 The Signicat Verify service component

2.1.1. Overview

The Signicat Verify service component (hereinafter referred to as "Signicat Verify") is a method compliant to the Use case for hybrid manual and automated operation as defined in section 9.2.3.3 of ETSI 119 461 v2.1.1. and the Use case for automated operation as defined in section 9.2.3.4 of ETSI 119 461 v2.1.1.

For the Use case for automated operation, Signicat Verify uses the ReadID SaaS with SDK (hereinafter referred to as "ReadID") component which is compliant to ETSI 119 461 v2.1.1 LoIP level extended to read the digital identity document (hereinafter referred to as "NFC chip"). The ReadID SaaS with SDK is ETSI 119 461 certified and has its own practice statement, which is an integral part of this document.

2.1.2. Description of the identification process

The identification process is developed on the basis of the following elements:

- Signicat Verify starts with the VideoID process as described in this document, but waits with executing the last step (Registration Authority Verification Tool/review of the process by a qualified human being).
- VideoID captures optical document evidence, MRZ, video evidence, and biometric evidence before verification of the NFC chip is attempted.

- When the document has an NFC chip and is supported by ReadID, Signicat Verify will use ReadID using the MRZ captured by VideoID. ReadID returns chip data and the chip portrait and Signicat Verify will then compare the VideoID face image with the chip portrait. The process is hereafter completed according to the Use case for automated operation as defined in section 9.2.3.4 of ETSI 119 461 v2.1.1.
- When the document has no supported chip or NFC chip reading cannot complete, Signicat Verify initiates the last step of the VideoID process as described in this document (Registration Authority Verification Tool/review of the process by a qualified human being). The process is hereafter completed according to the Use case for hybrid manual and automated operation as defined in section 9.2.3.3 of ETSI 119 461 v2.1.1.

2.1.3. End user obligations in relation to the video-identification process

The same end user obligations apply as to VideoID service component, with the addition that the end user is expected to scan the NFC chip of their document, as instructed via the Signicat Verify end user interface.

3. Legal and standards references

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS v1), as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
- Commission Implementing Regulation 2025/1566 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards reference standards for the verification of the identity and attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.

NOTE: While this implementing regulation is in force and can be referred, it applies, meaning it is mandatory, only from 17 August 2027.

- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
- Commission implementing Regulation C(2024) 7151 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers, and its Annex.
- Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services
- European standard ETSI EN 319 401 Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers, V3.1.1, June 2024
- ETSI Technical Specification ETSI TS 119 461 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects, V2.1.1, February 2025
- European standard ETSI EN 319 411-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, V1.5.1, April 2025

- European standard ETSI EN 319 411-2 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, V2.6.1, June 2025
- ETSI Technical Specification ETSI TS 119 471 Electronic Signatures and Trust Infrastructures (ESI); Policy and Security requirements for Providers of Electronic Attestation of Attributes Services, V1.1.1, May 2025

4. IPSP identification

Signicat SLU
Company code: VAT B86681533
Av. de la Ciudad de Barcelona, 81, 4º, 28007 Madrid, Spain.
https://www.signicat.com

This document differs from the policies defined by ETSI TS 119 461 in that this document is also a practice statement.

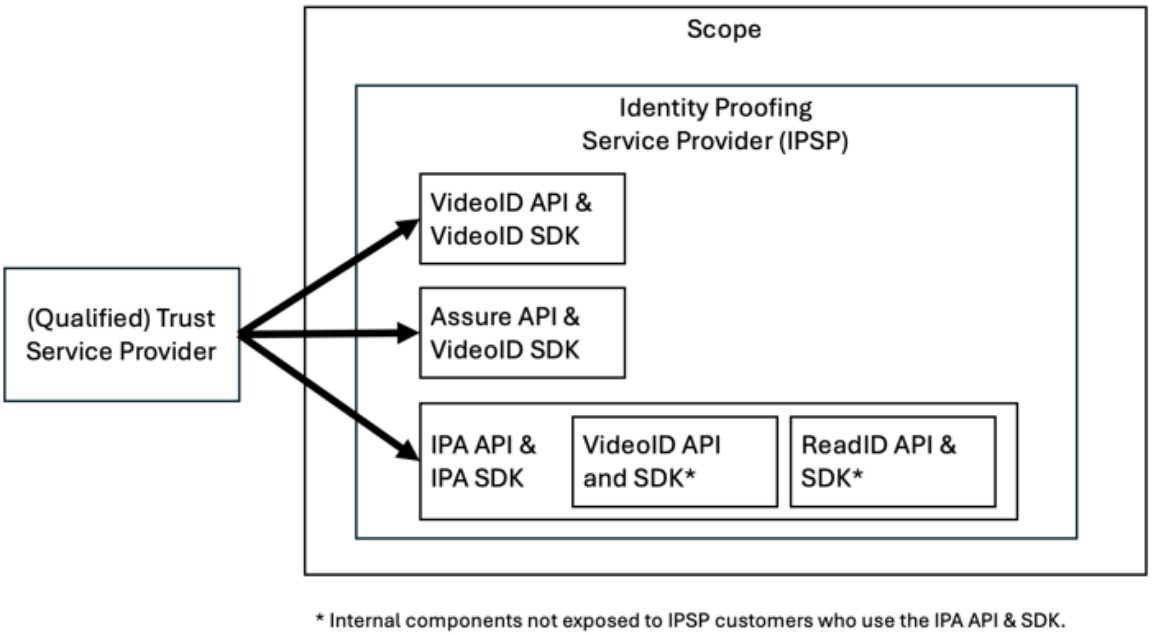
5. Service architecture

5.1. Identity proofing for (Qualified) Trust Service Providers issuing

The architecture and the flow for using the IPSP service to issue a qualified and non-qualified certificate or qualified and non-qualified electronic attestations of attributes (Q)EAA is shown in the figure below. There are 2 service provider roles:

1. The (Q)TSP
2. The Identity Proofing Service Provider (IPSP)

The IPSP provided by Signicat is the subject of this policy and practice statement.



For qualified certificate and QES, each service provider must comply with requirements from eIDAS and related standards as shown in the figure, and compliance must be assessed by an accredited, independent conformity assessment body (CAB). When the relationships between the service providers are governed by appropriate

agreements, conformity assessment can be done independently for each service provider following a principle of component conformity assessment.

As shown in the figure, the IPSP acts as an integrator of various identification means acting as authoritative evidence of identity according to ETSI TS 119 461. In the picture 3 technical integration methods are mentioned:

- The VideoID API & VideoID SDK (for the VideoID product)
- The Assure API & VideoID SDK (for the VideoID product)
- The IPA API & IPA SDK, which in its turn use the VideoID and ReadID SDKs and APIs (for the Signicat Verify product)

Each product must be explicitly approved for the requested certificate policy by the (Q)TSP. The approval process must assess that the identification means formally fulfills the requirements for the requested policy.

The IPSP may in addition to the authoritative evidence use supplementary evidence of identity according to ETSI TS 119 461. An example is lookup in trusted registers, notably registers for lost & stolen ID documents.

6. IPSP applicable roles and their relationships

The following actors are stakeholders of the IPSP service:

- The end user is a natural or legal person who has consented to sign one or more documents at the SCA, or to have a (Q)EAA issued, and whose identity shall be proven for issuing of the certificate or EAA.
  - The end user must be capable of using an authentication means that fulfils the requirements for the required policy level of the certificate or EAA.
  - The end user must accept the terms and conditions of the (Q)CA or (Q)EAA provider for issuing of the certificate or EAA. These terms and conditions cover the use of the IPSP as a trust service component of the (Q)CA or (Q)EAA provider service.
  - The end user may need to accept terms and conditions for the SSA unless these are covered by the terms and conditions for the (Q)CA.
- The (Q)TSP is an entity that provides one or more Qualified Trust Services, like Qualified and Non-Qualified Certificates and Qualified and Non-Qualified Electronic Attestations of Attributes.

7. Definitions and abbreviations

7.1. Definitions

Name	Abbreviation	Definition
eIDAS Regulation	eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.
General Data Protection Regulation	GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Name	Abbreviation	Definition
Network and Information Systems Directive	NIS 2	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
Information Security Management System	ISMS	Information Security Management System of Signicat Group, which is certified according to ISO/IEC 27001:2022 and extended by ISO/IEC 27018:2019.
Chief Information Security Officer	CISO	The overall responsible for information security in Signicat and the owner of the ISMS.
Trust Service Provider	TSP	An entity which provides a Trust Service.
Qualified Trust Service Provider	QTSP	An entity that provides one or more Qualified Trust Services and is granted qualified status by the Supervisory Body.
Supervisory Body		The authority that is designated by a member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state.
Signicat IPSP policy and practice statement		A statement of the policy and practices Signicat employs for the identity proofing - this document.
Identity Proofing Service Provider	IPSP	Trust service component for identity proofing of trust service subject, here for issuing of qualified or non-qualified certificates and qualified or non-qualified attestations of attributes.
Signature Creation Application	SCA	application within the signature creation system that creates an xAdES or other packaging format digital signature and relies on the SCDev to create a digital signature value
Server Signing Application	SSA	Application provided by a qualified or non-qualified trust service managing signature creation data (private signing keys) for signing or sealing within an QSCD/SCDev
Signicat Group		Signicat AS and its subsidiaries.
IPSP Director		The person responsible for the IPSP and for this document.
Trust Service Director		The management role responsible for approving the IPSP Policy and Practice Statement in accordance with section 8.5.3.
End user/signer		The legal or natural person whose identity is to be proven by the IPSP.
Certification Authority	CA	Trust Service Provider that issues certificates for electronic signatures and/or seals.
Qualified Certification Authority	QCA	Qualified Trust Service Provider that issues qualified certificates for electronic signatures and/or seals.
Registration Authority	RA	The component of a QCA/CA service that performs onboarding of the end user to the QCA/CA service.
Electronic Attestation of Attributes	EAA	Attestation in electronic form that allows attributes to be authenticated

Name	Abbreviation	Definition
Qualified Electronic Attestation of Attributes	QEAA	Electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in eIDAS Annex V
Authoritative evidence		Identity evidence that is presented by the end user, holds identifying attribute(s) of the identity, and is trusted for the binding of these attributes to the end user.
Supplementar y evidence		Identity evidence that is used in addition to authoritative evidence to strengthen the reliability of the identity proofing and/or as evidence for attributes that are not evidenced by the authoritative evidence.
Authoritative source		Any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.

7.2. Abbreviations

IPSP	Identity Proofing Service Provider
CA	Certification Authority
QCA	Qualified Certification Authority
RA	Registration Authority
QES	Qualified Electronic Signature or Qualified Electronic Seal
AES	Advanced Electronic Signature
QCP	Qualified Certificate Policy
NCP	Normalized Certificate Policy
LCP	Lightweight Certificate Policy
LoA	Level of Assurance
LoIP	Level of Identity Proofing
DTBS	Data To Be Signed
DTBS/R	Data To Be Signed Representation
TSA	Time stamping Authority
OID	Object Identifier
ETSI	European Telecommunications Standards Institute
CSC	Cloud Signature Consortium
SAM	Signature Activation Module
HSM	Hardware Security Module
QSCD	Qualified Signature Creation Device
SCDev	Signature Creation Device
ISM	Information Security Manager (CISO of the Signicat Group)
IPSP Director	Director of the IPSP service

ISMS	Information Security Management System
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
eID	Electronic Identification Means
eIDV	Electronic Identity Verification Means (remote use of identity documents)
EAA	Electronic Attestation of Attributes
QEAA	Qualified Electronic Attestation of Attributes
SCA	Signature Creation Application

8. Policies and Practices, Documentation

8.1. Organisation administering the TSP documentation

This document is administered by Signicat SLU.

Signicat SLU
Company code: VAT B86681533
Av. de la Ciudad de Barcelona, 81, 4º, 28007 Madrid, Spain.
https://www.signicat.com

8.2. Contact person

The contact person for the management of this document is the IPSP Director.

Further information can be requested via email compliance@signicat.com.

8.3. Identity proofing use cases for which compliance is claimed

The IPSP service provides verified identity in the form of an OIDC identity assertion, hence, the IPSP claims conformance to use cases defined by the following clauses of ETSI TS 119 461:

- Clause C.3.4 use case for identity proofing by other identification means, Extended LoIP.

NOTE: Compliance with clause 9.5 use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Enhanced LoIP can be added in future versions of this practice statement.

8.4. Identity proofing context

The identity proofing context is defined by the following:

- The IPSP service is provided under EU/Spanish legislation.
- As a component of a qualified or non-qualified trust service, the IPSP service shall be assessed to comply with the legislation of the country of the (Q)TSP providing the service.
- The IPSP service uses eIDV means to authenticate the identity of the applicant.
- The specific eIDV means used shall fulfil formal requirements for the applicable policy level and must be approved by the (Q)TSP relying on the identity proofing for that level.
- The IPSP monitors status of eIDV means for continued fulfilment of formal requirements.
- Based on the eIDV means used, the identity attributes required by the (Q)TSP shall be provided.
- Supplementary evidence according to ETSI TS 119 461, e.g. trusted registers, may be used for verification and extension of the identity attribute set provided by the eIDV means.

- The IPSP is responsible for correct execution of authentication and other protocols applied for the identity proofing.

8.5. TSP documentation applicability

8.5.1. IPSP Policy and Practice Statement

Signicat SLU is responsible for the management of the IPSP Policy and Practice Statement.
The document shall be approved by Signicat management and made public on the Signicat Compliance website.

The IPSP Director shall coordinate review of this Practice Statement at least once every 12 months and whenever material changes to the service, risks, applicable requirements or organisational responsibilities may affect it. Review outcomes and approval decisions shall be recorded in section 1 Change history or in supporting records referenced there, including reviews that result in no changes. Revisions shall be approved in accordance with section 8.5.3.

The IPSP Policy and Practice Statement must be accepted by the (Q)TSPs that decide to rely on the identity proofing provided by the IPSP.

As the IPSP is not a trust service itself, but only a component of the trust services using the IPSP, the IPSP is not directly supervised by the Spanish supervisory authority for trust services. However, Signicat maintains close contact with the supervisory authority, especially regarding use of the IPSP for qualified certificates and QEAA.

To provide identity for qualified policy level, the IPSP shall pass an audit by an accredited Conformity Assessment Body (CAB) leading to a Conformity Assessment Report (CAR) proving compliance with eIDAS and appropriate requirements from ETSI standards, notably for the referred use case(s) from ETSI TS 119 461. Before starting use of the IPSP for qualified certificates or QEAA, a QTSP shall inform its supervisory authority submitting the IPSP's CAR, and if needed further information on the IPSP service such as this Policy and Practice Statement, and obtain approval from the supervisory authority for use of the IPSP. The QTSP is responsible for involving its CAB to the extent necessary.

Significant changes in the provision of the IPSP service shall be mediated at least 1 month in advance to all (Q)TSPs using the IPSP service, to allow these (Q)TSPs to inform their supervisory bodies about the change in due time, where relevant. Significant changes shall be reflected in a new version of the IPSP Policy and Practice Statement that shall be available to concerned (Q)TSPs and other interested parties at least 1 month before that new version enters into force. An SCA is a non-qualified trust service, and all SCA providers using the IPSP are subject to the notification requirement. Signicat will additionally inform the CAB that has issued the IPSP's CAR for the applicable policy level and will informally inform the Spanish supervisory authority.

Minor updates to the IPSP Policy and Practice Statement shall be notified to all (Q)TSPs using the IPSP service without undue delay and no later than 3 working days after the changes are approved by Signicat management and published.

A new version of the IPSP Policy and Practice Statement shall be approved by Signicat management by applicable procedure and shall by published immediately after approval. The new version may take effect immediately if changes are minor or if significant changes have already been mediated to concerned actors at least 1 month in advance, see above. Else, the new version shall indicate the date when it becomes effective to cater for the requirement to mediate changes to concerned actors.

(Q)TSPs using the IPSP as a component of their services shall only take into account the effective version of the IPSP Policy and Practice Statement as of the time of using the IPSP service.

In the case of termination of the IPSP service, Signicat shall notify the Spanish supervisory body, the IPSP's CAB, and all affected (Q)TSPs about the planned termination of the trust service component at least 3 months before the termination.

8.5.2. Terms and conditions

There are no specific terms and conditions document for the IPSP service. The end user must accept the terms and conditions of the (Q)CA or (Q)EAA provider. The IPSP as a trust service component is covered by these terms and conditions. Terms and conditions between the IPSP and (Q)TSPs relying on the service, and towards customers, are regulated by agreements.

8.5.3. Risk assessment and information security policy

Signicat has an Information Security Management System (ISMS) certified to ISO/IEC 27001:2022 with the certification scope of “Providing digital identity and electronic signature solutions, including Qualified Trust Services (qualified timestamps, qualified signature and seal validation, and qualified certificate issuance for qualified electronic signatures) using ISO/IEC 27018:2019 and in accordance with Statement of Applicability latest version”. The ISMS covers the IPSP service.

The ISMS and the ISO/IEC 27001:2022 certification cover risk assessment and risk treatment methodology and the ISMS constitutes the information Security policy. As this applies to the entire organisation, ISMS requirements are clearly communicated to all employees according to how they are impacted.

ETSI TS 119 461 has specific requirements for threat intelligence. This is covered by the risk assessment process and the ISMS for general security risks, and by the procedure for approval and monitoring of compliance of eIDV means and supplementary evidence for identity proofing. A change in the status of e.g. an eIDV means shall lead to a reassessment of the means' applicability for a given policy level.

According to ETSI TS 119 461, the IPSP shall state in its practice statement goals for quality and security in terms of resilience to false acceptance and false rejection of applicants. The goals below are set at least at the level of industry best practice and at a level the service is able to achieve. They are measured at transaction (session) level, using the decision rule applied in production, and are reported with 95 % confidence intervals on held-out data not used for calibration. The detailed description of the controls, measurement methodology and test status is given in the document "Signicat VideoID High – Computer Vision and Biometrics Controls Description" (CVB).

a) Presentation attack detection (PAD), measured according to ISO/IEC 30107-3:

- APCER (Attack Presentation Classification Error Rate): ≤ 5 % for each presentation attack instrument (PAI) species (aligned with NIST SP 800-63A-4). APCER is reported for the worst-performing species, never as a mean.
- BPCER (Bona fide Presentation Classification Error Rate): ≤ 5 % on bona fide transactions representative of the population and of the capture channels.

b) Binding to applicant by automated face biometrics (1:1 comparison of the document portrait with the live face), measured according to ISO/IEC 19795-1:

- Extended LoIP: the comparison threshold is set at the operating point corresponding to an FMR of 0.006% (1:15,000).
- FRR (False Rejection Rate / FNMR): ≤ 3%.
- Demographic differentials are measured and reported according to ISO/IEC 19795-10; the operating threshold is chosen so that the applicable FMR goal is met in the worst evaluated group.

> The above operating points are based on the Innovatrics public documentation for Digital Identity Service since version 1.62, available as of October 2026: https://developers.innovatrics.com/digital-onboarding/docs/functionalities/face/matching/#digital-identity-service-since-version-162

All necessary controls required by eIDAS, GDPR and other relevant legal acts and corresponding standards, notably ETSI EN 319 401, are implemented and maintained within the ISMS. The IPSP service is assumed, in the context of NIS 2, to be classified as an essential entity.

The ISMS is reviewed in accordance with annual management reviews and scheduled external audits. Inventories of assets and risks are reviewed annually. Configuration of Signicat services is constantly monitored and regularly checked by vulnerability scanning and penetration testing.

Signicat Group's Information Security Board (ISB) approves policies and practices, and important changes to policies and practices, related to information security. The Trust Service Director is the Policy Owner of the IPSP Policy and Practice Statement and is responsible for approving its revisions. The ISB retains final authority for approval and approves changes affecting the level of security provided. The IPSP Director remains responsible for approving further IPSP documentation.

8.5.4. Liability for the IPSP service

The IPSP is not directly liable towards the end user; the SCA and the (Q)TSP relying on the IPSP service are the liable parties. The IPSP's liability towards the SCA and the (Q)TSP is covered by agreements.

9. IPSP management and operation

The IPSP service operates under the Information Security Management System (ISMS) of Signicat Group, which has achieved ISO/IEC 27001:2022 certification by an accredited international certification body. The ISMS covers all applicable controls specified in ISO/IEC 27001:2022 Annex A. These controls are from ISO/IEC 27002:2022, which is the basis for the controls of the ETSI EN 319 401 standard, hence, the ISMS covers the ETSI EN 319 401 requirements in general. Additionally, controls from ISO/IEC 27018 have been implemented ensuring the highest protection of personal data in cloud environments.

The paragraphs below summarise the management and operations of the trust service covering requirements from ETSI EN 319 401 and ETSI TS 119 461.

9.1. Internal organisation

9.1.1. Organisation reliability

Signicat SLU has the necessary financial stability and resources for operation in accordance with the IPSP Practice Statement. Signicat SLU maintains liability insurance to cover obligations arising from its operations in line with Article 13 of eIDAS. Resolution of complaints and disputes is governed by the customer's contract with Signicat and by the contract between the IPSP and the (Q)TSP using the IPSP service.

Signicat SLU reserves the right to, for competitive or other reasons, decline provisioning of the IPSP service to specific (Q)TSPs. All (Q)TSPs that are granted permission to use the IPSP service are treated in a non-discriminatory way.

9.1.2. Segregation of duties

The ISMS ensures that the necessary segregation of duties is verified and maintained. Specifically, the roles of Information Security Manager (ISM), IPSP Director, and Internal Auditor are separated. The four eyes principle is ensured in vital areas:

- Secure development and code reviews
- Software deployment

9.2. Human resources

The Human Resources Policy of the ISMS ensures that all required human resource controls are implemented. The controls are documented in the ISMS Statement of Applicability and cover the following topics:

- Background screening
- Terms and conditions of employment

- Non-disclosure after termination or change of employment
- Training and qualifications of staff
- Disciplinary sanctions
- Definitions and job descriptions for trusted roles
- Procedures and responsibility for appointment to and acceptance of trusted roles (responsibility of management and IPSP Director)
- Remote working

Employees and contractors receive adequate training and have the necessary experience for carrying out the duties specified in employment or contractor agreements as defined in the Human Resources Security policy for Signicat Group.

Signicat's CISO (Chief Information Security Officer) is responsible for network and information security and reports to top management.

9.3. Asset management

9.3.1. General requirements, assets inventory and classification

Signicat maintains up-to-date lists of assets and their characteristics, including information assets, with assigned ownership to all assets. Risk Assessment is aligned with the identification of assets, and risks are identified and listed as related to assets using elaborate mapping. Assets are classified according to requirements for protecting confidentiality, integrity, availability, and authenticity.

Asset management is part of Signicat Group's ISMS, including Acceptable Use Policy, Information Classification Policy and Risk Management Methodology. Personnel and other parties are required to return assets upon change or termination of employment.

The IPSP service is defined as a primary asset and is owned by the IPSP Director.

9.3.2. Media handling

Media containing sensitive information is handled securely and in accordance with Asset Management, Communications Security and Operations Security Policy parts of the ISMS. Media handling for the operational IPSP service is carried out by the cloud hosting operator.

9.4. Access control

Access Control Policy, which is a part of Signicat Group's ISMS, ensures that system access is limited to authorised individuals and that all necessary controls for secure access are implemented.

The basic principle applied in access controls is that access to all systems, networks, services, and information is denied by default, unless explicitly permitted on a need-to-know basis to individual users or groups of users. Any access granted is further restricted according to the principle of least privilege. The Access Control Policy provides a comprehensive framework for (electronic) access provision, requirements for corporate account security settings, privilege management, and regular review of access rights. According to the policy, associate traceable access control records must be ensured and kept. Remote access is supported in an encrypted manner only as per the Mobile Devices & Remote Work Policy.

The Access Control Policy provides a framework for registration of a user in the corporate directory, internal network, and information systems. Recommended technical (security) parameters supplement the user registration process. The Access Control Policy defines a user de-registration process, including requirements for account removal. Authorisation for access must be granted by the system (asset) owner and may, depending on the information classification of the processes and information that are to be protected, additionally need authorisation by management.

Acceptable Use Policy provides comprehensive requirements for users to manage and use secret authentication information. It enforces industry best practices, like enforced 2FA and encrypted password management tools for personnel in trusted roles. Detailed requirements for corporate account security settings are listed in the Access Control Policy.

9.5. Cryptographic controls

Cryptographic controls are defined following the Cryptography Policy, which is part of the ISMS. Communication towards the IPSP Service is secured by the TLS protocol using approved cryptography.

9.6. Physical and environmental security

The Operations Security Policy covers physical access to information assets and local equipment. The physical and environmental security of the equipment used to provide the IPSP service is handled by the cloud hosting provider, regulated by contractual clauses and subject to the Supplier Relationship Policy.

Relevant in-house equipment is located in secure areas only. The Scope document for the ISMS describes a list of secure areas and associated protection controls and procedures.

The physical security perimeter for relevant Signicat office premises is defined in the Scope document for the ISMS. Based on risk assessment, controls of physical security of Signicat premises are implemented to ensure the required level of protection. Physical security controls are subject to comprehensive risk management and assessment activities. In general, there are different levels of physical entry controls defined in the Access Control Policy and Physical and Environmental Security Policy that depend on the facility's vitality. For example, access to secure areas is “denied by default” (e.g. locked) except permitted. Due to the nature of Signicat’s activities and the use of a public cloud hosting provider, Signicat is not reliant on one or a few fixed physical locations.

9.7. Operation security

The Signicat Group’s ISMS covers this section by the Operations Security Policy, Communications Security Policy, System Acquisition, Development and Maintenance Policy, Supplier Relationship Policy, Incident Management Policy, Access Control Policy, Mobile Devices & Remote Work Policy, and Privacy Policy. The documentation covers, among others:

- Change control
- Malware protection
- Authentication, authorisation, and access control
- Patching
- Configuration management
- Monitoring and alarms
- Configuration and other reviews

9.8. Network security

The Signicat Group’s ISMS covers this section by the Operations Security Policy and Communications Security Policy. Segregation in networks is emphasised. As a result, production, staging/pre-production, development/test, and office support environments are segregated. Network connections and ports are by default closed and opened only on explicit demand. Vulnerability scanning is carried out at least quarterly, and penetration testing is carried out at least annually. Firewall configurations are reviewed regularly.

9.9. Vulnerabilities and incident management

9.9.1. Monitoring and logging

Signicat Group's ISMS covers this section by the Operations Security Policy, which includes comprehensive monitoring, alarm, and logging procedures. Security logs are regularly reviewed to support detection and investigation of suspicious events in production and corporate systems. All logs are sent to remote log aggregator systems that support monitoring.

9.9.2. Incident response

This section is covered by Signicat Group's ISMS by the Incident Management Policy and by the Incident Management Procedure. The Incident Management Procedure represents a comprehensive workflow for managing information security incidents. The procedure is aligned with GDPR, NIS 2 and eIDAS requirements for Qualified and Non-Qualified Trust Service Providers, relevant to the context, and represents all necessary responsibilities for reporting and handling an incident.

Lessons learned from previous incidents are part of the procedure by carrying out a review session for each incident. The Incident Management Procedure includes sections on Incident Containment and Eradication and Incident Recovery.

9.9.3. Reporting

As per Signicat Group's Incident Management Policy and Incident Management Procedure, information security events might be detected by internal controls or reported by internal or external parties.

The initial analysis phase of the Incident Management Procedure defines assessment criteria for a security event. If an event is confirmed as a security incident, it triggers further response actions (documented in the procedure) based on best international practices (primarily ENISA, GDPR, NIS 2 and eIDAS guidelines). Incidents, including those detected or reported from external services that Signicat integrates, are published on Signicat's status page that is monitored by Signicat's customers.

As the IPSP service is a component of the trust services of the (Q)TSPs that use the service, these (Q)TSPs are alerted in order to be able to fulfil their incident reporting obligations according to applicable laws and regulations. Incident reporting and management shall be part of the setup between the (Q)TSP and the IPSP.

ISM and IPSP Service Director are responsible for contacts with authorities relevant to information security, such as CERT institutions, the Personal Data Protection Inspectorate, and the Supervisory Body under the eIDAS Regulation. The Incident Management Procedure provides a special communication protocol in the form of predefined templates to ensure contact with authorities in a timely, precise, and compliant with applicable laws manner during the event of an incident. Applicable laws are defined in the List of Legal, Regulatory, Contractual and Other Requirements.

ISM and IPSP Service Director are responsible for contacts with special interest groups relevant to their role in information security. Furthermore, ISM owns the Responsible Vulnerability Disclosure policies, which enable community-based ("white and grey hats") vulnerability identification.

9.9.4. Event assessment and classification

The initial analysis phase of the Incident Management Procedure defines assessment criteria for a security event. An event is reclassified if information during the event handling indicates that the event is more or less severe than the conclusion of the initial analysis.

9.9.5. Post-incident reviews

The Incident Management Procedure defines post-incident activities, where lessons-learned analysis is performed, which might result in risk reassessment, controls review, ISMS documentation update, or specific improvement actions.

9.10. Collection of evidence

All events in Signicat's systems are logged securely with defined retention time in line with the Compliance Policy, which is part of Signicat Group's ISMS, and with the Privacy policy. The time of an event is recorded based on system clock, which is synchronized with UTC at least daily.

Identity assertions issued in the context of the IPSP service are by default stored for 30 days. It is the responsibility of the customer, hence (Q)TSPs, to request the IPSP to store assertions longer in case this is required to reach compliance to requirements in ETSI EN 319 411-1/-2.

9.11. Business continuity management

9.11.1. General

The Business Continuity Policy is part of Signicat's ISMS. The Disaster Recovery / Business Continuity Plan for Signicat's Authentication services covers the IPSP service. The plan addresses roles, responsibilities, and, when activated, triggers the restoration of services. Signicat's Digital Trust Platform (DTP) is instantiated in a primary data centre of the cloud hosting provider with a secondary instantiation in a different data centre in another country.

The Disaster Recovery / Business Continuity Plan addresses all relevant aspects of information security continuity, including recovery objectives, and incorporates them into associated procedures. Business continuity plans are rehearsed at least annually.

The incident response procedures shall allow (Q)TSPs using the IPSP service to initiate their business continuity plans according to the judgements made by the (Q)TSP itself.

9.11.2. Back up

Backups are the responsibility of the cloud hosting provider. The Operations Security Policy defines requirements and routine activities for information backups. The backup process is automated, fully aligned and tested to comply with declared recovery point objectives and recovery time objectives for services' restoration.

9.11.3. Crisis management

This is covered by the Signicat Group's crisis management plan. The threat intelligence processes of Signicat target early discovery of threats that can potentially cause a crisis. Crisis management is tested regularly in conjunction with rehearsal of business continuity plans.

9.12. TSP Termination and termination plans

The termination plan is limited to the event that Signicat discontinues the IPSP service but continues the eIDV services upon which the IPSP service is based. In this event, the concerned (Q)TSPs and all other relevant parties, including supervisory and other authorities as needed, will be informed at least 3 months in advance. There is no termination plan for Signicat's eIDV service. This is a core service that Signicat intends to continue indefinitely.

NOTE: The termination plan shall be verified to ensure fulfilment of the requirements of Commission Implementing Regulations laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards requirements for qualified trust service providers providing qualified trust service, when this Implementing Regulation is published.

9.13. Compliance

This section is covered by Signicat Group's ISMS via the Compliance Policy. The procedure defines the process of identification of interested parties, as well as legal, regulatory, contractual and other requirements and responsibilities for their fulfilment. Legal and standards documents that are relevant for compliance of the IPSP Service are listed at the beginning of this Policy and Practice Statement.

Universal design and accessibility according to Directive (EU) 2019/882 is a compliance requirement for all Signicat services.

Signicat's customer is the data controller according to GDPR for personal data processed in conjunction with Signicat services delivered to the customer. In the role of IPSP, Signicat acts as data processor for the customer according to a Data Processing Agreement that is part of Signicat's customer agreement.

The (Q)CA or (Q)EAA is the data controller for personal data that is included in certificates or EAAs or used in the process to issue certificates or EAAs. Signicat's customer shall, by the customer agreement, accept transfer of the necessary identity information to specific (Q)CAs and (Q)EAA providers.

The agreement between Signicat and the (Q)CA or (Q)EAA provider shall regulate transfer of identity information from Signicat as IPSP. Signicat may act as a data processor to the (Q)CA or (Q)EAA provider, or the data transfer may be between two independent data controllers, the (Q)CA or (Q)EAA provider and Signicat's customer with Signicat acting as data processor for the customer.

9.14. Supply chain

Signicat Group's ISMS includes a Supplier Relationship Policy, applied for the screening and management of all suppliers. The checks of supply chain integrity ensure that the underlying code and binaries in 3rd party components used in services are verified and that they pass attestation tests. All suppliers undergo a security assessment, which includes sub-suppliers involved.

All contracts with suppliers have a contract owner, who is responsible for regular, at least annual, verification of the status of suppliers. In case of an indication of contract break or increased risk, the contract owner may request an audit of the supplier.

In compliance with GDPR, Signicat signs (accepts after evaluation) as needed Data Processing Agreements with suppliers in the role of sub-processors to Signicat.

The IPSP service is part of the supply chain of (Q)TSPs using the service. The responsibility of Signicat in this context is regulated in the agreement between the (Q)TSP and Signicat.

10. Initiation of identity proofing

As per requirements in clause 6.3.4 of ETSI EN 319 411-1/-2, terms and conditions for certificate issuing shall be presented and explicitly be accepted by the end user as the subject of the certificate. This shall include information collected as part of the identity proofing and how long this information is retained. Evidence of the acceptance shall be recorded.

The (Q)CA, through the SSA, is responsible for obtaining the explicit consent with the required information and for recording the information. These tasks may be performed by the SCA or the IPSP on behalf of the (Q)CA subject to the agreement between the SSA and Signicat on the IPSP service and/or the commercial agreement between the SCA and the SSA.

As per requirements in clause 6.2 of ETSI TS 119 471, the (Q)EAA provider is responsible for displaying terms and conditions for issuing of (Q)EAA for acceptance by the end user as subject of the (Q)EAA, unless conditions exist where prior consent by the end user can be assumed. The consent by the user and related evidence shall be recorded. These tasks may be performed by the IPSP on behalf of the (Q)EAA provider subject to the agreement between the (Q)EAA provider and Signicat on the IPSP service.

11. Attribute and evidence collection

11.1. Attribute collection

In the present version, the IPSP only supports issuing of certificates and EAAs for natural persons.

The following identity attributes shall be collected:

- Family name
- Given name
- Date of birth
- Place of birth
- Nationality
- National identification number (NIN)
- Document number
- Document type
- Document issuing country
- Document issuing authority
- Date of issue
- Date of expiry

Optional:

- Gender (there are known cases of ETSI-compliant documents in circulation not featuring this information, e.g. DEU_ID_2010)
- Contact or address details
- Any identifier obtained from trusted, supplementary evidence

Use of trusted registers or other supplementary evidence must be approved by the (Q)TSP, including attributes to obtain and assessment that the attributes collected can be trusted to the same level as the authoritative evidence used.

If attributes required as mandatory by the context cannot be proven by available authoritative or supplementary trusted evidence, it is the responsibility of the (Q)TSP to regard the identity proofing as failed.

11.2. Accepted identity evidence

Under this Policy and Practice Statement (Extended LoIP), the IPSP accepts the following types of valid (not expired) identity documents as authoritative evidence, in accordance with ETSI TS 119 461 V2.1.1:

- Use case 9.2.3.3 (hybrid manual and automated operation): physical passports, national identity cards and other official identity documents assessed as equally or more reliable.
- Use case 9.2.3.4 (automated operation): digital identity documents, i.e. eMRTD according to ICAO 9303 part 10 and other digital identity documents assessed as equally or more reliable.

12. Attribute and evidence validation

As per ETSI TS 119 461 clause 8.3.4, a successful authentication of the end user by eIDV means shall imply that the means as authoritative evidence is validated and that the identity attributes conveyed are bound to the end user. The approval of eIDV means shall include assessment that the identity proofing protocol applied is secure.

With respect to requirements for initial identity validation from ETSI EN 319 411-1/-2, the IPSP provides an attestation of the end user's identity to the (Q)CA, and the IPSP is per agreement approved as an appropriate and authoritative source by the (Q)CA. To be approved as appropriate and authoritative source for issuing of qualified certificates and QEAAs, the IPSP service must pass conformity assessment by an accredited conformity assessment body.

For any supplementary evidence used, the approval by the (Q)TSP shall include assessment that:

- The source of the supplementary evidence is trustworthy.
- Specify whether attributes from supplementary evidence shall complement or override attributes from authoritative evidence.
- Assess that attributes conveyed by supplementary evidence provides the same or better confidence than attributes conveyed from authoritative evidence.
- Assess that communication between the IPSP and the supplementary evidence provider is secure.

A trusted register designated by a Member State as Authentic Source of information as per eIDAS Article 45e and Annex IV should be accepted as supplementary evidence, but the decision is made by the (Q)TSP.

The IPSP conveys identity attributes received from authoritative evidence without changing them, unless overridden by supplementary evidence. Any difference in identity attributes provided or in attribute encoding between different evidence (see ETSI TS 119 461 clause 8.3.1) is resolved by conveying the attributes from the approved authoritative source for the (Q)TSP, whether this is authoritative evidence (eIDV) or supplementary evidence.

12.1. Basis for relying on attributes from a valid accepted document

Signicat does not claim that every attribute is confirmed as current against an external source. No such source is generally available for the documents and jurisdictions in scope. Instead, the following controls give reasonable assurance that there is no reason to believe an attribute has changed since the document was issued. A failed required check or unresolved doubt prevents a successful result, as specified in section 3 of the Identity Attribute Freshness and Document Validity Procedure.

a) Classification of the mandatory attributes (PPS 11.1) by how likely they are to change

Category	Attributes	Freshness rationale
Immutable	Date of birth, place of birth, national identification number (where permanent for the issuing country)	Do not change over a person's life. Freshness does not apply.
Describe the document itself	Document number, type, issuing country, issuing authority, date of issue, date of expiry	These describe the evidence, not the person. They are current as long as the document is genuine and within its validity period.
Change rarely and require a new document	Family name, given name, nationality	A change usually requires the holder to get a new document. Where that duty is established for the document and jurisdiction, a valid document is evidence that no change applies.
Optional / volatile	Address and contact details	Not mandatory. If returned, they are conveyed "as printed on the document" and are not presented as verified current data.

b) Document-level controls applied in each session

1. **Validity period.** The expiry date is compared with the date of the identity proofing. Expired documents are rejected. Documents with no expiry date (e.g. Spanish ID cards issued as permanent) are recognised explicitly, not treated as a missing value.
2. **Accepted type, model and issuer.** The document is classified to a specific model and version, and checked against the acceptance rules for the route and context.
3. **Internal consistency of the data.**
    - MRZ check digits are verified for the document number, date of birth, expiry date and the composite value. Any failed control is reported.

- Fields with their own check algorithm are also validated, for example the Spanish NIF control letter and the Romanian CNP.
- Mandatory attributes must be present and readable.
- Any inconsistency marks the data as not reliable.

4. **NFC route.** Passive authentication proves that the chip data was signed by the issuer and has not changed since issuance. Chip authentication proves that the chip is genuine.
5. **Binding to the applicant.** Face comparison and liveness detection confirm that the person presenting the document is its holder at the time of the session (section 13)..

c) Inherent limitation on the age of the data. Because identity documents have a limited validity period, the information they contain cannot be older than that period. Permanent documents are the exception and are covered by the review described in section 4 of the Identity Attribute Freshness and Document Validity Procedure.

d) Reasons to doubt. A discrepancy between data sources (VIZ, MRZ, chip), a failed integrity control, or information from the applicant or the context that suggests a change all prevent a successful result. Without an authorised source to clear the doubt, the session ends without success.

13. Binding to applicant

As per ETSI TS 119 461 clause 8.3.4, a successful authentication of the end user by eIDV means shall imply that the means as authoritative evidence is validated and that the identity attributes conveyed are bound to the end user.

If supplementary evidence is used, the approval process for the (Q)TSP shall include verification that the supplementary evidence only conveys identity attributes bound to the authenticated end user.

14. Issuing of proof

14.1. Result of the identity proofing

The result of an identity proofing is delivered to the (Q)CA or (Q)EAA provider by an API as described on developer.signicat.com.

14.2. Evidence of the identity proofing process

As described in 9.10, identity assertions issued in the context of the IPSP service are by default stored for 30 days. It is the responsibility of the customer, hence (Q)TSPs, to request the IPSP to store assertions longer in case this is required to reach compliance to requirements in ETSI EN 319 411-1/-2.