

General Terms of Use

General Terms of Use

Remote identity verification

Quicksign

Version	Date	Description	Authors	Company
1.1	22/10/2026	GENERAL TERMS OF USE	A.BOUSSADIA	QuickSign

Document status – Classification	Reference
Final – External public distribution	Associated policy OID: 1.2.250.1.546.1.1.1.1

This document is the exclusive property of QuickSign
Its use is restricted to authorized persons, in accordance with its confidentiality level.
Its reproduction is governed by the Intellectual Property Code, which authorizes it only for the private use of the copier.

Purpose of the document

This document sets out the terms and conditions of use for QuickSign's remote identity verification service (the "Service"). The user must accept these terms before beginning the identity verification process.
It summarizes the QuickSign Remote Identity Verification Policy, referenced under OID 1.2.250.1.546.1.1.1.1. In case of discrepancy, the Policy prevails.

General Terms of Use

Service contact	QuickSign, 19-21 rue Poissonnière, 75002 Paris – RCS Paris B 450 439 963 Phone: +33 1 825 20 500 Questions, complaints and fraud reports: plainte-pvid@quicksign.com
Service description and processing time	The Service remotely verifies the identity of a natural person at the Extended LoIP level, as defined by ETSI TS 119 461. It is implemented at the request of a QuickSign customer, the "commissioning party" (for example, a bank or a qualified trust service provider), who integrates it into their own process. The Service comprises two processes. NFC process (ID documents equipped with an electronic chip): The user films their ID document and then presents it to the NFC reader on their smartphone. The data signed by the issuing state is read from the chip, and its electronic signature is verified against the issuing state's certificate. Access to the chip requires the access number printed on the card (CAN) or the information from the document's machine-readable zone (MRZ); the identity data retained is that of the chip. The user then records a video of their face: the service verifies that it is a living person in front of the camera, and not a photo, mask, or injected video stream, and then compares their face with the photo stored on the chip. When all automatic checks are successful, the identity is validated. When the face comparison fails, a trained QuickSign operator reviews the case and can validate or reject the identity. Prerequisites: a smartphone equipped with an NFC reader and a camera, and the commissioning party's application. Hybrid process (ID cards without a chip, or where chip reading is impossible): The user films their ID card while tilting it to reveal its security features, then records a video of their face, which undergoes the same checks. A trained QuickSign operator reviews the videos and the results of the automated checks and makes the decision. Prerequisite: a terminal equipped with a camera—ideally capable of capturing at least 720p (1280×720, 25 frames/s) for optimal processing—to which the user grants access.

©QuickSign – Public external dissemination

	Automatic rejection: the file is rejected without human review when a video injection attempt is detected, when the liveness check fails or, in the NFC process, when the chip data signature is invalid. Processing time: In the NFC process, the decision is immediate when all automatic checks are positive. When an operator reviews the file, the decision is made in less than 15 minutes; operators are available 24/7.
Accepted identity documents and verification process	Only original, valid identity documents in the user's possession, as listed in Appendix 1 of the Policy, are accepted: passports, national identity cards, French residence permits, and, exceptionally, certain other expressly listed official documents. Appendix 1 also indicates which documents are eligible for NFC processing. Copies, photographs, scans, or screenshots of a document, as well as expired, damaged, or altered documents, and documents not listed, are not accepted. The user positions themselves in front of the camera with their face uncovered and free of any accessories that might conceal it, and follows the instructions displayed. Before any capture, the process informs the user of the nature of the operation and requests their explicit consent to the processing of their biometric data. If the user does not wish to or cannot use the Service, they can use an alternative solution offered by the commissioning party (for example, face-to-face verification) or, where QuickSign offers it, use an electronic identification method (eID) or the European Digital Identity Wallet (EUDI Wallet). The user has a limited number of attempts, set at 3, to complete their identity verification. The user is informed of the result (success or failure) by the commissioning party; for security reasons, the details of the checks and the precise cause of a failure are not disclosed. The commissioning party receives the verdict, the level of verification achieved (Extended LoIP), a generic reason in case of failure, the extracted image of the identity document, and the verified identity attributes: surname(s), first name(s), gender, date and place of birth, number, type, and issuing authority of the document.

©QuickSign – Public external dissemination

Complaints and claims	The user can send a complaint to the Service contact (plainte-pvid@quicksign.com), in particular if they are acting in good faith and their verification has failed, in the event of suspected or confirmed identity theft, or in the event of a Service malfunction. Each complaint is logged, tracked, and processed according to QuickSign's complaint handling procedure. QuickSign acknowledges receipt of the complaint within two business days and provides a reasoned response within one month of receipt. This period may be extended if the complaint is complex; the user will be notified accordingly. A confirmed case of identity theft is treated as a security incident and reported to the commissioning party.
Limitations of use	The result of the verification may only be used to establish a remote business relationship with the client, in particular with regard to anti-money laundering and counter-terrorist financing obligations, and for identity verification prior to the issuance of a qualified certificate by a qualified trust service provider, as defined in Regulation (EU) No 910/2014 as amended (eIDAS). Any other use is excluded.
User obligations	The user is responsible for the proper use of the Service. They agree to: ● accept these terms and conditions of use before using the Service; ● explicitly give consent to the processing of their biometric data; ● use only their own original and valid identity document; ● provide accurate information and not attempt to manipulate the process, such as a pre-recorded video, a virtual camera or a falsified document; ● use a terminal that they control and protect;

©QuickSign – Public external dissemination

	• report any fraudulent use of their identity immediately to the Service contact or the commissioning party.
Limitation of liability	QuickSign implements the measures described in its Policy to deliver a reliable result. It has insurance covering its professional liability and cyber risks. Subject to applicable public policy provisions, QuickSign is not liable for damages resulting from: • use of the Service other than as provided for in the section "Limitations of use"; • fraudulent, erroneous or inaccurate information or identity documents provided by the user; • the inability to verify the user's identity, even where the user is acting in good faith, particularly for technical reasons related to their terminal; • force majeure. These limits do not apply in the event of fault by QuickSign in the performance of the Service, under the conditions provided for in Article 13 of the eIDAS Regulation.
Document references	QuickSign's Remote Identity Verification Policy, which takes precedence over these terms and conditions in the event of any conflict, and these terms and conditions are available at the following address: https://www.quicksign.com/fr/conformite/
Availability and accessibility	QuickSign strives to ensure the availability of the Service, subject to maintenance operations and service commitments agreed with the commissioning party. QuickSign strives to make the Service accessible to people with disabilities, in accordance with Article 15 of the eIDAS Regulation, based on the WCAG 2.1 standard. If a user is unable to complete

	the process, they can contact the commissioning party for an alternative solution (such as face-to-face verification) or, where offered by QuickSign, use an electronic identification method (eID) or the European Digital Identity Wallet (EUDI Wallet). No specific compensation is provided for under these terms and conditions.
Applicable law	These Terms and Conditions are governed by French law. In the event of a dispute, the user is encouraged to first contact the Service in order to seek an amicable solution. Failing that, the dispute will be brought before the competent courts within the jurisdiction of the Court of Appeal of Paris, subject to the mandatory rules applicable to consumers. QuickSign may modify these terms and conditions. The applicable version is the one accepted by the user at the time of verification. Any new version is published at the address indicated in the "Document references" section. Any modification concerning biometrics or identity documents is validated beforehand by the Expertise and Quality representative.
Personal data and biometrics	QuickSign processes user data in accordance with the GDPR and the French Data Protection Act, acting as an independent data controller for the processing necessary for identity verification and the creation of the evidence file. In particular: - The calculated biometric templates are never saved: they only exist in RAM during the process and are only used to establish the user's identity; - No biometric processing is carried out on the content of the evidence file, except upon judicial request; - The evidence file is securely archived, with a guarantee of integrity. For more information on the processing of personal data and the GDPR compliance measures implemented by QuickSign, please visit the following page: https://www.quicksign.com/en/privacy-policy/

©QuickSign – Public external dissemination

<table>
<tr><td>Conformity assessment</td><td>The Service is subject to regular audits. It is assessed by a conformity assessment body against the eIDAS Regulation and the ETSI TS 119 461 standard.
Certificates of conformity are published at https://www.quicksign.com/fr/conformite/ as soon as they are issued.
The Policy and these terms and conditions are reviewed at least once a year.</td></tr>
<tr><td>Retention periods for logs and evidence files</td><td>The retention periods are as follows:
<table>
<tr><td>Evidence file, including:
photos of the user's face and their identity document;
the date the data was captured;
the results and dates of the checks carried out, the identifier of the operator who carried out the check, the verdict and the reason;
the identity verification result (verification outcome and extracted data).</td><td>Duration set by the commissioning party, aligned with the contractual relationship; minimum 7 years.</td></tr>
<tr><td>Videos of the face and identity document (raw biometric data) and verification data, in the active QuickSign database
Calculated biometric templates</td><td>90 days after receipt, then deleted.

Not retained: in RAM only, during the process</td></tr>
<tr><td>Other technical logs (connection logs, etc.)</td><td>1 year.</td></tr>
</table>
In accordance with the GDPR, the user may exercise their rights (access, rectification, etc.) with QuickSign by contacting the Service. The content of the evidence file cannot be modified, but a correction can be requested from the commissioning party.</td></tr>
</table>