ubble

Remote Identity Verification Policy

Document for Public Distribution

Table of Contents

1 Classification....5
2 Introduction....6
2.1 Overview....6
2.2 Identification of the document....6
2.3 Definitions and acronyms....6
2.4 Entities involved in the identity verification process....7
2.5 Verification Policy (VP) management....7
2.6 Responsibilities concerning the provision of information which must be published....8
3 Description of the remote identity verification service....10
3.1 Identity verification procedure....10
3.2 Languages in which this service is available....10
3.3 Alternatives to remote identity verification....10
3.4 Appeal procedures and complaint....10
4 Remote identity verification procedure....12
4.1 Remote identity verification service activities....12
4.2 Acquisition of identification data....12
4.3 Verification of identification data....12
4.4 Creation of the evidence file....13
4.5 Sending the results....14
5 Procedure for detecting identity theft attempts....16

5.1 Detecting cases of suspected or proven identity theft....16
5.2 Alerts in the event of suspected or proven identity theft....16
6 Managing your personal data....17
6.1 Status....17
6.2 Identification of processed data....17
6.3 Purpose and nature of operations....17
6.4 Retention period....18
6.5 Subcontracting....18
6.6 User rights....18
6.7 Alternative methods....19
6.8 Research and development....19
7 Intellectual and industrial property rights....20
8 List of documents accepted by the service....21

1 Classification

Document status - Classification	Ref. OID VP	Policy version	Date
C1 (public document)	1.3.6.1.4.1.55559.1.1.1.0	1.1	15 Feb. 2023

2 Introduction

2.1 Overview

NJFVision, trading as ubble, is a Remote Identity Verification Service Provider which provides services to its clients involving the verification of identity documents and the verification of ownership of these documents.

This document outlines the Remote Identity Verification Policy (RIVP) for ubble's certified services. This document covers all of ubble's rules, requirements and commitments within the scope of the implementation, operation and lifecycle of identity verification in terms of technical and organisational security requirements.

2.2 Identification of the document

The identifier for this document is the OID: **1.3.6.1.4.1.55559.1.1.1.0** for the identity verification service with a substantial level of assurance, as defined by the RIVP standard[1] published by the French National Cyber Security Agency (ANSSI).

Items specific to an OID will be preceded by the OID in square brackets: [OID]. Several OIDs can be specified, separated by semicolons. OIDs may change in the event of important amendments to the . When a new OID is generated, the last digit is incremented. The initial version uses the number 0.

2.3 Definitions and acronyms

Acronym	Meaning
VP	Remote Identity Verification Policy
VPS	Remote Identity Verification Practice Statement

Term	Definition
Identity document	An official document certifying a person's identity.
Identification data	A set of personal data acquired and verified by the service to verify a natural person's identity. In the context of this standard, the identification data may be the video of the user's face, the video of the identity document provided by the user, or the identification data relating to the user (including the photo of the user's face) stored in the security component of the identity document.
Identity attributes	A subset of the identification data sent by the remote identity verification service to the business service. These attributes include surname at birth, preferred surname if applicable, first name, date of birth, place of birth, country of birth, nationality and gender.
Attributes relating to the identity document	A subset of the extracted data comprising all the fields specific to the document provided which enables its authenticity and validity to be verified. This includes, as a minimum, the issuing country, the document number, the expiry date and the date of issue.

1 https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf

2.4 Entities involved in the identity verification process

Remote identity verification service: A remote identity verification service aims to acquire and verify users' identification data to identify them, create the evidence file and send the result of the remote identity verification to the business service.

User: A user is a natural person who may be asked to verify their identity using the RIVP remote identity verification service.

Professional services: A service to which the user wishes to identify themselves, for which the business service is responsible, using the remote identity verification service.

Operators: Remote identity verification service staff responsible for verifying users' identity.

Identity fraud specialists: Remote identity verification service staff with in-depth knowledge of the security features of identity documents and expertise in detecting identity fraud.

Biometric fraud specialists: Remote identity verification service staff with in-depth knowledge of biometrics and expertise in detecting biometric fraud.

Fraud specialists: Remote identity verification service staff who are both specialists in identity document fraud and biometric fraud.

Team leaders: Remote identity verification service staff responsible for ensuring policies and internal regulations are applied. At least one team leader is always on the premises at all times.

2.5 Verification Policy (VP) management

2.5.1 The entity managing the VP

NJFVision, trading as ubble, is responsible for the VP. Its contact details are:
NJFVision, 12 rue Curial, 75019 Paris, France.

2.5.2 Point of contact

All requests relating to this VP should be addressed to:

- pvid@ubble.ai[2] if sending a request via email
- or by post to: ubble RIVP management, NJFVision, 12 rue Curial, 75019 Paris, France.

2.5.3 Amendments to the VP

2.5.3.a Amendment procedure

ubble has an **ubble RIVP Compliance Committee**, which checks that any proposed changes to its VP remain compliant with the requirements of this VP. In the event of an important change, the **RIVP ubble Compliance Committee** may call on external technical expertise if it deems this necessary.

Specifically:

2 mailto:pvid@ubble.ai

- the person in charge of the identity document fraud specialists must formally approve any change to the identity document;
- the person in charge of the biometric fraud specialists must formally approve any change relating to biometrics.

2.5.3.b Circumstances under which the OID must be changed

As the OID of the VP is recorded in the results of identity verifications, any changes to this VP that have a major impact on past identity verifications must be reflected in changes to the OID so that business services can clearly distinguish which verifications correspond to which requirements. In particular, the OID of the VP must be changed whenever a major change (which will be indicated as such, namely by a change in the OID of this VP) occurs regarding the requirements of this VP.

2.5.4 Entity determining the existence and compliance of a VPS with this VP

ubble produces and updates a Remote Identity Verification Practice Statement, which is a set of practices (organisation, operational procedures, technical and human resources, etc.) that apply to the provision of its service and are in accordance with this Remote Identity Verification Policy. The Remote Identity Verification Practice Statement is confidential and is only shared with people on a need-to-know basis. ubble has an **ubble RIVP Compliance Committee**. This Committee validates the compliance of the VPS with the VP.

2.5.5 VPS compliance approval procedure.

The **RIVP ubble Compliance Committee** carries out or commissions all the necessary measures (audits, etc.) to validate and approve the VPS.

2.5.6 Duration and early expiry of the VP

The VP for the service must remain in force until at least the end of the life of the last evidence file created. This VP remains in force until a new version is published.

2.6 Responsibilities concerning the provision of information which must be published

2.6.1 Entities responsible for providing information

ubble has set up a page consolidating all the information published: https://www.ubble.ai/en/verification-policy/.

2.6.2 Information which must be published

ubble publishes the following information: all the VPs managed by ubble, including this one. There is a section on the website where information is published, which has been specifically designed for archiving older versions of published data.

2.6.3 Publication deadlines and frequency

The VP is published before any identity verification containing the corresponding OID. This information is available seven days a week, twenty-four hours a day, with a maximum downtime of 4 hours. The **RIVP ubble Compliance Committee** decides which parties (clients, users, sub-processors providing the service,

supervisory bodies, etc.) should be informed when a new VP is published or will be published (an initial version or a modified version of an existing VP), depending on the nature of the changes made.

2.6.4 Controlling access to published information

All the information published above is public and read-only. Modification access to published data is restricted to the internal ubble teams responsible for publishing documents on the section of the site where the information is published.

3 Description of the remote identity verification service

3.1 Identity verification procedure

3.1.1 Identity verification

The remote identity verification service aims to validate that the identity document provided by the user is genuine and that the user is the rightful holder of the identity document. The verdict is determined based on the identification (personal) data acquired and verified by the service. The verdict, together with the identity and document attributes, is then communicated to the business service.

3.1.2 Identity attributes that characterise the uniqueness of an identity

The following identity attributes are deemed to characterise the uniqueness of an individual's identity and are therefore sent to client services: **surname(s), first name, date of birth, place of birth, country of birth, nationality and gender**.

3.1.3 Description of the identity verification procedure

The business service invites users whose identity it wishes to verify to use the identity verification service's web page. There are several possible ways to direct the user to this page and to access this page. The user is then asked to capture their identity document and face on video and is guided through this step in their own language. Once the identification data has been captured, the verification service verifies it **asynchronously**.

3.2 Languages in which this service is available

The identity verification service supports the following languages: **French**, German, English, Spanish, Italian, Dutch and Portuguese. When using the service, and before any identification data is acquired, the user chooses the language they want to use. The user is also informed of the location (country) of the operators responsible for verification.

3.3 Alternatives to remote identity verification

Any user who does not want to or cannot use the identity verification service under the conditions proposed may **request an alternative method of identity verification from the requesting party's business service.**

3.4 Appeal procedures and complaints

3.4.1 Contact

Users, business services and third parties have the right to send any request concerning the service (such as the cancellation of fraudulent identification or the refusal to identify a bona fide user) to:

- pvid@ubble.ai[3] if sending a request via email

3 mailto:pvid@ubble.ai

- or by post to: ubble RIVP management, NJFVision, 12 rue Curial, 75019 Paris, France.

3.4.2 Complaint handling procedure

Requests received by post or email are logged on a tracking system so that any requests can be monitored. ubble acknowledges that they have received requests upon receipt and is committed to responding within 7 working days of receiving the request.

Requests relating to the business services process, particularly the steps and procedures required by the business service, cannot be processed by ubble, who will redirect the requests to the business service concerned.

Requests relating to a specific natural person can only be processed for validated identifications, and if the request specifies the surname(s), first name, date of birth, place of birth, country of birth and nationality of the person concerned, as well as the business service that requested the identification and the day on which it took place.

Requests relating to one or more attempts (e.g. failed attempts) can only be processed if the request specifies the identification number, which is available from the business service.

4 Remote identity verification procedure

4.1 Remote identity verification service activities

The remote identity verification service involves four successive steps:

- acquisition of identification data
- verification of identification data
- creation of the evidence file, and
- sending the results.

4.2 Acquisition of identification data

The data acquisition phase is accessible from the user's device using a web browser. Only mobile devices are accepted and must use Apple's iOS or Google's Android operating system. The device must also be equipped with a front and rear camera and a compatible web browser to be compatible. The following web browsers are supported:

Type of phone	Safari	Chrome	Firefox	Samsung Internet
iOS 11 and above	✓			
iOS 13 and above	✓	✓	✓	✓
Android		✓ *≥73*	✓ *≥66*	✓ *≥6.2*

The user completes the acquisition phase themselves. However, the system may be required to guide them through it by suggesting alternatives to improve the capture quality. This phase includes the document capture step and face capture step.

During the document capture step, the user may receive the following requests:

- Place your document in the centre of the capture frame.
- Check the sharpness and lighting of the document.
- Rotate the identity document.
- Flip the identity document.
- Tilt the document from left to right.
- Take photographs of specific parts of the document.

During the face capture step, the user may receive the following requests:

- Place your face in the centre of the oval.
- Turn the document from left to right.
- Reproduce hand gestures.

No verification carried out on the user's device can contribute to the "successful" verdict of the remote identity verification.

4.3 Verification of identification data

After capture, the identification data is sent to ubble's verification servers, which verify the document's authenticity and whether the holder is the rightful holder of the document. This data takes the form of videos of the user's identity document and face. For these videos to be used, they must have an input and post compression resolution of no less than 1280 × 720 pixels at 25 frames per second when the document and face are captured.

No processing, including any partial processing, relating to verifying the identity document's authenticity, matching the user's face with the photo extracted from the identity document, or verifying proof of life is carried out on the device.

4.3.1 Identity documents

The identity document's authenticity is verified through a series of automated processes, and one or more operator(s) who are experts in identity verification make the final decision. If the identity document is invalid, for whatever reason, the verdict of the identity verification is always "unsuccessful". Reasons for invalidity include but are not limited to, non-authentic documents, documents reported lost or stolen, non-original documents (photocopies, for example), expired documents, documents not accepted by the service, documents that are too damaged, etc.

The full list of documents accepted by the service is attached. No other document will be accepted. ubble keeps a list of identity document fraud specialists qualified to analyse each accepted document.

Only documents that have not expired will be accepted by the service.

In the specific case of altered and/or damaged documents, the service can only process the document if the identity and security features are intact. These features depend on the nature of the document in question.

To confirm the document's validity and, where appropriate, whether it has been lost or stolen, the service systematically searches the databases of the issuing countries where available. If verification of the identity document's validity is carried out and it concludes that the identity document is invalid, then the verdict of the remote identity verification is automatically "unsuccessful".

4.3.2 Face comparison

To verify whether the document holder is the rightful holder and whether they are alive or not, they are verified through a series of automated processes, and one or more operator(s) who are experts in identity verification make the final decision. If the document holder is not the rightful holder, for whatever reason, the verdict of the identity verification is automatically "unsuccessful".

4.4 Creation of the evidence file

Each identity verification, regardless of the verdict ("successful" or "unsuccessful"), is subject to the creation of an
evidence file.

4.4.1 Content of the evidence file

The evidence file includes the following:

1. **Acquisition data**:
   - video(s) of the identity document
   - video of the user's face
   - their acquisition date.
2. **All the checks** carried out on the identification data, and for each check:
   - the date of the check
   - the activity associated with the verification, in particular:
     - the verification of the identity document's authenticity

        - liveness detection of the user
        - comparison of the user's face
    - the nature of the check: automatic or manual
    - the identity of the operator or the fraud specialist who carried out the verification when this is done manually
    - the country from which the operator or the fraud specialist carried out the verification when this is done manually
    - the version and configuration, if any, of the devices used for automatic verification
    - the intermediate report issued by the automated processing, the operator or the fraud specialist following verification.
3. **The result** of the remote identity verification sent to the business service consists of:
    - the verdict (successful or unsuccessful)
    - identity attributes relating to the user (surname(s), first name, date of birth, place of birth, country of birth, nationality and gender)
    - attributes relating to the identity document provided (issuing country, unique identity document number, date of issue, expiry date and MRZ)
    - the reasons the operator provides in the event of an "unsuccessful" verdict.

The purpose of this data is to resolve any disputes that may arise, and under no circumstances should it be subject to any biometric processing.

4.4.2 Retention of the evidence file

As soon as they are created, evidence files are encrypted using a unique encryption key for each file. The associated encryption algorithm is AES-256-GCM. Master keys are rotated daily and stored in secure cryptographic equipment under ubble's control. Access to master keys is only possible when several managers are present.

Unless otherwise requested by the business service, the data in the evidence file is kept for:

- a maximum of six (6) years in the event of a successful verdict,
- three (3) months in the event of an unsuccessful verdict.

During this retention period, the data in the evidence file is not subject to any processing, particularly biometric processing, except in the event of a legal request which complies with the applicable regulatory requirements.

4.4.3 Access rights to personal data in the evidence file

Evidence file data, and in particular personal data, is subject to the GDPR, and users' rights apply, with the exceptions outlined in the section below.

4.5 Sending the results

At the end of the verification phase, the service issues a verdict, which may be successful or unsuccessful. In both cases, a result is sent to the business service.

4.5.1 Content of the result sent to the business service

This result includes the following:

- **the verdict** (successful or unsuccessful)

- **identity attributes** relating to the user (surname(s), first name, date of birth, place of birth, country of birth, nationality and gender)
- **attributes relating to the identity document** provided (issuing country, identity document number, date of issue, expiry date and MRZ)
- **data** deemed to be **additional when required by the requesting party**
  - one or two photos of the identity document (front and back), captured in the video
  - stream one photo of the user's face, captured in the video stream
  - an email address
  - a telephone number
  - a unique identifier for the user of the business service
- **the reasons the operator provides** in the event of an "unsuccessful" verdict.

Please note that:

- the additional data does not in any way contribute to the verdict
- the following are not included in the results sent to the business service:
  - the videos of the document and the face are not sent, in whole or in part, to the business service,
  - nothing related to the verifications carried out by the service other than the verdict is sent to the business service, and in particular, no verification score.

4.5.2 Time taken to send results to the business service

The time between the start of the acquisition of identification data by the user and the notification of the identity verification result to the business service is generally a few hours and must not exceed 96 hours.

5 Procedure for detecting identity theft attempts

5.1 Detecting cases of suspected or proven identity theft

The purpose of ubble's remote identity verification service is to limit or even prevent cases of identity theft. Indicators of identity theft cases are evaluated and researched during the identity data verification phase to achieve this objective. Among these indicators, the following events trigger suspicion of identity theft:

- using a forged identity document
- alteration of identity data on a genuine identity document
- using an identity document that has been reported lost or stolen
- changing the photograph on an identity document
- overt modification of a user's appearance to resemble the holder of an identity document
- verification carried out under duress or without the user's knowledge
- user thinking of registering for another service.

5.2 Alerts in the event of suspected or proven identity theft

An alert is generated whenever identity theft is suspected or proven, whether detected by ubble or communicated by the business service. Each alert is analysed and used to prevent fraud and improve the system.

6 Managing your personal data

6.1 Status

ubble processes users' personal data as a sub-processor on behalf of the client whom the user requests and who has contracted with ubble to provide the identity verification service. The client is responsible for processing users' personal data.

As a data processor, ubble complies with the principle of minimisation of data collected and stored in accordance with the client's instructions.

6.2 Identification of processed data

The personal data relating to users processed by the remote identity verification service is as follows:

Type of data	Data details
Connection data	• 3G, 4G, wi-fi etc. • operating system version • browser type • time stamping • IP address • the type of device used (smartphone, tablet, computer) • email address • telephone number • unique identifier of the business service user
Civil status data	Filming the official identity document generates hundreds of images of the identity document. The following data is extracted from these high-quality images: • type of document • nationality • document registration number • surname • first name • gender • date of birth • place of birth • signature • expiry date • date of issue • face photograph
Face videos	Filming the face generates hundreds of images of the user's face.
Biometric data	ubble creates an imprint of the user's face from videos of the identity document and face so it can compare this user's imprints with others.
Metadata relating to the verification process	The following data is required to create the evidence file: • date of acquisition of identification data • operator identifier for the operator who verified the identification data • the country from which the operator carried out the verification • verification date of identification data • all checks carried out on identification data • the result of the remote identity verification sent to the client.

6.3 Purpose and nature of operations

ubble processes users' personal data, on behalf of the client, for the sole purpose of:

- verifying the identity of users as part of the performance of a contract between ubble and its client
- compiling an evidence file containing all the information needed to resolve disputes, and
- auditing the quality of the service and informing ubble's client of any shortcomings during the verification of the user's identity.

This processing involves collecting, encrypting, consulting, using, archiving and deleting users' personal data.

6.4 Retention period

As a matter of principle, and unless otherwise instructed by the client:

- Each user's data, including biometric data, is processed in an active database for the time required to verify the user's identity.
- Biometric data will be permanently and securely deleted no later than 96 hours after collection.
- The user's other personal data will be kept in an intermediary archive for up to three (3) months to audit the quality of the service.
- In the event of a dispute, the evidence file is kept in an intermediary archive from the time the result of the verification is sent to the client for:
  - a maximum of six (6) years in the event of a successful
  - verdict
    three (3) months in the event of an unsuccessful verdict.

Archived personal data may only be accessed by persons specially authorised to do so by virtue of their functions and strictly for the purposes set out above.

At the end of the archiving periods specified above, personal data will be securely and permanently destroyed, except in the event of ongoing litigation or proceedings requiring data to be kept for the entire duration of the proceedings.

6.5 Subcontracting

The following sub-processors are involved in processing the user's personal data:

- Outscale SAS, registered under number 527 594 493 of the Nanterre Trade and Companies Register, which provides the identity verification service. Data sent to Outscale SAS is encrypted,
- Sendinblue, registered under number 498 019 298 of the Paris Trade and Companies Register, which provides the SMS redirection service (only telephone numbers are provided).

6.6 User rights

With certain exceptions, the service allows users to exercise their rights of access, rectification and deletion of their data in accordance with the client's confidentiality policy. The exceptions to user rights are as follows:

- rectification or deletion of the evidence file and the results of the remote identity verification sent to the business service, as well as all the information required to compile the results,
- access to data subject to automated or manual processing, the disclosure of which is likely to provide information on the nature of the verifications carried out by the service and relating to the detection of identity fraud.

Users must contact the client, the data controller, to exercise their rights.

6.7 Alternative methods

If the user does not wish to verify their identity using the service described in this document, they must contact the client's business service to obtain an alternative means of verifying their identity.

6.8 Research and development

ubble, as data controller, processes users' personal data for research and continuous improvement of the service, based on its legitimate interest, for a maximum period of 3 months from the collection date. This processing, which aims to improve the reliability of the service, requires potential improvements to be compared with the wide variability of conditions experienced by real users, and therefore requires the use of data from users of the service. Only authorised ubble employees have access to user data.

Users have the right to access, rectify and delete their personal data, restrict the processing thereof, and object to the processing of their data for R&D purposes by ubble. To exercise their rights, users may contact ubble's DPO at

- privacy@ubble.ai[4] if sending a request via email
- or by post to: Ubble DPO, NJFVision, 12 rue Curial, 75019, Paris, France

Users may also lodge a complaint with any competent authority. In France, the competent authority is the National Commission for Information Technology and Civil Liberties (CNIL) (https://www.cnil.fr/en).

4 mailto:privacy@ubble.ai

7 Intellectual and industrial property rights

All intellectual property rights held by ubble are protected by current legislation and regulations. Users have no intellectual property rights over the various elements used by ubble to provide its identity verification service. Infringement of trademarks, service marks, designs, distinctive signs, and copyrights (e.g. software, web pages, databases, original texts, etc.) is punishable under the French Intellectual Property Code.

8 List of documents accepted by the service

Only ordinary identity documents (excluding diplomatic, service and temporary documents) are accepted for the purposes of this standard, provided that they meet the requirements set out in this policy and comply with the following criteria:

1. For French nationals and nationals of other Member States of the European Union, a State party to the Agreement on the European Economic Area or Switzerland, **a passport or identity card** is accepted provided that the document has an MRZ[5] and sufficient security features (such as optically variable inks[6]), in the spirit of Regulation (EU) No 2019/1157 of the European Parliament and of the Council of 20 June 2019.
2. For third-country nationals residing in France or another Member State of the European Union, a State party to the Agreement on the European Economic Area or Switzerland, **a residence permit** is accepted provided that it was drawn up in accordance with the model provided for by Regulation (EU) No 2017/1954 of the European Parliament and of the Council of 25 October 2017 or by Council Regulation (EC) No 1030/2002 of 13 June 2002 and was issued by the State of residence.
3. For third-country nationals who are exempt from the short-stay visa requirement to travel to mainland France[7] and who do not reside in the European Union, a State party to the Agreement on the European Economic Area or Switzerland, **an electronic passport** is accepted except for countries whose exemption from the visa requirement includes the requirement to have a biometric passport, for which no document will be accepted.
4. For third-country nationals who are refugees or recognised as stateless or who benefit from the protection provided for in Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011, and the content of the protection granted, the passport is replaced by **the travel document issued by the State which has recognised the status of refugee or stateless person or granted protection**.

The full list of acceptable documents is available in the document *List of acceptable forms of ID* version 1.0, dated 15 February 2023.

5 https://www.consilium.europa.eu/prado/en/prado-glossary/prado-glossary.pdf
6 https://www.consilium.europa.eu/prado/en/prado-glossary/prado-glossary.pdf
7 https://www.immigration.interieur.gouv.fr/Immigration/Les-visas/Les-dispenses-de-visa