RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Remote identity verification service providers

Requirements rule set

Version 1.1 of 1 March 2021

VERSION HISTORY			
DATE	**VERSION**	**DOCUMENT CHANGES**	**EDITOR**
19/11/2020	1.0	*Draft version for comment.*	ANSSI
01/03/2021	1.1	*First applicable version, curtesy translation*	ANSSI

Comments on this document should be addressed to:

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

commentaires-pvid@ssi.gouv.fr

CONTENTS

I. Introduction

I.1. General presentation

I.1.1. Background

The digital transformation of society has created the need to be able to remotely identify people wishing to access public or private online services, when they do not have a digital identity recognised by these services. In order to guarantee the reliability of these processes, the regulation establishes that the French National Cyber Security Agency (ANSSI), with the support of the Ministry of the Interior, can evaluate remote identity verification services.

A remote identity verification service[1] therefore has the same purpose as face-to-face identity verification, namely to verify that the identity document[1] presented by the user[1] is authentic and that the user is the legitimate holder of the identity document. The main objective of malicious persons against a remote identity verification service is the same as against face-to-face identity verification, namely identity theft or alteration.

A remote identity verification service is exposed to the same risks as a face-to-face identity verification but, by its nature, it is also exposed to specific risk scenarios.

This rule set contains the applicable requirements for remote identity verification services to provide an assurance level based on the risks and profiles of the attackers. The assurance levels referred to in this rule set attest to a remote identity verification that meets the security objectives defined by the European Regulation [EIDAS] for:

- assurance level substantial[1], which is intended to substantially reduce the risk of identity theft or alteration, the service must guarantee equivalence in terms of reliability with a physical face-to-face meeting carried out in the context of access to a public or private service requiring proof of identity (for example, by a person generally trained in the comparison of faces and in the detection of altered or falsified identity documents, but who does not have elaborate tools). The service must be able to withstand an attacker with a moderate attack potential[1];
- assurance level high[1], which is intended to prevent the risk of identity theft or alteration, the service must guarantee equivalence in terms of reliability with a physical face-to-face meeting carried out in the context of issuing an identity document (e.g. carried out by a person trained in the fight against identity fraud and with specific equipment enabling the authenticity of identity documents to be confirmed and trained in facial comparison). The service must be able to withstand an attacker with a high attack potential[1].

The present rule set does not impose any architecture for the information system of the remote verification service, so several implementations can be considered. Nor does the present rule set create any restrictions relating to the typology or organisation of remote identity verification service providers (which may be public or private bodies, that may or may not subcontract all or part of their activities) or to the interconnection between the remote identity verification service provider and the client (which may be totally external or operate an in-house remote verification service for its own needs).

I.1.2. Purpose of the document

This document constitutes the requirements rule set (hereinafter referred to as "the rule set") applicable to a remote identity verification service provider, hereinafter referred to as "the service provider".

This document does not formalise any requirements for the client of the remote identity verification service, hereinafter referred to as "the client".

[1] See definitions in chapter I.3.2.

This rule set is intended to be used in different regulatory frameworks, as described in chapter III.

I.1.3. Structure of the document

Chapter I corresponds to the introduction of the rule set.

Chapter II describes the activities covered by the rule set.

Chapter III presents the methods of evaluation and certification of service providers attesting their compliance with the requirements of the rule set.

Chapter IV presents the requirements that service providers must meet in order to comply with the rule set.

Annex 1 presents the references of the legislative, regulatory, normative and other texts mentioned in the rule set.

Annex 2 presents the tasks and skills expected of the service provider's staff.

Annex 3 presents the recommendations to clients of remote identity verification services.

Annex 4 presents the credentials that can be accepted by a service provider that complies with the rule set.

I.1.4. Scope of the document

The rule set specifies the requirements for remote identity verification service providers, whether these services are asynchronous[2], synchronous with human interaction[2], synchronous without human interaction[2], internal[2] or external[2].

The rule set does not cover:

- remote verification of the identity of legal persons or of the relationship between natural persons and legal persons;
- remote identity verification based on mechanisms other than facial comparison;
- verification of additional data[2] acquired by the remote identity verification service.

The rule set does not exclude the application of legislation and regulations on the protection of personal data, in particular [GDPR], nor the application of the general rules imposed on service providers in their capacity as professionals and in particular their duty to advise their clients.

I.1.5. Updating the document

The opportunity to update this rule set is evaluated by ANSSI and can in particular result from a change in the legislative, regulatory or normative framework, the state of the art, the threat assessment or the evaluation process for remote identity verification service providers.

ANSSI specifies the effective date of each update and the particulars for transition where applicable.

I.2. Document identification

This rule set is called "Remote identity verification service providers – Requirements rule set". It can be identified by its name, version number and date of update.

[2] See definitions in chapter I.3.2.

I.3. Acronyms and definitions

I.3.1. Acronyms

The acronyms used in this rules set are:

ANSSI	*Agence Nationale de la Sécurité des Systèmes d'Information* - French National Cyber Security Agency
OID	*Object Identifier*
PASSI	*Prestataire d'Audit de la Sécurité des Systèmes d'Information* - Cybersecurity Audit Service Provider
PRADO	Public Register of Authentic Travel and Identity Documents Online
IS	Information System
ISS	Information Systems Security
eIDAS	Electronic Identification, Authentication and Trust Services – European Regulation no. 910/2014 on electronic identification and trust services
GDPR	General Data Protection Regulation
FAR	False Acceptance Rate
FRR	False Rejection Rate

I.3.2. Definitions

The definitions below apply to this rule set. Some are based on the European regulations [EIDAS] and [GDPR].

Additional data – data acquired by the remote identity verification service and passed on to the business service in the remote identity verification result but on which no verification is performed by the service in the context of the rule set. The additional data is not part of the remote identity verification verdict. The acquisition by the remote identity verification service of this additional data and its transmission to the business service must be done in accordance with applicable regulation, and is generally requested by the client to meet regulatory requirements.

Administrator – Remote identity verification service staff with privileged access rights to all or part of the information system components of the remote identity verification service.

Assurance level high – this level aims to prevent the risk of identity theft or alteration. A remote identity verification service is said to be of assurance level high when it is demonstrated that it meets the requirements of the rules set for assurance level high.

Assurance level substantial – this level aims to substantially reduce the risk of identity theft or alteration. A remote identity verification service is said to be of assurance level substantial when it is demonstrated that it meets the requirements of the rules set for level substantial.

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

Attack potential – measure of the effort required to attack a remote identity verification service, expressed in terms of an attacker's expertise, resources and motivation. Annex B.4 of [CC_CEM] provides guidance on calculating a high or moderate attack potential.

Biometric data – personal data resulting from specific technical processing, relating to the physical, physiological or behavioural characteristics of a natural person, which enable or confirm their unique identification.

Biometrics fraud officer – remote identity verification service staff with extensive knowledge of biometrics and expertise in biometric fraud detection.

Business service – service to which the user wishes to identify, under the responsibility of the client, using the remote identity verification service.

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

Consent – any freely given, specific, informed and unambiguous indication of the user's wishes by which they, by a statement or by a clear affirmative action, indicate agreement to the processing of personal data relating to them.

Electronic means of identification – material and/or immaterial element containing personal identification data and used to authenticate for an online service.

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

External remote identity verification service – a remote identity verification service is said to be external if it does not meet the criteria of an internal service.

Hybrid remote identity verification service – a remote identity verification service is said to be hybrid when the "successful" verdict of the result of the remote identity verification can only be declared by an operator once they have validated the results of the verifications carried out by automated processes and carried out their own verification of the identification data.

Identification data – set of personal data acquired and verified by the service in order to verify the identity of a natural person. In the context of this rule set, the identification data can be the video of the user's face, the video of the identity document presented by the user, or the user data (including the user's facial photograph) stored in the security component of the identity document.

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

Identity document – official document certifying the identity of a person. The identity documents referred to in Annex 4 of this rule set are accepted in the context of this rule set.

Identity document fraud officer – remote identity verification service staff with extensive knowledge of identity document security features and expertise in detecting identity document fraud.

Identity theft – the act of fraudulently using another person's identification data. In the context of this rule set, the notion of identity theft also includes the alteration of identity, involving the use of fraudulent identification data that does not belong to an existing person.

Information system component – any software or hardware element of the information system involved in the provision of the remote identity verification service.

Intermediate finding of the remote identity verification – information generated by the remote identity verification service in the context of analyses carried out by automatic processes or by operators, and necessary for the elaboration of the remote identity verification verdict. Several intermediate findings can contribute to the same verdict.

Internal remote identity verification service – a remote identity verification service is said to be internal in the following two cases: if it is offered exclusively to business services having a legal link within the meaning of Articles L. 233-l et seq. of the French Commercial Code with the same legal entity and operated

by a service provider also having a legal link of the same nature with the same legal entity; if it is offered to business services belonging to the same administrative authority, within the meaning of Article I-1 of Ordonnance No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and operated by a service provider belonging to the same administrative authority.

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

Liveness detection – the detection of the user's "liveness" is intended to authenticate the video of the user's face, to verify that it has not been physically or digitally altered.

Operator – remote identity verification service staff in charge of verifying the identity of users, declaring the "successful" or "unsuccessful" verdict of the remote identity verification and alerting a fraud officer in cases of suspected identity theft.

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

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

Reason for failure – cause of an "unsuccessful" verdict for the remote identity verification. The reason for the failure is communicated by the remote identity verification service to the business service or user and is used in particular to distinguish between a failure due to suspected fraud and a failure due to technical reasons (insufficient terminal camera resolution, insufficient light, focus problem, etc.). In the case of suspected fraud, the reason does not include any information on the verifications carried out or on the type of fraud suspected.

Remote identity verification policy – set of rules, which has a unique reference identified by an OID, defining the requirements with which a remote identity verification service provider complies in setting up and delivering its service. A remote identity verification policy may also, if necessary, identify obligations and requirements on other stakeholders, including users and clients. The remote identity verification policy is made available to users.

Remote identity verification result – all information sent by the remote identity verification service to the business service, including the verdict (successful or unsuccessful) of the remote identity verification, the reason for the failure if any, the user-related identity attributes required by the business service and verified by the service provider, and any additional data required by the business service.

Remote identity verification service – service covered by this rule set, responsible for acquiring and verifying user identification data in order to identify users, producing the evidence file and sending the result of the remote identity verification to the business service.

Remote identity verification verdict – binary verdict ("successful" or "unsuccessful") generated by the remote identity verification service after the identification data acquisition and verification phases. The verdict is "successful" if the remote identity verification service concludes firstly that the identity document presented by the user is authentic, and secondly that the user is the legitimate holder of the identity document, otherwise the verdict is "unsuccessful".

Security component – electronic component of an identity document, used as a secure storage medium for civil status data and the photograph of the legitimate holder of the document. Access to the information contained in the security component of an identity document may be subject to restrictions under national law of States.

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

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

Service provider – legal entity that provides a remote identity verification service.

State of the art – all publicly available best practices, technologies and reference materials relating to information systems security or identity verification, and the information that is evidently derived from them. These documents may be posted on the Internet by the information systems security community, disseminated by reference organisations or be of legislative, regulatory or normative origin.

Statement of remote identity verification practices – set of practices (organisation, operational procedures, technical and human resources, etc.) that the remote identity verification service provider applies in the context of the provision of its service and in accordance with the remote identity verification policy that it has undertaken to respect. The statement of remote identity verification practices is confidential and is made available only to those with a need to know.

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

Synchronous remote identity verification service – a remote identity verification service is said to be synchronous when it does not meet the criteria of an asynchronous remote identity verification service.

Synchronous remote identity verification service with human interaction – a remote identity verification service is said to be synchronous with human interaction when it is synchronous and allows interactions between the user and the operator during the identification data acquisition or verification phase. A synchronous remote identity verification service with human interaction may, for example, allow an operator to guide the user through the acquisition of the identification data.

Synchronous remote identity verification service without human interaction – a remote identity verification service is said to be synchronous without human interaction when it is synchronous and does not allow any interaction between the user and the operator during the identification data acquisition and verification phases. However, the service can implement automated interactions with the user.

Terminal – hardware (mobile phone, tablet, computer, etc.) used to acquire user identification data. The terminal can be the user's, the service provider's or the client's. The acquisition of the user's identification data through the terminal can be carried out using any type of app: dedicated mobile app, browser, etc.

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

II. General description of the remote identity verification service

II.1. Activities of the remote identity verification service

The remote identity verification service performs the following four steps in succession:

- acquisition of the identification data, described in chapter II.1.1;
- verification of the identification data, described in chapter II.1.2;
- creation of the evidence file, described in chapter II.1.3;
- sending of the result of the remote identity check, described in chapter II.1.4.

The diagram below presents a simplified functional view of a remote identity verification service (asynchronous in this example) and illustrates the four successive steps of the remote identity verification service.

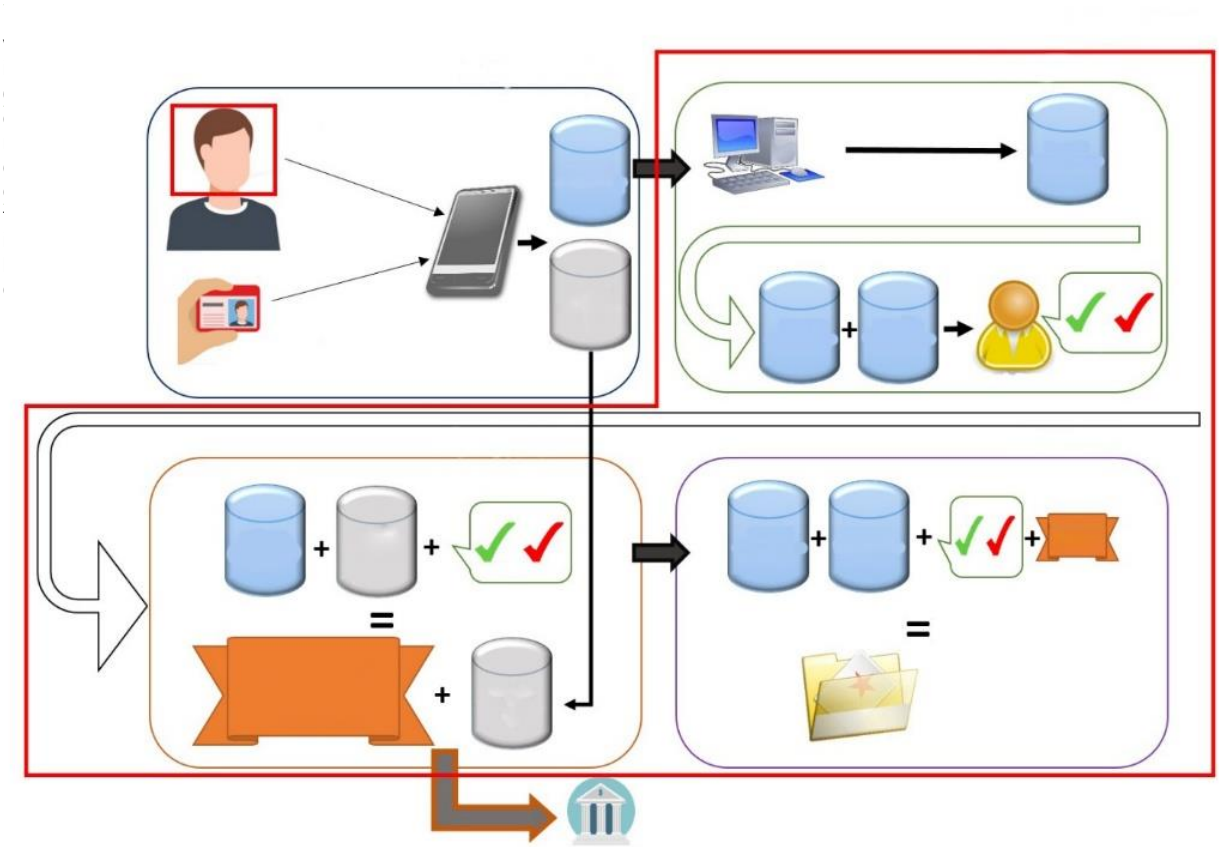

Figure 1: Simplified functional view of a remote identity verification service

II.1.1. Acquisition of the identification data

This step involves acquiring the identification data relating to the user, namely:

- a video of the user's face;
- [when the authenticity of the identity document is not cryptographically verified using the security component] a video of the identity document presented by the user;

- [when the authenticity of the identity document is cryptographically verified using the security component] the user's identification data (including the photograph of the user's face) stored in the security component of the identity document presented by the user.

The acquisition of the different identification data can be carried out simultaneously or successively, in any order. Thus, the acquisition of the videos of the user's face and the identity document presented by the user can be done in two different ways:

- acquisition of a single video in which the user presents their face and identity document;
- acquisition of two separate videos: a video of the user's identity document and a video of the user's face. The video of the identity document can be acquired first, followed by the video of the user's face, or vice versa.

The terminal used to acquire the identification data may be the user's, the service provider's or the client's.

The remote identity verification service protects the confidentiality and integrity of the user's identification data as it passes between the terminal and the remote identity verification service.

II.1.2. Verification of the identification data

On the basis of the identification data acquired in the previous step, this step involves verifying, using both automated and human processing, that the identity document presented by the user is authentic and that the user is the legitimate holder of the identity document.

The verification that the user is the legitimate holder of the identity document includes:

- verification of the authenticity of the identity document presented;
- detection of the "liveness" of the user shown in the video;
- a comparison of the user's face from the user's video with:
    - [when the authenticity of the identity document is not cryptographically verified using the security component] a photograph of the user's face extracted from the video of the identity document;
    - [when the authenticity of the identity document is cryptographically verified using the security component] the photograph of the user taken from the security component of the identity document.

These verifications give rise to intermediate findings and may be carried out simultaneously or successively, in any order.

II.1.3. Production of the evidence file

This step involves creating an evidence file comprising the acquired identification data, the intermediate findings from the automated and human processing of the identification data verification and the result of the identity verification sent to the business service.

The remote identity verification service protects the confidentiality and integrity of the evidence file.

II.1.4. Sending of the result of the identity verification

This step involves sending the business service the result of the identity verification process, including the verdict (successful or unsuccessful), the reason for the failure if applicable, the identity attributes relating to the user verified by the service provider, and any additional data requested by the business service that is not covered by this rule set.

Any additional data must be collected and sent in accordance with the applicable regulations.

The remote identity verification service protects the confidentiality and integrity of the user's identity verification result as it travels between the remote identity verification service and the business service.

III. Evaluation of remote identity verification service providers

III.1. Evaluation methods

The rule set contains requirements and recommendations for remote identity verification service providers.

The requirements must be met by the service provider in order for the service to be certified as compliant with this rule set.

The recommendations are given as good practices and are not subject to evaluation.

Unless otherwise specified, the requirements and recommendations are the same for remote identity verification systems, whether asynchronous, synchronous with human interaction, synchronous without human interaction, internal or external, implemented as part of a trust service, an electronic means of identification or a remote business contact service, regardless of whether the terminal used for the acquisition of the identification data is that of the user, that of the service provider or that of the client.

The requirements are applicable regardless of the assurance level sought, with the following exceptions:

- the requirements and recommendations identified by the prefix [SUBSTANTIAL] are only applicable for the assurance level substantial;
- the requirements and recommendations identified by the prefix [HIGH] are only applicable for the assurance level high.

If the service provider subcontracts part of the activities of the remote identity verification service, then the subcontractors implementing all or part of the human, technical and organisational means necessary to comply with the requirements of this rule set must be assessed to verify that they comply with the requirements incumbent upon them.

The rule set also makes recommendations to clients in Annex 3. These recommendations are not subject to evaluation.

III.2. Applicable regulatory frameworks

This rule set is applicable within the framework of:

- **the certification under [DECREE_2020-118] of remote business contact services** implemented by organisations subject to the fight against money laundering and terrorist funding. In this case, certification is granted by ANSSI, in accordance with the process [PROCESS_CERTIF_SERVICE], for a maximum period of two years.
- **the qualification of trust services under the [EIDAS] regulation when they use remote identity verification.** In this case, qualification is granted by ANSSI, in accordance with the [PROCESS_QUALIF_SERVICE] process, for a maximum period of two years. The use of a remote identity verification service certified under [DECREE_2020-118] provides a presumption of compliance with the remote identity verification requirements for a given assurance level.
- **the assessment of the compliance of electronic means of identification under the [EIDAS] regulation and their certification under Article L.102 of [CPCE], for the assurance levels substantial and high, when they use remote identity verification**. In this case, certification is granted by ANSSI for a maximum period of two years. The use of a remote identity verification service certified under [DECREE_2020-118] provides a presumption of compliance with the remote identity verification requirements for a given assurance level.

The same remote identity verification service can be used in different regulatory settings.

IV. Requirements to be met by the service provider

IV.1. General requirements

a) The service provider must be a legal entity or part of a legal entity.

b) The service provider must be responsible for the activities carried out on behalf of the client in the course of the provision of the service and in particular for any damage caused to the client. As such, the service provider must specify the types of damage involved and the liability sharing arrangements in the service agreement, taking into account any subcontracted activities.

c) The service provider must take out professional insurance covering any damage caused to the client and in particular to their information system in the course of the provision of the service.

d) The service provider must develop and maintain a termination plan to ensure that the relevant information remains accessible, for an appropriate period of time, for the purposes of providing legal evidence and business continuity.

e) The service provider must ensure that the information provided, including advertising, is not false or misleading.

f) The service provider must provide sufficient evidence that the way it operates, particularly financially, is not likely to compromise its impartiality and the quality of its service to the client or to give rise to conflicts of interest.

g) The service provider must provide the service impartially, in good faith and with respect for the users, the client, its staff and its infrastructure.

h) The service provider must have valid licenses for the tools (software or hardware) used to provide the service.

i) The service provider must ask the client to inform them of any specific legal and regulatory requirements to which they are subject, particularly those relating to their sector of activity.

j) The service provider must draw up a service agreement with the client which meets the requirements of chapter IV.7.2 of this rule set and which is formally approved in writing by the client before the service is provided.

IV.2. Risk assessment and management

IV.2.1. Common provisions for risk assessments

a) The service provider must produce, in accordance with the [ISO27005] approach:

- an assessment of the risks relating to identity theft[3];
- an assessment of the risks relating to information systems security[4].

It is recommended that the [EBIOS_RM] method be used to produce risk assessments.

b) The service provider must review the risk assessments identified in requirement IV.2.1.a) at least once a year, as well as in accordance with the conditions specified in chapters IV.2.2 and IV.2.3.

c) The service provider must, in the risk assessments identified in requirement IV.2.1.a), consider the following attacker profiles: any malicious person, group of persons or organisation, internal or external.

[3] The specific requirements for this risk assessment are set out in chapter IV.2.2.

[4] The specific requirements for this risk assessment are set out in chapter IV.2.3.

d) **[SUBSTANTIAL]** For the assurance level substantial, the service provider must, in the risk assessments identified in requirement IV.2.1.a), consider attackers with a moderate attack potential.

e) **[HIGH]** For the assurance level high, the service provider must, in the risk assessments identified in requirement IV.2.1.a), consider attackers with a high attack potential.

f) The provider must, in the risk assessments identified in requirement IV.2.1.a), identify all residual risks.

g) The service provider must have the risk assessments identified in requirement IV.2.1.a) formally validated in writing by their management, as well as all residual risks associated with each risk assessment.

h) The service provider must ensure the confidentiality of the risk assessments identified in requirement IV.2.1.a).

IV.2.2. Assessment of the risks relating to identity theft

a) In this risk assessment, the service provider must at least explicitly identify the following feared event: identity theft.

b) In defining the scope of the risk assessment, the service provider must explicitly identify the main functions described in chapter II.1, namely:

- acquisition of the identification data,
- verification of the identification data,
- production of the evidence file,
- sending of the result of the remote identity check.

c) It is recommended that the service provider use standard [ISO30107-3] as a guide to identify risk scenarios for biometric presentation attacks.

d) In the risk assessment, the service provider must identify risk scenarios relating to counterfeiting and falsification of identity documents by physical means, including at least the following:

- use of a counterfeit identity document to create a false identity;
- use of a counterfeit identity document to steal the identity of an existing person;
- use of a falsified identity document to create a false identity;
- use of a falsified identity document to steal the identity of an existing person;

e) The service provider must, in the risk assessment, identify risk scenarios relating to counterfeiting and falsification of identity documents by digital means, including at least the following:

- [when the authenticity of the identity document is not cryptographically verified using the security component] presentation of a "virtual" document (for example modelling of an image to be transposed onto the video of the identity document) to create a false identity;
- [when the authenticity of the identity document is not cryptographically verified using the security component] injection of fraudulent data (photograph, identity data, etc.) in place of the data present on the identity document to create a false identity;
- [when the authenticity of the identity document is cryptographically verified using the security component] compromise of cryptographic secrets or exploitation of a vulnerability in the cryptographic protocol to modify the identification data extracted from the identity document.

f) In the risk assessment, the service provider must identify risk scenarios relating to the alteration of the user's appearance by physical means, including at least the following:

- use of a "physical" mask (e.g. latex) that resembles an existing person to steal their identity;
- use of make-up to make oneself look like an existing person to steal their identity;

g) In the risk assessment, the service provider must identify risk scenarios relating to the alteration of the user's appearance by digital means, including at least the following:

- use of a "virtual" mask (e.g. modelling a virtual mask from videos or photographs) that resembles an existing person to steal their identity;
- injection of fraudulent photographs or videos of an existing person's face to replace data captured during the acquisition phase to steal their identity.

h) In the risk assessment, the service provider must identify risk scenarios relating to the user's resemblance to an existing person in order to steal that person's identity (lookalike, twin, etc.).

i) In the risk assessment, the service provider must identify risk scenarios relating to the influence on user behaviour, including at least the following:

- generation of a constraint on the user forcing them to identify themselves remotely (e.g. physical threat, blackmail, etc.);
- entrapment of the user by inviting them to identify themselves remotely to a service other than the one they think they are accessing, in order to collect their identification data.

j) The service provider must revise the risk assessment whenever the remote identity verification policy or statement of verification practices is changed, and in the light of developments in the state of the art and the threat assessment.

IV.2.3. Assessment of the risks relating to information systems security

a) In this risk assessment, the service provider must explicitly identify at least the following feared events:

- personal data leak;
- leak of sensitive information relating to fraud detection processes.

It is recommended that the service provider identify in its risk assessment the feared events relating to deterioration of the user experience and system downtime.

b) The service provider must review the risk assessment in the event of any structural changes to the information system of the remote identity verification service, including changes to its hosting, infrastructure or architecture or changes to the identity verification policy.

IV.2.4. Risk management plan

a) The service provider must develop a risk management plan covering the entire scope of the electronic identity verification service and associated with all the risk assessments identified in requirement IV.2.1.a).

b) **[SUBSTANTIAL]** For the assurance level substantial, the application of the risk management plan must ensure that the service can withstand attackers with a moderate attack potential.

c) **[HIGH]** For the assurance level high, the application of the risk management plan must ensure that the service can withstand attackers with a high attack potential.

d) The service provider must have the risk management plan formally validated in writing by their management.

e) The service provider must periodically monitor the implementation of the risk management plan and notify their management of any significant deviation.

f) The service provider must revise the risk management plan at least once a year, and if there is a change in any of the risk assessments identified in requirement IV.2.1.a).

g) The service provider must ensure the confidentiality of the risk management plan.

IV.2.5. Plan for testing the effective ability of the service to detect attempted identity theft

a) The service provider must develop and maintain a plan to test the effective ability of the service to detect attempted identity theft

- For the authenticity of the identity document:
  - [When the authenticity of the identity document is not cryptographically verified using the security component] test the effectiveness of the measures applied under the risk management plan to reduce the risks relating to counterfeiting and falsification of identity documents by physical or digital means identified in the assessment of risks relating to identity theft;
  - [When the authenticity of the identity document is not cryptographically verified using the security component] measure the false rejection (FRR) and false acceptance (FAR) rates actually achieved by the service in the context of detecting risks relating to the counterfeiting and falsification of identity documents by physical or digital means identified in the assessment of risks relating to identity theft.
- For the liveness detection:
  - test the effectiveness of the measures applied under the risk management plan to reduce the risks relating to the alteration of the user's appearance by physical or digital means identified in the assessment of risks relating to identity theft;
  - measure the false rejection (FRR) and false acceptance (FAR) rates actually achieved by the service in detecting risks relating to the alteration of the user's appearance by physical or digital means identified in the assessment of risks relating to identity theft.
- For the comparison of the user's face:
  - test the effectiveness of the measures applied under the risk management plan to reduce the risks relating to the user's natural resemblance to another person (lookalike, twin, etc.);
  - measure the false rejection (FRR) and false acceptance (FAR) rates actually achieved by the service in comparing the user's face with the photograph in the identity document.
- For risks relating to influencing user behaviour:
  - test the effectiveness of the measures applied under the risk management plan to reduce the risks relating to influencing user behaviour identified in the assessment of risks on identity theft.

b) The test plan must be validated by the Identity document and Biometrics fraud officers for the aspects concerning each of them.

c) The service provider must execute the test plan annually and whenever there is a structural change to the service, an update of the risk assessments or the risk management plan.

d) The service provider must record the results of each execution of the test plan in a report and have this report validated by the Identity document and Biometrics fraud officers for the aspects concerning each of them.

e) It is recommended that tests relating to alteration of the user's appearance be developed in accordance with standard [ISO30107-3].

f) If the rates measured during the execution of the test plan are lower than the rates defined in the remote identity verification policy, the service provider must immediately inform the Identity document and Biometrics fraud officers for the aspects concerning each of them.

g) If the rates measured during the execution of the test plan are lower than the rates defined in the remote identity verification policy, the service provider must consider this situation as a breach and, as such,

in accordance with [PROCESS_CERTIF_SERVICE] and [PROCESS_QUALIF_SERVICE], immediately inform ANSSI.

h) The service provider must ensure the confidentiality of the test plan and the associated results.

IV.3. Remote identity verification policy and practices

a) The service provider must develop and maintain a remote identity verification policy[5].

b) The remote identity verification policy must be uniquely identified by an OID, and each major update to the policy must have a separate OID.

c) The service provider must ensure that users and clients have easy, direct and permanent access to the remote identity verification policy.

d) The service provider must develop and maintain a statement of remote identity verification practices, referencing the OID of the remote identity verification policy to which it relates[6].

e) The statement of remote identity verification practices is confidential and should only be made available to those with a need to know.

IV.3.1. General

a) The remote identity verification policy must identify the attributes of the identity document that characterise the uniqueness of a natural person's identity.

b) The remote identity verification policy must identify whether the remote identity verification service is "asynchronous", "synchronous with interaction" or "synchronous without interaction".

c) The statement of remote identity verification practices must identify all reasons for remote identity verification failure that can be communicated to the user and the business service. These reasons must not include information on the verifications carried out and the type of fraud suspected, if any.

d) The remote identity verification policy must specify whether additional data is required by the business service and, if so, what that data is.

e) The remote identity verification policy must state that additional data must not be included in the calculation of the remote identity verification verdict.

IV.3.1.1. Fraud

a) The remote identity verification policy must define indicators for detecting identity theft attempts relating to the risk scenarios identified in the assessment of the risks relating to identity theft.

b) The statement of remote identity verification practices must describe the technical and organisational means implemented by the service provider to measure indicators for detecting attempted identity theft (requirement IV.3.1.1.a).

c) The remote identity verification policy must state that for each suspected or proven identity theft, whether detected by the service provider (requirement IV.3.1.1.b) or reported by the business service, an alert is generated.

d) The statement of remote identity verification practices must identify procedures for handling alerts generated when identity theft is suspected or proven (requirement IV.3.1.1.c). These procedures must allow the Identity document fraud officer to be informed systematically when the suspected or proven

[5] The information to be included in the remote identity verification policy is identified in chapters IV.3.1 to IV.3.5.

[6] The information to be included in the statement of remote identity verification practices is identified in chapters IV.3.1 to IV.3.5.

identity fraud concerns the identity document, and the Biometrics fraud officer to be informed systematically when the suspected or proven identity fraud concerns the biometrics.

e) The statement of remote identity verification practices must specify the measures implemented by the service provider to notify the user of the nature of the operation in progress, and to prevent the risk of entrapment of the user.

f) The remote identity verification policy must specify the remedies available to users of the service, including for the purpose of cancelling fraudulent identification or refusing to identify a bona fide user.

IV.3.1.2. Personal data

a) The remote identity verification policy must describe the alternatives to remote identity verification available to users when needed.

b) The remote identity verification policy must specify that the service provider respects the principle of minimisation of data collected and preserved.

c) The remote identity verification policy must identify all personal data relating to users processed by the remote identity verification service.

d) The remote identity verification policy must identify which of the user's personal data processed by the service may be subject to biometric processing.

e) The remote identity verification policy must identify, for each personal data item relating to users processed by the remote identity verification service: the preservation period based on the "successful" or "unsuccessful" verdict, the methods of preservation, destruction, access and rectification offered to users, as well as the processing carried out by the service provider on this data. The preservation period must be proportionate to the purpose. With regard to the principle of accountability, it is important for the controller to define a preservation period.

f) The identity verification policy must specify that the preservation period of data for which biometric processing is intended must not exceed ninety-six hours.

g) The remote identity verification policy must specify the purpose(s) for which the personal data of users processed by the verification service is preserved.

h) It is recommended that the controller use the guide [CNIL_Guide_conservation] to define the preservation periods and methods.

i) The remote identity verification policy must prohibit the correction or deletion by the user of the evidence file and the results of the remote identity verification sent to the business service, as well as all information necessary to establish the result.

j) The remote identity verification policy must prohibit user access to data that has been subject to automated or manual processing, the disclosure of which may provide information on the nature of the verifications carried out by the service and relating to the detection of identity theft.

IV.3.1.3. Languages

a) The remote identity verification policy must identify all languages supported by the remote identity verification service.

b) The remote identity verification policy must indicate that the service supports at least the French language.

c) The remote identity verification policy must state that the service, prior to acquiring identification data, must ask the user for the language that they wish to use, when the service supports one or more languages other than French.

d) The remote identity verification policy must state that the service must inform the user of the country in which the operators responsible for carrying out the verifications and delivering the remote identity verification verdict are located.

IV.3.1.4. Registration and handling of complaints

a) The remote identity verification policy must state that the service provider must make available to the client, users and third parties a process for registering and handling complaints relating to the remote identity verification service.

b) The remote identity verification policy must describe the process for registering and handling complaints.

IV.3.2. Acquisition

IV.3.2.1. Terminal

a) The remote identity verification policy must identify whether the acquisition of user identification data is carried out by the user's terminal or a service provider or business service terminal.

b) The remote identity verification policy must, when the acquisition of user identification data is carried out by the user's terminal, specify whether the installation of an app on the user's terminal is required.

IV.3.2.2. Identity documents

a) The remote identity verification policy must indicate that it can only be updated on matters relating to identity documents after formal validation by the Identity document fraud officer.

b) The remote identity verification policy must identify the demands that can be made by the service to the user for correct acquisition of the identity document (brightness, focus, glare, etc.).

c) The statement of remote identity verification practices must describe the mechanisms implemented to ensure that the acquisition of the identity document video is not predictable, and cannot therefore be reused by an attacker.

IV.3.2.3. Face

a) The remote identity verification policy must indicate that it can only be updated on matters relating to biometrics after formal validation by the Biometrics fraud officer.

b) The remote identity verification policy must describe the requests that may be made by the service to the user in the acquisition and verification of identification data (e.g. brightness, focus, removal of user's glasses, etc.).

c) The statement of remote identity verification practices must describe the mechanisms implemented to ensure that the acquisition of the face video is not predictable and cannot therefore be reused by an attacker.

IV.3.3. Verification

IV.3.3.1. Terminal

a) The remote identity verification policy must specify that, when the terminal is the user's own, no check performed on the user's terminal can contribute to the "successful" verdict of the remote identity verification.

b) The remote identity verification policy must, when the terminal is that of the service provider or business service, specify whether processing, even partial, relating to the verification of the authenticity of the identity document, the matching of the user's face with the photograph extracted from the identity

document or the verification of proof of liveness is carried out on the terminal. Where applicable, the statement of remote identity verification practices must specify such processing.

IV.3.3.2. Identity documents

a) The remote identity verification policy must identify the identity documents accepted by the remote identity verification service. These identity documents must be included in the list provided in Annex 4.

b) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must identify, for each accepted identity document, the security features verified by the service. In particular, the service provider can make use of the public register of authentic travel and identity documents online (PRADO[7]) to identify the security features associated with each identity document.

c) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must, for each verified security feature of the accepted identity documents, describe all the verifications performed, specify for each verification whether it is performed automatically or by a human operator, and whether it is performed systematically or only under certain conditions. Where appropriate, these conditions are described.

d) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must identify, for each accepted identity document, the security features of the identity document that are not verified by the service provider and that are listed in the public register of authentic travel and identity documents online (PRADO[7]) and, for each security feature that is not verified by the service, provide a justification.

e) The remote identity verification policy must state that the service provider must develop and maintain a list identifying at least one competent identity document fraud officer for each accepted identity document.

f) The remote identity verification policy must indicate that only unexpired identity documents are accepted by the service.

g) The declaration of remote identity verification practices must identify, for each accepted identity document, whether verification of the validity[8] of the identity document via a service provided by the issuing State is carried out, and if so:

- identify the validity verification service;
- specify whether this validity verification is carried out automatically or by a human operator;
- specify whether this validity verification is carried out systematically or only under certain conditions, and if applicable, describe these conditions;
- specify the consequences if the validity verification service is unavailable.

h) The remote identity verification policy must state that the service provider must systematically verify that the identity document is valid whenever such a service is made available to the service provider by the State responsible for issuing the identity document.

[7] See acronym in chapter I.3.1.

[8] Confirmation of validity assumes at least that the document is known to exist, has not expired, and has not been reported lost or stolen or been invalidated for any other reason. Depending on the service, it may indicate only whether the document is valid or invalid, or it may indicate reasons for invalidity (reported lost, reported stolen). The information on validity is sufficient to meet the requirements of the rules set.

i) The remote identity verification policy must state that if a validity verification of the identity document is carried out and the validity verification concludes that the identity document is invalid, then the verdict of the remote identity verification is always "unsuccessful".

j) The statement of remote identity verification practices must specify whether special security measures are applied for certain types of users to strengthen controls to prevent identity theft, and if applicable, what those measures are.

k) The statement of remote identity verification practices must specify what measures, if any, have been implemented to limit recurring attack attempts.

l) [When the authenticity of the identity document is not cryptographically verified using the security component] the remote identity verification policy must describe how physically altered identity documents (torn or tattered identity documents, etc.) are verified.

m) [When the authenticity of the credential is not cryptographically verified using the security component] the remote identity verification policy must state the minimum post-compression resolution of the identity document video accepted by the service. This minimum resolution cannot be lower than 720p: 1280 × 720 at 25 frames per second.

n) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must describe the controls[9] performed by the remote identity verification service on the quality of the acquired video of the identity document. These controls include as a minimum the resolution identified in requirement IV.3.3.2.m) and may be supplemented by other controls: brightness of the environment, etc.

o) [When the authenticity of the identity document is cryptographically verified using the security component] the remote identity verification policy must state that the verdict given by the service is automatically "unsuccessful", without operator intervention, if the automated processes for verifying the authenticity of the identity document conclude that the document is not authentic.

p) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must indicate the false rejection (FRR) and false acceptance (FAR) rates accepted by the service for the verification of the authenticity of the identity document.

q) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must specify the procedures applied when an operator announces a "successful" verdict whereas the results of the automated processing relating to the authenticity of the identity document give an "unsuccessful" verdict. These procedures must include, as a minimum, an alert to the Identity document fraud officer.

r) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must specify the procedures applied when an operator announces an "unsuccessful" verdict whereas the results of the automated processing relating to the authenticity of the identity document give a "successful" verdict. These procedures must include at least a record of the event for analysis purposes.

s) **[HIGH]** The remote identity verification policy must state that the authenticity of the identity document is cryptographically verified using the security component of the identity document. If it is technically or legally impossible to use the security component of the identity document, or if the identity document has no security component, the identity document cannot be accepted.

t) **[HIGH]** The remote identity verification policy must state that, for each accepted identity document, the validity of the identity document is systematically verified using a service provided by the State issuing the identity document. If this service does not exist or is unavailable, the identity document cannot be accepted.

[9] These controls are to be dissociated from any controls carried out on the terminal.

IV.3.3.3. Facial comparison

a) The remote identity verification policy must specify the minimum resolution after compression accepted by the service for the video of the user's face. This resolution cannot be lower than 720p: 1280 × 720 at 25 frames per second.

b) The statement of remote identity verification practices must describe the controls carried out[10] by the remote identity verification service on the quality of the acquired video of the user's face. These controls include as a minimum the resolution identified in requirement IV.3.3.3.a) and may be supplemented by other controls: brightness of the environment, etc.

c) The statement of remote identity verification practices must describe all the verifications carried out in the context of the comparison between the user's face and the photograph of the identity document, and specify for each verification whether it is carried out automatically or by a human operator, and whether it is carried out systematically or only under certain conditions. Where applicable, these conditions are described in the statement of remote identity verification practices.

d) The statement of remote identity verification practices must specify the procedures applied when an operator announces a "successful" verdict whereas the results of the automated processing relating to the comparison of the user's face give an "unsuccessful" verdict. These procedures must include at least one alert to the Biometrics fraud officer.

e) The statement of remote identity verification practices must specify the procedures applied when an operator announces an "unsuccessful" verdict whereas the results of the automated processing relating to the comparison of the user's face give a "successful" verdict. These procedures must include at least a record of the event for analysis purposes.

f) The statement of remote identity verification practices must indicate the false rejection (FRR) and false acceptance (FAR) rates accepted by the service for the comparison of the user's face.

g) [When the authenticity of the identity document is cryptographically verified using the security component] the remote identity verification policy must state that the photograph used to perform the facial comparison is the one extracted from the security component.

IV.3.3.4. Liveness detection

a) The statement of remote identity verification practices must describe all the verifications carried out in the context of liveness detection and specify for each verification whether it is carried out automatically or by a human operator. Where appropriate, these conditions are described.

b) The statement of remote identity verification practices must specify the procedures applied when an operator gives a "successful" verdict whereas the results of the automated processing relating to liveness detection give an "unsuccessful" verdict. These procedures must include at least one alert to the Biometrics fraud officer.

c) The statement of remote identity verification practices must specify the procedures applied when an operator announces an "unsuccessful" verdict whereas the results of the automated processing relating to liveness detection give a "successful" verdict. These procedures must include at least a record of the event for analysis purposes.

d) The statement of remote identity verification practices must indicate the false rejection (FRR) and false acceptance (FAR) rates accepted by the service for the liveness detection.

IV.3.4. Production of the evidence file

a) The remote identity verification policy must state that an evidence file must be created for each identity verification regardless of the verdict ("successful" or "unsuccessful").

[10] These controls are to be dissociated from any controls carried out on the terminal.

b) The remote identity verification policy must identify the components of the evidence file. These elements must provide all the information necessary for the resolution of disputes.

c) The remote identity verification policy must indicate that the evidence file contains at least the following elements:
   - identification data:
     - [when the authenticity of the identity document is not cryptographically verified using the security component] the video of the identity document
     - [when the authenticity of the identity document is cryptographically verified using the security component] the photograph of the user extracted from the security component of the identity document
     - the video of the user's face
   - the date of acquisition of each identification data
   - a list of all verifications carried out on the identification data, and for each verification:
     - the date of the verification
     - the activity associated with the audit, in particular:
       - verification of the authenticity of the identity document
       - detection of the "liveness" of the user
       - comparison of the user's face
     - the nature of the verification: automatic or manual
     - the identity of the operator or the fraud officer who carried out the verification if carried out manually
     - the country from which the operator or the fraud officer carried out the verification if carried out manually
     - the version and configuration, if any, of the tools that carried out the verification if carried out automatically
     - the intermediate finding returned by the automated processing, the operator or the fraud officer following the verification
   - the verdict of the remote identity check (successful or unsuccessful)
   - the reasons given by the operator in the event of an "unsuccessful" verdict
   - the identity of the operator who delivered the verdict
   - the date on which the verdict was delivered by the operator
   - the country from which the operator delivered the verdict
   - the full name of the user
   - the date and place of birth of the user
   - the unique number of the identity document
   - the date of issue of the identity document
   - the expiry date of the identity document
   - the result of the remote identity verification sent to the business service.

d) The remote identity verification policy must state that the evidence file does not contain any data for biometric processing.

e) The conservation period of evidence files must take into account the period during which litigation may occur.

f) The remote identity verification policy must state that the service provider encrypts evidence files as soon as they are created, and whether the decryption key is implemented in secure cryptographic equipment.

g) The remote identity verification policy must specify that encrypted evidence files are kept offline if the decryption key is not implemented in secure cryptographic equipment.

h) The remote identity verification policy must specify the management methods for the decryption key of the evidence file and in particular allow access to this key only to those who have a need to know.

i) The remote identity verification policy must state that users can exercise their right to access their personal data held by the service provider in the evidence file, but cannot exercise the right to rectification of that file.

j) The statement of remote identity verification practices must indicate whether the video of the user's face is lossy compressed when stored in the evidence file. Where applicable, information on the lossy compression method is described.

k) [When the authenticity of the identity document is not cryptographically verified using the security component] the statement of remote identity verification practices must indicate whether the video of the identity document is lossy compressed when stored in the evidence file. Where applicable, information on the lossy compression method is described.

IV.3.5. Sending of the result

a) The remote identity verification policy must state that the result of the remote identity verification is sent to the business service systematically, regardless of the verdict (successful or unsuccessful).

b) The remote identity verification policy must indicate that the result of the remote identity verification consists only of the verdict (successful or unsuccessful) of the verification and the identity attributes of the user (e.g.: surname(s), first name(s), gender, date of birth, place of birth, identity document number, a photograph of the user's face taken from the video of the user's face, a photograph of the identity document taken from the video of the user's identity document, etc.), as well as any additional data requested by the business service.

c) The remote identity verification policy must identify the identity attributes relating to users contained in the identity verification result.

d) The remote identity verification policy must state that the videos of the user's identity document and face are not sent to the business service in any way, either in full or in part[11].

e) The remote identity verification policy must specify the maximum delay between the start of the acquisition of the user identification data and the notification of the result of the identity verification to the business service. This delay may not exceed ninety-six hours.

f) The remote identity verification policy must state that the result of the remote identity verification shall contain no elements relating to the findings of the verifications carried out by the service other than the verdict indicated in requirement IV.3.5.b), and in particular no score calculated on the basis of those verifications.

IV.4. Activities of the remote identity verification service

IV.4.1. Acquisition of the identification data

IV.4.1.1. Acquisition of the identity document

a) The service provider must acquire a video of the identity document in accordance with the remote identity verification policy and the statement of remote identity verification practices.

IV.4.1.2. Face acquisition

a) The service provider shall acquire a video of the user's face in accordance with the remote identity verification policy and the statement of remote identity verification practices.

[11] A photograph of the user's face taken from the video of the user's face and a photograph of the identity document taken from the video of the identity document may nevertheless be part of the result of the remote identity verification, as required by IV.3.5.b)

IV.4.2. Verifying the identification data

IV.4.2.1. Verification of the authenticity of the identity document

a) The service provider shall verify the authenticity of the document in accordance with the remote identity verification policy and the statement of remote identity verification practices.

IV.4.2.2. Facial correspondence verification

a) The service provider must verify that the user's face matches the photograph taken from the identity document in accordance with the remote identity verification policy and the statement of remote identity verification practices.

IV.4.2.3. Liveness detection

a) The service provider must detect the "liveness" of the user in accordance with the remote identity verification policy and the statement of remote identity verification practices.

IV.4.3. Production of the evidence file

a) The service provider must generate evidence in accordance with the remote identity verification policy and the statement of remote identity verification practices.

IV.4.4. Sending of results

a) The service provider must, for each identity verified, generate a result in accordance with the remote identity verification policy and the statement of remote identity verification practices.

b) The service provider must send the result to the business service in accordance with the information systems security policy.

IV.5. Protection of information

IV.5.1. Terminal

a) The service provider must protect the confidentiality and integrity of the identification data exchanged between the terminal, whether it be the user's terminal, the service provider's terminal or the business service's terminal, and the remote identity verification service.

b) The service provider must authenticate the terminal if it is its responsibility or that of the business service (authentication by certificate, for example).

c) If the service requires the installation of a specific app[12] on the user's terminal, the service provider must implement measures to ensure that this app does not reduce the level of security of the terminal. The qualification of this app to the basic level [PROCESS_QUALIF_PRODUCT] is a means of certifying compliance with this requirement.

It is recommended that, if the service requires the installation of a specific app on the user's terminal, mechanisms should be available to limit the risk of alteration or substitution of that app.

d) **[HIGH]** If the service requires the installation of a specific app on the user's terminal, the service provider must have the app qualified to the basic level [PROCESS_QUALIF_PRODUCT] to ensure that it does not reduce the security level of the terminal.

[12] A "specific" app is considered to be one that is not related to the business service but installation of which is required by the service provider to enable remote identity verification. An app provided by the business service that includes an interface to the service provider's service in addition to its native functions is not considered to be a specific app.

e) If the service requires the installation of a specific app on the user's terminal, the service provider must make this app available to users on official app stores.

f) If the service requires the installation of a specific app on the user's terminal and this app is made available to users on official app stores, the service provider must monitor official app stores to detect the availability of fraudulent apps intended to replace the legitimate app of the service.

IV.5.2. Information systems security policy

a) The service provider must define and implement an information systems security policy based on the information systems security risk assessment identified in chapter IV.2.3 and the associated risk management plan.

b) The service provider must review the information systems security policy at least every two years, and in the event of a change in the risk assessment or risk management plan.

c) The service provider must have the information systems security policy formally validated in writing by its management.

IV.5.3. Accreditation

a) The service provider must accredit the information system of the remote identity verification service.

> It is recommended that the service provider use the approach described in the [ACCREDITATION] guide to accredit the information system of the remote identity verification service.
>
> It is recommended that the service provider use an information systems security audit service qualified under decree [DECREE_2015-350] as part of the accreditation process.

b) **[HIGH]** The service provider must comply with the rules relating to the protection measures for information systems handling sensitive information [II_901].

c) **[HIGH]** The service provider must use an information systems security audit service qualified under [DECREE_2015-350] as part of the accreditation process. The audit plan drawn up by PASSI must include at least the following audit activities: organisational and physical audit, configuration audit, architecture audit and penetration testing.

d) The service provider must have the accreditation decision formally validated in writing by their management.

IV.5.4. Territoriality of the service

a) The service provider must store and process the data relating to the remote identity verification service exclusively within the territory of a Member State of the European Union.

b) The service provider must operate and administer the remote identity verification service exclusively from the territory of a Member State of the European Union.

IV.5.5. Security level

a) [When the authenticity of the identity document is cryptographically verified using the security component], the service provider must protect the integrity and, where appropriate, the confidentiality of all data used to authenticate the cryptographic calculations carried out by the security component of the identity document.

b) The service provider must restrict operator access to the information system of the remote identity verification service to that which is strictly necessary for the completion of their tasks.

c) The service provider must comply with the requirements of the [SecNumCloud] rule set if the service is hosted as part of a cloud computing service. The [SecNumCloud] qualification meets this requirement.

d) **[SUBSTANTIAL]** The service provider must apply all the rules of the standard level of the ANSSI cyber hygiene guide [HYGIENE] to the information system of the remote identity verification service.

It is recommended that the service provider apply all the rules of the enhanced level of the ANSSI cyber hygiene guide [HYGIENE] to the information system of the remote identity verification service. It is recommended that for each enhanced level rule, the service provider identify whether or not it is compliant with the rule, and that for each enhanced level rule it claims to be compliant with, describe the measures in place to comply with the rule, and that for each enhanced level rule it claims not to be compliant with, provide justification.

e) **[HIGH]** The service provider must process and store sensitive information (which may affect the result of the verification, infringe the privacy of users or affect the ability of the service to provide evidence in the event of a dispute) on a class 1 network in accordance with annex 2 of the interministerial instruction on the protection of sensitive information systems [II_901].

f) **[HIGH]** The service provider must apply all rules of the enhanced level of the ANSSI cyber hygiene guide [HYGIENE] to the information system of the remote identity verification service.

g) **[HIGH]** For each [ADMIN_SEC] recommendation, the service provider must identify whether or not it is compliant with the recommendation. For each recommendation with which it claims to be compliant, the service provider must describe the measures put in place to comply with the recommendation. For each recommendation with which it claims not to be compliant, the service provider must provide justification.

h) **[HIGH]** For each [ARCHI_DR] recommendation relating to the security of sensitive information, the service provider must identify whether or not it is compliant with the recommendation. For each recommendation with which it claims to be compliant, the service provider must describe the measures put in place to comply with the recommendation. For each recommendation with which it claims not to be compliant, the service provider must provide justification.

i) **[HIGH]** For each [INTERCO_INTERNET] recommendation, the service provider must identify whether or not it is compliant with the recommendation. For each recommendation with which it claims to be compliant, the service provider must describe the measures put in place to comply with the recommendation. For each recommendation with which it claims not to be compliant, the service provider must provide justification.

IV.5.6. Controls

a) The service provider must develop and implement a control plan covering the entire scope of the remote identity verification service to ensure that the information systems security policy, the remote identity verification policy and the statement of remote identity verification practices are applied.

b) The service provider must review the control plan at least once a year and in the event of structural changes to the information system of the remote identity verification service, in particular changes to its hosting, infrastructure and architecture, or in the event of structural changes to the risk assessment, the risk management plan, the information systems security policy, the remote identity verification policy or the statement of remote identity verification practices.

c) The service provider must update the risk management plan to incorporate the results of the controls.

d) The service provider must have the results of the controls formally validated by their management in writing.

IV.5.7. Physical security

a) The service provider must draw up and maintain a list of persons authorised to access the premises hosting the information system of the remote identity verification service.

b) The service provider must implement mechanisms to ensure that only authorised persons can access the premises hosting the information system of the remote identity verification service.

c) The service provider must implement mechanisms to log access to the premises hosting the information system of the remote identity verification service.

d) The service provider must define and implement measures to ensure the confidentiality and integrity of the logs of access to the premises hosting the remote identity verification service.

IV.5.8. Logging

a) The service provider must log all automated processing and actions carried out by operators and fraud officers as part of a remote identity verification, and centralise them on a component of the service's information system to which the operators and fraud officers have no access.

b) The service provider must correlate the logs between the different components of the information system of the remote identity verification service.

c) All actions carried out by operators and fraud officers must be recorded and available for consultation for auditing purposes.

d) The service provider must carry out a sample review of the logs, and in particular of the operations carried out by the operators and the fraud officers.

IV.5.9. Backups

a) The service provider must develop and implement a backup and recovery plan for the remote identity verification service devices, including as a minimum: backup of systems, configurations and data.

It is recommended that the service provider test the backup and recovery plan at least once a year.

b) The service provider must define and implement measures to ensure the confidentiality and integrity of backups to the same level as that for which the remote identity verification service has been accredited.

It is recommended that the service provider comply with all the measures and recommendations on securing backups in [ISO27002].

IV.5.10. Partitioning of the service's information system

a) The service provider must develop and maintain a detailed description of the information system architecture of the remote identity verification service.

It is recommended that the information system be dedicated exclusively to the remote identity verification service and that all other services be performed on an information system that is physically partitioned from the service's information system.

b) The service provider must develop and maintain the flow matrix for the remote identity verification service and the associated filtering policy, which shall only allow flows that are strictly necessary for the operation of the remote identity verification service.

IV.5.11. Administration and use of the service

a) The workstations of administrators, operators and fraud officers must be connected exclusively to the information system of the remote identity verification service.

b) If access to the Internet or other information systems (the service provider's internal information system, for example) is required, administrators and operators must have a separate workstation deployed in an area outside of the information system of the remote identity verification service.

IV.5.12. Interconnections of the service information system

a) The service provider must identify in the detailed description of the architecture of the information system of the remote identity verification service identified in requirement IV.5.10.a) all

interconnections of the information system of the identity verification service with third party information systems, in particular the business service information system.

b) The service provider must filter all flows at the interconnections of the information system of the remote identity verification service.

> **[SUBSTANTIAL]** It is recommended that all flows on the interconnections of the information system of the remote identity verification service be filtered using filtering solutions qualified to standard level by ANSSI.

c) The service must perform mutual authentication with the business service when sending it results, and ensure the integrity, confidentiality and impossibility of replaying sent data.

d) **[HIGH]** The service provider must ensure that all interconnections of the information system of the remote identity verification service comply with annex 2 of the interministerial instruction on the protection of sensitive information systems [II_901].

IV.5.13. Remote access

The requirements of this chapter shall apply only if the service provider allows all or some of their staff remote access to the information system of the remote identity verification service.

a) For each recommendation in the [MOBILITY] guide, the service provider must identify whether or not they comply with the recommendation. For each recommendation with which it claims to be compliant, the service provider must describe the measures put in place to comply with the recommendation. For each recommendation with which it claims not to be compliant, the service provider must provide justification.

b) The service provider must set up a dedicated remote access gateway in accordance with [NT_ADMIN].

> It is recommended that separate gateways be set up for remote access by administrators and operators.

c) If the service provider uses a single gateway for remote access by administrators and operators, they must implement a solution to ensure strict separation of administrator and operator flows.

d) The mobile workstations used by administrators and operators must be dedicated to remote identity verification services.

e) Administrators and operators must use at least two-factor authentication on their mobile workstation.

> It is recommended that the service provider implement authentication for remote access based on electronic certificates issued by electronic certification service providers qualified by ANSSI in accordance with the RGS [RGS] to the two- or three-star level (**/***) and therefore involving the use of cryptographic media qualified by ANSSI to standard or enhanced level.

f) Mobile workstations must have a filtering solution that authorises only strictly necessary flows, in accordance with the filtering policy of the remote identity verification service.

g) Mobile workstations must only allow the use of removable media authorised by the information systems security policy.

h) Mobile workstations must have their entire disks encrypted with cryptographic mechanisms compliant with [CRYPTO_B1].

> It is recommended that the encryption solution for mobile workstation disks be qualified by ANSSI to standard level and used in accordance with the conditions set out in the qualification decision.
>
> It is recommended that flows between mobile workstations and gateways be encrypted using *IPsec* encryption and authentication solutions qualified by ANSSI to standard level and used in accordance with the conditions set out in their qualification decision.

i) The mobile workstations must be configured to be able to communicate only with the remote access gateway via an encrypted and authenticated *IPsec* connection *(full tunnelling).*

j) **[HIGH]** The encryption solution for the disks of mobile workstations must be qualified by ANSSI to standard level and used in accordance with the conditions set out in the qualification decision.

k) **[HIGH]** The flows between the mobile workstations and the gateways must be encrypted using IPsec encryption and authentication solutions qualified by ANSSI to standard level and used in accordance with the conditions set out in the qualification decision.

IV.5.14. Software development and security

The requirements of this chapter apply to all software that contributes to the processing allowing the acquisition and verification of identification data, the creation of the evidence file and the sending of the result of the identity verification to the business service.

a) The software must be subject to regular code reviews[13].

b) The software must undergo non-regression testing before production of a new version.

c) The software must be the subject of a documented acceptance test suite for each version that is to be produced.

d) The software must generate suitable record logs for correlating records between different processes of the service.

e) The software developer must be aware of the specific risks associated with identity verification, and be bound by an obligation of discretion.

f) The software must be developed under conditions allowing a record of the actions of each developer and consultation for audit purposes.

g) Each software supplier is obliged to inform the service provider of any internal fraud or attack aimed at altering the software supplied.

IV.5.15. Security breach management

a) It is recommended that the remote identity verification service provider implement a crisis management process in the event of a major security breach affecting the remote identity verification service.

b) The remote identity verification service provider must inform ANSSI immediately, in accordance with [PROCESS_CERTIF_SERVICE] and [PROCESS_QUALIF_SERVICE], in the event of a breach affecting or likely to affect the remote identity verification service.

IV.6. Service provider organisation and governance

IV.6.1. Recruitment

a) The service provider must check the training, qualifications and professional references of the candidates (operators, fraud officers, etc.) for the remote identity verification service and the veracity of their CV before they are hired.

b) The service provider must use all legal means at their disposal to ensure the honesty of their staff. In particular, these staff must not have any court convictions that are inconsistent with their duties[14]. These

[13] See the various ANSSI guides on programming rules for secure development: https://www.ssi.gouv.fr/administration/bonnes-pratiques

[14] Under French law, employers can ask their staff to present a copy of bulletin no. 3 of their criminal record. The employer may decide in the event of a refusal to present this copy or in the event of the presence of a court conviction incompatible with the person's duties, to withdraw these duties.

verifications should be carried out prior to recruitment and reviewed regularly (the period between two reviews must not exceed three years). The operators and the fraud officers must be contractually bound to the service provider.

c) The service provider must, after recruitment, make the operators and fraud officers aware of the specific risks relating to their role, and inform them of their obligation of discretion

IV.6.2. Ethics charter

a) The service provider must have an ethics charter integrated into the internal rules and regulations and which specifies in particular that:

- the services are provided with loyalty, discretion and impartiality;
- staff only use methods, tools and techniques validated by the service provider;
- staff undertake not to disclose any information to a third party, even anonymised and decontextualised, obtained or generated in the course of the service, unless formally authorised in writing by the client;
- staff undertake to report to the service provider any illegal content discovered during the service;
- staff undertake to comply with the national laws and regulations in force and with the good practices relating to their activities.

b) The service provider must have all of their staff sign the ethics charter set out in requirement IV.6.2.a) prior to providing the service.

c) The service provider must ensure compliance with the ethics charter and provide for disciplinary action against operators, administrators and experts of the verification service who violate the security rules or the ethics charter.

IV.6.3. Organisation and management of skills

a) The service provider shall employ a sufficient number of operators and fraud officers with the skills identified in Annex 2 to fully deliver all aspects of the remote identity verification service.

b) The service provider must provide the operators and fraud officers with all the educational and technical material that will enable them to carry out their assigned tasks.

c) The service provider must produce and implement a regular training plan for operators and fraud officers in line with the tasks and skills identified in Annex 2.

d) The service provider must develop and implement a regular control plan to verify that the operators and fraud officers have the skills identified in Annex 2.

e) The service provider must ensure that each operator and fraud officer, prior to carrying out the service, has followed the training plan and passed the control plan.

IV.6.4. Operational bulletins

a) The service provider must establish operational bulletins and include, since the last operational bulletin, at least:

- the operational indicators of the service (requirement IV.7.1.b) ;
- a review of the complaints (requirements of chapter IV.3.1.4) received, being processed and closed;
- a review of the security breaches relating to information systems security;
- a review of the security breaches reported to ANSSI (requirements IV.2.5g) and IV.5.15b));
- the date of the last execution of the plan for testing the effective ability of the service to detect attempted identity theft (requirements in chapter IV.2.5);

- the false rejection rate (FRR) and false acceptance rate (FAR) for the verification of the authenticity of the identity document measured during the last execution of the plan for testing the effective ability of the service to detect attempted identity theft (requirements of chapter IV.2.5);
- the false rejection rate (FRR) and false acceptance rate (FAR) for the comparison of the user's face measured during the last execution of the plan for testing the effective ability of the service to detect attempted identity theft (requirements in chapter IV.2.5);
- the false rejection rate (FRR) and false acceptance rate (FAR) for liveness detection measured during the last execution of the plan for testing the effective ability of the service to detect attempted identity theft (requirements of chapter IV.2.5);
- a review of any changes made to:
    - the information system of the remote identity verification service,
    - the assessment of risks relating to identity theft (requirements of chapter IV.2.2), especially if the list of risk scenarios has been modified,
    - the assessment of risks relating to the security of information systems (requirements of chapter IV.2.3), particularly if the list of risk scenarios has been modified,
    - the risk management plan (requirements of chapter IV.2.4),
    - the remote identity verification policy (requirements of chapter IV.3),
    - the statement of remote identity verification practices (requirements of chapter IV.3),
    - the information systems security policy (requirements of chapter IV.5.2),
    - the plan for testing the effective ability of the service to detect attempted identity theft (requirements of chapter IV.2.5).

b) The service provider must send the client, at the frequency defined in the service agreement, the operational bulletins relating to the remote identity verification service.

It is recommended that the service provider send operational bulletins on a monthly basis.

c) The service provider must ensure the confidentiality of the operational bulletins.

IV.6.5. Relations with State departments

a) The service provider must appoint a security officer responsible in particular for liaising with the relevant State departments in the event of fraud or attack.

IV.7. Quality and level of service

IV.7.1. Quality of the service

a) The service provider must develop and implement a process for drawing on detected breaches and fraud in order to continuously improve the effectiveness of its remote identity verification service.

b) The service provider must define with the client the operational indicators of the remote identity verification service.

c) As a minimum, the service provider must put in place the means to measure the following operational indicators:

- the average, minimum and maximum waiting time for users;
- the number of remote identity verifications carried out;
- the number of remote identity verifications by verdict (successful or unsuccessful);

- the number of remote identity verifications for which the service declared an “unsuccessful" verdict, based on the reason for the failure;
- the number of remote identity verifications for which the service declared an "unsuccessful" verdict on the basis that identity theft was suspected or proven, based on the nature of the attempted identity theft[15];
- the number of remote identity verifications for which the service gave a "successful" verdict and which later turned out to be identity theft, depending on whether the theft was detected by the service provider or by the client;
- the number of complaints received, being processed or closed;
- the average, minimum and maximum time for closing complaints.

d) The service provider must develop and maintain an indicator measurement process describing, for each operational indicator (requirement IV.7.1.b), the methods and means used by the service provider to measure the indicator.

IV.7.2. Service agreement

IV.7.2.1. Terms and conditions of the service

a) The service agreement between the service provider and the client must describe the organisation, scope and objectives of the remote identity verification service.

b) The service agreement must describe the technical and organisational means used by the service provider to provide the service.

c) The service agreement must specify how the remote identity verification policy is to be updated and, where appropriate, how the client is to validate such changes.

d) The remote identity verification policy must be annexed to the service agreement.

IV.7.2.2. Organisation of the service

a) The service agreement must stipulate that the service provider must designate a contact person for the client within the company who will be responsible for the operational monitoring of the service.

b) The service agreement must stipulate whether the service provider authorises remote access to the information system of the remote identity verification service by some of its staff.

IV.7.2.3. Location

a) The service agreement must describe the location of the processing and storage of data relating to the remote identity verification service for that client, in particular user data.

IV.7.2.4. Responsibilities

a) The service agreement must stipulate that the service provider shall not commence the service until the client has formally approved the service agreement in writing.

b) The service agreement must stipulate that the service provider shall inform the client of any breach of the service agreement.

c) The service agreement must stipulate that the service provider shall inform the client in the event of a security breach detected on the information system of the remote identity verification service, and specify the procedures and the maximum time limit for sending information on the security breach to

[15] In order to identify the nature of an attempted identity theft, it is recommended that the service provider work on the basis of the risk scenarios identified in the identity theft risk assessment identified in chapter IV.2.2.

the client.

d) The service agreement must stipulate that the service provider only carries out actions that are strictly in line with the objectives of the service.

e) The service agreement must stipulate that the service provider automatically registers as a complaint (see requirements in chapter IV.3.1.4) all remote identity verifications for which the provider has given a "successful" verdict and the client suspects or has detected identity theft.

f) The service agreement must stipulate that the client declares that they fulfil all the legal obligations necessary for the service to be provided and in particular those relating to the collection, processing and transfer of personal data and biometric processing. The service agreement must specify the purposes of such collection, processing and transfer, and identify the applicable regulatory framework.

g) The service agreement must define the responsibilities and measures taken by the service provider and the client respectively to reduce potential risks relating to the service, in particular those relating to identity theft and the collection and processing of personal data.

h) The service agreement must stipulate that the service provider has professional insurance to cover any damage to the business service and in particular to its information system in the course of providing the service, specify the insurance coverage and include the insurance certificate.

i) The service agreement must specify the measures implemented by the service provider under its termination plan.

IV.7.2.5. Confidentiality and protection of information

a) The service agreement must stipulate that the service provider collects and processes only data that is adequate, relevant and limited to what is necessary for the purposes for which it is processed.

b) The service agreement must stipulate that the service provider will not disclose any user data to third parties, except with the express written consent of the client and in accordance with the personal data protection regulations [GDPR].

c) The service agreement must specify clauses relating to the ethics of the service provider and include the service provider's ethics charter.

d) The service agreement must specify the terms and conditions for accessing, storing, transporting, reproducing, destroying and returning data relating to that client, in particular user data.

IV.7.2.6. Laws and regulations

a) The service agreement must be written in French. The service provider can provide a courtesy translation of the service agreement if requested by the client.

b) The service agreement must stipulate that only the French version is binding, particularly in the event of a dispute.

c) The service agreement must specify the technical and organisational means implemented by the service provider to ensure compliance with the applicable legislation and regulations, in particular those relating to the protection of personal data [GDPR].

d) The service agreement must specify any specific legal and regulatory requirements to which the client is subject, in particular those relating to its sector of activity.

e) The service agreement must specify that the law applicable to the service agreement is French law.

IV.7.2.7. Subcontracting

a) The service agreement must specify that the service provider may, if necessary, subcontract all or part of the service to another service provider, hereinafter the "subcontractor", provided that all the conditions set out below are met:

- there is a service agreement between the service provider and the subcontractor;
- the use of subcontracting is known and formally accepted in writing by the client;
- the subcontractor complies with the requirements of this rules set.

IV.7.2.8. Deliverables

a) The service agreement must define the deliverables expected as part of the service, the ownership rules and sensitivity levels relating to these deliverables, and the associated protection arrangements.

b) The service agreement must specify that the deliverables of the service are in French unless the client makes a formal written request to the contrary.

IV.7.2.9. Service level

a) The service agreement must identify the operational indicators for measuring the service level of the service (requirements of chapter IV.6.4).

b) The service agreement must identify the frequency with which the service provider sends the business system operational bulletins (requirements of chapter IV.6.4).

c) The service agreement must stipulate that the service provider defines and implements a process for continuous improvement of the effectiveness of the remote identity verification service, based in particular on the operational indicators.

d) The service agreement must identify the operational time slots for the remote identity verification service.

Annex 1 Documentary references

I. Codes, laws and regulations

Referral	Document
[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. Available at https://www.eur-lex.europa.eu
[GDPR]	Regulation (EU) No. 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) Available at https://www.eur-lex.europa.eu
[RGS]	General security baseline, subject of decree no. 2010-112 of 2 February 2010 taken for the application of articles 9, 10 and 12 of Ordonance no. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities Available at http://www.legifrance.gouv.fr (French only)
[DECREE_2015-350]	Decree No. 2015-350 of 27 March 2015 on the approval of security products and trust service providers for the purposes of information systems security. Available at http://www.legifrance.gouv.fr (French only)
[DECREE_2020-118]	Decree n°2020-118 of 12 February 2020 reinforcing the national system to combat money laundering and terrorist financing. Available at http://www.legifrance.gouv.fr (French only)
[II_910]	Interministerial instruction on controlled items of information systems security (ACSSI), No. 910/SGDSN/ANSSI, 22 October 2013. Available at http://www.legifrance.gouv.fr (French only)
[II_901]	Interministerial instruction on the protection of sensitive information systems, No. 901/SGDSN/ANSSI, 28 January 2015. Available at http://www.legifrance.gouv.fr (French only)
[CPCE]	French Post and electronic communications code, current version Available at http://www.legifrance.gouv.fr (French only)

II. Standards and technical documents

Referral	Document
[ADMIN_SEC]	Recommendations to secure administration of IT systems, ANSSI, reference ANSSI-PA-022, current version. Available at http://www.ssi.gouv.fr
[EBIOS_RM]	Ebios Risk Manager, ANSSI, 2018. Available at http://www.ssi.gouv.fr
[CC_CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, current version. Available at http://www.ssi.gouv.fr
[CRYPTO_B1]	Requirements and recommendations concerning the choice and dimensioning of cryptographic mechanisms, ANSSI, version 2.03. Available at http://www.ssi.gouv.fr (French only)
[CRYPTO_B2]	Requirements and recommendations concerning the keys used in cryptographic mechanisms. Available at http://www.ssi.gouv.fr (French only)

Referral	Document
[CRYPTO_B3]	Requirements and recommendations regarding authentication mechanisms, ANSSI. Available at http://www.ssi.gouv.fr (French only)
[ACCREDITATION]	Security accreditation in nine easy steps, ANSSI, current version. Available at http://www.ssi.gouv.fr (French only)
[HYGIENE]	Cyber hygiene guide, ANSSI, current version. Available at http://www.ssi.gouv.fr (French only)
[MIE]	Security requirements rule set, Electronic identification means, ANSSI, current version.
[NT_ADMIN]	Recommendations on the secure administration of information systems, ANSSI, current version. Available at http://www.ssi.gouv.fr (French only)
[INTERCO_INTERNET]	Recommendations on the interconnection of an information system to the Internet, ANSSI, reference ANSSI-PA-066, current version. Available at http://www.ssi.gouv.fr (French only)
[ISO27002]	International standard ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls. Available at http://www.iso.org
[ISO27005]	International standard ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management. Available at http://www.iso.org
[ISO30107-3]	International standard ISO/IEC 30107-3. Information technology — Biometric presentation attack detection — Part 3: Testing and reporting. Available at http://www.iso.org
[MOBILITY]	Recommendations on digital mobility, ANSSI, reference ANSSI-PA-054, current version. Available at http://www.ssi.gouv.fr (French only)
[ARCHI_DR]	Recommendations for the architecture of sensitive or restricted distribution information systems, ANSSI, reference ANSSI-PG-075, current version. Available at http://www.ssi.gouv.fr (French only)
[SecNumCloud]	Cloud computing service providers (SecNumCloud), ANSSI, requirements rules set, version 3.1 of 11 June 2018. Available at http://www.ssi.gouv.fr (French only)
[CNIL_Guide_conservation]	Practical guide – Retention periods, CNIL, current version. Available at https://www.cnil.fr (French only)

III. Other documentary references

Referral	Document
[PROCESS_QUALIF_SERVICE]	Service qualification process, ANSSI, current version. Available at http://www.ssi.gouv.fr (French only)
[PROCESS_QUALIF_PRODUCT]	Product qualification process, ANSSI, current version. Available at http://www.ssi.gouv.fr (French only)
[PROCESS_CERTIF_SERVICE]	Service certification process, ANSSI, current version. Available at http://www.ssi.gouv.fr (French only)

Annex 2 Tasks and skills of the service provider's staff

IV. Operator

IV.1. Tasks

The operator must carry out the following tasks:

a) verify, in accordance with the remote identity verification policy, the identity of users on the basis of the acquired user identification data and the results of the automated processing of such identification data;

b) if the service is "synchronous with human interaction", make requests to users in the chosen language for the acquisition and verification of identification data (e.g. brightness, focus, removal of the user's glasses, etc.) in accordance with the remote identity verification policy;

c) give the "successful" or "unsuccessful" verdict of the remote identity verification[16].

d) generate an alert whenever identity theft is suspected or detected.

IV.2. Skills and knowledge

The operator must have the following skills:

a) know and apply the remote identity verification policy;

b) know and apply the information systems security policy;

c) know the threat assessment relating to identity theft;

d) know and apply the legislation and regulations in force relating to the protection of personal data, and in particular the [GDPR];

e) know the modus operandi of the attackers leading to the risk scenarios identified in the assessment of the risks relating to identity theft;

f) be good at remembering faces, recognise and compare faces from photos and videos;

g) know the security features of identity documents and the verifications to be carried out to identify falsified or altered identity documents;

h) know and master the use of the PRADO register[17].

V. Identity document fraud officer

V.1. Tasks

The identity document fraud officer must carry out the following tasks:

a) formally validate changes to the remote identity verification policy where these changes relate to identity documents;

b) [when the authenticity of the identity document is cryptographically verified using the security component] validate the design and implementation of the identity document authenticity verification function;

[16] According to requirement IV.3.3.2.o), when the authenticity of the identity document is cryptographically verified using the security component, the verdict of the remote identity verification given by the service is automatically "unsuccessful", without any operator intervention, if the automated processes relating to the verification of the authenticity of the identity document conclude that the document is not authentic.

[17] See acronym in chapter I.3.1.

c) [when the authenticity of the identity document is not cryptographically verified by the security component] process alerts generated by operators when they suspect or detect a risk scenario identified in the risk assessment relating to identity theft and concerning identity documents;

d) [when the authenticity of the identity document is not cryptographically verified using the security component] handle alerts generated when an operator has proposed a "successful" verdict for the remote identity verification whereas the automated processing suspects or detects identity document fraud;

e) [when the authenticity of the identity document is not cryptographically verified using the security component] provide training for operators in identity document verification, in particular controls on the security features of identity documents in order to identify falsified or altered identity documents;

f) [when the authenticity of the identity document is not cryptographically verified using the security component] provide training for operators in the attackers' modus operandi leading to the risk scenarios identified in the risk assessment relating to identity theft and identity documents;

g) [when the authenticity of the identity document is not cryptographically verified using the security component] check that operators have the skills expected in chapter IV.2 and relating to identity documents.

V.2. Skills and knowledge

The Identity document fraud officer must have the following skills:

a) know and apply the remote identity verification policy;

b) know and apply the information systems security policy;

c) have detailed knowledge of the threat assessment relating to falsified or altered identity documents;

d) know and apply the legislation and regulations in force relating to the protection of personal data, and in particular the [GDPR];

e) **[SUBSTANTIAL]** know the threat assessment relating to identity theft;

f) **[SUBSTANTIAL]** have detailed knowledge of the attackers' modus operandi leading to the risk scenarios identified in the assessment of the risks relating to identity theft and identity documents;

g) **[SUBSTANTIAL]** have detailed knowledge of the security features of identity documents and the verifications to be carried out to identify the occurrences of the risk scenarios identified in the assessment of the risks relating to identity theft and identity documents;

h) **[SUBSTANTIAL]** know and apply the procedures for alerts generated by an operator when they suspect or detect identity theft involving a falsified or altered identity document;

i) **[SUBSTANTIAL]** know and apply the procedures relating to alerts generated when an operator gives a "successful" remote identity verification verdict whereas the automated processing suspects or detects identity document fraud.

VI. Biometrics fraud officer

VI.1. Tasks

The Biometrics fraud officer must carry out the following tasks:

a) process alerts generated by operators when they suspect or detect an occurrence of a risk scenario identified in the assessment of the risks relating to identity theft and biometrics;

b) handle alerts generated when an operator has given a "successful" remote identity verification verdict whereas the automated processing suspects or detects biometric fraud;

c) provide training for operators in biometric verifications, in particular verification of biometric identification data, facial comparison;

d) provide training for operators in the modus operandi of attackers leading to the risk scenarios identified in the assessment of the risks relating to identity theft and biometrics;

e) check that operators have the skills expected in chapter IV.2 and relating to biometrics;

f) formally validate changes to the remote identity verification policy where these changes relate to biometrics;

g) validate the design and implementation of biometric verifications performed by automated processing.

VI.2. Skills and knowledge

The Biometrics fraud officer must have the following skills:

a) know and apply the remote identity verification policy;

b) know and apply the information systems security policy;

c) know the threat assessment relating to identity theft;

d) detailed knowledge of the threat assessment relating to biometrics;

e) know and apply the legislation and regulations in force relating to the protection of personal data, and in particular the [GDPR];

f) detailed knowledge of the modus operandi of the attackers leading to the risk scenarios identified in the assessment of the risks relating to identity theft and biometrics;

g) detailed knowledge of the verifications to be carried out to identify the occurrences of the risk scenarios identified in the assessment of the risks relating to identity theft and biometrics;

h) know and apply the procedures for alerts generated by an operator when they suspect or detect an occurrence of a risk scenario identified in the risk assessment and related to biometrics;

i) know and apply the procedures relating to alerts generated when an operator gives a "successful" remote identity verification verdict whereas the automated processing suspects or detects biometric fraud.

Annex 3 Recommendations to clients

This annex lists ANSSI's recommendations to clients.

a) If the client is an administrative authority or an essential operator or essential service, it may ask ANSSI to participate in the definition of the specifications that are the subject of a call for tender or a contract.

b) It is recommended that the client designate an operational contact person from among its staff to be the main contact with the service provider regarding the operation of the remote identity verification service.

c) It is recommended that the client identify in the service agreement any specific legal and regulatory requirements to which it is subject, particularly those related to its sector of activity.

d) It is recommended that the client require the service provider to provide monthly operational bulletins as a requirement of the service agreement.

e) It is recommended that the client notify the service provider of all remote identity verifications for which the service provider has given a "successful" verdict and that the client suspects or has detected identity theft. In accordance with the service agreement, the service provider automatically registers these notifications as complaints and processes them as such.

f) It is recommended that the client establish a crisis management process in the event of a major security breach affecting the service provider.

Annex 4 Accepted identity documents

Only the following identity documents are accepted in the context of this rule set, provided that they have the characteristics to meet the requirements defined in this rule set:

a) For French nationals, nationals of other European Union Member States, of a State party to the Agreement on the European Economic Area or of Switzerland, the passport or identity card.

b) For third-country nationals residing in France or in another Member State of the European Union, in a State party to the Agreement on the European Economic Area or in Switzerland, the residence permit, drawn up in accordance with the model provided for in Regulation (EU) No. 2017/1954 of the European Parliament and of the Council of 25 October 2017 laying down a uniform format for residence permits for third-country nationals, issued by the State of residence.

c) For third-country nationals exempt from the short-stay visa requirement who are not resident in the European Union, a State party to the Agreement on the European Economic Area or Switzerland, the passport, provided that the issuing country makes available the means necessary to verify the validity of the document. If the visa waiver is accompanied by the requirement to have an e-passport, only the e-passport is recognised as an authoritative source for the country concerned.

d) For third-country nationals who are refugees or recognised as stateless or who are beneficiaries of the protection provided for in Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted, the passport shall be replaced by the travel document issued by the State which has recognised the status of refugee or stateless person or granted protection.