Remote Identity Verification Policy

(RIVP)

Version 1.1

IDnow GmbH
Auenstr. 100
80469 Munich

13.04.2022

IDnow Remote Identity Verification Policy

Version	1.1
Date	13.04.2022
Author	Armin Bauer, IDnow GmbH (armin.bauer@idnow.de)
Classification	Public, Published at https://www.idnow.io/certification-policies/
Security Policy	IDnow Security Policy, Version 1.6
Identification Center Infrastructure Policy	IDnow Identification Center Infrastructure Policy, Version 1.0
Data Center Infrastructure Policy	IDnow Data Center Infrastructure Policy, Version 1.1
AutoIdent Qualified Electronic Signature Process Description	IDnow AutoIdent Qualified Electronic Signature Process Description, Version 1.0
Risk Assessment AutoIdent Qualified Electronic Signature	IDnow AutoIdent Qualified Electronic Risk Assessment Signature, Version 1.6
Risk Assessment VideoIdent Qualified Electronic Signature	IDnow AutoIdent Qualified Electronic Risk Assessment Signature, Version 1.1
OID Policy	IDnow OID Policy 1.0
ANSSI PVID standard	Prestataires de vérification d'identité à distance, Référentiel d'exigences, Version 1.1 du 1er mars 2021
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[NT_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[NOMADISME]	Recommandations sur le nomadisme numérique, ANSSI, référence ANSSI-PA-054, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[CRYPTO_B1]	Règles et recommandations concernant les mécanismes d'authentification, ANSSI. Disponible sur http://www.ssi.gouv.fr

History		
Date	Version	Comment
13/04/2022	1.1	• Clarification regarding confidentiality of the document • Clarification regarding accepted documents OID-V: 1.3.6.1.4.1.56907.2.1.4.1.2 OID-A: 1.3.6.1.4.1.56907.2.2.4.1.2
31/03/2021	1.0	Creation of the document. OID-V: 1.3.6.1.4.1.56907.2.1.4.1.1 OID-A: 1.3.6.1.4.1.56907.2.2.4.1.1

Table of Contents

1. PURPOSE OF THE DOCUMENT

IDnow GmbH acts as a qualified Remote Identity Verification Provider according to ANSSI requirements and evaluation process. IDnow only performs the remote identity verification of a natural person (also named Subscriber in the present document), using 2 distinct services:

- VideoIdent: Subscriber is in a session with an Operator of IDnow using a computer or mobile phone and an ID document. Then IDnow proceeds to a second manual review to give the result of the identification. It is a "Synchronous remote identity verification service with human interaction" as defined in the PVID 1.1 standard.
- AutoIdent: Subscriber is in session with a technical service of IDnow using a computer or mobile phone and an ID document. The identification data verification is performed synchronously by the system during that session. IDnow then proceeds to a manual review to give the result of the identification. If that manual review cannot be completed the Subscriber has to redo the identification. It is therefore a "Synchronous remote identity verification service without human interaction" as defined in the PVID 1.1 standard.

This document is the full Remote Identity Verification Policy (RIVP) for both processes. Each service is identified by a distinct OID as follow:

- OID-V: 1.3.6.1.4.1.56907.2.1.4.1.2
- OID-A: 1.3.6.1.4.1.56907.2.2.4.1.2

The last section of the OID ("E") details the version of the policy. Please refer to the versioning table at the beginning of the document regarding the complete OID for previous versions. Please also refer to the IDnow OID Policy to understand how OIDs are set up. In the present document, when a requirement applies only to a service, then the symbol OID-V or OID-A will be used to detail the difference between the 2 services. Services are sold to a Customer (named "Commanditaire" in ANSSI standard).

The 2 OID-A and OID-V are compliant with Substantial assurance level as stated by ANSSI in the standard PVID.

The present RIVP is completed by Remote Identity Verification Practice Statement (RIVPS) that is confidential and not communicated to Subscriber or relying party and only to people who need to know.

The RIVP has a contact identified in section 1.5.2. This contact is responsible for the following duties:

- Report all security incidents to the Customer,
- Manage the changes within this document upon validation of ANSSI,
- Control that the operational procedures regarding the Customer activities are performed in compliance with the present RIVP.

IDnow performs the following four process steps to assure that the identification of a natural person online has an "equivalent assurance" to a face-to-face identification:

1) Check of the actual existence of the person in real life ("Liveness Detection")
2) Check whether the ID document belongs to this specific person

3) Proof that the present person is the same as the one specified in ID document
4) Check the authenticity of the ID document

IDnow acting primarily as a Provider of Remote Identity Verification acts on behalf of:

- A relying party (Customer, e.g. financial institute) to transmit documents that need a signature of the subscriber to the subscriber
- on behalf of the Subscriber as a Registration Policy (RA), performing remote face to face as stated in eIDAS article 24 to request a qualified certificate to be issued by the CA,
- on behalf of the Subscriber as an agent to request the electronic signature of one or more documents delivered together with the request,
- on behalf on behalf of the relying party as an agent receiving the signed documents, performing all required checks requested by the applicable law and creating a quality report allowing the relying party to identify the new customer according to the law,
- on behalf of the CA as contact place to start a revocation process

This RIVP references the IDnow Security policy, the IDnow Identification Center Infrastructure Policy, IDnow Data Center Infrastructure Policy, IDnow AutoIdent Qualified Electronic Signature Process Description, as well as the Risk Assessments and the ANSSI standard used to certify the services. They provide further details but have been outsourced due to the sensitivity of the content. The correct version of those documents for this RIVP is mentioned at the beginning of this document. IDnow risk assessments are compliant with ISO 27005 norm and take into account the risks related to identity theft and security of IT system used for RIV services. The risk assessments are reviewed every year as defined in PVID standard from ANSSI and following major changes as defined in those documents. IDnow in its risks analysis considers the following attacker profiles: any malicious person, group of people or organization, internal or external with a moderate attack potential.

Risk analysis contains a risk treatment plan and a test plan for testing the effective ability of the service to detect identity theft attempts.

The present RIV Policy is defined based on IDnow risk analysis taking account the ANSSI requirement. RIVPS gives the details.

In addition to that, the present RIVP is completed by IDnow Security Policy that covers all aspect of PVID standard from ANSSI. IDnow reviews the IDnow security policy at least once per year, and in the event of a change in the IDnow risk assessment or risk treatment plan.

Contact identified in the present RIVP validates the IDnow Risk analysis and IDnow security policy and sign it as part of the homologation process requested by ANSSI. RIV services, as defined in the present RIVP, can only be run after official homologation from IDnow and qualification from ANSSI.

1.2. PARTICIPANTS

IDnow uses a supplier for the operation of the datacenter. The supplier provides the server hardware, racks, firewall, electricity, internet, etc. (“Housing”). IDnow then takes over at the hardware level (operating system and higher layers).

IDnow has 2 main contacts with the operator of datacenters. One for business/contract questions and one for technical questions.

In addition, there is a technical emergency hotline.

In the other direction, there is a notification system (e.g., mailing list) provided by the datacenter operators, which notifies IDnow about forthcoming maintenance work.

There is a contract that governs the commercial relationship between the datacenter operators and IDnow. The scope of services provided is regulated in this contract. There is also a commissioned data processing agreement with the associated technical and organizational measures.

Details can be found in the document “IDnow Security Policy”, section 8.4 and the document “IDnow Data Center Infrastructure Policy”, section 3.

In addition to its own Identification Center, IDnow partners with other call center providers to provide the identification service.

To further improve the quality of the face recognition and liveness detection IDnow uses SDKs from experts in those fields.

There are contracts for all sub-contractors in place that regulate the scope of service and liabilities. The implemented controls that are required to provide this service are documented in the “IDnow Identification Center Infrastructure Policy”, section 3 and are part of the contract.

1.3. POLICY ADMINISTRATION

1.3.1. ORGANIZATION ADMINISTERING THE DOCUMENT

This document is published and maintained by IDnow GmbH, Germany. IDnow makes its RIVP publicly available through the website at https://www.idnow.io/certification-policies/

It is regularly reviewed at least once a year or on the basis of changes and approved by a member of the management board. The IT Security Officer is responsible for the implementation of the practices. Changes to the document will be published on the IDnow website after approval from the management board.

The present RIVP is written according ANSSI standard PVID and according to the result of IDnow’s risk analysis.

The IDnow Risk Assessment AutoIdent Qualified Electronic Signature and the IDnow Risk Assessment VideoIdent Qualified Electronic Signature provides an analysis of attack scenarios and their counter measures in chapter Annex A: Threat Matrix.

1.3.2. CONTACT PERSON

Address:

IDnow GmbH
Auenstr. 100
80469 Munich
Germany

Contact:

Service Desk Portal (24x7): https://support.idnow.de
Telephone (9am – 6pm, Low & Medium Priority only): +49 89 413 24 600 (select language -> press 3)
Email (9am – 6pm, Low & Medium Priority only): tickets@idnow.de.

IDnow appoints a Security Officer whose duties include liaising with the relevant government departments and ANSSI in the event of fraud or attack.

1.4 DEFINITIONS AND ACRONYMS

1.4.1 ACRONYMS

ANSSI: Agence nationale de la sécurité des systèmes d'information

OID: Object Identifier

PASSI: Prestataire d'audit de la sécurité des systèmes d'information (accredited lab to audit IDnow against ANSSI PVID standard and the present RP).

PRADO: Public Register of Authentic Travel and Identity Documents Online3 - Registre public en ligne de documents authentiques d'identité et de voyage

IT: Information Technology

eIDAS: Electronic Identification, Authentification and Trust Services – Règlement européen n°910/2014 sur l'identification électronique et les services de confiance

GDPR: General Data Protection Regulation

FAR: False Acceptance Rate – Taux de faux positifs (acceptation à tort)

FRR: False Rejection Rate – Taux de faux négatifs (rejets à tort)

1.4.2 DEFINITIONS

The definitions below apply to this repository. Some of them are based on the European regulations [EIDAS] and [GDPR].

Administrator - remote identity verification service personnel with privileged access rights to all or part of the remote identity verification service information system components.

Identity attributes - a subset of the identification data transmitted by the remote identity verification service to the business service.

Customer - the entity responsible for a business service that uses a remote identity verification service.

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

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

Consent - any free, specific, informed and unambiguous expression of will by which the user accepts, by means of a declaration or a clear positive act, that personal data concerning him or her may be processed.

Remote identity verification intermediate finding - information generated by the remote identity verification service as part of the analyses performed by automatic or operator processing, and necessary for the remote identity verification verdict. Several intermediate findings may contribute to a single verdict.

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

Remote Identity Verification Practice Statement - the set of practices (organization, operational procedures, technical and human resources, etc.) that the remote identity verification provider applies while providing the service and in accordance with the Remote Identity Verification Policy to which it has committed itself. The statement of remote identity verification practices shall be confidential and shall be made available only to persons with a need to know.

Live detection - the detection of the "live" character of the user aims at authenticating the video of the user's face, to verify that it has not been physically or digitally altered.

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 standard, identification data can be the video of the user's face, the video of the ID presented by the user, or the user data (including the user's facial image) stored in the security component of the ID.

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 his or her physical, physiological, genetic, mental, economic, cultural or social identity.

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

Supplementary data - data acquired by the remote identity verification service and transmitted to the business service as part of the remote identity verification result but on which no verification is performed by the service as part of the repository. Additional data is not included in the remote identity verification outcome. The acquisition by the remote identity verification service of this additional data and its transmission to the business unit must be in accordance with applicable regulations and is generally requested by the Customer to meet regulatory requirements.

Identity Verification Proof - a record kept by the service provider of relevant information to be produced for the purposes of dispute resolution or investigation, and to provide evidence in court. This

standard specifies the minimum data to be retained. The data contained in the evidence file is not retained for biometric processing.

State of the art - a set of publicly available best practices, technologies and reference materials related to information systems security or identity verification, and information that is clearly derived from them. These documents may be posted on the Internet by the information systems security community, disseminated by reference organizations, or be of legislative, regulatory, or normative origin.

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

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

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

High assurance level - this level is intended to prevent the risk of identity theft or alteration. A remote identity verification service is said to be of high assurance level when it is demonstrated that it meets the requirements of the repository for the high level.

Substantial assurance level - this level is intended to substantially reduce the risk of identity theft or alteration. A remote identity verification service is said to have a substantial level of assurance when it is shown to meet the requirements of the standard for the substantial level.

Operator - the staff of the remote identity verification service responsible for verifying the identity of users, pronouncing the "pass" or "fail" verdict of the remote identity verification and alerting a fraud specialist in case of suspected identity theft.

Remote Identity Verification Policy - a set of rules, uniquely referenced by an OID, defining the requirements that a remote identity verification service provider complies with 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 Customers. The remote identity verification policy shall be made available to users.

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

Provider - a legal entity that provides a remote identity verification service. IDnow is the Provider.

Service - the provision of the remote identity verification service to a customer, as part of the service agreement between the provider and the customer.

Identity Fraud Specialist - staff of the remote identity verification service who have in-depth knowledge of the security features of identity documents and expertise in detecting identity fraud.

Biometrics Fraud Specialist - staff of the remote identity verification service with in-depth knowledge of biometrics and expertise in the detection of biometric fraud.

Remote Identity Verification Result (RIVR) - the set of information transmitted by the remote identity verification service to the business service, including the verdict (success or failure) of the remote identity verification, the reason for the failure, if any, the user identity attributes required by the business service and verified by the provider, and any additional data required by the business service.

Subcontracting - the process by which the service provider subcontracts all or part of the performance of the service agreement (and contract, if any) with the customer.

Remote identity verification service - the service covered by this standard, responsible for acquiring and verifying user credentials in order to identify users, compiling the evidence file and transmitting the result of the remote identity verification to the business service.

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

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 if the remote identity verification result can only be pronounced "successful" by an operator after the operator has validated the results of the verifications carried out by automated processes and carried out its own verification of the identification data.

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 acquisition or verification of identification data. A synchronous remote identity verification service with human interaction may, for example, allow an operator to guide the user during the acquisition of 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 acquisition and verification of identification data. The service may, however, implement automated interactions with the user.

Business service - the service to which the user wishes to identify himself, under the responsibility of the Customer, using the remote identity verification service.

Terminal - the hardware (mobile phone, tablet, computer, etc.) used to acquire the user's identification data. The terminal can be the user's, the provider's or the Customer's. The acquisition of the user's identification data through the terminal can be carried out using all types of applications: dedicated mobile application, browser, etc.

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

Identity document - an official document certifying the identity of a person. The identity documents referred to in Annex 4 of this standard are accepted in the context of this standard.

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

Identity theft - the act of fraudulently using the identification data of a third party. In the context of this standard, the notion of identity theft also encompasses the alteration of identity, consisting of the use of fraudulent identification data that does not belong to an existing person.

Remote identity verification verdict - a binary verdict ("pass" or "fail") generated by the remote identity verification service after the acquisition and verification phases of the identification data. The verdict is "pass" if the remote identity verification service concludes that the identity credential presented by the user is genuine on the one hand and that the user is the legitimate holder of the identity credential on the other, otherwise the verdict is "fail".

2. REMOTE IDENTITY VERIFICATION PROCESS

2.1 LANGUAGE OF THE SERVICE

For OID-V, an Operator is available that can at least speak the following language:

- French
- English
- German

For OID-V and OID-A, the user interface is at least available in the following languages:

- French
- English
- German

At least the French language is available with the following service level: 8:00 – 22:00, 7 days a week.

Before to use the service, the Subscriber is requested to select its language. The selection of the language can either be done through a selector in the user interface or by changing the device language.

All Operators of IDnow are located in EU Member states country. The countries are communicated by opening then Terms of Use by the Subscriber.

2.2 TERMINAL

Terminal to run the service is either the mobile phone or computer of the Subscriber.

If the Terminal is a mobile phone, the app is either provided by IDnow (e.g., “IDnow AutoIdent” app) or provided by the Customer where the technology of IDnow is integrated using an SDK. These apps are only available in the authorized trust store of the mobile phone vendor (e.g., Apple, Google). IDnow monitors official app stores to detect the availability of fraudulent applications designed to replace the service's legitimate one.

This app whatever the owner of the Terminal, is not used to help in the calculation of the RIV verdict or performs a technical control used in the RIV operation. This app is only used to take control on camera on the mobile phone.

The camera of the Terminal shall be able to have minimum resolution not less than 720p: 1280 × 720 at 25 frames per second to allow the service after compression of the video of the ID document and face of Subscriber.

2.3 ID DOCUMENT

The RIVP can only be updated on matters relating to ID documents after formal validation by an Identity Fraud Specialist.

Only ID document compliant with rules defined in Annex 1 are authorized to be used in the service.

All ID documents used by IDnow in the service are supervised by a fraud specialist from the Quality Management Team.

Only non-expired ID document can be used in RIV service.

When available and legally authorized, IDnow uses ID document control service, to check the validity of the ID document, provided by the country that has issued the ID document used by Subscriber for a RIV operation. If the service returns an invalid result for an ID document, the result will always be unsuccessful.

IDnow checks if ID document has some physical alteration (torn or scratched identity document, etc.) as described in the RIVPS.

IDnow has taken additional measures to support users with disabilities like ensuring high contrast. Due to the nature of the process (video recording), there are certain limitations regarding the disabilities that can successfully perform the process (e.g., blind users).

The number of the passport or the identity document is being checked against the ICAO standard and PRADO. If a validity check of the ID document is carried out and it concludes that the ID document is invalid, then the verdict of the RIV is always "failed".

RIV service acquires a video of the identity document.

During the acquisition of the ID document of the Subscriber, the Subscriber will be requested to:

- OID-A:
    - Subscriber interacts only with the Terminal
    - Take a picture of the front side of the document
    - Take a picture of the back side of the document
    - Tilt the document to make the security features visible
    - Follow instructions on the screen regarding quality of the images (Document not in focus, glares covering the document, fingers on the document, not bright enough)
- OID-V:
    - Subscriber interacts with an Operator by video during all session.
    - Take a picture of the front side of the document
    - Take a picture of the back side of the document
    - Tilt the document to make the security features visible
    - Follow instructions by the agent regarding quality of the images (Document not in focus, glares covering the document, fingers on the document, not bright enough)

2.4 FACE MATCHING AND LIVENESS DETECTION

The present RIVP can only be updated on biometrics-related subjects after formal validation by an Biometrics Fraud Specialist.

IDnow has taken additional measures to support users with disabilities like ensuring high contrast. Due to the nature of the process (video recording), there are certain limitations regarding the disabilities that can successfully perform the process (e.g., blind users).

RIV service acquires a video of the face of the Subscriber.

During the acquisition of the face of the Subscriber, the Subscriber will be requested to:

- OID-A:
  - Subscriber interacts only with the Terminal.
  - Take a picture of his face (“Selfie”)
  - Move his face according to the instructions on the screen (“Liveness Detection”)
  - Follow instructions on the screen regarding quality of the images (Face not in focus, not bright enough)
- OID-V:
  - Subscriber interacts with an Operator by video during all session.
  - Take a picture of his face (“Selfie”)
  - Make movements based on the instructions by the agent (“Liveness Detection”)
  - Follow instructions by the agent regarding quality of the images (Face not in focus, not bright enough)

It is ensured that no biometric processing is performed after more than 96 hours.

2.5 INITIAL REMOTE IDENTITY VERIFICATION

2.5.1 RIV PROCESS

In any case, the Subscriber needs a Terminal, an ID document and, only in case of OID-V, be able to speak the language understood by Operator. If Subscriber cannot use the RIV for any reason, distinct from the one listed in section 2.3 and 2.4 above, it the responsibility to the Customer to provide an alternative solution to a RIV service.

Subscriber is requested to present a valid ID document and her/his face to be acquired by the service (refer to section 2.3 and 2.4 above).

Once the acquisition is done, Operator verifies the Identification data, face of Subscriber against the face contained in the ID document, the liveness of the face of Subscriber and genuineness of ID Document and the result from the automatic checks (only for OID-A) and gives a verdict or an intermediate report in case of contradictory opinion with the automatic check. In case of intermediate report, the Operator requests the Identity Fraud Specialist and/or Biometrics Fraud Specialist, according to the point to be verified and/or the contradiction with the automatic checks, to take a decision.

For OID-V, there is always a second Operator that verifies the checks made by the initial Operator. It is the second Operator that gives the final verdict.

2.5.2 NON-VERIFIED SUBSCRIBER INFORMATION

There is no non-verified information used by IDnow in the RIV services. Identity Attributes are verified against the ID document and Supplementary data are at least collected during the RIV session so IDnow can confirm that they are claimed by the Subscriber.

2.5.3 VALIDATION OF AUTHORITY

IDnow only accepts natural persons as identified in an ID Document and does not verify others attribute of the Subscriber.

2.5.4 RIV VERDICT

The RIV verdict given by the service is automatically "failure", without the intervention of an operator, if the automated processing relating to the verification of the authenticity of the ID document concludes that the ID document is not authentic.

2.6 SUBSCRIBER IDENTITY

Within RIV service, the name of the Subscriber is being checked against a copy of the ID document.

IDnow collects the data of the user and checks them. The following data will be collected at the minimum if applicable for Customer:

- Identity Attribute:
  - Full Name
  - Place of birth
  - Date of birth
  - Nationality
  - ID card number
  - Issuing country
  - Type of identity document
  - Date of issuance
  - Validity date
  - A photograph of the Subscriber's face extracted from the video of the Subscriber's face
  - A photograph of the ID document extracted from the video of the Subscriber's ID document

- Supplementary data (optional):
  - Mobile phone number
  - Email address of Subscriber
  - Information about the agent performing the identification
  - Information when the identification was performed
  - The video of the Subscriber's face
  - The video of the Subscriber's ID document

Details can be found in the document “IDnow AutoIdent Qualified Electronic Signature Process Description” section 3.4.

The Supplementary data are not taken in account in the process to conclude on the verdict of RIV.

2.6.1. ANONYMITY OR PSEUDONYMITY

All names are real names and have been checked against evidence in form of a copy of ID document. Anonymity or pseudonymity will not be accepted by IDnow.

2.6.2. RULES FOR INTERPRETING IDENTITY IN RIVR

The identity contained in the RIVR will always be taken from the ID document used to identify the Subscriber.

2.6.3. UNIQUENESS OF IDENTITY

The uniqueness of each Subscriber identity is ensured by providing the full name of the Subscriber associated with type of ID document and serial number of ID document used by Subscriber to be identified.

2.7 REMOTE IDENTITY VERIFICATION RESULT (RIVR)

2.7.1 CREATION

Each time that an Operator has decided of a verdict (success or failure) for a RIV for one Subscriber, IDnow generates a unique RIVR associated to this Subscriber.

The result of the RIV is only the verdict (success or failure) for the verification and the Subscriber's Identity Attributes related to the Subscriber (refer to section 2.6 above), as well as any additional data requested by the business service. The RIVR contains only the Subscriber Identity Attribute as defined in section 2.6 above.

The RIVR does not contain any element relating to the findings of the checks carried out by the service other than the verdict (success or failure) and in particular no score calculated on the basis of those checks.

The Subscriber is prohibited from correcting or deleting the evidence record and the RIVR transmitted to the Customer, as well as all the information required to compile the result. The Subscriber is also prohibited to access data that has been subject to automated or manual processing.

2.7.2 STORAGE

The RIVR is stored in same manner as the RIV proof in same location.

2.7.3 TRANSMISSION

Whatever the result of the verdict (success or failure) the RIVR is transmitted to the Customer.

RIVR is transmitted to Customer through TLS communication.

The maximum delay between the start of the acquisition of the Subscriber's Identification data and the transmission of the RIVR to the Customer cannot exceed 96 hours.

2.8 REMOTE IDENTITY VERIFICATION PROOF

For each RIV operation, whatever the verdict given by Operator, IDnow generates a unique RIV proof.

RIV proof contains at minimum the following data:

- Identification data:
  - Video of ID document captured during the RIV process.
  - Video of face of Subscriber captured during the RIV process.
- Date and time of the capture of the video of ID document.
- Date and time of the capture of the video of face of Subscriber.
- The list of all checks carried out on the Identification data, and for each check:
  - Date and time of check.
  - Operation associated with the check, including:
    - Verification of the authenticity of the ID document.
    - Detection of liveness of the Subscriber's face.
    - Comparison of the Subscriber's face with face contained in the ID document.
  - The type of the check: automatic or manual.
  - The identity of the Operator or the fraud specialist (Identity Fraud Specialist and/or Biometrics Fraud Specialist) who carried out the check when the latter is manual.
  - The country from which the Operator or the fraud specialist (Identity Fraud Specialist and/or Biometrics Fraud Specialist) who carried out the check when it is manual.
  - The version and configuration, if any, of the tools that carried out the check when it is automatic. This can be done by storing the timestamp of the identification and storing the version and configuration of the tool that was active at that time.
  - Intermediate reports issued by the automated processing, the Operator, or the fraud specialist (Identity Fraud Specialist and/or Biometrics Fraud Specialist) following the check.
- The verdict of the remote identity verification (success or failure).
- The reasons given by the Operator in case of a "failed" verdict.
- The identity of the Operator who issued the verdict.
- The date on which the Operator issued the verdict.
- The country from which the Operator delivered the verdict.
- The full name of the Subscriber as contained in the ID document.
- The date and place of birth of the Subscriber.
- The unique number of the ID document.
- The date of issuance of the ID document.
- The expiry date of the ID document.
- The RIV result (RIVR) transmitted to the Customer.

The RIV proof does not contain any data for biometric processing.

By default, the RIV proof is not transmitted to Customer. Only German specific Customer covered by German law "Geldwäschegesetz", "Vertrauensdienstegesetz" or the "Telekommunikationsgesetz" can receive the copy of the RIV proof that includes the video of ID document captured during the RIV process and the video of face of Subscriber captured during the RIV process.

2.9 WALLET

After the initial RIV, the Subscriber can define a password of at least 8 characters, which must be upper and lower case and must contain a special character, to have an account in the IDnow platform. This account allows the Subscriber to be authenticated again in the platform without performing again a RIV. If Subscriber has lost its password, then the Subscriber has to redo a RIV to create a new password.

IDnow records the mobile phone number of the Subscriber in the IDnow platform. Subscriber cannot change this Supplementary data without a RIV session.

With Wallet function, IDnow can resend to the Customer the RIVR created during the initial RVI after Subscriber authentication in IDnow platform for 2 years. After 2 years, the Subscriber must confirm again its identity with RIV and creates a new RIVR.

2.10 CHANGE OF IDENTITY

If Subscriber changes its identity, then current RIVR used in Wallet is not valid anymore. In such case, the Subscriber shall do again a new RIV to create a new RIVR if Customer needs to have a RIVR for this Subscriber. If the password of the Wallet of the Subscriber is stolen, then Subscriber shall immediately request the change of its password to IDnow.

2.11 FRAUD

IDnow generates an alert for each suspected or actual identity theft, whether detected by the service provider or reported by the Customer.

The complaints available to Subscriber of the service, in particular for the purpose of cancelling a fraudulent identification or in the event of refusal to identify a user in good faith can be direct to support@mail.idnow.de.

IDnow defines indicators to detect identity theft attempts related to the risk scenarios identified in the identity theft risk assessment.

2.11 OPERATIONAL BULLETINS

IDnow sets up operational bulletins and includes, since the last operational bulletin, at least the following:

- The operational indicators of the service (refer to section 2.12).
- A review of complaints received, in progress and closed.
- A review of security incidents relating to the security of IT systems.
- A review of security incidents notified to the ANSSI.
- The date of the last execution of the test plan for the effective capability of the RIV service to detect identity theft attempts.
- The False Negative Rate (FNR) and False Positive Rate (FPR) for the verification of the authenticity of the ID document measured at the last execution of the test plan of the effective capability of the service to detect identity theft attempts.

- The False Negative Rate (FNR) and False Positive Rate (FPR) for the comparison of the Subscriber's face measured during the last execution of the test plan of the service's effective ability to detect identity theft attempts.
- The False Negative Rate (FNR) and False Positive Rate (FPR) for live detection measured during the last execution of the test plan of the effective ability of the service to detect identity theft attempts.
- A review of any changes made to:
    - The information system of the RIV service.
    - To the assessment of risks relating to identity theft, particularly if the list of risk scenarios has been modified.
    - The assessment of risks relating to the security of information systems, particularly if the list of risk scenarios has been modified.
    - The Risk Treatment Plan.
    - The RIV policy.
    - The RIV practice statement.
    - The IDnow security policy
    - The test plan for testing the effective ability of the service to detect identity theft attempts.

IDnow transmits to the Customer, at the frequency defined in the Contract with the Customer, the operational bulletins relating to the remote identity verification service.

IDnow ensures the confidentiality of the operational bulletins.

2.12 RIV SERVICE CONTRACT AND SLA

IDnow and Customer must establish a contract to allow Customer to use the RIV service that contains the required information set in PVID standard (§ IV.7.2 of this standard).

The contract describes:

- the organization, scope, and objectives of the remote identity verification service as well as the technical and organizational means.
- the procedures for updating the remote identity verification policy and, where applicable, the procedures for validation of these changes by the Customer.
- whether remote access is allowed.
- that this policy is appended to the contract.
- a point of contact for the Customer.
- location of the processing and storage of Remote Identity Verification Service data for this Customer, including User Data.
- that IDnow shall notify the Customer of any breach of the contract.
- that IDnow shall notify the Customer in the event of a security incident detected on the Remote Identity Verification Service information system.
- the manner and maximum time period for transmitting the information regarding the security incident to the Customer.
- that IDnow shall only perform actions that are strictly in line with the objectives of the service.

- that the Customer must records a complaint for all remote identity checks for which the service provider has pronounced a "success" verdict and the client suspects or has detected identity theft.
- That the Customer fulfils all the legal obligations necessary for the service and those relating to the collection, processing and transfer of personal data and biometric processing. The contract must specify the purposes of such collection, processing and transfer and identify the applicable regulatory framework.
- the responsibilities and measures taken respectively by IDnow and the Customer to reduce the potential risks related to the service, those relating to identity theft and the collection and processing of personal data.
- that IDnow has professional insurance covering any damage caused to the business service and to its information system in the course of providing the service, specify the insurance coverage and include the insurance certificate.
- the measures implemented by IDnow under its business discontinuation plan.
- that IDnow only collects and processes data that are adequate, relevant, and limited to what is necessary for the purposes for which they are processed.
- that IDnow does not disclose any User Data to third parties, except with the express written consent of the Customer, and in accordance with the GDPR.
- the clauses relating to IDnow's ethics and include IDnow's code of conduct.
- the modalities of access, storage, transport, reproduction, destruction, and restitution of the data relating to this sponsor, in particular those relating to users.
- that only the French version is authentic, particularly in the event of litigation.
- the technical and organizational means implemented by IDnow to ensure compliance with applicable laws and regulations, those relating to the GDPR.
- any specific legal and regulatory requirements to which the customer is subject, those related to its sector of activity.
- that the legislation applicable to the contract is French law.
- that IDnow may, if necessary, subcontract all or part of the service to another provider, hereinafter referred to as the "subcontractor", provided that all the conditions set out below are met:
    - there is a service agreement between IDnow and the subcontractor;
    - the use of subcontracting is known and formally accepted in writing by the Customer;
    - the subcontractor complies with the requirements of these standards.
- the deliverables expected as part of the service, the ownership rules and sensitivity levels relating to these deliverables, as well as the associated terms and conditions of protection.
- that the deliverables of the service shall be in the French language unless the Customer formally requests otherwise in writing.
- operational indicators to measure the level of service provided.
- the frequency at which IDnow transmits operational bulletins to the Customer.
- that IDnow defines and implements a process for continuous improvement of the efficiency of the remote identity verification service based in particular on operational indicators.
- identify the operational time slots for the remote identity verification service.
- that the service must perform mutual authentication with the business service when transmitting results to it, and guarantee the integrity, confidentiality and impossibility of replaying transmitted data.

IDnow will not provide any service until the contract has been formally approved in writing by the Customer. The contract is written in French. A courtesy translation of the contract is provided if requested by the Customer.

IDnow develops and implements a process for capitalizing on detected incidents and fraud in order to continuously improve the effectiveness of its RIV service. IDnow defines with the Customer the operational indicators of the RIV service. IDnow develops and maintains an indicator measurement process describing, for each of the operational indicators defined for the Customer, the methods and means used to measure the indicator.

As a minimum, IDnow puts in place the means to measure the following operational indicators:

- The average, minimum and maximum waiting time for Subscribers.
- The number of remote identity checks performed.
- The number of remote identity checks by verdict (Success or failure).
- The number of remote identity checks for which the service issued a "failure" verdict, according to the reason for the failure.
- The number of remote identity checks for which the service issued a 'failure' verdict on the reason that identity theft was suspected or proven, according to the nature of the identity theft attempt.
- The number of remote identity checks for which the service issued a "success" verdict, and which turned out to be identity theft after the fact, depending on whether the identity theft was detected by the service provider or by the Customer.
- The number of claims received, in process or closed.
- The average, minimum and maximum time taken to close claims.

3. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

3.1. PHYSICAL CONTROLS

Physical controls have been implemented for the locations, which are used to process and store the personal data of the enrollment process in order to prevent unauthorized access to such facilities: The identification center and the data center.

IDnow draws up and maintain a list of persons authorized to access the premises hosting the information system of the RIV service. IDnow implements mechanisms to log access to the premises hosting the information system of the RIV service.

IDnow defines and implements measures to ensure the confidentiality and integrity of access logs to the premises hosting the RIV service.

The following measures (see IDnow Identification Center Infrastructure Policy, chapter3) have been implemented for the identification center:

- Closed windows and doors
- Physical access restriction, authentication only by chip + pin
- Records of access by door to the identification center
- Video surveillance
- Supervision or monitoring of third parties
- Control of ident center access

In addition, IDnow uses several separate ident center locations to minimize the impact of water and fire exposure. No data is permanently stored at the identification centers.

IDnow uses a sub supplier for the operation of the datacenter. It provides the hardware, racks, grid connection, electricity, and climate control for the operation of the servers. IDnow takes over the operation including the operating-system level upwards.

The following measures (see Data Center Infrastructure Policy, chapter 3) have been implemented for the data center:

- Closed windows and doors
- Fire / Water controls
- Redundant connections / power supplies
- Door access records
- Danger alarm system
- Video surveillance
- Perimeter protection / porter cabins
- Supervision or monitoring of third parties
- Control of datacenter access
- Control tours
- Secure destruction / disposal

In addition, all data at the data center is backed up to an off-site location.

IDnow operates an asset management and classification system in which all relevant systems are recorded and categorized based on their required level of security. The IT security manager is responsible for this and checks the asset management twice a year.

It is ensured that the physical controls are in place to protect assets in accordance with their classification.

3.2. PROCEDURAL CONTROLS

IDnow has implemented a role concept that ensures that the relevant tasks are separated in such a way to ensure effective controls. Personnel in a trusted role is named and accepted by the management. The person to fulfil the role also has to accept it. Evidence is documented accordingly. For each trusted role, responsibilities are defined in the respective job descriptions. Data access is only granted to employees with the respective roles after the necessary checks are completed. Such rights are only granted if the specific role was assigned with a task which requires such data access in accordance with the least privileges' principle.

A segregation of conflicting duties and areas of responsibility is implemented.

Details can be found in chapter 5 "Role concept" in the "IDnow Security Policy".

3.3. PERSONNEL CONTROLS

IDnow ensures that the agents reviewing the enrolment process possess the necessary qualifications and skills. This is implemented by conducting a multi-day training after the recruitment and before deployment in production operations. IDnow provides a detailed training plan in which all initial training and recurrent training is listed. The training plan also includes training on new threats and current security practices which is done at least every 12 months. The documentation of the training takes place in the HR management system and in a fireproof safe. The responsibility for carrying out the training rests with the team lead of the identification center and the HR Manager.

The reliability of the employee is determined by IDnow by requiring all relevant documents (in particular police clearance certificate, credit worthiness information and CV) of that employee. In the examination of the police clearance certificate every entry of the employee in the certificate must be checked separately by the HR Manager and the IT security officer and approved or rejected and, if no entry should exist, no separate authorization is required. If a country does not have one of the mechanisms listed above (e.g., no credit worthiness information), IDnow shall use other measures with an equivalent level of assurance regarding the reliability of the employee. These checks must be carried out prior to recruitment and reviewed regularly (the period between two reviews must not exceed three years). The Operators and fraud specialists must be contractually bound to IDnow.

IDnow, after recruitment, makes the operators and fraud specialists aware of the specific risks related to their function, and inform them of their obligation of discretion.

IDnow employs a sufficient number of Operators and fraud specialists performing the tasks and having the skills identified in Annex 2 of ANSSI PVID standard to fully perform all aspects of the RIV service.

IDnow provides the Operators and the fraud specialists with all the educational and technical material enabling them to carry out the missions entrusted to them.

IDnow elaborates and implements a regular training plan for the Operators and the fraud specialists in accordance with the missions and competences identified in Annex 2 of ANSSI PVID standard.

IDnow develops and implements a regular control plan to verify that the Operators and fraud specialists have the competences identified in Annex 2 of ANSSI PVID standard.

IDnow ensures that each Operator and fraud specialist, prior to the performance of the service, has followed the training plan and passed the control plan.

IDnow ensures that all personal with trusted roles relating to the RA operations are free from conflicting interests that might prejudice the impartiality of the operations. The HR manager is responsible for disciplinary sanctions (including up to termination of contract) if personnel violate IDnow policies or procedure. This is also the case for employees of third parties IDnow outsources to. Employees with trusted roles of those parties must fulfill the same requirements as internal employees with regard to trustworthiness.

IDnow uses a review process to detect incorrect identifications and to check if the identification policies and procedures have been adhered. Additionally, IDnow conducts test identifications for quality control. Goal of these test identifications is to check of all procedures are followed. These test identifications are done at least yearly. Responsible is the team lead identification center.

The details regarding the personal controls can be found in in the “IDnow HR Policy”.

3.3.1 INDEPENDENT CONTRACTOR REQUIREMENTS

IDnow uses a sub supplier for the housing of the server hardware. It provides the hardware, racks, grid connection, electricity, and climate control for the operation of the servers. IDnow takes over the operation including the operating-system level upwards.

IDnow either stores the RIV proof files itself or uses a sub supplier for the long term archival of the RIV proof files.

IDnow uses both internal identification centers as well as sub suppliers for external identification centers.

3.3.2. DOCUMENTATION SUPPLIED TO PERSONNEL

IDnow makes available to their personnel the present RIVP and the corresponding RIVPS, and any relevant statutes and policies. Other technical, operational, and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided to enable the trusted personnel to perform their duties.

3.3.3 ETHICS CODE

IDnow has a code of ethics which is integrated into the internal rules and regulations and which stipulates in particular that:

- Services are provided with loyalty, discretion, and impartiality.
- Staff only use methods, tools and techniques validated by the service provider.
- Staff undertake not to divulge any information to a third party, even anonymized and decontextualized, obtained or generated within the framework of the RIV service, unless formally authorized in writing by the Customer.
- The staff undertake to inform the service provider of any illicit content discovered during the RIV service.
- Staff undertake to comply with the national laws and regulations in force and with good practice in relation to their activities.

IDnow has all its staff signing the ethics code provided for in requirement described above before carrying out the service.

IDnow ensures compliance with the code of ethics and provides for disciplinary action against Operators, Administrators and fraud specialist of the verification service who have breached the security rules or the code of ethics.

3.4. AUDIT LOGGING PROCEDURES

Audit log files are generated by IDnow for all events related to security and RIV services. Where possible, security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits. The logs contain also the following information:

- start-up and shutdown of the logging functions; and
- availability and utilization of needed services with the RA network; and
- system start-up and shutdown; and
- system crashes and hardware failures; and
- firewall and router activities

IDnow operates external logging and monitoring which is protected against unauthorized access. Logging is controlled regularly for critical or personal data. The logs and monitoring are regularly checked for discrepancies. A system administrator checks the logs in the case of a security incident.

IDnow performs itself internal security audits of all systems and networks to find vulnerabilities. This is done at least twice a year. The IT security officer is responsible.

Any alteration, deletion, or copying of data is logged with the help of log files through the IDnow software so that alterations in personal data are always traceable. The allocation to the appropriate employee and client accounts is guaranteed at all times.

In addition, it is ensured that IDnow logs the following events:

- Physical facility access
- Changes to trusted roles
- Backup management
- Log management

- Date, time, phone number used, persons spoken to, and end results of verification processes
- Acceptance and rejection of certificate requests
- IT and network management, as they pertain to the RA systems
- Security management

In addition to that, IDnow records all the following information:

- The RIV proof and RIV R as described in section 2 above.
- By all automated processing and actions carried out by operators and fraud specialists as part of a remote identity check and centralize them on a component of the service's information system to which operators and fraud specialists have no access.
- All actions carried out by Operators and fraud specialists are available for audit purposes.
- The list of all RA Operator that are authorized to enroll and manage subscribers.

IDnow correlates logs between the different components of the RIV service information system.

IDnow performs a sample review of the logs, including the operations performed by the Operators and the fraud referents.

3.5. RECORDS ARCHIVAL

The long-term storage ensures that,

- All media used for archiving are protected against damage and unauthorized access
- Media is available for the required lifetime
- All media are properly disposed at the end of its lifetime

Details about the process like results of performed checks, involved employees and applications used are archived by IDnow. These procedures apply to all personal data.

The duration that the RIV proof is kept takes into account the length of time during which litigation may occur. The storage duration is defined in each contract for each Customer according to the needs of each Customer. The process of destruction of the data is defined in the appropriate policy. Access to the data as required by the GDPR is provided according to the law. If data needs to be rectified, the identification has to be repeated.

The results of the identification (“success” or “failure”), the time of the identification are kept without time limit.

Immediately after the RIV proof is generated, IDnow encrypts it.

3.6. DISASTER RECOVERY

IDnow regularly conducts risk analysis to identify any risk and countermeasures in the business and processes which covers assets relevant for the RIV services. Taking into account the risk assessment results, IDnow selects appropriate technical or organizational risk treatment measures to be implemented. Risks are regularly reviewed and revised. The management board is responsible for approving the risk assessment and the acceptance of residual risks. In addition, IDnow has defined an incident management process.

IDnow ensures that all necessary data for the RIV operations, essential information and software are backed up and stored in a safe place, more than 5km from the primary site, suitable to allow IDnow to timely go back to operations in case of incident/disasters.

Back-up arrangements are regularly tested to ensure that they meet the requirements of business continuity plans and are performed by the relevant trusted roles.

IDnow maintains a business continuity plan (BCP) which list the applicable risks, remediation measures and acceptable recovery times. A key part of the BCP is also how to avoid repetition of the cause that triggered the BCP.

IDnow develops and implements a backup and recovery plan for the RIV service devices, including as a minimum: system, configuration, and data backup.

IDnow defines and implement measures to ensure the confidentiality and integrity of backups to the same level as that for which the RIV service has been approved.

IDnow tests the backup and recovery plan at least once a year.

Details can be found in the “IDnow Security Policy”, chapter 9.2, “IDnow Incident Management” and “IDnow Risk Assessment AutoIdent Qualified Electronic Signature”, chapter 7.3 “Residual Risks”.

3.6.1. INCIDENT AND COMPROMISE HANDLING PROCEDURES

Incidents are submitted via the contacts defined in the present RIVP and processed in the context of service management. For any vulnerability, given the potential impact, IDnow either creates and implement a plan to mitigate the vulnerability; or documents the factual basis for the determination that the vulnerability does not require remediation. Critical vulnerabilities are addressed within 48 hours after its discovery.

IDnow will inform without undue delay but in any event within 24 hours after having become aware of it, the Supervisory Body and, where applicable, other relevant bodies of any breach of security or loss of integrity that has a significant impact on the Trust Service provided. The IT Security Officer is responsible for this process as part of his/her overall responsibility for security.

IDnow will also inform natural persons in case a breach of security or loss of integrity is likely to adversely them without undue delay.

ANSSI is alerted by IDnow Security Officer in 24H00 after knowledge of the major incident affecting the security of the RIV service or personal data according ANSSI procedure.

3.7. TERMINATION

At the moment when IDnow notifies the discontinuation of its RIV services, IDnow will:

- Promptly inform the ANSSI and Customers and implement decommissioning activities on the basis of the contract concluded with the Customer and ANSSI.
- Return or destroy all keys, API keys etc. existing and received privately up to the cessation of operations excepts the keys used to encrypt the RIV proof.

- Authorize the German customers to keep the RIV proof file and follow instructions gave by ANSSI about the RIV Proof records.
- Protect the RIV proof with same level of security as described in the present RIV policy waiting their transfer according to the plan agreed with ANSSI.
- Stop sending RIVR to the Business service, and
- Inform business partners, as far as they are affected by the closure of the business area.

IDnow aims to reduce potential disruptions as a result of the cessation of the RIV services. IDnow has an internal up-to-date termination plan.

IDnow has arrangements to cover the costs to fulfil these minimum requirements in case the IDnow goes bankrupt, or for other reasons, is unable to cover the costs by itself.

4. TECHNICAL SECURITY CONTROLS

4.1. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING

The key used to encrypt RIV proof data, and the result is protected by an HSM that is certified FIPS 140-2 level 3 or EAL 4+ CC. HSM is configured by IDnow authorized person in a trusted role only. The HSM uses a schema MofN, requesting at least 2 distinct persons in trusted role from IDnow, to protect the access to key used in the HSM and to restore the backup of key inside an SHM configured with same secret as the initial one. Only authorized technical process can use the key in production.

4.2. IT SECURITY CONTROLS

IDnow applies all the rules of the standard level of the ANSSI computer hygiene guide [HYGIENE] to the information system of the RIV service.

4.2.1. SPECIFIC IT SECURITY TECHNICAL REQUIREMENTS

User management is performed for all data processing systems which require protection. The user management is carried out using personal accounts only. No impersonal collection accounts are used.

The general guidelines for creating passwords (such as minimum length and password complexity) are the basis of the password policy. All employees are informed about the proper handling of passwords and have signed an appropriate guideline.

There is a defined timeout for sessions.

The consciousness of security of their work environment is refreshed for all employees in regular security awareness trainings.

Only system administrators can access the server system and always through encrypted connections. All accesses are personalized and protected by passwords + 2-factor authentication.

Security requirements shall be analyzed during the design and requirements specification stage of system development projects to ensure that security is built into IT systems.

Network components are in locked racks to secure them physically. The networks used for the identification services are logically separated from other components to prevent unauthorized access. Firewalls protect those networks from attacks and unauthorized access. The configuration and hardening measures of those components is regularly reviewed.

Administrative accounts are used for administrative purposes only.

Human Resources management issues with the respective superiors the appropriate rights which are specified according to the HR processes. The rights are then reviewed by the IT security officer. When leaving the company, the withdrawal of access rights takes place within maximum 24 hours.

Details can be found in the “IDnow Security Policy”, chapter 7.

4.2.2 LIFE CYCLE TECHNICAL CONTROLS

The requirements of this section apply to all software that contributes to the processing of Identification data (face and ID document) acquisition and verification in RIV, the creation of the RIV proof file and the submission of RIVR to the business unit.

The R&D department of IDnow regularly develops and tests new countermeasures against attacks. In addition, IDnow has processes in place to ensure that information about undetected fraud cases is received from customers, users, or law enforcement. Details can be found in the IDnow Quality Management Policy.

The software should be subject to regular code reviews.

The software should be tested for non-regression before a new version is released.

The software must be subject to a documented release path for each version to be released.

The software must generate suitable record logs for correlating records between different processes in the department.

The software developer must be aware of the specific risks related to the field of identity verification and be bound by an obligation of discretion.

The software development must be carried out in conditions that allow a record of the actions of each developer and consultation for audit purposes.

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

4.2.3 ACCESS TO PRODUCTION

Administrator and Operator uses only 2 FA and VPN to have access remotely to RIV service. Administrators and Operators are authenticated with a minimum of two factors on their nomadic workstations. IDnow restricts the access of Operators to the information system of the RIV service to that which is strictly necessary for the performance of their tasks.

The workstations of Administrators, Operators and fraud referents are connected exclusively to the information system of the RIV service.

If access to the Internet or other information systems (e.g., the provider's internal information system) is required, Administrators and Operators shall have a separate workstation deployed in an area external to the RIV service information system.

IDnow sets up a dedicated gateway for remote access of Administrator and Operator in accordance with [NT_ADMIN].

The mobile stations used by Administrators and Operators are dedicated to RIV services.

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

Mobile workstations only allow the use of removable media authorized by the IDnow security policy.

Mobile workstations have all their disks encrypted with cryptographic mechanisms that comply with [CRYPTO_B1].

IDnow, for each recommendation in the [NOMADISM] guide, identifies in RIVPS whether or not it complies with the recommendation. For each recommendation that IDnow claims to comply with, the IDnow describes the measures put in place to comply with the recommendation. For each recommendation that IDnow states that it does not comply with, IDnow provides a justification in the RIVPS.

The mobile workstations are configured so that they can only communicate with the remote access gateway via an encrypted and authenticated IPsec connection (full tunneling).

Any secret information exchanged in authentication protocols are cryptographically protected in transit. Two or more credentials implementing different authentication factors are used (e.g., something you have combined with something you know).

4.3. NETWORK SECURITY CONTROLS

The connection to the Business Service is made over TLS and Business service and RIV services are mutually authenticated.

IDnow develops and maintains a detailed description of the information system architecture of the RIV service. The information system is dedicated exclusively to the remote identity verification service and all other services are performed on an information system that is physically separated from the service's information system.

IDnow develops and maintains the RIV service flow matrix and associated filtering policy, which allow only those flows that are strictly necessary for the operation of the RIV service. IDnow identifies in the detailed description of the RIV service information system architecture all interconnections of the RIV service information system with third party information systems, including the Business service information system. IDnow filters all flows at the remote identity verification service information system interconnections.

All systems use virus scanners that run automatically in the background and are also automatically updated.

IDnow uses security gateways (firewalls) or if necessary appropriate additional solutions such as application firewalls, next generation firewalls, etc. which, in turn, can perform (for example by portscans, etc.) intrusion prevention or intrusion detection.

Security checks, such as through vulnerability scans with subsequent evaluation, are carried out:

- at least once per quarter or
- if IDnow receives a request for a vulnerability scan from the CA or the CA/Browser Forum or
- after any system or network changes that the CA determines are significant.

The vulnerability scans will be conducted by a specialized external company.

In addition, IDnow performs penetration tests through an external specialized company:

- at least once per year or
- if IDnow receives a request for a penetration test from the CA or the CA/Browser Forum or
- after any system or network changes that the CA determines are significant.

All personal data that are sent between the identification center and the datacenter is encrypted through a VPN, and in addition TLS. The network for the processing of identification data is physically separated from the network of offices.

The transfer of the data to the client is always encrypted (TLS, SFTP, S/MIME, etc.).

The transfer of data between the user and IDnow during identification is also always encrypted (TLS, DTLS for video).

There is no physical shipment of data.

IDnow ensures the secure operation of all technical systems by "hardening". This includes in particular:

- Removal of unnecessary software/services
- Removal of unnecessary accounts
- Modifying the configuration in regards to security
- If necessary activation of security components
- Protection of network ports

Details can be seen in “IDnow Security Policy”, chapter 7.

4.4 TIME STAMPING

All systems have their time with a time zone reference against UTC synchronized through NTP at least daily.

5. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Prior to performing the role as RIV provider, an external auditor has to confirm the compliance with PVID standards from ANSSI.

RIV service can be used only after a first successful audit realized by external auditor accredited by ANSSI and the qualification from ANSSI. The audit is valid for 2 years, and every 2 years IDnow is audited by an external auditor accredited by ANSSI.

In addition to that, IDnow has an internal audit plan, to make a control of the entire scope of the RIV service to ensure that the IDnow security policy, the RIVP and the RIVPS are applied.

IDnow revises the control plan at least annually and in the event of structural changes to the information system of the RIV service, including changes to its hosting, infrastructure, and architecture, or in the event of structural changes to the IDnow risk assessment, the risk treatment plan, the IDnow security policy, the RIV policy or the RIV practice statement.

IDnow updates the risk treatment plan to incorporate the results of the controls. IDnow has the results of the controls formally validated by his management in writing.

In case of major findings discovered during internal audit made by the accredited auditor or by Customer as to fix it and an external audit will be conduct during the same year in order to check the findings.

The RIV Policy for OID-A and OID-V are covered by ANSSI audit according the ANSSI PVID standard.

6. OTHER BUSINESS AND LEGAL MATTERS

6.1. FINANCIAL RESPONSIBIBILITY

IDnow maintains sufficient financial resources and obtained appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

6.2. PRIVACY OF PERSONAL INFORMATION

IDnow has a privacy plan that is shown to the Subscriber at the start of the process and has to be confirmed by the subscriber. The privacy plan is according to the GDPR.

Subscriber can only have access to its personal data as listed in section 2.6. Subscriber can't have access to any other kind of data that have been subject to automated or manual processing or whose communication of which is likely to provide information on the nature of the checks carried out by the service and relating to the detection of identity theft.

Subscriber cannot request modification or deletion of the Personal data contained in the RIV proof as it is evidence required to be kept by IDnow as a qualified RIV provider and proof for Customer using the verified Subscriber's identity by IDnow acting as a RIV.

The Customer has to communicate to the Subscriber the duration of retention of the Subscriber's Personal data. Personal data contained in the RIV proof can only be deleted after the end of time of duration period defined by the Customer. Whatever the verdict (success or failure), the RIV proof (that contains all personal data listed in section 2, included the RIVR) are recorded by IDnow according to a retention period defined by Customer.

Only the OID-A uses an automated check but there is no automated verdict based on this automated check. The verdict is always given by an Operator.

All Identification data listed in section 2 above are collected and stored for; evidence purpose, verification of the Identity of the Subscriber and transmission of RIVR to a Customer, and in some cases transmission of RIV proof to some specific German customers, respecting the principle of minimization of data collected and retained according GDPR.

All data listed in section 2 above are not used in any biometric processing.

IDnow can optionally work in accordance with a commissioned data processing agreement with the Customer. The Customer is then the responsible entity in the sense of Art. 4 No. 7 GDPR. The subcontractor must observe the principles of proper data processing. The subcontractor must ensure the contractually agreed and legally prescribed information security measures, in particular compliance with the principles in Art. 5 I lit. f, 25 and 32 GDPR.

IDnow hosts and processes the personal data relating to the RIV service exclusively within the territory of a Member State of the European Union. Operator and Administrator and data center used to host and run the RIV service are only located in the territory of a Member State of the European Union.

In addition, IDnow has appointed a privacy officer.

Every new agent, newly recruited at IDnow, goes through privacy training during his period and takes an online test on data protection.

6.3. REPRESENTATIONS AND WARRANTIES

IDnow insures as RIV Provider that each subscriber has been identified and authenticated properly prior to transmit a RIVR whatever the verdict. Furthermore, IDnow is responsible for the correct performance and authorization of the RIV service. For this matter, IDnow uses a large array of automated checks which are performed by the IDnow software as well as further manual checks performed by a trained Operator.

Before entering in a RIV service, the Subscriber can review the terms and conditions regarding the use of the RIV service. Furthermore, the Subscriber has to accept such terms and conditions by clicking on a check box shown on the screen. The Subscriber can access the terms and conditions via IDnow's website.

IDnow ensures that data contained in the RIVR is complete and accurate. IDnow supports the audit teams and has to make any reasonable effort to complete an audit and to communicate the results.

In case of a loss, stolen or compromised Subscriber's Wallet, IDnow will notify the Subscriber. If the Customer notifies IDnow that a Subscriber's Wallet has been compromised, IDnow ensures that no Wallet function is being used by the Subscriber.

IDnow ensures that records concerning the operation of services will be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

6.4. LIMITATIONS OF LIABILITY

IDnow guarantees to have performed the RIV process and the transmission of the RIVR to the Customer according to level of risks for RIV service associated to Substantial level only.

IDnow is not liable regarding the suitability or the authenticity of operation realized by Customer issued under this RIV Policy based on the usage of the RIVR.

6.5. INDEMNITIES

IDnow makes no claims as to the suitability of operation realized by Customer issued under this RIV Policy based on the usage of the RIVR for any purpose whatsoever. Relying parties use the RIVR and operation based on RIVR at their own risk. IDnow has no obligation to make any payments regarding costs associated with the malfunction or misuse of RIVR issued under this RIV Policy.

6.6. DISPUTE RESOLUTION PROVISIONS

In the event of disputes, the parties shall come to an agreement taking into account any applicable laws, regulations, and agreements made.

IDnow provides the Customer, Subscriber and third parties with a process for registering and handling complaints about the RIV service. For all disputes arising from or in connection with the identification of the Subscriber, the registration authority IDnow GmbH can be contacted directly at support@mail.idnow.de. For all disputes arising from or in connection with the Customer or any Third Party, the Customer Success Team can be contacted at the email address provided during onboarding of the Customer.

6.7. GOVERNING LAW

French law shall apply.

6.8. MISCELLANEOUS PROVISIONS

IDnow operates its business in accordance with the German non-discriminatory law.

ANNEX 1: AUTHORIZED ID DOCUMENTS

Only the following identity documents shall be accepted under this standard, provided that they have the characteristics to meet the requirements set out in this standard:

a) For nationals of Member States of the European Union, 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 a 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 by 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 territory of the European Union, in a State party to the Agreement on the European Economic Area or in Switzerland, the passport, provided that the issuing country makes available the means necessary to verify the validity of the document. If the exemption from the visa requirement is accompanied by the requirement to have an e-passport, only the e-passport is recognized as an authoritative source for the country concerned.

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