Trust Services Policy & Practice Statement

for READID SaaS with SDK

Colophon

DATE	20-12-2022
VALID FROM	1-1-2023
VERSION	2.0
CONFIDENTIALITY	Public
STATUS	Published
COMPANY	Inverid (formerly InnoValor)
AUTHOR (S)	Bob Hulsebosch CCO CISSP

Synopsis

This Trust Services Policy and Trust Services Practice Statement (TSPS) describes Inverid's ReadID SaaS with SDK practices and procedures for remote identity establishment and verification as part of the practice of (qualified) trust service providers issuing and managing public key certificates.

Table of contents

inverid

Version history

Version	Modifications	Author	Approved by	Date
1.0	First version (internal)	Bob Hulsebosch		16-10-2020
1.1	Updated version (internal)	Bob Hulsebosch		9-11-2020
1.2	First published version	Bob Hulsebosch	CEO	24-11-2020
2.0	Updated version for new Inverid name and including minor changes in section 5.8 Termination	Bob Hulsebosch	CEO	20-12-2022

1 Introduction

The European eIDAS regulation 910/2014 regulates electronic identification and trust services for electronic transactions in the internal market. The eIDAS regulation:

- ensures that people and businesses can use their own national electronic identification schemes (eIDs) to access public services in other EU member states.
- creates an European internal market for trust services from Trust Service Providers (TSPs) that provide electronic signatures, electronic seals, time stamp, electronic delivery service and website authentication services; it does this by ensuring that they will work across borders and have the same legal status as traditional paper based processes.

For trust services provided by TSPs it is of paramount importance that the user's identity has been established and verified. ReadID acts as an identity data and document verification technology provider that enables (qualified) TSPs operating under eIDAS to provide their services.

This Trust Services Policy and Practice Statement (TSPS) therefor does not cover the whole set of practices that a TSP covers, but focusses on the relevant electronic identification parts that are provided by ReadID. In particular it focusses on the ReadID SaaS with SDK solution (ReadID SDK for short), that TSPs can integrate in their mobile app for remote identity data and identity document verification. During the certificate application process of a qualified certificate, ReadID enables the TSP to effectively and reliably establish the identity of the applicant.

The Trust Services Policy applicable to this TSPS is contained within the shaded text boxes in the appropriate clause spaces. Text inside the boxes is the policy; the text outside of the boxes is the detailed response of Inverid, as the TSPS.

Pursuant to the IETF RFC3647 this document is divided into nine parts. To preserve the outline specified by RFC3647, section headings that do not apply have the statement "Not applicable". Sections that describe actions specific to a single service contain only references to service-specific practice statements. If the subsections are omitted, a single reference applies to all of them.

1.1 OVERVIEW

The Trust Service Practice Statement MUST be structured in accordance with RFC 3647. The Certification Practice Statement MUST include all material required by RFC 3647.

This Trust Services Policy and Trust Services Practice Statement (TSPS) describes the practices and procedures that Inverid's ReadID SaaS with SDK employs to support (qualified) TSPs operating under eIDAS to provide their services.

It describes the practices that are necessary for achieving the required security level and that are approved by Inverid management. Inverid is ISO/IEC 27001: 2013 certified. The Statement of Applicability includes detailed description of security measures and covers all aspects.

The ReadID SaaS with SDK TSPS describes the practices, scoped to identity document reading and verification, that allow TPSs to provide Qualified Trust Services in conformity with the eIDAS regulation [eIDAS - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;], ETSI EN 319 401 General Policy Requirements for Trust Service Providers [ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers]. Particularly, ReadID covers essential parts of the identity verification and registration processes that the TSP shall implement for end-users applying for a qualified certificate.

Inverid's ReadID SaaS with SDK provides identity data and identity document verification functionality for (qualified) TSPs operating under eIDAS. The client-side is provided as an SDK. Using the ReadID SDK, TSPs can via their own mobile app collect and verify identity data of a user applying for a qualified certificate. It does that by reading identity information from the chip of government-issued identity documents via NFC and by providing identity information and identity document verification services. ReadID's SDK solution ensures that the identity information read is authentic. This means that the issuer of the data is known and the data has not been corrupted after its creation. Moreover, for chips that support this, it also verifies the authenticity of the chip, i.e. that it is not cloned. All processing is done on a secured ReadID server that is hosted on a public cloud. Access to the chip is based on the scanned MRZ information of the identity document, or alternatively can be manually entered by a user. ReadID MRZ enables the mobile application of the TSP to use the camera of the mobile device to scan the Machine Readable Zone of ICAO DOC 9303 compliant identity documents and ISO18013 compliant electronic driving licenses using Optical Character Recognition technology.

The ReadID Server is provided to the TSP as a SaaS solution, via a REST API and management portal. Inverid provides a management portal that allows TSPs to configure the ReadID Server as well as the configuration and customisation of the SDK. The portal also provides access to session information and technical documentation. Access to the portal is based on strong authentication. The ReadID Server is provided as a single or multi-tenant environment hosted by a public cloud provider. The security of the server, i.e. the public cloud provider, must meet the requirements eIDAS and ETSI poses on the TSP. Inverid is responsible for this and structurally monitors the cloud provider accordingly.

ReadID implements the reading and verification of the contactless chips in identity document that are ICAO 9303 compliant, such as electronic passports, identity cards and residence cards. The reading of the chip is done using the ReadID SDK, the verification and interpretation is done by ReadID SaaS server. Specifically, ReadID implements for ICAO 9303 compliant identity documents:

- the Basic Access Control security mechanism for getting access to the chip;
- the Password Authenticated Connection Establishment (PACE) security mechanism for getting access to the chip;
- the Passive Authentication security mechanism for verifying the authenticity of the read data;
- the Active Authentication security mechanism for verifying the authenticity of the chip (i.e. clone detection);
- the Chip Authentication (EAC-CA) security mechanism for verifying the authenticity of the chip (i.e. clone detection); and
- the reading and interpretation of DG1 with the MRZ information, DG2 with the face image, D7 with written signature (if present), DG11 with additional personal information (if present) and DG12 with additional document information (if present)

In addition, ReadID also implements the reading and verification of the contactless chip in ISO 18013 compliant electronic driver's licences. Specifically implemented for these documents are:

- the Basic Access Protection security mechanism;
- the Passive Authentication security mechanism;
- the Active Authentication security mechanism;
- the Chip Authentication (EAC-CA) security mechanism and
- the reading and interpretation of DG1 with the MRZ information, DG6 with the face image and DG11 with additional personal information.

Inverid provisions as part of the ReadID Server with reasonable efforts a list of country certificates that it considers trusted. This list is provided as-is, and it is the responsibility of the TSP to decide to trust or not trust these country certificates. New country certificates may be missing, or some countries may not provide their country certificates in a manner that Inverid can include them in a trusted manner. At request of the TSP Inverid provides information on the sources of the country certificates. The process of gathering the certificates may change at the discretion of Inverid. Any and all use of the list provided by Inverid is at all times for the TSP's own account and risk.

Besides the identity data and document verification functionality provided by ReadID SDK, the TSP may also need identity document holder verification. This proves that the applicant holding the identity document is indeed the rightful owner of the document. Identity document holder verification can be done via biometric (facial) identity verification in combination with liveness detection (Presentation Attack Detection). In this case the read face image of the chip will be matched against a selfie of a real user. This is done via a separate SDK, in combination with a server, that is provided by a so-called biometric verification provider. Depending on the orchestration model, the biometric verification provider can be a sub-contractor of Inverid or the TSP. In the first case, Inverid is responsible for the fact that the biometric verification provider's security measures meet the relevant eIDAS and ETSI requirements. Furthermore, Inverid structurally monitors if this is indeed the situation. In the latter case, this is the TSP's responsibility.

The operation and security details of the SDK of the biometric verification provider itself are out of scope for this TSPS. The focus is on the technical interfacing and contractual agreements with the biometric verification provider. The same holds for the TSP: only the technical and contractual interfaces between the TSP and ReadID are in scope. The TSP internal practices for issuing of qualified digital certificates and corresponding trust services are out of scope for this TSPS. Figure 1 below shows the scope of this TSPS.

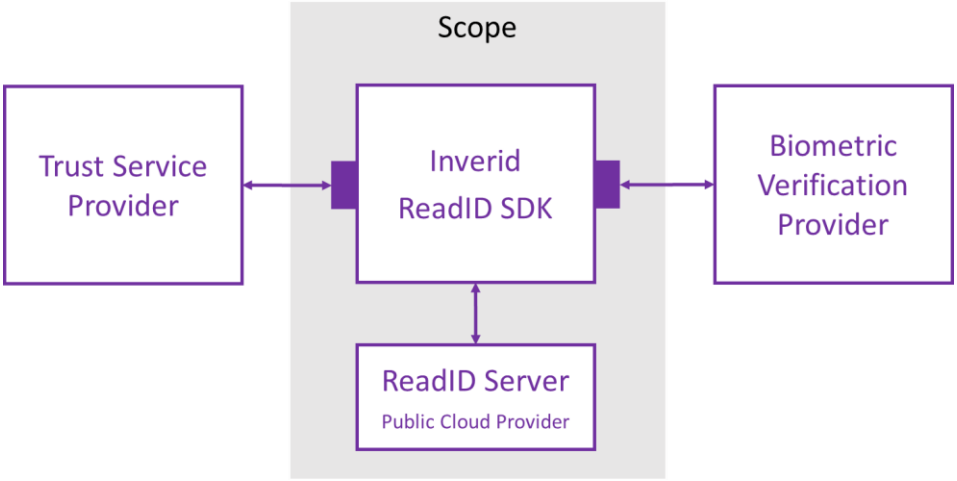
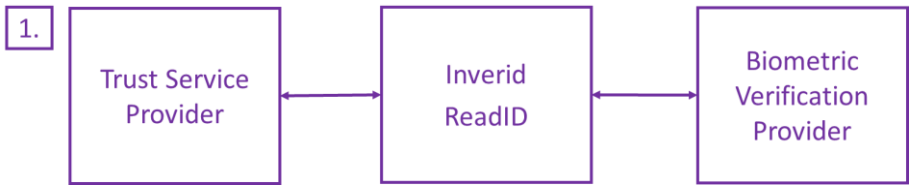


Figure 1: Scope of the TSPS.

For the TSP, various ways of orchestration with ReadID and the biometric verification provider are possible:

1. TSP does the orchestration: this means that the TSP has separate contracts and interfaces with ReadID and with the biometric verification provider.
2. ReadID does the orchestration: this means that the TSP has a single contract and interface with ReadID and that ReadID interfaces with the biometric verification provider as a sub-contractor. ReadID and the biometric verification provider have a separate bilateral contractual agreement that is aligned with that between ReadID and the TSP.
3. Hybrid orchestration of options 1 and 2: this means that the TSP has a bilateral contractual agreement with both ReadID and the biometric verification provider and only one interface with ReadID; the biometric verification provider has a technical interface with ReadID.

The various orchestration modus operandi are shown in Figure 2.



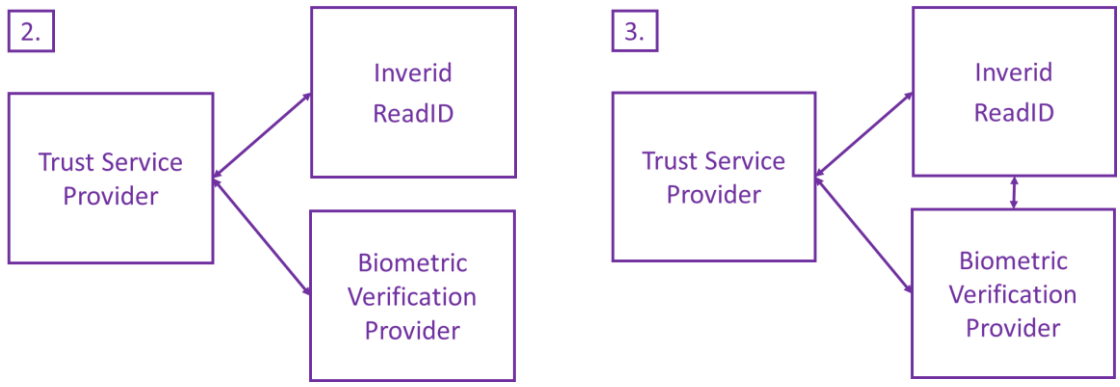


Figure 2: ReadID orchestration modus operandi.

ReadID thus supports the following two interfaces that are also relevant and in scope of this TSPS:

1. Between ReadID and TSP for the transfer of identity data and verification outcomes. Depending on the orchestration model these outcomes may include facial verification and liveness verification outcomes.
2. Between ReadID and the biometric verification provider for the transfer of face images and selfies and verification outcomes. Note that except for the face images no other identity data is shared with the biometric verification provider.

In case ReadID does the orchestration, the ReadID SaaS Server orchestrates with the facial matching service of the biometric verification provider, which means that the ReadID SaaS Server takes care of securely enrolling the face images to the facial matching service, and combining the answer (pass or fail) with the results of the chip reading and verification. This pass and fail combines both actual facial verification, i.e., if a selfie taken by the user matches the face image from the chip, and the result of a Presentation Attack Detection algorithm. Presentation Attack Detection is used to detect impersonation, replays and spoofing attempts, and is also sometimes referred to as liveness. Both the facial verification and Presentation Attack Detection may produce false rejects and false accepts.

Each orchestration model is contractually established. If Inverid does the orchestration, the template contract with the TSP also includes stipulations regarding biometric verification providers as sub-contractors. Specifically, as a sub-contractor of Inverid, biometric verification providers must abide by all the relevant requirements of this TSPS. This is to ensure that the requirements coming from the TSP will not only be transferred to Inverid but to the sub-contractor as well. Consequently, the template contract with biometric verification providers addresses aspects such as:

- Service and support;
- Duration and termination;
- Conformity and liability;
- Confidentiality and personal data including a Data Processing Agreement appendix;
- Service Level Agreements;
- Security measures including right to audit.

The biometric verification provider can have its own eIDAS module certification or will be audited separately during the audit of the TSP.

1.2 DOCUMENT NAME AND IDENTIFICATION

The CA has identified which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply. The CA makes available the CPs supported by the TSP to its user community.

This document is identified as: “Inverid ReadID SaaS for SDK Trust Services Policy and Practice Statement”

The Certificate Policies adopted by Inverid are aligned with the certificate policies defined in ETSI EN 319 411-1 and ETSI EN 319 411-2 and according to eIDAS Regulation (EU) No 910/2014. The scope of the policies relate to the issuance of qualified certificates for natural persons and Inverid’s role in this. Since Inverid is neither a CA or a TSP, it uses a subset of the above-mentioned policies.

1.3 PKI PARTICIPANTS

The following participants are relevant.

1.3.1 Trust service provider

A party that provides trust services under eIDAS regulation. A TSP is a customer of Inverid.

1.3.2 Certificate authorities

Entities that issue certificates.

1.3.3 Registration authorities

Entities that establish enrolment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a Certificate Authority.

1.3.4 Subscribers

Holders of certificates.

1.3.5 Relying parties

A relying party is anyone who acts trusting a certificate issued by a TSP.

1.3.6 Other participants

Inverid’s ReadID SDK provides remote identity document reading and verification services for TSPs during their CA/RA activities, i.e. enrolment, renewal and reactivation of electronic identities for digital certificates for natural persons. Inverid is ISO/IEC 27001 certified and scoped to digital identity services.

A **public cloud provider** is a sub-contractor of Inverid and hosts the ReadID Server that processes all identity document data and may orchestrate data exchanges. There is contractual agreement between the public cloud provider and Inverid. The ReadID server is provided as a SaaS. The ReadID SaaS environment is fully redundant, self-repairing and able to scale automatically to changing load. The organisational/contractual and technical security measures provided by the cloud provider meet the relevant requirements laid down by eIDAS and ETSI for TSPs. It is the responsibility of Inverid to control and monitor this. Consequently, security requirement in terms of certifications are set for the public cloud provider (for instance an ISO/IEC 27001 certification and a SOC2 report or similar).

Biometric Verification Provider is an organisation offering identity document holder verification services. It does that by providing biometric verification (i.e. facial verification) and liveness detection of the applicant or subscriber. The organisational and technical security measures provided by the biometric verification provider meet the relevant requirements laid down by eIDAS and ETSI for TSPs. Depending on the orchestration model this the responsibility of either Inverid or the TSP. In the first case the biometric verification provider is a sub-contractor of Inverid; in the latter case it is a sub-contractor of the TSP.

1.4 CERTIFICATE USAGE

Does not apply.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation administration

This ReadID TSPS is administered by Inverid B.V and its affiliate Inverid Software B.V.

Inverid B.V. and Inverid Software B.V.
Moutlaan 32

7523 MD Enschede
The Netherlands
Tel +31 53 4878178
Chamber of Commerce nr: 59467274 and 64870596

1.5.2 Contact person

The contact person for the TSPS is compliance officer Bob Hulsebosch (bob.hulsebosch@inverid.com).

1.5.3 Approval

This document is subject to a review at least once a year and is included in the internal audit schedule. Compliance of this document with RFC 3647, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, CA/B Forum Baseline Requirements, and eIDAS will be assessed, and any inconsistency remedied. Before publishing, this document is approved by ReadID management. This document will be published, and thus made available to all stakeholders involved after approval from ReadID management.

Amendments which do not change the meaning of trust services practice, such as corrections of misspellings, translation and updating of contact details, are documented in the versions and changes section of the present document and the fraction part of the document version number shall be incremented.

In the case of substantial changes, the new TSPS version is clearly distinguishable from the previous ones. The new version bears a serial number enlarged by one. The amended TSPS along with the enforcement date, which cannot be earlier than seven days after publication, is published electronically on ReadID's website.

ReadID has the right to publish a draft version of the TSPS prior to publishing the amended version. This allows stakeholders to provide feedback on the draft version. The amended version of the TSPS is published electronically on ReadID's website seven days before its enforcement.

This ReadID TSPS is approved and enforced by the ReadID Chief Executive Officer. ReadID ensures that the practices are properly implemented by conducting regular internal audits and conformity assessments.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Terminology

Applicant: New user that applies for a certificate.

Certificate Pinning: The process of associating a host with their expected X509 certificate or public key.

Datagroup: Digitally signed file on the chip of an identity document that contains personal or other (meta-) data.

Holder verification: the process of verifying if the holder of the identity document in indeed the rightful owner of the document.

Document verification: the process of verifying the authenticity of the chip of an identity document.

Identity data verification: The process of verifying the authenticity of the data read from the chip of an identity document.

Identity document: An official and government issued identity document such as passports, driving licenses, or identity cards.

Registration: The process of an applicant signing up and the subsequent verification of their identity.

Selfie: biometric data provided by the applicant for facial verification purposes. Examples of a selfie are one or more pictures or a short video of the applicant's face.

Software as a service (SaaS): A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted on a public cloud.

Subscriber: An Applicant who has been verified and been issued a certificate. Before the identity of the Subscriber is verified, a Subscriber is an applicant.

Trust service: An electronic service which is normally provided in return for remuneration and which consists of:

- the creation, verification, and validation of Electronic Signatures, electronic seals or electronic time-stamps, electronically registered delivery services and certificates related to these services or
- the creation, verification and validation of certificates for website authentication or
- the preservation of Electronic Signatures, seals or certificates related to these services.

Trust Service Provider: An entity that provides one or more electronic Trust Services.

Qualified Trust Service Provider: A trust service provider who provides one or more qualified trust services and is granted the qualified status by the Supervisory Body.

Supervisory Body: The authority which is designated by member state to carry out the supervisory activities over Trust Services and Trust Service Providers under eIDAS in the territory of that member state.

Biometric verification provider: the party that provides biometric matching and liveness detection services for holder verification purposes.

Public cloud provider: the party that provides cloud services via the internet.

1.6.2 Acronyms

API	Application Programming Interface
CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation List
DG	Datagroup
DMZ	Demilitarised Zone
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HSM	Hardware Security Modules
ISMS	Information Security Management System
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
RA	Registration Authority
SaaS	Software as a service
TSA	Time-Stamping Authority
TSP	Trust Service Provide
TSPS	Trust Service Poly / Trust Service Practice Statement
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time
NFC	Near Field Communication
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
eMRTD	electronic Machine Readable Travel Document
eDL	electronic Driving License
ICAO	International Civil Aviation Organization
eID	electronic Identity
(Q)TSP	(Qualified) Trust Service Provider
SDK	Software Development Kit
SLA	Service Level Agreement

2 Publication and Repository Responsibilities

2.1 REPOSITORIES

Inverid ReadID has an online repository, accessible through www.inverid.com or www.readid.com.

2.2 PUBLICATION OF INFORMATION

The CA SHALL publicly disclose its Trust Service Policy and/or Trust Service Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis.

Inverid provides public repositories for its TSPS and other important policy documents. The Inverid repository is located at the ReadID website (https://www.inverid.com).

The following read-only information is accessible in the online repository:

- this ReadID SaaS with SDK Trust Services Policy and Practice Statement
- Additional product information: https://www.inverid.com/papers-reports.

As a rule, the electronic repository is accessible at any time. In the case of (planned) maintenance or a calamity, accessibility can be interrupted for a maximum of several hours; ReadID aims to restore the website and/or repository as soon as possible in the event they become unavailable.

2.3 TIME AND FREQUENCY OF PUBLICATION

The CA develops, implements, enforces, and annually updates a Trust Service Practice Statement that describes in detail how the Trust Service Policy is implemented.

ReadID publishes updates of this information in the repository at least once per year or when significant changes are implemented.

2.4 ACCESS CONTROL ON REPOSITORIES

The CA provides all repository information and documentation in a read-only format.

The repository is protected against unauthorised changes. Only authorised employees of ReadID have writing/modifying/deleting permissions for the repository.

3 Identification and Authentication

This section describes the identification and authentication processes during initial registration and prolongation. It particularly focusses on remote identification services that are provided by ReadID in order to enable a TSP to issue qualified certificates.

NFC-based remote identity verification using ReadID SDK and face matching provides an alternative for physical verification at the TSP during registration. ReadID identity data and document verification is being done by reading the chip of government-issued identity documents such as passports, ID-cards, residence permits or driving licenses with a mobile app on a smartphone with NFC capabilities.

The contactless chip in passports and similar documents contains reliable personal data about the holder, including their full name, birthdate and nationality. This data has been provided by the issuing country, based on strict government identity verification processes. In addition, the chip contains a high-resolution photo, suitable for facial verification. Because this photo is of a higher quality than the photo printed in the identity document, using the photo from the chip can reduce look-alike fraud. The personal data and photo are digitally signed, so they cannot be altered without detection by ReadID.

For ICAO compliant documents this data is stored in various so-called datagroups. Datagroup 1 contains, similar to the MRZ, the full name and date of birth, datagroup 2 the face image, datagroup 7 a written signature, datagroup 11 non-mandatory personal attributes, datagroup 12 additional document details, datagroup 13 country specific data. Also, security-specific datagroups exist. The exact contents of the datagroups depend on country and can include personal number and nationality. For ISO18013 compliant documents such as driving licenses similar datagroups are processed.

Datagroup 1 and the security data groups are the minimum needed to provide the basic personal information on the identity document and to verify the authenticity of the document. If the ReadID SDK is used, then the TSP in the person of the app developer can decide to also send other datagroups to the ReadID server for further processing.

Optionally, ReadID may also process a photo of the datapage(s) of the identity document, the MRZ and/or scanned MRZ information. This is done to detect possible fraud, to analyse failures, if a photocopy is needed by the TSP, and/or to get data from the datapage that is not in the chip. The TSP in the person of the app developer decides if a photo of the MRZ and/or the scanned MRZ data is sent to the ReadID Server. The MRZ photo and scanned MRZ data do not provide additional personal data more than is in datagroup 1.

ReadID may orchestrate with a biometric verification provider that verifies if a selfie matches with the face image on the chip, and checks liveness (not present attacks). In this case, the NFC-read face image is shared via a secure communication channel with the biometric verification provider. The outcomes of the verification are returned to ReadID. Facial verification and liveness is done to establish if the holder is also the owner of the identity document, i.e. holder verification.

In case the TSP is responsible for the orchestration, ReadID only communicates the read identity and verification data directly to the TSP via a secure channel. It is up to the TSP to interpret the data for the continuation of the certificate registration and issuing process.

The retention period of all the data on the ReadID server is limited and conform GDPR. This also holds for the data processed by the biometric verification provider during holder verification. Moreover, as soon as the TSP has fetched the data from the ReadID server, the data will be removed.

Inverid provides a Management Portal that allows the TSP to view ReadID sessions, view an audit log of relevant events, view the current list of trusted country certificates, view billing information, and perform user and application (API key) management.

User management involves configuration of roles for developers, system admins, billing duties, etc. of the TSP that need access to the ReadID server. This is a responsibility of the main technical contact from the TSP. Each TSP has an account in the management portal.

Management of applications (and their API access keys) is a responsibility of the TSP as well. The per-application options are quite extensive but include at least which permissions are attached to the application (such as posting new sessions or viewing existing sessions), how long until the sessions expire, how the server should handle new sessions, which identity documents are allowed, which Country Signing Certificates are accepted, and how to orchestrate with a biometric verification provider.

The ReadID server contains an audit log that captures relevant security events in each of the following categories:

- Users logging in and out to the management portal;
- ReadID sessions being created, accessed or deleted;
- User management like creating, deleting changing permissions, performing password reset;
- Application management like creating, deleting or changing settings;
- ReadID administrators making changes to the list of trusted certificates;
- Other configuration changes.

For all events, the following is captured: timestamp, actor (that is an application, user or 'system'), affected object and a description of the change if applicable.

The audit log can be viewed from the management portal. It is possible for a TSP to setup one or more email addresses to receive notifications on when relevant ReadID configuration changes. Except for the Inverid administrator, only TSP-users have access to the management portal.

The portal also provides access to session information and technical documentation. Access to the portal is based on strong authentication and uses role based access controls.

3.1 NAMING

ReadID recognises and interprets names as obtained from the legal identity documents.

Note that the use of diacritical characters in the MRZ and datagroup 1 is not permitted. For such characters, datagroup 11 may be consulted, but the use of this datagroup is not mandatory.

3.1.1 Type of Names

See above for the types of names used by ReadID.

3.1.2 Need for Names to be Meaningful

The names are meaningful, unambiguous, and unique and allow the TSP to create/compile a Distinguished Name for a certificate that enables any relying party to identify the subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

The interpreters are used for translating ICAO and ISO 18013 level Logical Data Structure (LDS) data types to the Inverid data model. This data is shared with the TSP.

In principle ReadID uses the names obtained from the MRZ. These are validated against the names obtained from the datagroups on the chip. Checks are done on the full length of the name and the existence of diacritics. If that is the case, names extracted from the datagroups are used.

3.1.5 Uniqueness of Names

No stipulation.

3.1.6 Recognition, Authentication and Role of Trademarks

No stipulation.

3.2 INITIAL IDENTITY VALIDATION

An Issuer CA may use any legal means of investigation to determine the identity of an organisational or individual Applicant.

With the exception of sections 3.2.2.4 and 3.2.2.5, the CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfils all of the requirements of Section 3.2.

Before explaining the ReadID identity data and document verification process in more detail, it is important to understand the security features that are present in electronic identity documents:

- Privacy – protect the privacy of the document holder by implementing access control and preventing eavesdropping.
- Authenticity – ensure that the contents of the chip is not forged or manipulated.
- Clone detection – detect if the chip is original or a copy.

The first of these features is to protect the holder of the identity document from unwillingly sharing the contents of the chip of his identity document, while the other features are to protect the reader of the identity document against fraudulent documents. The ReadID website contains a series of blogposts on these security mechanisms with more details.

When an applicant applies for an electronic identification means or qualified certificate at a TSP, the ReadID part in this process is as follows:

1. The TSP informs the applicant about the terms and conditions and the applicant expresses his/her will to enrol for a qualified certificate. Note that this is done by the TSP, not Inverid.
2. The applicant is asked to register. The registration is done via the mobile app of TSP that contains the ReadID SDK.
3. The personal data from the identity document can now be retrieved by ReadID. By scanning the MRZ with optical character recognition (OCR) technology, information is gathered which is used for unlocking the NFC chip of the identity document. This is called Basic Access Control (BAC). The relevant datagroups are subsequently read from the chip. The datagroups contain data such as first name, surname, gender, nationality, date of birth, personal number (optional), high resolution photo, and other identity document related data such as expiry date and document type.
4. After the NFC chip has been read, the personal information is sent to the ReadID Server for verification. The server performs the following verifications:
    - Verification of read datagroups is performed by the server by cryptographically validating a digital signature over the files read from the identity document and checking against a list of trusted country certificates of document signers, i.e. Passive Authentication. This certificate list effectively determines which documents will be marked as valid. It is maintained by ReadID. Moreover, it can depend on the specific TSP what sources of trusted certificates are used. What certificate was actually used is communicated to the TSP as well, i.e., it is transparent to the TSP. Passive Authentication is always based on the principle of digital signatures and uses a ‘chain of trust’. A country that issues an identity document constitutes a Country Signing Certificate Authority (CSCA), and issues one or more Country Signing Certificates. A Country Signing Certificate is used to cryptographically sign Document Signing Certificates, which in turn can be used to sign the contents of an identity document. Consequently, the contents of a document may be considered authentic if signed using a Document Signing Certificate, which in turn has been signed by a trusted Country Signing Certificate.
    - Whether all datagroups (that were actually read and submitted to the server for verification) indeed hash to the same value as reported in the Security Object of the chip.
    - Whether a chain can be established from the document signer to a trust anchor.
    - Verification of the chip not being a clone, i.e. whether the chip returned a correct response to the challenge during execution of the Active or Chip Authentication protocol. The ReadID server

verifies the challenge-response pairs for active and chip authentication received from the ReadID client. Note that not all identity documents support clone detection.

5. This step is optional and involves the utilisation of biometrics via a biometric verification provider. Depending on the orchestration model, the high resolution photo retrieved from the chip with NFC technology is shared with the TSP or with the biometric verification provider via a secure channel. The biometric verification provider verifies if the photo matches with a live image ('selfie') or stills from a video stream of the applicant. Liveness or presentation attack detection must be part of this facial verification process. It verifies if the applicant is indeed the holder of the identity document that is presented and read by ReadID. The facial verification is done via an SDK that is part of the mobile app of the TSP.
6. Finally, there is the closure of the flow. The applicant closes the app and the session is finished. Then, the ReadID server will send a notification to a server of the TSP. Their server can then get the actual outcomes from the ReadID Server.

The overall outcome of the ReadID efforts contains:

- Personal and document data of the applicant as obtained from the chip of the identity document:
  - Name, date of birth, gender, document number, face image, etc.
- Verification checks on the authenticity of the read identity data and the chip of the document:
  - Signature and hash validations and clone detection.
- Holder verification outcomes (in case Inverid does the orchestration).

These data and verification results are made available to the TSP through a backend secured communication channel and management portal. Optionally, (parts of) the interpreted data or verification results may be returned to the mobile client for presentation. The ReadID server only caches the identity document details until it has been fully processed by the TSP; the TSP controls how long this caching is. The TSP can utilize the date of expiry obtained from datagroup 1 of the chip to check if the document is not expired.

Alternatively, the TSP may choose to contract and interface with its own biometric verification provider. This means that the TSP has to do the orchestration of data exchanges with ReadID and the biometric verification provider itself to come to the required identity validation outcome.

3.2.1 Method to prove possession of private key

Not applicable.

3.2.2 Authentication of organization identity

Not applicable.

3.2.3 Authentication of individual identity

The CA will verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type).

ReadID performs the following verifications when a natural person applies for a qualified certificate:

- Verifying the authenticity of the presented applicant's identity document.
- Reading and verifying the applicant's personal data from chip of the presented identity document. This data includes full name, date of birth, a unique identifier, document expiry date, document number, nationality (except for electronic driving licenses), gender, and a facial image.

Depending on the orchestration model, ReadID may via a sub-contracted biometric verification provider:

- perform liveness detection of the applicant's facial image, and
- match the applicant's facial image captured in the liveness session during registration with the image read from the chip on the presented identity document.

3.2.4 Non-verified subscriber information

ReadID only verifies information obtained from identity documents. It does not verify any other information that might be needed for user registration by the TSP, such as mobile phone number, address, email address or IP-address.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

The RA SHALL implement identification and authentication procedure that provide reasonable assurance that the requestor of the re-key request is the Subscriber or an authorised representative of the Subscriber acting on behalf of the Subscriber.

TSPs that support re-key requests may make use of the identification features described in section 3.2.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

The RA SHALL implement identification and authentication procedure that provide reasonable assurance that the requestor of the revocation is the Subscriber or an authorised representative of the Subscriber acting on behalf of the Subscriber.

For revocation requests the TSP may make use of the identification features described in section 3.2.

4 Certificate life-cycle operation requirements

4.1 CERTIFICATE APPLICATION

The Subject SHALL register with an RA either prior to, or at the time of, applying for a Certificate. 3.2 defines necessary requirements for identification and authentication.

The Subject SHALL accept the terms and conditions regarding the use of certificates including to the storing of records by the CA of data used in the registration.

For certificate application with ReadID, the applicant must have a valid government issued electronic identity document (eMRTD or eDL). Applicants are natural persons.

During the application, the applicant's acceptance of the terms and condition is captured by the TSP, not by Inverid.

4.2 CERTIFICATE APPLICATION PROCESSING

The Issuer CA may refuse to issue a certificate in its sole discretion.

ReadID carries out identity data and document verification services during the registration process (see section 3.2). The outcomes of these procedures are used by the TSP to either approve or refuse a certificate application.

The TSP shall at least refuse to issue a certificate if:

- the applicant's identity data in the Certificate application does not match with the data read from the chip of the identity document via ReadID;
- the identity data and document validity and authenticity verifications fail;
- the biometric verification and liveness detection fail.

4.3 CERTIFICATE ISSUANCE

Does not apply.

4.4 CERTIFICATE ACCEPTANCE

Does not apply.

4.5 KEY PAIR AND CERTIFICATE USAGE

Does not apply.

4.6 CERTIFICATE RENEWAL

Does not apply.

4.7 CERTFICATE RE-KEY

Does not apply.

4.8 CERTIFICATE MODIFICATION

Does not apply.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Does not apply.

4.10 CERTIFICATE STATUS SERVICES

Does not apply.

4.11 END OF SUBSCRIPTION

Does not apply.

4.12 KEY ESCROW AND RECOVERY

Does not apply.

5 Management, Operational, and Physical Controls

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of certificate data and certificate management processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the certificate data and certificate management processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any certificate data and certificate management processes;
4. Protect against accidental loss or destruction of, or damage to, any certificate data and certificate management processes; and
5. Comply with all other security requirements applicable to the CA by law.

The Certificate Management Process MUST include:

1. Physical security and environmental controls;
2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. Network security and firewall management, including port restrictions and IP address filtering;
4. User management, separate trusted-role assignments, education, awareness, and training; and
5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

The CA's security program MUST include an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data and certificate management processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the certificate data and certificate management processes. The security plan MUST include administrative, organisational, technical, and physical safeguards appropriate to the sensitivity of the certificate data and certificate management processes.

Inverid has implemented and maintains an Information Security Management System (ISMS) which is certified against ISO27001:2013 and subject to annual audit by an accredited external auditor. ReadID is in scope of the certificate.

Inverid's security management policy documents include the security controls and operating procedures for ReadID facilities, personnel, systems and information assets providing the services. InnValor carries out and revises the risk assessment annually in order to evaluate business risks, determine the necessary security requirements and optimise operational procedures. Inverid management is involved throughout the analysis.

Inverid management establishes and supports the security policy, which forms the basis for the consistency and completeness of the information security. Inverid management approves policies and practices related to information security of the overall ReadID services. Inverid management communicates information security

policies and procedures to employees and relevant external parties who are impacted by it (i.e. TSPs and subcontractors). In addition, Inverid management sets out the ReadID approach to manage information security objectives for Trust Services, including auditable procedures for internal control.

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 Site Location & Construction

All Inverid's operations facilities are specifically designed for computer operations and have been customised to meet the security requirements that apply to ReadID as an identity document verification service provider for trust services providers.

Inverid performs its operations from secure datacentres located in Europe. The data centres are equipped with logical and physical controls that make ReadID's identity establishment and verification operations inaccessible to non-trusted personnel. ReadID operates under a security policy designed to detect, deter, and prevent unauthorised access to ReadID operations.

Relevant prevention and detection mechanisms are to address environmental incidents, such as power loss, loss of communication, water exposure, fire and temperature changes.

5.1.2 Physical Access

Physical access to Inverid premises is controlled conform a physical access policy.

Access to Inverid's facilities are restricted to authorised personnel only. Non-authorised personnel, including visitors, are only allowed to access the facilities under escort and continuous surveillance by authorised personnel.

Within our offices we have a clean desk policy. No laptops or mobile devices are allowed in the office when the office is closed, unless locked away. Testing devices are stored in a locker; its keys are distributed to a few engineers. Personal information is in a locked closet, where the keys are restricted to the managing partners.

Since all data is stored in the cloud, physical access to the data-centre of the public cloud provider is relevant. This cloud provider ensures that physical components are housed in nondescript facilities and physical barrier controls are in place to prevent unauthorised entrance to the facilities. Access to the facilities is only provided to employees and contractors who have a legitimate business need. Access points to the facilities are monitored by video surveillance cameras designed to record all individuals accessing the facilities. Intrusion detection systems are also in place to detect unauthorised access. All physical access is logged and routinely audited. The public cloud provider has an ISO27001 certification or similar.

5.1.3 Power and Air Conditioning

Inverid has proper heating, ventilation, air conditioning systems to control the temperature and relative humidity. This is primarily for the well-being of its own employees. The public cloud provider offers even better facilities in this regard.

There are no extra measures taken for securing power systems to ensure continuous, uninterrupted access to electric power as this is not considered as a critical dependency. Services can continue from other locations without any problems.

5.1.4 Water Exposures

Inverid has not taken extra precautions to minimise the impact of water exposure to the information systems.

5.1.5 Fire Prevention and Protection

Inverid has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke.

5.1.6 Media Storage

Media is stored in on-site safes.

5.1.7 Waste Disposal

Adequate measures are taken to dispose sensitive information.

5.1.8 Off-Site Backup

Inverid performs routine backups of critical system data, audit log data, and other sensitive information. For ReadID, Inverid has dual data centres to ensure availability requirements. Databases in dual data centres are synchronised in real time. In addition, routine backups are performed. Backups of the most critical information (e.g. keys and configurations) are kept off-site in secure storage. For disaster recovery purposes, another data centre in a different region is available.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

The following trusted roles critical for security are:

- ReadID product owners – The ReadID product owners are overall responsible for the development process of ReadID. This responsibility includes ensuring that changes are made according to the definition of done, and that new versions of the software are well tested. Importantly, the product owner is authorized to approve ReadID software for production use.
- Cloud managers – Cloud managers are responsible for the secure managing of Inverid resources in the cloud. Responsibilities are the availability of cloud services including ReadID environments, maintenance of ReadID environments according internal and customer requirements, performing updates according to internal requirements and creating maintaining and deleting resources at our public cloud provider. Cloud manager are authorized to make changes according to established change controls. Because of the broad permissions needed for fulfilling this role, supervision is organized by Cloud Auditors.
- Team 247 – Team 247 is a subset of the Cloud Managers responsible for keeping the 24x7 availability of critical systems and provide outside office hour support to customers for urgent support. They are authorized to bypass regular change controls if this is required in course of their duties. Use of this authorization is subject to incident evaluation and reported to Cloud Auditors. People in this role take turns in providing urgent support outside office hours on a weekly basis.
- Security officers – Security officers are charged with the organization of Information Security at Inverid. They are responsible for organizing activities required by the ISMS. Examples include organizing periodic asset reviews, awareness sessions and risk assessments, but also include organizing incident evaluations when necessary. Security officers are authorized to approve exceptions to security policies, approve software to be added to the software whitelist for equipment, and to close incidents that where not opened by Cloud auditors. The work of security officers is indirectly checked by internal auditors are charged with checking compliance of the organization to its own security policies and the requirements of ISO27001.
- Developers – Developers are charged with software development. In this role, developers need a broad variety of permissions and access to systems and source code within the development intranet. This does not include access to customer production systems. Because malicious changes may impact the security of ReadID server or SDKs, this role is regarded a 'trusted role'.
- Senior management – Senior management is responsible for managing and allocating resources of the organization, managing people, strategic direction. They are authorized to appoint trusted roles to other people and to approve changes to security policies.
- Internal auditor – Internal auditor or compliance officer is responsible for auditing the organization against internal and ISO/IEC 27001 requirements. No special authorizations.
- Cloud auditor – Cloud auditor is charged with supervising Cloud Managers and authorized to close incidents that were opened by them.

Employees with trusted roles have job descriptions that define the functions and responsibilities related to the trusted role. All requirements and rules for or concerning personnel with trusted roles apply equally to employees with a temporary or permanent employment contract.

Inverid keeps track of the persons that have achieved a trusted status. Approval for this is required by senior management. This also holds for persons whose trusted role has been revoked.

5.2.2 Number of Individuals required per task

Inverid ensures that the number of staff available for tasks is adequate to meet demand, but also adequate to ensure that all security, risk and compliance regulation requirements are met.

5.2.3 Identification & Authentication for Trusted Roles

Employees in Trusted Roles at Inverid undergo background screening, and all employees are verified and authenticated, including face-to-face checks and identification checks based on government issued identity documents.

User accounts are created for personnel in specific roles that need access to the system in question. All users must log in with their personal account, and administrative commands are only available with explicit permission and auditing of the execution. For critical systems two-factor authentication is required.

Access to 'live' production data of a ReadID customer TSP by a trusted Inverid employee is restricted to exceptional situations such as the investigation of attempts of document fraud or debugging purposes with explicit consent of the affected TSP. All access to such data is captured in audit logs for the TSP, for which technical controls are in place to prevent tampering. Also, accessing live TSP data is performed by two persons and the TSP will be informed. Access by TSP-employees is also audited in the same manner.

5.2.4 Roles requiring separation of duties

When assigning trusted roles, separation of duties is taking into account. Conflicting duties and areas of responsibility have been identified and are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of assets.

5.3 PERSONNEL SECURITY CONTROLS

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA verifies the identity and trustworthiness of such person. CA personnel SHALL provide proof of their identity, background, qualifications and experience, as well as any other information required by the CA.

Inverid performs pre-employment checks for all employees (and contractors) with access to ReadID source code or cloud services and employees that have a senior management position. These checks are in line with contractual obligations and include at least a criminal background check. The relevant pre-employment checks are periodically repeated. Generally, all employees are highly educated in the field for which they have been employed. Specifically, the security officers both have an academic background in security.

The employees of Inverid have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions. The training continues during the contractual agreement.

The employment contracts signed by the employees of Inverid contain the following obligations:

- to have taken notice of and respect the Inverid information security policy, and
- to maintain the secrecy of confidential information during and after employment.

All employees in trusted roles are free from conflict of interest that might prejudice the impartiality of ReadID operations.

5.3.1 Qualifications, Experience, and Clearance Requirements

Applicants are screened before entering into service at ReadID, involving, as a minimum, a request for a Certificate of Conduct and a self-declaration. A Certificate of Conduct is a document by which the Dutch Minister of Legal Protection declares that the applicant has not been convicted for any crime relevant to the performance of his or her duties. Each Certificate of Conduct is renewed every five years. For employees from outside the Netherlands similar screening procedures are followed.

Each applicant's resume and compulsory identity document are verified. Screening intensity is adjusted to the confidentiality level linked to the employee's role. All employees sign a nondisclosure agreement as part of their employment contract.

5.3.2 Background Check Procedures
See section 5.3.1.

5.3.3 Training Requirements and Procedures
Security training shall be followed by all personnel every year. The contents must be determined by Security Officers. Training depends on the role of the employee. Specific training/certification can be organised via the personal yearly plan that each employee has.

Upon employment, all new employees follow a training plan. The training includes security awareness and other training related training associated with their specific function, which includes (where applicable) software, hardware, office procedures and security awareness.

Inverid maintains records of who received training and what level of training was completed.

5.3.4 Retraining Frequency and Requirements
All employees are required to attend regular security awareness training sessions.

5.3.5 Job Rotation Frequency and Sequence
Inverid does not use this method.

5.3.6 Sanctions for Unauthorized Actions
Inverid employees failing to comply with this TSPS, whether through negligence or malicious intent, are subject to internally maintained processes specifying guidance on administrative or disciplinary actions, up to and including termination of employment and legal sanctions.

5.3.7 Independent Contractor Controls
Inverid employs contractors. Contractors employed in trusted roles at ReadID are background checked per the procedures used for direct personnel.

5.3.8 Documentation Supplied to Personnel
All employees are provided with a contract of employment, a defined job role, and a personnel handbook. Collectively these documents provide necessary information regarding role, rights, laws and procedures pertaining to employment at Inverid.

5.4 AUDIT LOGGING PROCEDURES
The CA SHALL ensure that records of all relevant events and related information regarding the services are retained for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. The CA SHALL record in detail every action taken to process a certificate application and to issue a certificate, including all information generated or received in connection with a certificate application, and every action taken to process the application, including time, date, and personnel involved in the action. These records SHALL be available as auditable proof of the CA’s practices. The foregoing also applies to all Registration Authorities (RAs) and subcontractors as well.

All registration information including the following shall be recorded:

1. type of document(s) presented by the applicant to support registration;
2. record of unique identification data, numbers, or a combination thereof (e.g. subject's identity card or passport) of identification documents, if applicable;
3. method used to validate identification documents.

The CA shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

Inverid ensures that all relevant information concerning the operation of the Trust Services is recorded for providing evidence for the purpose of legal proceedings.

Logging sensors are deployed on the level of the public cloud provider, operating system, application server, and identity document server (audit trail).

ReadID servers expose monitoring metrics, logs and anonymised usage information to a central service. Personal details such as name or face image are never communicated to this central monitoring service. The central service actually consists of two services: a central monitoring and logging service that monitors the ReadID server's 'health' metrics and collects several types of logging data. The other service is "ReadID Analytics" that is used to anonymously log and analyse what phones and documents are processed.

The central logging service is located in EU and hosted by the public cloud provider. Monitoring metrics include statistics about CPU load, memory usage, disk usage, processing time for requests, and number of requests. If any of these are not within normal range, an operator is notified to resolve the situation. Technical application logs, system logs, IDS logs and the application audit trail are collected centrally as well to facilitate debugging and investigation.

In addition to this monitoring, Inverid also performs continual end-to-end checks to the API that closely mimics how a TSP interacts with the API. This allows us to quickly detect and resolve issues if something is wrong with the service even if this does not show in metrics or logs.

ReadID log files contain a session identifier, this session identifier is communicated to the TSP. Moreover, the session identifier is also linked to the face matching session of the biometric verification provider. This allows the TSP to trace back the overall identity document and holder verification audit trail for a specific applicant.

Alerts from monitoring, logging and end-to-end checks are being monitored 24x7 by a team of trained Inverid employees, who will also respond to potential issues according to relevant SLAs as agreed with TSPs. This may include that members of the 24x7-team can be contacted for critical issues by the TSP.

ReadID Analytics collects anonymized statistics for each use of ReadID. The statistics include for example details of the phone that was used, identity document type specifics, verification results etc. This is used by Inverid to detect possible issues with certain phones or identity documents.

5.4.1 Types of Events Recorded

ReadID's logging system records the following types of events:

- Security Events
    a. Access attempts
    b. System actions performed, including system start-up and shutdown.
    c. Profile and policy setting changes
    d. System activity
    e. Firewall and router activity
    f. Activities of system users with super-user rights
- Events involving:
    a. Routers, firewalls, and network system components
    b. Database activities and events
    c. Transactions
    d. Operating systems
    e. Access control systems
    f. Mail servers
    g. System failure, hardware failure and other irregularities
    h. Reading, writing and deleting data

All log entries provide the date and time, the identity of the person and a description of the event.

ReadID delivers an evidence package for every identity document we verify, automatically generated, crucial for auditability of the TSP and of the transactions. This makes proving compliance much easier than when done through the physical channel. Audit packages are provided to the TSP for archiving.

For ReadID Analytics anonymised metadata of read and verified identity documents is collected.

5.4.2 Frequency for Processing & Archiving Audit Logs

Audit logs are processed following previously mentioned events. Daily backups are made of all audit data. Logs are provided with a timestamp using a clock that is synchronized at least once a day with a trusted time source.

Security officers are responsible for regular reviewing of system logs and reporting of possible security related incidents.

Service managers are responsible for reviewing their applications logs from central log system and creating automated searches for product failure discovery and event correlation. They are also responsible for a periodic (weekly) review of reports generated by the log system about their services.

Product owners are responsible for proper functioning of the ReadID products. This includes testing and controlled change management based on audit logging processing outcomes.

Cloud-related logs are reviewed weekly by the internal cloud auditor.

5.4.3 Retention Period for Audit Logs

Audit logs are stored and accessible for ten years unless required otherwise by specific legislation or TSP demands.

5.4.4 Protection of Audit Logs

All audit events recorded are digitally signed to ensure logs have not been tampered with. Any modification of records will be noticed. The audit log data is available in a read-only format and subject to access restrictions. Logs are stored in more than one location, in such a way that they are accessible for ten years.

Should the audit log concerning the operation of services be required for the purposes of providing evidence of the correct operation of the services and for the purpose of legal proceedings, they are made available to legal authorities and/or persons whose right of access to them arises from the law.

5.4.5 Audit Log Backup Procedures

ReadID performs daily backups.

5.4.6 Audit Log Accumulation System (Internal vs. External)

The internal audit logger records events as they pass through the system. Upon unavailability of the audit logger, dependent services stop functioning.

5.4.7 Notifications to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The audit log and components supporting the audit log are in scope of ReadID's periodic risk assessment policy and procedures.

ReadID's systems are assessed via internal and external vulnerability scans and penetration tests. The tests are carried out periodically. Penetration tests are carried out by external contractors at least once per year. All foreseeable internal and external threats are assessed with the risk analysis of ReadID at least once per year or in case of significant changes to the infrastructure or applications.

For any vulnerability, given the potential impact, Inverid creates and implements a plan to mitigate the vulnerability. In case the identified vulnerability does not require remediation, the factual basis for this determination will be documented.

5.5 RECORDS ARCHIVAL

5.5.1 Types of records archived

All data that can be relevant for the compliance audit is archived. For the purpose of user identity and document verification and fraud detection, this data includes personal data collected during identification and data related to the verification of the personal data including outcomes.

For the purpose of security and access management TSP's employee login information (username, email, mobile phone) is recorded.

For security and incident management purposes access and audit logs are recorded. Access logs contain an IP-address and audit logs contain the name of the user.

Data subject to archiving may be collected from audit logs, databases or in physical documents. These are all archived appropriately. Private keys are not archived.

5.5.2 Retention period for archive

Archives are retained for ten years.

5.5.3 Protection of archive

Archive data associated with identity document verification and related processes are subject to access restrictions and controls. Archives are secured against modification and deletion. To this end, both organizational and technical controls are in place. Archives are also protected against storage media deterioration. The archives are stored on monitored, redundant hard disks.

5.5.4 Archive backup procedures

Digital archive data is automatically generated via the internal systems processes. Backups of systems are made daily and in accordance with the backup procedures and policies at ReadID. The entire archive is backed up off-site.

5.5.5 Requirements for time-stamping of records

Records are provided with a timestamp using a clock that is synchronized at least once a day.

5.5.6 Archive collection system (internal or external)

Please refer to section 5.5.3 and 5.5.4

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 KEY CHANGEOVER

Not applicable.

5.7 COMPROMISE AND DISASTER RECOVERY

Information security incidents are events leading to or have led to:

- Unavailability of service, e.g. downtimes of the API
- Integrity breaks, e.g. verification bypasses or return of invalid information
- Loss of confidentiality, e.g. data breaches or unauthorized viewing of TSP applicant data

Such incidents will be handled and evaluated in accordance with legislation, SLA's and internal procedures. This process is in scope of periodic internal and external audits.

Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

Inverid has a business continuity management plan in place, which covers procedures of risk assessment, incident handling (includes a response to incidents and disasters), recovery and recovery exercises.

Inverid's business continuity plan ensures continuity when an incident or disaster occurs. The aim of these plan is to ensure the orderly recovery of business operations, communication to subscribers and relying parties, and continuity of services for the subscriber affected.

Recovery plans are tested annually and updated periodically. Back-up arrangements are also regularly tested to ensure that they meet the requirements of Inverid's business continuity plan.

In the event of a data breach, regulatory bodies must often be informed timely by the party responsible for the data. Inverid therefore informs its ReadID TSP customers of such events timely and in accordance with SLA.

5.7.1 Incident and Compromise Handling Procedures

Incidents or compromises are handled according to the Inverid internal incident response procedure.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

In case of corruption of computer resources, software and data, Inverid falls back to its incident response procedure.

5.7.3 Recovery Procedures After Key Compromise

No stipulation.

5.7.4 Business Continuity Capabilities after a Disaster

No stipulation.

5.8 TERMINATION

The following procedure applies before Inverid Software B.V. terminates its ReadID services contractually or otherwise:

- the TSP and other relying parties, including supervisory bodies, will be informed about the termination conform the contractual agreements and conform regulatory and legal requirements,
- an exit plan will be drawn up together with the TSP, dealing with post-contractual services that may be provided by Inverid Software B.V. after the termination being effective, as well as dependencies on the part of the customer in that respect. The purpose of the exit plan is to allow the TSP to migrate to an alternative and to minimise the impact as much as possible. Topics to be addressed in the exit plan are at least:
    - termination of any applicable authorizations of sub-contractors to act on behalf of Inverid Software B.V. in carrying out any functions relating to TSP processes,
    - secure transfer of all relevant data collected by Inverid Software B.V. for identity verification purposes via ReadID to the TSP. This applies to data read from identity documents, the ReadID audit logs and technical application logs, and the logs of sub-contracted partners such as biometric verification providers,
    - the availability of ReadID-related service tokens to allow TSP access to data for a reasonable period,
    - the destruction or withdrawal of any TSP private keys from use, including backup copies, in a manner such that these private keys cannot be retrieved,
- where possible Inverid ReadID will make arrangements to transfer the provision of its ReadID services for its existing customers to another party.

Termination or dissolution of the contract between Inverid Software B.V. and the TSP expressly shall not release both parties from the provisions regarding confidentiality, evidence storage, transfer, liability, warranties, intellectual property, governing law and competent court and other provisions that are intended by their nature to remain in force also after termination or dissolution.

In the context of an unscheduled termination of the Inverid Software B.V. activities, the procedure for expected termination as described above will, as far as possible, be executed by Inverid B.V. and with more urgency. As a minimum effort, at least the transfer of the collected data to the TSP shall be executed.

Inverid B.V. has arrangements to cover the possible costs to fulfil the above-mentioned minimum requirements in case Inverid Software B.V. goes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

In case of a contract termination between Inverid and the biometric verification provider, the TSP will be informed about this as well and has the right to object.

6 Technical Security Controls

6.1 KEY PAIR GENERATION AND INSTALLATION

Not applicable.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Not applicable.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

Not applicable.

6.4 ACTIVATION DATA

Not applicable.

6.5 COMPUTER SECURITY CONTROLS

Application services are hardened, meaning that the attack surface is minimized. Firewall rules ensure that application servers only communicate with the intended load balancer and database servers. Environments are therefore completely isolated from each other. For production environments, remote shell access to the machines is blocked as well, because the lifecycles of these servers are automated, and logs are exported to another machine.

Security mailing lists are monitored continually by the security department to ensure a timely response to possible vulnerabilities. In case an update is needed, application servers will be patched in a controlled manner.

Environments are protected with intrusion detection systems at the network and system level.

6.5.1 Specific computer security technical requirements

ReadID ensures that the identity verification system components are secure and correctly operated, with an acceptable risk of failure.

ReadID has a variety of security controls in place:

- Two-factor authentication for systems,
- Cryptographically secured connections,
- Cryptographically secured audit logs,
- Separation in development, acceptance and production environments,
- Network zoning, physical and logical access control, hardening of systems,
- Risk based logging, monitoring and alerting implemented,
- Trusted roles assigned and training for operating these systems,
- Security assessments; including vulnerability scanning and penetration testing.

Inverid's information security policy embodies the commitment of ReadID to maintaining an appropriate level information security. The document sets security objectives of ReadID, describes how information security is organized and acts as a reference document for our other policies. Among its purposes is to comply to applicable legislation and the contents of this document are available to interested parties in required. This policy applies to all Inverid employees, contractors and other affiliates.

Inverid's operation instruction policy sets the security requirements of ReadID deployments in accordance with contractual obligations. It serves as a checklist for Cloud managers and Team 247 to adhere to. The scope of this instruction are ReadID production networks that host ReadID server deployments for TSPs that choose not to host the ReadID server themselves. This includes multi-tenant deployments (saas.readid.com) and specific single-tenant deployments with different purposes: development, testing, pre-production/acceptance and

production. The requirements of this instruction only apply to production deployments, although for practical reasons most requirements are applied for the other deployments as well.

Inverid's development instruction for ReadID addresses the security of software development process at Inverid and describe how Inverid employees should handle information security while developing and changing software. The requirements of this instruction apply only to the development of production software.

Changes to the ReadID software are managed in accordance with defined change management procedures. These procedures include system testing in an isolated test environment and the requirement that changes must be approved by another developer (4-eyes principle). Security-related changes must be approved by the security officer. Each change approval or rejection is documented for further reference.

All critical software components of ReadID are installed and updated from trusted sources only. There are also internal procedures to protect the integrity of ReadID IT-infrastructure against viruses, malicious and unauthorised software.

The Inverid working instruction contains concrete information security instructions to empower all Inverid employees to abide by the Information Security Policy. It covers topics like office environment security, equipment security, communications security, portable media security, and credentials security.

ReadID's supplier information security policy defines the requirements for suppliers with access to company data or TSP data of ReadID. Not in scope are suppliers who only provide software for processing other types of information. The purpose of this policy is to control information security risks related to other organisations with processing data under responsibility of ReadID. Often, the requirements in this policy depend on the classification of information that are processed by the supplier.

Inverid security operations include: operational procedures and responsibilities, secure systems planning and acceptance, protection from malicious software, backups, network management, active monitoring of audit logs event analysis and follow-up, media handling and security, data and software exchange.

Inverid has implemented security measures and enforced access control in order avoid unauthorized access and attempts to add, delete or modify information in applications related to the services. User accounts are created for personnel in specific roles that need access to the system in question after proper training and explicit permission. Multifactor authentication is required for getting access to critical systems. File system permissions and other features available in the operating system security model are used to prevent any other use. User accounts are removed as soon as possible when the role change dictates. Access rules are audited annually.

Furthermore the security processes comply to the specific requirements in ETSI 319-411-1, ETSI 319-411-2 and ISO27001. Inverid is certified against these standards by an independent and accredited auditor.

6.5.2 Computer security rating

Please refer to section 6.5.1. ReadID uses standard computer systems.

6.6 LIFE CYCLE TECHNICAL CONTROLS

The software development process adheres to common practices to limit the risk of bugs and vulnerabilities. A few highlights are:

- Version control is applied to all code to ensure control over what code is to be released, and what is in development, and also provides an audit trail of all changes to our code;
- Code changes have to pass several approval gates before being promoted to production environments. This includes peer reviewing, static code analysis, (unit) testing, approval testing and in some cases even approval by TSPs;
- Static code analysis is applied to detect common vulnerabilities and deficits in code automatically;
- All code is built and tested using a trusted build server;
- New code is thoroughly tested using automated tests during development and manual acceptance tests before software is released to TSPs;

- Larger features are subject to internal or external pen-tests before being declared a production feature;
- We do a yearly external pentest, also if there would not be larger new features that would require this;
- General responsibility for a particular piece of code is always assigned.

ReadID functions for Android 5.0 and higher, on smart phones and tablets with NFC. Inverid will stop supporting Android versions when this is commercially unreasonable and/or because of security concerns and/or because of technical concerns. The TSP will be notified through the change log of this. Unless there is an urgent technical or security reason that reasonably inhibits this, dropping support for an Android version will be announced at least one month in advance.

ReadID will work for on the current iOS version and one version lower, unless there are specific reasons to not support this one version lower. As an exception, ReadID will not work for iOS versions below 13.1. There may be iPhones and iPads on which ReadID does not function, or not function properly, because the NFC capability is not present or not suitable, including problems with certain types of identity documents

Transparency to TSPs w.r.t. application changes is important. TSPs will receive advance notification of application updates of environments that they use. Depending on the agreement, it is also possible for a TSP to conduct acceptance testing and fix any problems before a production environment is updated.

New releases of the software may be announced at a, typically, monthly interval. This includes both the client SDK and server application. All new versions of ReadID software are thoroughly tested before being released to TSPs, using a combination of automated and manual testing. Should a bug occur after a release, it may be fixed as a hotfix, in the next version of the software, or both. TSPs are required to update the client SDK and cooperate with updating the server. Only the latest two versions of the mobile client and server are supported, and client and server may differ by one version, which is necessary to allow migrations. The ReadID server does not allow skipping a version (because of the database update, and roll-back, scripts).

In most cases ReadID server updates do not need downtime to perform. Nevertheless, an update window may be agreed with the TSP since doing an update also has a small risk of service disruptions. There may infrequently be updates that will cause downtime, these will be communicated or agreed before these are done.

In case of urgent security issues, we reserve the right to do updates without advance notice.

6.6.1 System Development Controls

ReadID's Development instruction provides instructions that apply to the software development process at Inverid and describe how Inverid employees should handle information security while developing software. The requirements of this instruction apply only to the development of production software. The instruction covers aspects of assessing dependencies on external software libraries or applications, source code quality checks to limit the risks of vulnerabilities or other bugs in developed software, source code versioning and release procedures, approval procedures regarding software changes, and test procedures.

6.6.2 Security Management Controls

All operational systems and networks of ReadID are monitored, managed and controlled to ensure their integrity and correct operation. ReadID has procedures and schedules for the systems and the related maintenance of them. Those responsible are required to carry out regular systems monitoring and checks. Additional to manual monitoring, it is also an automated process, where the relevant trusted personnel are alerted upon any activity which is out of the expected behaviour.

6.6.3 Life Cycle Security Controls

Inverid policies, assets and practices for information security are reviewed periodically by their owners at least annually or in case of significant changes to ensure their continuing suitability, adequacy and effectiveness.

The configurations of the ReadID systems are regularly checked for changes that violate ReadID security policies. The Security Officer approves changes that have an impact on the level of security provided.

Inverid has procedures for ensuring that security patches are applied to the identity verification system within a reasonable time period after they become available, but not later than six months following the availability of the security patch. The reasons for not applying any security patches will be documented.

Inverid manages an overview of information assets that are classified in terms of security levels and in a manner consistent with the risk assessment. Persons have been appointed that are responsible for keeping the security of the most important assets up-to-date.

6.7 NETWORK SECURITY CONTROLS

Inverid uses secure networking measures to prevent unauthorised and malicious activity. Access to networks is under the conditions of strict access controls. The controls are preventive, detective, repressive and corrective in nature and are subject to periodical assessments. Internet communications are all encrypted. On the internal network, only the communication of sensitive information is encrypted; a pragmatic encryption approach is taken for other information.

There are firewalls in place for enforcing the network security policy. Firewalls configured such that connections are explicitly allowed or forbidden. Services or connections that are not needed will be deactivated.

Inverid operates multiple data centres in separate sites and with separate duplicated external network connection for redundancy to ensure high level availability of the Trust Services. Communication between sites is cryptographically secured.

Communication channels between ReadID SDK, ReadID Server as well as the interfaces with the biometric verification provider and TSP for the exchange of identity data are secured against modification and disclosure. Furthermore, assured identification of end points is provided.

Development and test environments are (logically) isolated from production environments.

The security of Inverid's internal network and external connections is constantly monitored to prevent all access to protocols and services not required for the operation of the Trust Services.

Inverid quarterly performs vulnerability scans on critical public and private IP-addresses.

ReadID undergoes a penetration test on critical systems annually or after significant changes to the infrastructure or application upgrades or modifications.

ReadID records evidence that each vulnerability scan and penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

The ReadID server is provided as a SaaS via a public cloud provider. The ReadID SaaS environment is fully redundant, self-repairing and able to scale automatically to changing load. The main elements of this environment are:

- Load balancer: a managed application load balancer service is used for terminating https connections and equal balancing over the available application servers. Communication between load balancers and application servers has been encrypted using https as well. The main advantages of using managed load balancers are automatic scalability and resilience.
- Application servers: for actually handling the requests. At all times, at least two instances are running in different data centres for resilience to outages. Application servers can receive https encrypted HTTP requests from the load balancers as soon as the self-diagnostics of the server is successful. The lifecycles of application servers are fully automated: as soon as the self-diagnostics of a server fails, it no longer receives requests from the load balancer, is terminated and a replacement instance is started. Fine-grained access control is applied to prevent environments from accessing other cloud storage resources.
- Database: All state of an environment is kept in a relational database. The database is replicated in a master-slave setup, whereby the slave is a hot standby: it does not actively handle traffic but can take over from the master immediately when needed. Connections to the database are encrypted using

strong TLS encryption. All database servers have been encrypted at the filesystem level. Additionally, (privacy) sensitive data in the database is encrypted at the application level. This setup also minimizes the likelihood of data loss. Failing of application servers does not result in data loss, because all state is stored in the database. Data loss in the database is very unlikely because all data is synchronously replicated from master to slave.

Two deployments options are offered to fit the needs of different ReadID customer TSPs:

1. Multi-tenant deployment. The virtual machines within the environment are shared with other TSPs or ReadID customers. Applicant data from TSP A is logically separated from applicant data from TSP B.
2. Virtual single-tenant deployment. This environment is not shared with other customers, i.e. a TSPs has separate virtual machines and virtual databases.

The single-tenant and multi-tenant environments are strictly separated from each other using firewall rules. These rules prohibit communication between load balancers and application servers of different environments and database servers and application servers of different environments. All other traffic is blocked by default as well, unless required for correct functioning of the service.

A single-tenant deployment has several advantages over a multi-tenant deployment. For the processing location of data any region the cloud provider is active may be chosen, the infrastructure is not shared with other customers ensuring less dependability , and more flexibility with respect to updates is possible (within limits, a TSP shall have to keep up with new server versions). Other than that, there are no differences between both deployments.

The public cloud provider is responsible for the security of the cloud, i.e. it is responsible for protecting the infrastructure that runs all of the services offered in the cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run cloud services. The latter includes operating the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. And on top of that, the physical and logical access control to the infrastructure. Inverid is responsible for the security in the cloud. Mainly this involves the management and configuration of the operating system (including updates and security patches), any application software or utilities installed by Inverid on the instances, and the configuration of cloud-provided firewalls on each instance. Moreover, Inverid is also responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions. Despite the shared responsibility, it is Inverid's responsibity to ensure and monitor that the combined service meets all relevant (security) requirements specified by eIDAS and ETSI and that apply to the TSP. Consequently, it is required for the public cloud provider to have an ISO/IEC 27001 certificate and a SOC2 report or similar.

6.8 TIME-STAMPING

Audit logs and transactions are time-stamped based on a Reference Clock service.

7 Certificate, CRL & OCSP Profiles

7.1 CERTIFICATE PROFILE

Not applicable.

7.2 CRL PROFILE

Not applicable.

7.3 OCSP PROFILE

Not applicable.

8 Compliance Audit and other Assessment

The CA SHALL at all times:

1. Issue Certificates and operate its PKI in accordance with all laws applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with applicable requirements;
3. Comply with the audit requirements; and
4. Are licensed as a CA.

8.1 FREQUENCY OF COMPLIANCE

Inverid undergoes an audit for ETSI EN 319 411-1 and ETSI EN 319 411-2, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied). The audit is conducted by a Qualified Auditor, as specified in Section 8.2.

The conformity of information system, policies and practices, facilities, personnel, and assets of Inverid are periodically assessed by a conformity assessment body pursuant to the eIDAS regulation, the corresponding requirements and standards or whenever a major change is made to its Trust Services (i.e. identity data and document verification) operations.

Twice a year Inverid's internal auditor carries out an internal audit.

Inverid is also certified against the ISO27001:2013 standards on a yearly basis. ReadID is in scope of the certificate. The statement of applicability of the ISO27001 certification also includes the privacy-related controls from ISO/IEC 27701:2019. This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) in the form of an extension to ISO/IEC 27001.

The public cloud provider is at least ISO/IEC 27001 certified.

8.2 IDENTITY AND QUALIFICATIONS OF THE ASSESSOR

The CA's audits are performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities who possess the correct qualifications and skills.

Inverid's conformity assessment body is accredited in accordance with Regulation EC no 765/2008 as competent to carry out conformity assessments of Trust Services.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

External auditors are independent and have no business interests in Inverid. No external auditor has any business affiliation with Inverid.

8.4 TOPICS COVERED BY ASSESSMENT

The conformity assessment covers the conformity of information system, policies and practices, facilities, personnel, and assets with respect to the eIDAS regulation, respective legislation and standards. The conformity assessment body specifically audits the parts of ReadID that are used to provide the Trust Service.

The scope of the audit covers all the quality, security, operational, procedural, performance, and contractual requirements from the standards with in particular the subject of:

- Identification and authentication;

Other, more generic areas of activity that are subject to the audit include amongst others:

- Software development and change management
- Risk Management
- Network Security
- Logical and Physical Access
- Logging and Monitoring
- Compliance
- Human Resource Security
- Business Continuity Management

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If, unexpectedly, deviations are found, a Corrective Action Plan is drafted to correct the deviations. The Corrective Action Plan is agreed upon with the external auditor and are given to the disposal of national supervisory bodies.

8.6 COMMUNICATION OF RESULTS

The Audit Report states explicitly that it covers the relevant systems and processes used in the issuance of all certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. The CA make the Audit Report publicly available.

Compliance audit certificates and their scope can be consulted on Inverid's ReadID website: www.readid.com. The underlying audit reports are confidential, and are given to the disposal of national supervisory bodies.

8.7 SELF-AUDITS

During the period in which the CA issues certificates, it monitors its adherence to its Certificate Policy, Certification Practice Statement and these Requirements and strictly control its service quality by performing self-audits.

Inverid carries out regular internal audits to continuously assess compliance with the laws, regulations, internal policies and requirements mentioned in this document. Critical processes are subject to an internal audit twice a year, for less critical processes this is once a year.

9 Other Business and Legal Matters

9.1 FEES

TSPs pay per ReadID transaction, specific commercial arrangements can vary per TSP.

9.2 FINANCIAL RESPONSIBILITY

To cover the liabilities of art. 13 of the eIDAS regulation, ReadID has a full liability insurance policy which provides coverage of more than the required €1.000.000. More details about liability can be found in the contractual agreement between the TSP and Inverid.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of confidential information

Inverid considers all data provided within the framework of the trust service as confidential.

9.3.2 Information not within the scope of confidential information

All data not mentioned in 9.3.1

9.3.3 Responsibility to protect confidential information

Inverid and all participants described in this TSPS have a responsibility to protect confidential information.

9.4 PRIVACY OF PERSONAL DATA

Note that Inverid, within the scope of this TSPS, is not a controller of personal data, i.e. Inverid is a processor of personal data for the TSP. The TSP remains responsible for the data. In the situation that the biometric verification provider is a sub-contractor of Inverid, it is contractually arranged that this sub-processor processes personal data according to prevailing law and legislation.

Conform GDPR, Inverid has performed a data protection impact assessment for ReadID. This DPIA provides an overview the personal data being processed, identifies the risks associated to the processing of the data and describes the technical and organisational control measures implemented to mitigate the risks.

Access to personal data of applicants of a TSP by employees of Inverid is constraint. Only in exceptional situations such data may be accessed.

Nevertheless, to demonstrate that Inverid is a trustworthy partner with respect to the processing of personal information and compliant with GDPR, a data processing impact assessment has been made. Furthermore, the scope of Inverid's ISO/IEC 27001 ISMS has been extended with the ISO/IEC 27701 privacy controls.

The public cloud provider Inverid makes use of for ReadID is also considered as sub-processors of personal data. Inverid has a data processing agreement with this cloud provider. Furthermore, a data processing agreement is part of the contractual agreement with the TSP.

Inverid has a Data Protection Officer. The task of the DPO is to ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules.

9.4.1 Privacy plan

Please refer to the ReadID privacy statement available on the public website: https://readid.com/about/privacy.

9.4.2 Information treated as private

See above.

9.4.3 Information not deemed private

See above.

9.4.4 Responsibility to protect private information

Inverid ensures protection of personal information by implementing security controls as described in section 5 of this TSPS.

9.4.5 Notice and consent to use private information

See above.

9.4.6 Disclosure pursuant to judicial or administrative process

Inverid will only fulfil the requirements to supply data for forensic purposes as required by law enforcement and for the judicial process, per the legal administrative procedures.

9.4.7 Other information disclosure circumstances

There are no other information disclosure circumstances.

9.5 INTELLECTUAL PROPERTY RIGHTS

Any intellectual property rights associated with products and services supplied by Inverid, and associated materials, remain the property of Inverid, the licensee or supplier. All information regarding conditions pertaining to intellectual property rights can be found in the associated terms and conditions and any contractual agreements with ReadID.

9.6 REPRESENTATION AND WARRANTIES

Inverid is party to the mutual agreements and obligations between the TSP and other participants. This ReadID TSPS forms an integral part of these agreements.

The inter-working between Inverid ReadID and the TSP focusses on the identification and registration processes that the TSP has to perform during a certificate application by an end-user. The main steps are:

1. Initialization of the certificate request at the TSP by the applicant;
2. Collecting data from the applicant by the TSP: identity data but also contact data;
3. Reading the data from the chip of an identity document with the ReadID Ready app;
4. Verification if the read data and the document used are authentic at the ReadID Server;
5. Verification of the applicant as the holder of the identity document by the biometric verification provider (optional, depending on the orchestration model);
6. Validation of the data read from the identity document against the data placed by the applicant in the certificate request by the TSP;
7. Interpretation of the various verification outcomes of steps 4 and 5 by the TSP;
8. Collecting the consent of this person to receive a qualified certificate and accepting terms and conditions;
9. Providing the information ready for certificate issuance.

The first two steps are facilitated by the TSP via its website or mobile app. For the third step, the applicant uses the mobile app of the TSP that has integrated ReadID SDK functionality. Using this functionality, the applicant can read identity data from the identity document. The ReadID Server verifies if this data is authentic and if the read document is authentic, i.e. not a clone or copy. The verified identity data is shared with and used by the TSP to validate the data provided by the applicant (step 6). It is up to the TSP to interpret the verification output of ReadID and decide what to do with it in the course of the application process (step 7). More specific:

- The TSP shall decide if it will accept the CA signer certificate used for signing the data read from the chip and verified by ReadID;
- The TSP shall decide what to do in the situation that identity document verification (i.e. clone detection) was not successful or not possible to execute (not all identity documents support clone detection);

Being the primary point of contact for the applicant, the TSP is responsible for obtaining the applicant's informed consent and submitting the terms and conditions (step 8). This step may also take place earlier in the application process.

Step 5 involves a biometric verification provider. The face image read from the chip of the identity document (step 3) may be used by the biometric verification provider for holder verification purposes. Regarding the verification results provided by the biometric verification provider, the TSP shall decide if they are suitable for further use whilst taking into account the false acceptance rate and/or false rejection rate (FAR/FRR) of the solution.

The TSP may also make use of ReadID when re-identification of the subscriber is required. For instance during certificate renewal, re-key requests (section 3.3), or revocation requests (section 3.4).

9.6.1 Trust Service Provider Representations and Warranties

Towards a TSP in general Inverid shall:

- provide its services, i.e. identity document data verification and identity document verification, consistent with the requirements and the procedures defined in this TSPS and service-based policies and practice statements;
- carry overall responsibility for conformance with the procedures defined in this TSPS and service-based policies and practices statements;
- comply with eIDAS regulation and related legal acts defined in this TSPS and service-based policies and practice statements;
- publish its TSPS and service-based policies and practice statements and guarantee their availability in a public data communications network;
- publish and meet its claims in terms and conditions for subscribers and guarantee their availability and access in a public data communications network;
- maintain confidentiality of the information which has come to its knowledge in the course of supplying the service and is not subject to publication;
- inform the TSP of any significant changes to its processes;
- without undue delay but in any event within 24 hours after having become aware of it, notify the TSP and, where applicable, other relevant bodies as eIDAS supervisory body or national CERT of any breach of security or loss of integrity that has a significant impact on the services provided;
- without undue delay but in any event within 48 hours after initial discovery address newly emerged critical vulnerabilities;
- where the breach of security or loss of integrity or personal data breach is likely to adversely affect a natural or legal person to whom the trust service has been provided, notify the TSP of the breach without undue delay;
- preserve all the documentation, records and logs related to trust services according to the clauses 5.4 and 5.5;
- ensure a conformity assessment according to requirements and present the conclusion of conformity assessment body to the TSP to ensure its continual status of trust services in the Trusted List;
- have the financial stability and resources required to operate in conformity with this TSPS;
- publish the terms of the compulsory insurance policy and the conclusion of conformity assessment body in a public data communications network.

From the TSP it is expected that it:

- Shall decide whether to use a single or multi-tenant environment based on its own risk assessment.
- Shall securely implement the ReadID SDK in its own mobile app.
- Shall store recorded data and results collected during the whole process (including ReadID and/or biometric verification provider outputs).
- Shall ask the applicant for consent and to agree with the terms and conditions.

9.6.2 RA Representations and Warranties

Towards the specific RA part of the TSP Inverid shall:

- provide its services consistent with the requirements and the procedures defined in the contract between ReadID and RA, in this TSPS and service-based Policies and Practice statements;
- provide its employees with necessary training for supply of high-quality service;
- without undue delay after having become aware of it, notify RA of any breach of security or loss of integrity that has a significant impact on the Trust Service provided or on the personal data maintained therein.

9.6.3 Subscriber Representations and Warranties

Towards a Subscriber Inverid shall:

- supply true and adequate information in the application for the services, and in the event of a change in the data submitted, he/she shall notify the correct data in accordance with the rules established in the service-based policies and practice statements;
- raise awareness of the fact that Inverid may refuse to provide the service if the Subscriber has intentionally presented false, incorrect or incomplete information in the application for the service;
- raise awareness concerning statements and service terms and conditions;
- strive to optimise the experience of its services by the subscriber in terms of usability, intuitively, and accessibility as much as possible;
- do its best to provide its services in a way suitable for subscribers with disabilities.

9.6.4 Relying Party Representations and Warranties

All questions of liability for subscribers, relying parties and other participants, are covered in contractual agreements.

9.6.5 Representations and Warranties of Other Participants

Sub-contractors that provide biometrics-based face verification and liveness detection shall ensure towards Inverid adequate:

- Service delivery and support;
- Duration and termination;
- Conformity and liability;
- Confidentiality and personal data including a DPA appendix;
- SLAs;
- Security measures including right to audit.

Similar warranties are in place for the public cloud provider.

9.7 DISCLAIMERS OF WARRANTIES

No limitations of warranties apply other than those mentioned in section 9.6.

9.8 LIMITATIONS OF LIABILITY

No limitations of liability apply other than those mentioned in section 9.2 or contractually specified.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

The TSPS is effective immediately after publication in the public repository and remains effective until a new version is published.

9.10.2 Termination
By publishing a new version of the TSPS, the previous version of the TSPS is terminated.

9.10.3 Effect of termination and survival
No stipulation.

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS
Inverid does not provide notifications to participants; this will always be done by the TSP.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment
Inverid has the right to amend or supplement this document. Inverid will review and update this document when:

- The scheduled yearly review is performed;
- There are changes to the process, procedures or policy described in this document;
- There are changes to the law, regulations or requirements;
- There are changes to the business interests of Inverid and changes are required.
- Any changes which are not noted in the document history are grammatical, typographical or format changes which do not impact the underlying information pertaining to processes, procedures and policy.

9.12.2 Notification Mechanism and Period
Please refer to 9.10.1.

If applicable, the changes will be implemented in the General Terms & Conditions or Product Terms & Conditions that apply to the service of ReadID and which are published via the ReadID website.

9.12.3 Circumstances Under Which OID Must be Changed
Not applicable.

9.13 DISPUTE RESOLUTION PROVISIONS
All disputes between the parties will initially be settled by negotiations. If the parties fail to reach and amicable agreement, the dispute will be resolved at the court of the location of Inverid or its contractor.

Other parties will be informed of any claim or compliant not later than 30 calendar days after the detection of the basis of the claim, unless otherwise provided by law.

The Subscriber or any other party can submit their claim or complaint on the following email: ReadID@Inverid.nl.

9.14 GOVERNING LAW
Inverid, situated in The Netherlands, is subject to national Dutch Laws and European Regulations for the provision of services and products.

9.15 COMPLIANCE WITH APPLICABLE LAW
Inverid's ReadID provides identity verification services to Trust Service Provider (TSP) as defined in EU Regulation 910/2014 also known as eIDAS.

This requires ReadID to be compliant to the applicable requirements of the following standards, requirements and regulations:

- ISO/IEC 27001:2013 Information Security Management System (ISMS)
- ISO/IEC 27701:2019 Extension to ISO/IEC 27001 for privacy information management (PIMS)
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers

- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates
- eIDAS Regulation (EU) N 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
- Underlying eIDAS implementing acts such as CIR 2015/1502 on assurance levels for electronic identification solutions.
- GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council 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)
- CA/Browser Forum Baseline Requirements
- CA/Browser Forum Network and Certificate System Security Requirements

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement
No stipulation

9.16.2 Assignment
No stipulation

9.16.3 Severability
No stipulation

9.17 OTHER PROVISIONS
Any provision within this document that is declared invalid or unenforceable will be outside operation. This does not affect the applicability of the remaining provisions in this TSPS.