ReadID eIDAS eID level of assurance mapping

Compliance with eIDAS 2015/1502 level High

Colophon

DATE	20-12-2022
VERSION	2.0
CONFIDENTIALITY	Public
STATUS	Second version for publication
COMPANY	Inverid
AUTHOR (S)	Bob Hulsebosch CCO CISSP

Synopsis

This document maps the characteristics of ReadID to the requirements of the eIDAS Level of Assurance High as defined in Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of the eIDAS Regulation [eIDAS]. ReadID is software provided by Inverid (formerly InnoValor) for identity document reading and verification via NFC technology.

Table of contents

COLOPHON 2

TABLE OF CONTENTS 3

VERSION HISTORY 4

1 INTRODUCTION 5

1.1 ABOUT READID 5
1.1.1 Overview ReadID products 5
1.1.2 ReadID SaaS Server 5
1.1.3 ReadID SDKs 5
1.1.4 ReadID Ready: Basic, Branded, Enterprise 6
1.1.5 Management Portal 6
1.1.6 Machine Readable Zone (MRZ) scanning 6
1.1.7 Chip reading and verification 6
1.1.8 Android support 7
1.1.9 iOS support 7
1.1.10 Supported identity documents 7
1.1.11 Data processing 7
1.1.12 Facial matching and orchestration 8
1.2 TYPICAL READID FLOW 9
1.3 SCOPE OF THE ASSESSMENT 10
1.4 DEFINITIONS 10
1.4.1 Acronyms 10
1.4.2 Acronyms 11

2 TECHNICAL SPECIFICATIONS AND PROCEDURES 13

2.1 ENROLMENT 13
2.1.1 Application and registration 13
2.1.2 Identity proofing and verification (natural person) 14
2.1.3 Identity proofing and verification (legal person) 16
2.1.4 Binding between the electronic identification means of natural and legal persons 16
2.2 ELECTRONIC IDENTIFICATION MEANS MANAGEMENT 16
2.2.1 Electronic identification means characteristics and design 16
2.2.2 Issuance, delivery, and activation 17
2.2.3 Suspension, revocation, and reactivation 17
2.2.4 Renewal and replacement 18
2.3 AUTHENTICATION 18
2.3.1 Authentication mechanism 18
2.4 MANAGEMENT AND ORGANISATION 19
2.4.1 General provisions 19
2.4.2 Published notices and user information 20
2.4.3 Information security management 21
2.4.4 Record-keeping 22
2.4.5 Facilities and staff 22
2.4.6 Technical controls 24
2.4.7 Compliance and audit 26

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	Bob Hulsebosch	CEO	20-12-2022

1 Introduction

This document maps the characteristics of the identity verification services provided by Inverid's ReadID software to the requirements of the eIDAS Level of Assurance High as defined in Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of the eIDAS Regulation [eIDAS].

Inverid is not an eIDAS notified electronic identity provider or an eIDAS qualified trust service provider. Its ReadID software provides essential identity verification services for these eIDAS parties that help them offering their services. More specific, ReadID provides identity document verification services based on Near Field Communication technology.

Near Field Communication (NFC) leverages government-issued identity documents with contactless NFC chips and smartphones for remote identity verification. The chip on these documents contains data, including a high resolution face image, provided and digitally signed by the issuing country.

ReadID reads the identity data from the chip and not only verifies their authenticity, it also verifies if the identity document presented by the user is authentic and valid. Based on the facial image read from the chip, additional services such as holder verification are possible to increase the assurance level of the identity of the user. This is typically done by partner organisations such as biometric verification providers that also participate in the electronic identification scheme.

The assessment of ReadID against eIDAS 2015/1502 is therefore scoped to the identity registration and identity document verification services and its provisions for enabling face matching and identity document holder verification services. The face matching and identity document holder verification services offered by other partners participating in the scheme are out of scope of the assessment.

1.1 ABOUT READID

1.1.1 Overview ReadID products

ReadID provides functionality for identity document Machine Readable Zone (ReadID MRZ) scanning and for chip reading and verification (ReadID NFC). The client-side (Client Software) can be provided as an SDK and/or as a ready-to-use app called ReadID Ready App. The SDK can be provided in two versions: ReadID SDK Base and ReadID SDK UI. The ReadID Ready App is available in three different version (Basic, Branded, Enterprise). As part of the Client Software a facial matching capability may be included, and if this is the case, then also the corresponding server capabilities. The below table indicates which Client Software is provided in this Agreement. Below the table we describe these in more detail.

If facial matching is included then the ReadID SaaS Server will orchestrate with a facial matching capability provided by a partnering biometric verification provider and the Client Software will include functionality to help the user take a selfie. Details are described below in the Facial Matching section.

1.1.2 ReadID SaaS Server

Independent of the client-side, the ReadID SaaS Server, or ReadID Server for short, is provided to the Customer as a SaaS solution, with a ReadID Server that has a REST API and management console. The Customers has to use the management portal to configure the Application and/or ReadID Ready App. The server does all the processing and verifications of the read data by the client. A public cloud provider hosts the server.

The ReadID SaaS Server can be provided as a single- or multi-tenant environment and is hosted by a public cloud provider. A single-tenant environment will not be used by other customers. In a multi-tenant setting, the same environment is used by multiple customers.

1.1.3 ReadID SDKs

ReadID SDKs are so-called native SDKs. For iOS is based on SWIFT, for Android on Java. On both platforms it exists in low-level versions called SDK Base, which does not include screens, and a high-level version called SDK UI that implements a best-practice user experience (UX) with the screens and animations included and less detailed options. Which versions of the SDK and for which mobile OSes are provided as part of this Agreement is indicated in the above table with the boxes that are checked.

1.1.4 ReadID Ready: Basic, Branded, Enterprise

ReadID Ready can be considered a version of ReadID SDK but with a ready-to-use app contrary to having ReadID SDK to integrate. The ReadID Ready app is provided by Inverid. It implements MRZ scanning and NFC reading, with the verification of the chip being done at the ReadID SaaS server. The Customer has to implement a website and/or app to get a ReadID Ready token from SaaS server, and use this to initiate the ReadID Ready app.

The Basic version of the ReadID Ready app does not contain any branding for the Customer. The Basic version of the ReadID Ready app is provided to users via the Play Store and/or App Store using Inverid/ReadID branding.

The Branded version of the ReadID Ready app extends the Basic version in that it displays Customer branding after the ReadID Ready token is known (for example after a QR scan).

The Enterprise version is provided in the Play Store and/or App Store using Customer branding, and does not display any ReadID branding (white-label). Unless agreed otherwise, the Enterprise version is provided in the Play Store and/or App Store under an account of the Customer. The Customer is responsible for setting up the account and the app listing. The Customer will provide developer accounts to the Play Store and/or App Store for Inverid to upload new ReadID Ready versions. The Customer is responsible for the actual promotion of the new version to production. The Customer will promptly do this when a new version is available, after doing appropriate testing. The Customer understands that if this is not done promptly that the ReadID Ready app may not work properly or not work at all. The exact procedure is described in the Documentation and Inverid may change this over time.

1.1.5 Management Portal

Inverid provides a Management Portal that allows customers to configure the ReadID Server as well as the configuration and customisation of the ReadID Ready app and the configuration of the SDK. The portal also provides access session information and to technical documentation. Access to the portal is based on strong authentication.

1.1.6 Machine Readable Zone (MRZ) scanning

The MRZ SDK or the ReadID Ready app enable the User to use the device camera of their mobile device to scan the Machine Readable Zone of ICAO DOC 9303 compliant identity documents (TD1, TD2 and TD3) and ISO18013 compliant electronic driving licenses using Optical Character Recognition technology.

1.1.7 Chip reading and verification

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

- the Basic Access Control (BAC) or Password Authenticated Connection Establishment (PACE) security mechanisms for getting access to the chip;
- the Passive Authentication security mechanism for verifying the authenticity of the read data;
- the Active Authentication or Chip Authentication (EAC-CA) security mechanisms 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 implements the reading and verification of the contactless chip in Dutch electronic driver's licences (ISO 18013 compliant, these are in circulation since around November 2014). Specifically, ReadID implements for Dutch electronic driving licences:

- 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.

Password Authenticated Connection Establishment (PACE) is a successor of BAC that uses more modern cryptography to provide an increased level of security. EU mandates the implementation of PACE by its member states for newly issued travel documents. Passports that have support for PACE also support BAC to remain compatible with the ICAO 9303 standard, that requires documents that support PACE to also support the older BAC.

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 Customer 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 Customer Inverid provides information on the sources of the country certificates.

ReadID works with identity documents from over 100 countries, including all countries from the EU, Canada, USA, Australia and New Zealand.

1.1.8 Android support

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 Customer 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.

Problems may occur with specific smart phones due to the NFC implementation, or with new Android versions. In that case, if possible and commercially reasonably, ReadID will be updated. Examples of problems are phones that do not support NFC-B or do not support extended length ADPUs. There may be smart phones or tablets on which ReadID does not function or functions less efficiently.

1.1.9 iOS support

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.

1.1.10 Supported identity documents

There may be identity documents that are not, or not fully, standard compliant or otherwise cause problems when scanning, reading or verifying them. In that case, if possible and commercially reasonably, ReadID will be updated. For some documents Inverid may not have the correct country certificate to be able to execute passive authentication. Some identity documents may not work with certain smart phones or tablets.

1.1.11 Data processing

Data read from the identity documents is not stored on the mobile phone of the applicant but directly send to ReadID server that is hosted by a public cloud provider. The ReadID server stores the identity and verification data until it is retrieved by the TSP. A hard-coded maximum retention period of 50 days is enforced for data storing. TSPs, however, are advised to set a smaller period, e.g., no more than a few days. This period is sufficient to allow for investigation of possible bugs or fraud attempts. After the retention period expires, the data is permanently removed. By default, ReadID Server creates a snapshot of the database once every day and retains it for one or two weeks depending on the agreements with TSPs or other customers.

The ReadID Server is provided to the TSP as a SaaS solution, via a REST API and management portal. The TSP has to use the management portal to configure the SDK in its own mobile app. The ReadID Server is provided as a single or multi-tenant environment. For the latter environment, multiple customers are using the same environment. When the ReadID Server is provided as a single-tenant environment, the environment will not be used by other customers.

The data exchanged between ReadID NFC and ReadID Server is protected using strong TLS-encryption. For the use of specific TLS versions and cypher suites we . For the use of specific TLS versions and cypher suites we strive for an ‘A-rating’ at Qualys SSL Labs[1]. The customer can and is recommend to ‘pin’ the server certificate in the mobile client, to further prevent man-in-the-middle attacks. By default, ReadID NFC is configured with two certificates, either one of which must be present in the certificate chain. The interface of this communication is a RESTful API, but not further exposed to the customer and prone to changes.

1.1.12 Facial matching and orchestration

Additionally, identity document holder verification can be done by matching the facial image read from the chip with a selfie image of the user. The facial matching and liveness detection capability is not provided by Inverid but by a partnering biometric verification provider. For the Customer, various ways of orchestration with Inverid’s ReadID and the biometric verification provider are possible:

1. Customer does the orchestration: this means that the Customer has separate contracts and interfaces with ReadID and with the biometric verification partner.
2. ReadID does the orchestration: this means that the Customer has a single contract and interface with ReadID and that ReadID interfaces with the biometric verification provider. ReadID and the biometric verification provider have a separate contract that is aligned with that between ReadID and the Customer.
3. Hybrid orchestration of options 1 and 2: this means that the Customer has a contractual agreement with both ReadID and the biometric verification provider and only one interface with ReadID; the biometric verification provider has an interface with ReadID.

ReadID thus has to support the following two interfaces that are relevant in the scope of this eID assessment:

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

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 matching, 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 and spoofing attempts, and is also sometimes referred to as liveness. Both the facial matching and Presentation Attack Detection may produce false rejects.

The Customer needs to use one of the NFC SDKs and/or ReadID Ready to be able to use the facial matching service. In case the Customer uses one of the NFC SDKs, then the Customer will additionally be provided with a facial matching SDK. This SDK helps the User to take a good selfie and securely sends this to the facial matching server. If ReadID Ready is used, then the facial matching SDK is also integrated by Inverid in the app.

Each orchestration model is contractually established. If ReadID does the orchestration, the template contract with facial partners addresses aspects such as:

- Service and support;
- Duration and termination;
- Conformity and liability;
- Confidentiality and personal data including a DPA appendix;
- SLA;

[1] See https://www.ssllabs.com/.

- Security measures including right to audit.

The required security measures overlap with those required for compliance to the generic "Management and organisation" requirements of eIDAS CIR 2015/1502.

1.2 TYPICAL READID FLOW

When an applicant applies for an electronic identification means or qualified certificate at an eID means or trust service provider, the ReadID part in this process is as follows:

1. The eID means or trust service provider informs the applicant about the terms and conditions and the applicant expresses his/her will to enrol for an eID means or qualified certificate. Note that this is done by the eID means or trust service provider, not Inverid.
2. The applicant is asked to register. The registration is done via the mobile app of the eID means or trust service provider that contains the ReadID SDK or the ReadID Ready app. In the latter case, the a ReadID Ready session has to be created that is bound to the Ready app of the applicant. The binding can be done by either scanning a QR code shown on a website of the TSP or by starting the app via a website or mobile app of the TSP, the result of which is validated on the ReadID Server.
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. The relevant datagroups are read from the chip. The data contains 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 data is performed by the server by validating a digital signature over the files read in the identity document and checking against a list of trusted country certificates of document signers. This certificate list effectively determines which documents will be marked as valid. It is maintained by ReadID. Moreover, it can depend on the specific customer what sources of trusted certificates are used. What certificate was actually used is communicated to the customer as well, i.e., it is transparent to the customer.
   - 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 out of scope for the assessment but illustrates how extra identity assurance can be achieved by doing biometrics based verification. In this case, the high resolution photo retrieved from the chip with NFC technology is shared with a 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.
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 eID means provider or trust service provider. Their server can then get the actual outcomes from the ReadID Server.

The overall outcome of the identity validation process 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 (out of scope for this assessment).

These identity data and verification results are made available to the eID means provider or trust service provider 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 eID means or trust service provider; they control how long this caching is. They can use the date of expiry obtained from datagroup 1 of the chip to check if the document is not expired.

Alternatively, the eID means provider or trust service provider may choose to contract and interface with its own biometric verification provider. This means that they have to do the orchestration of data exchanges with ReadID and the biometric verification provider themself to come to the required identity validation outcome.

Read data is not persisted to the phone storage by the ReadID MRZ and ReadID NFC libraries. It is however cached by ReadID Server until deleted using an API call from the customer backend, or if the session expires after a pre-configured retention period. A hard-coded maximum retention period of 50 days is enforced for sessions, but the customer is advised to set a smaller period, e.g., no more than a few days, to allow investigation of possible bugs or fraud attempts. After the session expires it is permanently removed, unless it was captured in a backup of the database. By default, ReadID Server creates a snapshot of the database once every day and retains it for a maximum of 14 days. Shorter periods may be agreed with a customer.

The data exchanged between the ReadID SDK or the ReadID Ready app and ReadID server is protected using strong TLS encryption. The server certificate is ‘pinned’ in the mobile client, to further prevent man-in-the-middle attacks.

The exchange of face images to the server of the sub-contracted biometric verification provider and its holder verification outcomes are protected using strong TLS-encryption and certificate pinning as well.

1.3 SCOPE OF THE ASSESSMENT

This eIDAS electronic identification self-assessment is scoped to the ReadID SDK/SaaS and Ready solutions. Moreover, it takes into account the technical and organisational aspects of the interfaces for data exchange with customers and biometric verification providers as facial partners for holder verification. It does not assess the remaining electronic identification activities that take place at their sites. For the technical interfaces the focus is on the security (i.e. confidentiality and integrity) of the data exchange between ReadID and its customers and facial partners. For the organisational interfaces the focus is on contractual aspects (e.g. data protection agreement, availability, and right to audit) as well as communication aspects (e.g. points of contact and problem solving procedures). The assessment of the biometric verification providers is outside the scope of this assessment.

1.4 DEFINITIONS

1.4.1 Acronyms

Applicant: End-user that applies for a qualified certificate or eID means.

Biometric verification provider: sub-contractor of Inverid that does holder verification, i.e. face matching and liveness or presentation attack detection.

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

Customer: The party to whom Inverid provides its services, typically this is an eIDAS electronic identification provider or trust service provider.

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.

Partner: An organisation that participates in an electronic identification scheme and provides complementary services to Inverid's ReadID services. A biometric verification provider is an example of a partner.

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

Subject: The subject of a certificate is the party named in the certificate as the holder.

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. A public cloud provider is a sub-contractor of Inverid and hosts the ReadID server.

1.4.2 Acronyms

CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation List
DG	Data group
DMZ	Demilitarised Zone
eID	Electronic identification
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HSM	Hardware Security Modules
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
RA	Registration Authority
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TSP	Trust Service Provide
TSP/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
eMRTD	e-machine readable travel documents
eDL	electronic driving license
AA	Active Authentication
APDU	Application Protocol Data Unit
BAC	Basic Access Control
BAP	Basic Access Protection
CA	Chip Authentication
EAC	Extended Access Control
EAP	Extended Access Protection
MAC	Message Authentication Code
PA	Passive Authentication
RFID	Radio Frequency Identification
SM	Secure Messaging
TA	Terminal Authentication

2 Technical specifications and procedures

The elements of technical specifications and procedures outlined in the annex of the Commission Implementing Regulation (EU) 2015/1502 will be used to determine how the requirements and criteria of article 8 of Regulation (EU) no. 910/2014 will be applied for electronic identification means issued under an electronic identification scheme.

The assurance levels as defined by article 8 are:

- Low, referring to an electronic identification solutions which provides a limited degree of confidence in the claimed or asserted identity of a person,
- Substantial, referring to an electronic identification solution, which provides a substantial degree of confidence in the claimed or asserted identity of a person,
- High, referring to an electronic identification solution, which provides a high degree of confidence in the claimed or asserted identity of a person.

2.1 ENROLMENT

2.1.1 Application and registration

LOW

1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means.

Since Inverid is not the primary issuer of the electronic identification (eID) means, this requirement does not directly apply. For transparency reasons Inverid nevertheless publishes a generic privacy statement and underlying policies. Moreover, for ReadID Ready the applicant is informed by the app about its purposes.

The ReadID privacy policy is published on our website: https://readid.com/about/privacy.

The ReadID Ready privacy statement can be found here: https://readid.com/docs/readid-ready/privacy-policy.

2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means.

Since ReadID is not the primary issuer of the eID means, this requirement does not apply.

Basic Access Control is implemented to prevent unauthorised access to data on the chips of identity documents supported by ReadID.

3. Collect the relevant identity data required for identity proofing and verification.

ReadID collects relevant identity data from official identity documents in an optical or electronic manner via an SDK that is integrated in the mobile app of the customer or via the ReadID Ready app itself. Optically the identity data is obtained from the Machine Readable Zone (MRZ) with Optical Character Recognition technology. The MRZ contains amongst others the family name, first name(s) and date of birth of a natural person. This set of attributes corresponds with the minimum data set as specified in eIDAS CIR 2015/1501 to uniquely identify a natural person.

Electronically the data is read from the chip by ReadID and via NFC technology. The data read from the chip contains family name, first name(s) and date of birth and also meets the minimum data set requirement of eIDAS CIR 2015/1501 to uniquely identify a natural person. Additionally, the read data may also contain several optional eIDAS attributes such as gender, nationality, and place of birth.

This information has been provided by the issuing country of the identity document, based on strict government identity verification and issuing processes. Besides providing very reliable personal information, another major advantage is that all data is electronically available. There is no manual input required, so there can be no mistakes in the data.

In addition, the chip contains a high-resolution photo, suitable for face matching. 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 information and photo are signed digitally, they cannot be altered.

SUBSTANTIAL

Same as level low except that the optical option for data collection is excluded.

HIGH

Same as level substantial.

2.1.2 Identity proofing and verification (natural person)

LOW

1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity.

For identity proofing and verification ReadID makes use of official and chip-containing identity documents, e.g.:

- passports and residence permits that meet the International Civil Aviation Organisation (ICAO) specifications for machine-readable travel documents,
- identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards, or,
- EU or EEA driving licences that follow the European Directive 2006/126/EC.

As said, these identity documents are government issued with strict identity verification and issuing requirements and, as such, provide an authoritative source for identity proofing and verification.

2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.

Covered by levels ‘Substantial’ and ‘High’ below.

3. It is known by an authoritative source that the claimed identity exists, and it may be assumed that the person claiming the identity is one and the same.

See above and covered by levels ‘Substantial’ and ‘High’ below.

SUBSTANTIAL

Level low, plus one of the alternatives listed in points 1 to 4 has to be met:

1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity

Covered by level ‘High’ below.

and
The evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person.

The validity can be checked by looking at the expiration date of the identity document. The authenticity is checked by validating the digital signature of the data obtained from the chip via NFC against a list of country signing certificates.

Several online databases of trustworthy Country Signing Certificates exist. For example, the French, German, Italian, Schengen, Swiss and Spanish CSCA master lists are published by each of these respective countries, specifying which certificates it considers trustworthy. Typically, the Country Signing certificates are obtained through diplomatic exchanges. ReadID is flexible in this regard and can work with any provided database. Our customers may deviate from these lists by adding or removing certificates at their own discretion. Currently, the ReadID SDK is equipped with the German list. Providing ReadID with a recent and correct list of trusted Country Signing Certificates is a continuous effort conducted by the ReadID team to the best of our efforts, as a service to our customers. For each new release of the ReadID SDK the most recent version of the list is included.

Furthermore, clone detection mechanisms are in place to check the authenticity of the chip itself.

and
Steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked, or expired evidence.

ReadID does not check for lost/stolen documents. When combined with biometrics and liveness detection functionality utilized for proofing holder verification this does not make any sense. In case ReadID is used without holder verification functionality, the eID means or trust service provider has to do the lost/stolen check.

2. An identity document is presented during a registration process in the Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account, for instance, the risk of lost, stolen, suspended, revoked, or expired documents.

See option 1 above.

3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2. for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in article 2 (13) of Regulation (EC) no. 765/2008 of the European Parliament and of the Council (1) or by an equivalent body.

Does not apply to ReadID.

4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in article 2 (13) of Regulation (EC) no. 765/2008 or by an equivalent body.

Does not apply to ReadID.

HIGH

Requirements of either point 1 or 2 have to be met:

1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met:

(a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according

to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source.

Via NFC, ReadID obtains the high resolution face image from the chip of a valid identity document. This face image could be shared via a secure channel with a biometric verification provider that compares it with biometric evidence provided by the user himself and performs presentation attack or liveness detection. Such biometric evidence typically consists of a video recording of the user's face by the mobile phone. Stills from the recording are matched against the face image obtained from the chip. In doing so, it can be demonstrated that the user scanning the identity document is indeed the rightful owner of that document (i.e. identity document holder verification).

(b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2. for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in article 2 (13) of Regulation (EC) no. 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid.

Does not apply to ReadID.

(c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in article 2 (13) of Regulation (EC) no. 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid.

Does not apply to ReadID.

OR

2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.

Does not apply to ReadID.

2.1.3 Identity proofing and verification (legal person)

ReadID is used only for identification of natural persons; therefore, 2.1.3. is not applicable.

2.1.4 Binding between the electronic identification means of natural and legal persons

ReadID is used only for identification of natural persons; therefore, 2.1.4. is not applicable.

2.2 ELECTRONIC IDENTIFICATION MEANS MANAGEMENT

2.2.1 Electronic identification means characteristics and design

LOW

1. The electronic identification means utilises at least one authentication factor.

Does not apply to ReadID.

2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.

Does not apply to ReadID.

SUBSTANTIAL

1. The electronic identification means utilises at least two authentication factors from different categories.

Does not apply to ReadID.

2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.

Does not apply to ReadID.

HIGH

Level substantial, plus:

1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential.

Does not apply to ReadID.

2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

Does not apply to ReadID.

2.2.2 Issuance, delivery, and activation

LOW

After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.

Does not apply to ReadID.

SUBSTANTIAL

After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.

Does not apply to ReadID.

HIGH

The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

Does not apply to ReadID.

2.2.3 Suspension, revocation, and reactivation

LOW

1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.

Does not apply to ReadID.

2. The existence of measures taken to prevent unauthorised suspension, revocation, and/or reactivation.

Does not apply to ReadID.

3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.

Does not apply to ReadID.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.2.4 Renewal and replacement

LOW

Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.

ReadID-based identity data and document verification can be used for renewal and replacement purposes.

SUBSTANTIAL

Same as level low.

HIGH

Level low, plus:

Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

ReadID-based identity data and document verification can be used for renewal and replacement purposes. It uses identity data that is verified with an authentic (i.e. not cloned or copied) government issued identity document.

2.3 AUTHENTICATION

2.3.1 Authentication mechanism

LOW

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.

Does not apply to ReadID.

2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against compromise, including analysis offline.

Does not apply to ReadID.

3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay, or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.

Does not apply to ReadID.

SUBSTANTIAL

Level low, plus:

1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication.

Does not apply to ReadID.

2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay, or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.

Does not apply to ReadID.

HIGH

Level substantial, plus:

The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay, or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.

Does not apply to ReadID.

2.4 MANAGEMENT AND ORGANISATION

ReadID is based on nationally issued official identity and travel documents that can be read via NFC.

2.4.1 General provisions

LOW

1. Providers delivering any operational service covered by this regulation are a public authority or a legal entity recognised as such by national law of a Member State, with an established organisation, and fully operational in all parts relevant for the provision of the services.

ReadID is registered under number 64870596 in the Commercial Register of the Dutch Chamber of Commerce.

2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity-proofing is conducted, what information may be retained, and for how long.

ReadID is GDPR compliant. Any other additional customer specific national or sector specific legislation and that ReadID has to comply to is taken care of in contractual agreements.

3. Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services.

ReadID has a liability insurance with sufficient financial coverage.

4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties.

ReadID makes use of a public cloud provider that hosts the ReadID server. It is contractually, organisationally and technically ensured that this cloud provider fulfils the relevant requirements to remain compliant with eIDAS CIR 2015/1502.

5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.

ReadID in itself is not an identification scheme. It may, however, provide its services in the context of an electronic identification scheme, i.e. as a sub-contractor for an identity provider that participates in such scheme. In such case, contractual provisions are in place to cater for a controlled termination of the ReadID services.

In case of Inverid's termination of ReadID activities, contractually or otherwise, all customers and other relying parties (e.g. partners) will be informed about this conform the contractual agreements and conform regulatory and legal requirements.

An exit plan will be drawn up, dealing with post-contractual services that may be provided by Inverid 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 customer to migrate to an alternative and to minimise the impact as much as possible.

Furthermore, before termination of its services, Inverid will terminate any applicable authorisations of sub-contractors to act on behalf of it in carrying out any functions relating to customer processes.

All data collected by ReadID for identity verification purposes will be archived in such a way that both its confidentiality and its accessibility for required consult are ensured. ReadID has an audit log which Inverid will retain for 10 years and will provide to the customer at contract end. This also holds for sub-contracted partners such as biometric verification providers. Technical application logs will remain available for one year after contract end.

Should Inverid ReadID ceases its activities then the technical application logs will remain available via Inverid B.V.

Termination or dissolution of the contract between Inverid and the customer 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. These obligations may be transferred to Inverid B.V.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.2 Published notices and user information

LOW

1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy.

Applicable terms and conditions are defined and explained under section 1.2 of this document.

Fees are contractually established between Inverid and the electronic identity provider acting under eIDAS. The fees of the electronic identity provider may be bound to national legislation.

The Trust Service Practices statements of ReadID SaaS with SDK and Ready describe the practices for reading and verifying identity documents. These document are published on the Inverid website (www.inverid.com). Obviously, applicants without a chip-containing identity document cannot be provisioned by ReadID.

Usage of personal data and privacy is regulated by the GDPR, which provides the conditions and procedure for processing of personal data, the procedure for the exercise of state supervision and administrative supervision upon processing of personal data, and liability for a violation of the requirements for processing of personal data, which must be followed by public and private parties.

The general ReadID privacy policy is published on our website: https://readid.com/about/privacy.

The ReadID Ready specific privacy statement can be found here: https://readid.com/docs/readid-ready/privacy-policy.

2. Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service.

Not being the primary identity provider, ReadID itself does not have direct contact with the user of the service. Consequently, this requirement does not apply to ReadID.

3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.

This is taken care of in the contract between ReadID and the primary customer. In case of a data breach, the primary customer will be informed about this in a GDPR-compliant manner.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.3 Information security management

LOW

There is an effective information security management system for the management and control of information security risks.

ReadID has implemented an Information Security Management Systems (hereafter “ISMS”).

Please see the description below under substantial and high.

SUBSTANTIAL

Level low, plus:

The information security management system adheres to proven standards or principles for the management and control of information security risks.

ReadID’s ISMS is ISO/IEC 27001:2013 certified with a scope that is related to identity verification services. The Statement of Applicability covers all aspects. Moreover, it is extended with the privacy-related controls from ISO/IEC 27701:2019. This standard 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 that hosts the ReadID Server that processes all identity document data, does all the verifications and may orchestrate data exchanges is a sub-contractor of Inverid. 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 for eID providers or trust service providers operating under eIDAS. 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).

HIGH

Same as level substantial.

2.4.4 Record-keeping

Collecting data and records, maintenance, archiving, and protection of all relevant records and data is conform GDPR and any other applicable national legislation, subordinate regulations, and internal procedures.

LOW

1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.

Primary customers have to collect the scanned data from our servers within a certain period of time. Scanned data is kept for a limited period at the ReadID servers; data will be permanently deleted if this period expires. ReadID servers are hosted on a public cloud provider environment in Europe.

All the records are accessible only for personnel that have a trusted role within the Inverid organisation.

All security events, events related to identity document reading and verification are logged. This logging data is stored for a period of time in accordance with national or customer requirements.

2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.

While stored at our servers data is being encrypted. Audit logs are secured and stored for a period of minimal 7 years.

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.5 Facilities and staff

LOW

1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil.

Training, qualifications and experience requirements related to the staff and subcontractors are covered by ReadID’s ISMS, as part of the controls “A.7. Human resource security” of the ISO/IEC 27001 standard.

At ReadID staff are employed and trained according to dedicated job profiles (general framework and qualification requirements) and job descriptions (detailed work characteristics and responsibilities). Each ReadID employee has to follow basis security training courses. Where relevant, additional dedicated training programmes for staff members also exist (e.g., identity-proofing and fraud). This ensures that procedures are performed by trained, qualified, and experienced staff. Background checks are implemented during recruitment and employment as a routine precautionary measure. Duties are performed according to formalised processes, and special obligations of due diligence exist. Job profiles, training programmes, procedures, and processes are monitored and updated on a regular basis.

The requirements for contractors come from the eIDAS Regulation and the contract with ReadID.

2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.

The availability requirements related to the staff and subcontractors are covered by ReadID’s ISMS, as part of the controls “A.12. Operations security” of the ISO/IEC 27001 standard. In particular, adequate capacity management for human resources is implemented including projections based on the needs in business resources. ReadID is constantly hiring new employees in the areas of software development and security in order to be able to adequately operate and resource our services.

In addition, ReadID includes service level agreements in their contracts with subcontractors covering the need for sufficient subcontractors to adequately operate and provide resources for the services. Regarding subcontractors there is policy to have multiple parties to choose between.

3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access, and other factors that may impact the security of the service.

The physical and environmental security, access control and operations security requirements related to the facilities used for providing the service are covered by ReadID's ISMS, as part of the controls "A.11. Physical and environmental security" and "A.9. Access control" and "A.12. Operations security" of the ISO/IEC 27001 standard.

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 registration and document verification service provider for electronic identification 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.

Additionally, business continuity and disaster recovery plans are available to address damage caused by for instance external environmental threats, internal malicious actors and the compromise or suspected compromise of services.

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.

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 cloud provider has ISO27001 certification or similar.

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, keys are distributed to a limited set of engineers. Personal information is in a locked closet, where the keys are restricted to the managing partners.

The physical and environmental security, access control and operations security requirements are also covered as part of the relevant controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401].

4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic, or other sensitive information is limited to authorised staff or subcontractors.

The access control requirements related to the areas holding or processing personal, cryptographic or other sensitive information are covered by ReadID's ISMS, as part of the controls "A.9. Access control", "A.10. Cryptography" and "A.18.1.5. Regulation of cryptographic controls" of the ISO/IEC 27001 standard.

Moreover, the access control requirements related to the areas holding or processing personal, cryptographic or other sensitive information are also covered as part of the relevant controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401].

SUBSTANTIAL

Same as level low.

HIGH

Same as level low.

2.4.6 Technical controls

LOW

1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity, and availability of the information processed.

The risk management and technical controls implemented to manage the risk posed to the security of the services are covered by ReadID's ISMS, as part of the controls "A.10. Cryptography", "A.12. Operations security", "A.17. Information security aspects of business continuity management" and "A.18.1.5. Regulation of cryptographic controls" of the ISO/IEC 27001 standard.

ReadID has implemented a risk management methodology in order to identify and implement proportionate technical controls to manage the risks posed to the security of the services. In particular,

- ReadID periodically performs risk analyses (at least once a year);
- ReadID implements proportionate technical controls as part of the risk treatment activities.

For ReadID as well as for other partners involved in the provision of identity verification services for eID and qualified trust service providers operating under eIDAS, the risk management and technical controls implemented to manage the risk posed to the security of these services are also covered as part of the relevant controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401].

Please refer to the ReadID Security Architecture whitepaper for more details on the implemented security controls[2].

Inverid has a business continuity management policy in place to ensure the availability of our services.

2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation, and replay.

The protection of communication channels used to exchange personal or sensitive information are covered by ReadID's ISMS, as part of the controls "A.10. Cryptography", "A.13. Communications security" and "A.18.1.5. Regulation of cryptographic controls" of the ISO/IEC 27001 standard.

The electronic communication channels used to exchange personal or sensitive information between the ReadID components, customers and partners for identity verification purposes are protected against eavesdropping, manipulation and replay as described in our ReadID Security Architecture whitepaper[2].

For ReadID as well as for other partners involved in the provision of identity verification services for eID and qualified trust service providers operating under eIDAS, the protection of communication channels used to

[2] Security and architecture overview for ReadID SaaS, whitepaper, version 1.3, 2019.

exchange personal or sensitive information is also covered as part of the relevant controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401].

3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text.

The access control to sensitive cryptographic material is covered by ReadID's ISMS, as part of the controls "A.9. Access control" and "A.10. Cryptography" of the standard [ISO/IEC 27001], as well as the controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401]. Please refer to the ReadID Security Architecture whitepaper for more details[2].

4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents, and security breaches.

The procedures for ensuring that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches are covered by ReadID's ISMS, as part of the controls "A.14. Security in development and support processes" and "A.16. Information security incident management" of the standard [ISO/IEC 27001]. These controls are described in ReadID's internal security policies. Examples of these are:

a) Risks are evaluated once a year.

b) For emergency patches, there are separate, secure procedures.

c) There is a 24/7 team that is able to handle and solve incidents adequately.

d) Subcontractors are assessed periodically by ReadID employees.

e) Monitoring controls are in place to detect and respond to abnormal, malicious or, disrupting events impacting the supporting IT systems, users of the IT systems, and/or the critical services provided.

There are processes in place to respond to these events in a timely and co-ordinated manner to limit the potential impact of security breaches and notify the relevant, impacted parties. Procedures are in place to investigate the root-causes of a security breach and remediate the previously unaddressed security vulnerabilities.

Incident management procedures are put in place for correct prioritization and notification, also to external stakeholders.

For ReadID as well as for other subcontractors involved in the provision of identity verification services for electronic identification and qualified trust service providers operating under eIDAS, the procedures for ensuring that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches are also covered as part of the relevant controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401].

5. All media containing personal, cryptographic, or other sensitive information are stored, transported, and disposed of in a safe and secure manner.

The asset management procedures (including storage, transport and disposal) are covered by Inverid's ISMS, as part of the controls "A.8. Asset management" of the standard [ISO/IEC 27001]. These controls are described in Inverid's internal security policies.

Being a provider of identity data and document verification services for trust service provider operating under eIDAS, Inverid's asset management procedures are also covered as part of the relevant controls from the standards [ETSI EN 319 411-1], [ETSI EN 319 411-2] and [ETSI EN 319 401].

This means that all personal, cryptographic or other sensitive data in transit or at rest is encrypted and that access to it is limited to authorised staff only. Moreover, personal data is always processed and stored within Europe.

SUBSTANTIAL

Same as level low, plus:

Sensitive cryptographic material, if used for issuing electronic identification means, and authentication is protected from tampering.

Cryptographic keys are securely generated, stored and transported without compromising its confidentiality and are backed-up to ensure that no information can be lost permanently due to lost keys.

When cryptography is used, only suites of standardized algorithms are used, for example "NSA Suite B" or "TLS 1.2" standardized algorithms. Its implementation is supervised by educated personnel.

Note that the cryptographic keys in scope here are not the keys that are directly associated to the electronic identification means. It concern keys that Inverid requires to secure the processing of the personal data read from identity documents.

HIGH

Same as level substantial.

2.4.7 Compliance and audit

LOW

The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

Internal audits are conducted at least once a year by the compliance officer of Inverid. Critical services are audited twice a year.

SUBSTANTIAL

The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

Please see the description in the following section HIGH.

HIGH

1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.

ReadID is periodically audited by an external auditor for its ISO27001 certification.

ReadID is periodically audited by a conformity assessment body (CABs) accredited against the requirements of the eIDAS Regulation.

ReadID software is periodically pentested by an external professional pentester.

2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.

Does not apply to ReadID.