January 2026

Signicat B.V.

G-Cloud 15 Service Definition for ReadID

Service Definition

What does ReadID do?

ReadID is a UK (DSIT) Digital Identity and Attributes Framework (DIATF) Component and Orchestration Certified Service Provider for verifying people's identity; essential in preventing identity fraud, ensuring Know Your Customer (KYC) and regulatory compliance, as well as building trust in digital citizen engagements. ReadID is the leading solution for verifying biometric identity documents using smartphones and Near Field Communication (NFC) technology.

The validation of such chipped ID documents is widely recognised as the most secure remote identity verification method and is the cornerstone of ReadID. NFC-based document checking can be combined with biometric facial verification to ensure the holder of the document is genuinely present in the process and at the same time preventing common fraud attack methods such as generative AI/deepfakes. Where a chipped document cannot be presented, ReadID offers the fall-back option of an optical document assessment.

Many passports, identity cards, biometric residence permits and other identity documents contain a contactless chip, which ReadID reads to verify the authenticity of these documents. Generally following the ICAO9303 global standard for electronic identity documents, the chip contains 100% reliable personal information about the holder, including the full name, date of birth and nationality. In addition, it contains a high-resolution face image, suitable for facial verification. The information contained in the document chip is validated by the issuing state and thus provides a reliable source of basic identity information.

All modern smartphones have NFC communication capabilities to access and read the chip. ReadID uses this technology to extract document data and prove, via established cryptographic methods, that the data as well as the document itself, is authentic and has not been manipulated.

As well as providing the highest level of assurance that the document is valid, ReadID is completely automated and requires no manual verification steps whatsoever where NFC is the document assessment method used. This implies it can scale almost unlimitedly. NFC-based identity verification is a deterministic, rather than a probabilistic, assessment method and is the only fully-secure solution for remote and automated identity checking with no known false accepts.

To provide full coverage of all document types from different issuing nations, ReadID can be combined with optical document verification as a fallback. This is based on assessment of image(s) of the non-chipped document captured during the verification process. Such assessment is known to be vulnerable to error and fraud attempts but does allow the relying party to widen the document types that can be accepted.

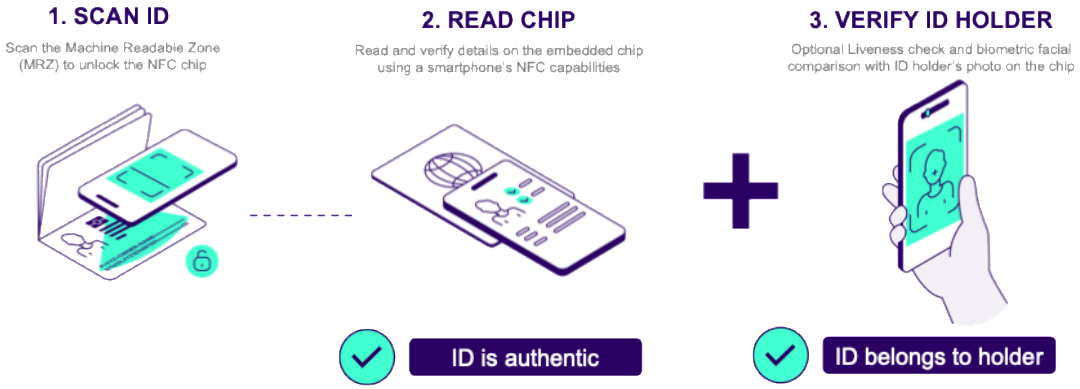
ReadID is the flagship identity verification product of Signicat. It is a core component of the GDS One Login service as well as being used by the UK Home Office - GIDV - in services such as the Electronic Travel Authorisation (ETA).

It has been used in Eurostar SmartCheck for seamless travel. More recently, ReadID has been selected by Frontex and EU Member States for Entry Exit System pre-registration.

Signicat has the responsibility to not only be secure, but also to provide evidence that we are secure. We therefore have a world-unique certification package (ISO27001, ISO27701, eIDAS component certifications, SOC2 type II, ETSI TS 119 461, Cyber Essentials Plus). ReadID is also WCAG 2.2 AA compliant to ensure the service is accessible to a broader range of users.

By verifying the NFC-chip of identity documents, ReadID can help achieve "Score 3" or identity confidence level “high” under GDS Good Practice Guide 45 (GPG 45).

How does it work?



The ReadID verification process consists of three easy steps: (1) Scanning the Machine-Readable Zone (MRZ), (2) reading the chip and (optional, 3) binding the identity to the holder. The user first scans the MRZ in the identity document with their smartphone camera. This is necessary because the MRZ contains the data (specifically the document number, date of birth, and expiration date) used to generate the necessary cryptographic keys required to access the chip, thus preventing unauthorised access. At the same time, if required by the verification process chosen, the ReadID MRZ scan can capture a high-quality photograph of the entire data page from the identity document and extract the printed facial image. This is called Visual Inspection Zone (VIZ) capturing.

In the second step, the user holds their identity document to the back of the smartphone, allowing the chip to be read. Via a secure connection between the smartphone and document, ReadID reads the chip contents, extracts the document’s data, including the high-quality colour photo of the holder and then verifies the authenticity of the data from the chip. Moreover, for chips that support cloning detection, ReadID also verifies the authenticity of the chip, i.e. that it is not cloned. All data processing and each authentication action are performed on a secured ReadID server that is hosted on a public cloud. No security-related processes are executed on the user's smartphone as a further protection against fraud or cybersecurity threats.

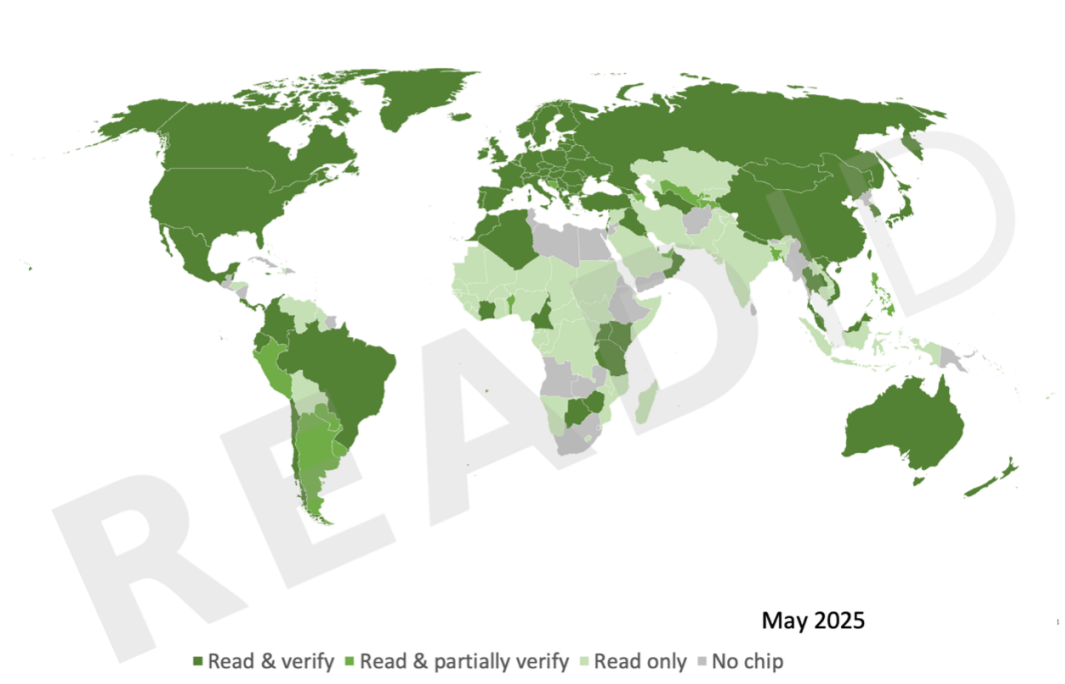
The original and validated passport photo taken from the chip can be used by ReadID biometric facial verification partners for holder verification purposes, via matching of the document photo with a facial image captured via selfie during the live verification process. This verifies that the user is a real person, they are present right now during the remote identity verification process, and that the user is the right person, corresponding to the identity represented by the document being used. The same step also seeks to stop known spoofing methods such as injection and presentation attacks which are ever-more prevalent in the age of accessible and effective AI-powered fraud tools.

If the document is non-chipped, ReadID can fall back to an alternative document verification method, where the Visual Inspection Zone (VIZ) capture process is used to obtain a full image of the passport data page or both sides of an identity or residence permit. These images are then sent to a ReadID optical verification partner during the overall identity verification flow. The optical verification is an automated or hybrid process that uses a combination of technologies, primarily Optical Character Recognition (OCR) and Artificial Intelligence (AI), to extract data from the ID document images and then validate its authenticity.

For facial biometric assessment, using the much-higher quality image from the chip results in a higher reliability for face verification than when using the cropped face image from the VIZ capture and should therefore be preferred if a document with chip is available, resulting in more accepted identities and less friction for the user due to inconclusive face matching results.

ReadID relies on the global ICAO 9303 standard (issued by the UN organisation) that defines specifications for Machine Readable Travel Documents (MRTDs) such as biometric passports, ensuring they have consistent layouts, security features, and data formats, improving interoperability and fraud detection. ReadID can this process any ICAO 9303-compliant document with a chip. This includes passports, (and depending on the country) national identity cards and residence cards. In addition, ReadID supports the Dutch electronic driver's license (which follows the similar, but different, ISO18013 standard).

ReadID thus works with identity documents from over 180 countries, including all countries from the EU, Canada, USA, Australia, and New Zealand. See the figure below for a high-level view of the latest coverage for passports.



ReadID Use Cases

There are two types of use cases: Remote and Face-To-Face. In remote use cases, users verify their own identity using their smartphone, typically as part of a self-service online onboarding or user registration process.

In face-to-face use cases, the verification is executed by an employee who has physical access to the identity document, typically as part of an identity verification process in presence of the user. For example: a bank employee, police or border control officer.

For both use cases, the way a document is captured and authenticated are the same - with a mobile device and using NFC. The main differences lie in the role of a user in the execution of the identity verification operation.

ReadID architecture

ReadID has a client-side component, that runs on a mobile device, such as a smartphone, and a server-side. NFC-based document verification can only be performed using a native mobile application and so the client-side is provided as an SDK (for inclusion in a 3rd party application) or our own ready-to-use app, ReadID Ready. The server-side is provided as a ReadID SaaS server which takes care of all security-related processes. This is the most common architecture to be found with ReadID.

For specific use cases, however, a ReadID Client-only option may be offered. In such cases, all data processing, security checks, cryptographic operations and overall documentation authentication steps can take place client-side.

Machine Readable Zone (MRZ) scanning and Visual Inspection Zone (VIZ) capture (Client-side)

The scanning of the MRZ by ReadID enables the user's mobile device camera to access the chip of an ICAO DOC 9303 compliant identity documents (for TD1, TD2 and TD3 document types) and ISO18013 compliant electronic driving licenses using Optical Character Recognition technology. In addition to the MRZ, ReadID can take a high-quality photograph of the data page from the above-mentioned

identity documents, as well as non ICAO9303-compliant documents and extract the face image from it.

Chip reading and verification

ReadID implements the reading and verification of the contactless chips in identity documents that are ICAO 9303 compliant, as well as for ISO 18013 compliant electronic driver's licences. The reading of the chip is done by the client-side of ReadID, the verification and interpretation of the extracted data is done by the ReadID SaaS server. In addition, the ReadID SaaS server can also verify so-called Digital Travel Credentials Type 1 (DTC Type 1). A DTC type 1 basically is the copy of the content of the chip including the signatures.

Specifically, ReadID implements for chipped identity documents the following:

- Basic Access Control (BAC) security mechanism for gaining access to the chip.
- Password Authenticated Connection Establishment (PACE - the successor to BAC) security mechanism for getting access to the chip.
- Passive Authentication security mechanism for verifying the authenticity of the read data.
- Active Authentication security mechanism for verifying the authenticity of the chip (i.e., clone detection).
- Chip Authentication (EAC-CA) security mechanism for verifying the authenticity of the chip, as an alternative to Active Authentication (i.e., clone detection).
- Reading and interpretation of the data groups (DG) contained within the chip: DG1 with the MRZ information, DG2 with the face image, DG7 with written signature (if present), DG11 with additional personal information (if present) and DG12 with additional document information (if present).

Active Authentication and Chip Authentication do not apply for DTCs, as they are copies by their very nature. Besides the identity data and document verification functionality provided by ReadID SDK and ReadID Ready, the Customer may also need identity document holder verification. This is done via a separate SDK for biometric facial verification (bundled with the ReadID SDK or integrated in the ReadID Ready app) in combination with a server-side for biometric authentication, that is provided by a ReadID biometric verification partner.

ReadID client-side versions

On the client-side, where SDKs are used by the Customer, the ReadID native SDKs are provided for iOS (version 14 and up) and Android (version 8 and up) to be integrated by the Customer into their own mobile application. For iOS these are based on SWIFT, for Android on Java. The SDKs implement best-practice user experiences with screens and animations that guide the user in the execution of the identity verification process.

If the Customer does not want to implement its own application, ReadID Ready offers a ready-to-use application for mobile identity verification. ReadID Ready is managed by and published by Signicat. To use ReadID Ready, the Customer needs to implement a (mobile) website and/or app to get a ReadID Ready token from the ReadID SaaS server and offer this to end users to initiate the ReadID Ready app (often as a QR code). This is particularly useful for web-based customer flows, allowing the user to divert to the ReadID Ready app for the document authentication step before returning the main web flow.

The client-side 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:

- SDK Base - Customer needs to build their own UI in their app and call the ReadID SDK at all the appropriate moments in the flow.
- SDK UI - UI is supplied in the SDK, customer needs to incorporate these UI elements in their own app.

The ReadID Ready App can be provided in three different versions (Basic, Branded, Enterprise):

- The Basic version does not contain any branding for the customer, is is provided to users by Signicat via the Play Store and/or App Store using Signicat/ReadID branding that cannot be altered,
- The Branded version extends the Basic version in that it displays Customer branding. The customer needs to configure the branding via the ReadID management portal.
- The Enterprise version is provided in the Play Store and/or App Store under an account of the Customer and using Customer branding, does not display any ReadID branding (white label).

ReadID can also be provided as a Client-Only option for specific use cases. This is only recommended for trusted devices, i.e., devices under control of the customer. ReadID Client-only cannot orchestrate with face verification or optical fallback, as these are proved as SaaS services.

ReadID SaaS Server

Independently of the client software version, the ReadID SaaS Server is provided to the Customer as a SaaS solution, including a REST API and management console. The Customer uses the management console to configure applications, for security settings, user management and other management settings including the application and/or ReadID Ready App.

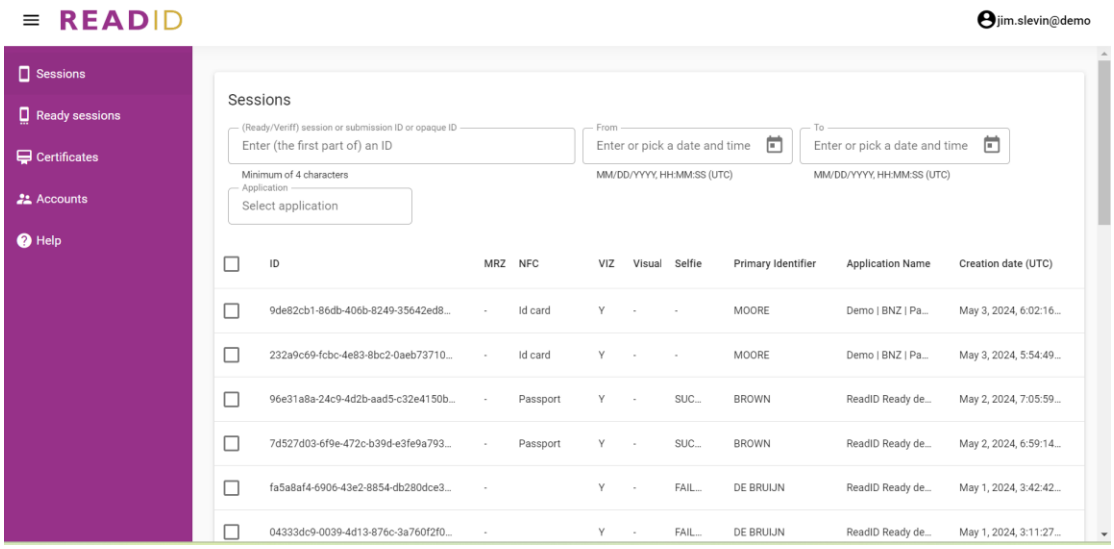
The ReadID SaaS Server is either provided as a multi-tenant environment (i.e., other Customers are using the same environment), or as a single-tenant environment (i.e., the environment will not be shared with other Customers). Signicat may impose transaction limits of the use of the ReadID SaaS Server for performance or other reasons.

Signicat provisions as part of the ReadID SaaS Server a master list of country signing certificates that it considers trusted. Such certificates are issued by the appropriate authorised entity in each document-issuing nation. This list is provided as-is, and it is the responsibility of the Customer to decide to trust or not trust these country certificates. For multi-tenant ReadID Server installations, the master list is shared across the customers using that multi-tenant environment. For Customers with specific requirements, the Customer can provide a different masterlist or their own as well as extensions to the standard country signing certificate master list - such cases will require the Customer to adopt a single tenant deployment. In all cases, the masterlists are managed by Signicat.

All ReadID processing is in European Economic Area (EEA) or UK. Processing outside EEA/UK and/or the use of other sub-processors is subject to approval by Customer. Signicat only caches Personal Data. The Customer controls how long Signicat caches data, but Signicat does not allow more than 50 days. Exception is personal data processed by the facial verification provider, this is in normal cases kept for 30 days and in case of potentially fraudulent sessions up to 1 year. With respect to the processing of personal data: Signicat and its partners are never a controller but only a processor or sub-processor.

ReadID Management Portal

ReadID provides an IAM secured, browser based, Management Portal where the customer can self-manage aspects of their service provision.



ReadID Analytics

In addition to the Management Portal ReadID provide a browser-based analytics platform, ReadID Analytics, which is the customers window to the database of meta information and **anonymous** data gathered from ReadID, including customer SaaS (Software as a Service) transactions. The customer can view their anonymous transaction data, via dashboards, to measure performance without storing any personal data from the identity document. For example, ReadID Analytics will never contain an individual's date of birth, only confirmation as to whether a date of birth was present in the chip at time of verification.

iOS support

ReadID will work 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 14. 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.

ReadID Professional Services

Signicat provides professional support for implementation, onboarding and configuration of the software as well as in the integration of our SDK in the customers app software. End user support is done by the customer. The customer has access to support during working hours. Additional professional services support is available on request.

We can also help in compliance issues as well as in clarifying how our extensive certification package fulfils the customers' needs.

ReadID supporting services

Signicat optionally provides production and supply of ICAO 9303 compliant Test Documents for development, testing and training purposes. Documents are provided in ID Card and Passport formats from country 'Utopia' and are customised for both happy and unhappy flows. Customisation in terms of both the printed data on the cards/passports and more critically the data on the NFC chip.

Documents from Utopia have Digital Certificates in the SaaS pre-production environment only, permitting full authentication of those documents in that environment.

ReadID Security

Signicat is ISO 27001 certified, with ReadID in scope. Signicat regularly tests compliance to the organizational and technical measures both by internal and independent ISO 27001 audits and by organizing regular penetration tests.

Signicat has additionally:

- ISO 27701 certification on privacy management
- eIDAS module certification for Qualified Trust Service Providers
- eIDAS eID module certification for assurance level High
- SOC2 type 2
- ETSI TS 119 461 for capture, processing, and validation of identity evidence
- Cyber Essentials Plus
- UK Digital Identity and Attributes Framework (DIATF) Component and Orchestration Certification

Signicat can at its own discretion decide to maintain these additional certifications or not. Current status of these additional certifications is available upon request.

ReadID Accessibility

ReadID UI SDK and our ready-to-use app ReadID Ready currently fully cover WCAG 2.2 level AA for its mandatory screens and for both Android and iOS.

ReadID Service Level Agreement (SLA)

The following service level agreement only applies to production use of ReadID. Support for non-production use, e.g., demos or testing, is limited to Office Hours and is provided as-is. Office Hours are 08:00 – 18:00 CE(S)T, all working days.

Uptime Percentage

Signicat will take reasonable efforts that the ReadID SaaS Server will be operational 24/7 with at least 99,5% uptime measured on a monthly basis. This percentage is referred to "Uptime Percentage". Excluded Time is not considered downtime.

The Customer is eligible for a Service Credit if this Uptime Percentage is not met in a specific month.

Support

Signicat will provide support on technical issues with ReadID, including on the APIs. Signicat will not support Users of the Customer's Applications. Signicat may require employees or others asking for support on behalf of the Customer to first receive training on ReadID.

Support will unless otherwise agreed with Customer be provided remotely. Should travel be required, then Customer shall reimburse Signicat for all out-of-pocket cost relating to the Support. This includes hotel, travelling and all other out of pocket expenses reasonably and properly incurred by Signicat.

ReadID Orchestrated Service - Facial Verification

Introduction

iProov is a sub-contractor for Signicat that has a service called Enroller that is provided as an Orchestrated Service for facial verification.

Description of the Enroller service

The Enroller service consists of a hosted software-as-a-service platform ("Platform"), the capabilities of which can be consumed through appropriate use of the defined API endpoints in conjunction with SDKs and iProov software that facilitates access to the Platform ("Front-end Software"). References to "Enroller Service" in this document include SDKs and Front-end Software.

ReadID Orchestrated Service - Optical Verification

Description of the core functionalities

Customer can use the Orchestrated Service as provided by the Orchestrated Service Provider (referenced here as: "Veriff") through Signicat.

With a photo (or, when applicable, also a photo of the back) of the User's identification document as input, the Orchestrated Service shall perform the following:

(a) Verification/Fraud Checks

- Quality of document photos
- Document Presence, Tampering and Counterfeit.

(b) Document Data (Depending on selected data extraction fields)

- Data Extraction, including cropping of the face image from the identity document

Integration Types

Customer can submit data through the Veriff SDK or via the ReadID SDK. The following integration types are available:

(a) iOS/Android SDK;

(b) Web (JS SDK); or

(c) API.

Customers are recommended (where applicable for the document) to submit the document front and document back for the session.

Reaching the Verification Decision

After carrying out the verification process and checking the data, Veriff shall make one of the following verification decisions (each a "Verification Decision") which is passed to the Customer via the ReadID Server:

a) A positive Verification Decision: approved; the document photo and the User's portrait photograph are clear and readable, the User's photograph matches the image on the document, there is no suspicion of the manipulation of the data or any other non-compliance of the submitted data.
b) Resubmission of a Verification Decision: resubmission; expected input is missing, poor quality of the submitted data and/or the document type is not supported by Customer.
c) A negative Verification Decision: declined; the verification and inspection of the User is deemed to have suspicious or fraudulent elements.

Please contact us at uk-gov@signicat.com for any questions.