onfido

Remote IDV Practice Statement & Security Policy

V1.4 (03/2025)

onfido

onfido

1. Scope

This document contains or references the policies, processes and technologies used for the identity verification services provided by Onfido acting as an Identity Proofing Service Provider (IPSP).

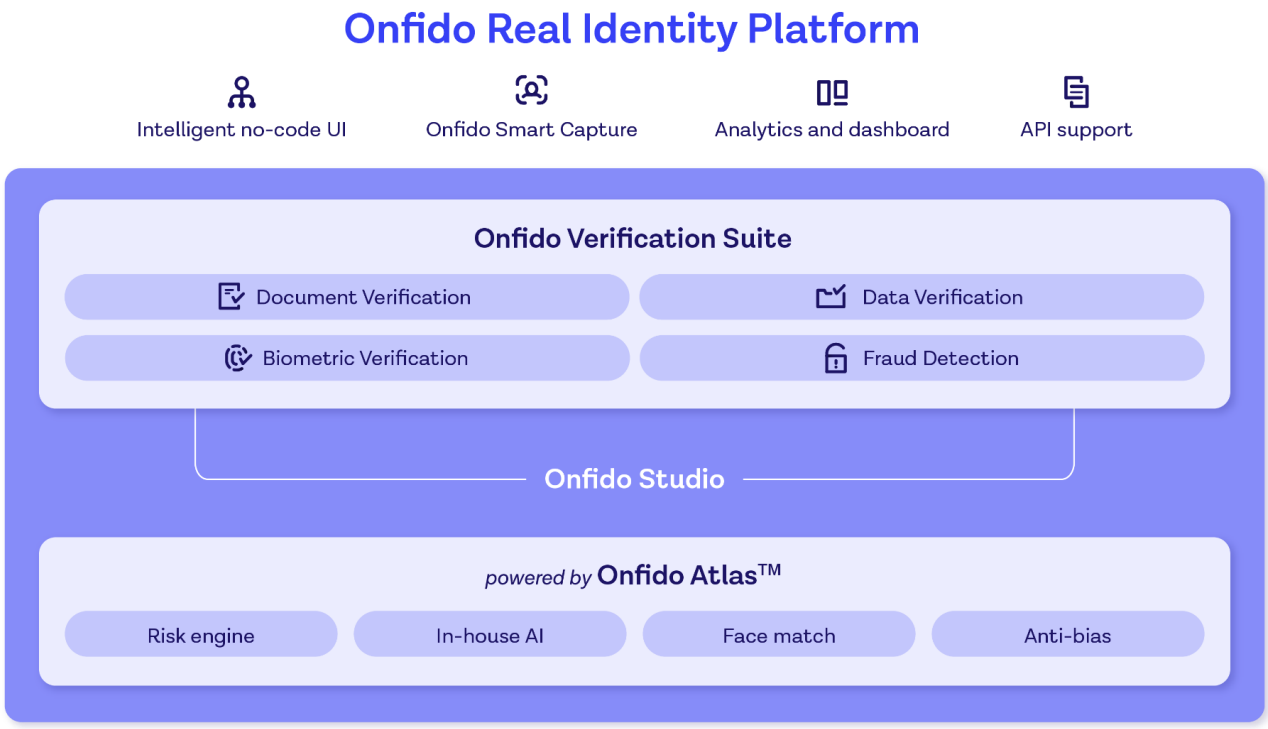
2. References

Title	Version & Date
ETSI 119 461 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects	V1.1.1
ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers	V3.3.1
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS)	2014-08
Commission Implementing Regulation (EU) 2015/1502 for eIDAS	2015-09
Onfido Privacy Policy	Latest (2022-09)
Onfido Services Agreement (OSA)	Latest (2024-01)
Onfido Terms of Use	Latest (2019-04)
Onfido Developer Hub - API, SDK and Product Guides	Latest
Onfido ETSI Certified IDV (Product Guide)	Latest
Onfido ETSI Certified IDV with Qualified Electronic Signature (Product Guide)	Latest
Terms and conditions for ETSI certified identity verification	2023-12

3. Onfido Product Platform Overview

Onfido's Real Identity Platform is an end-to-end flexible identity framework designed to secure trust between Onfido's "**clients**" and their customers ("**users**") at onboarding and throughout the customer lifecycle.

Onfido's platform leverages Document, Biometric, Databases and Passive Fraud Signals to enable identity proofing and verification across a wide range of use cases and defend against increasingly more sophisticated threats.

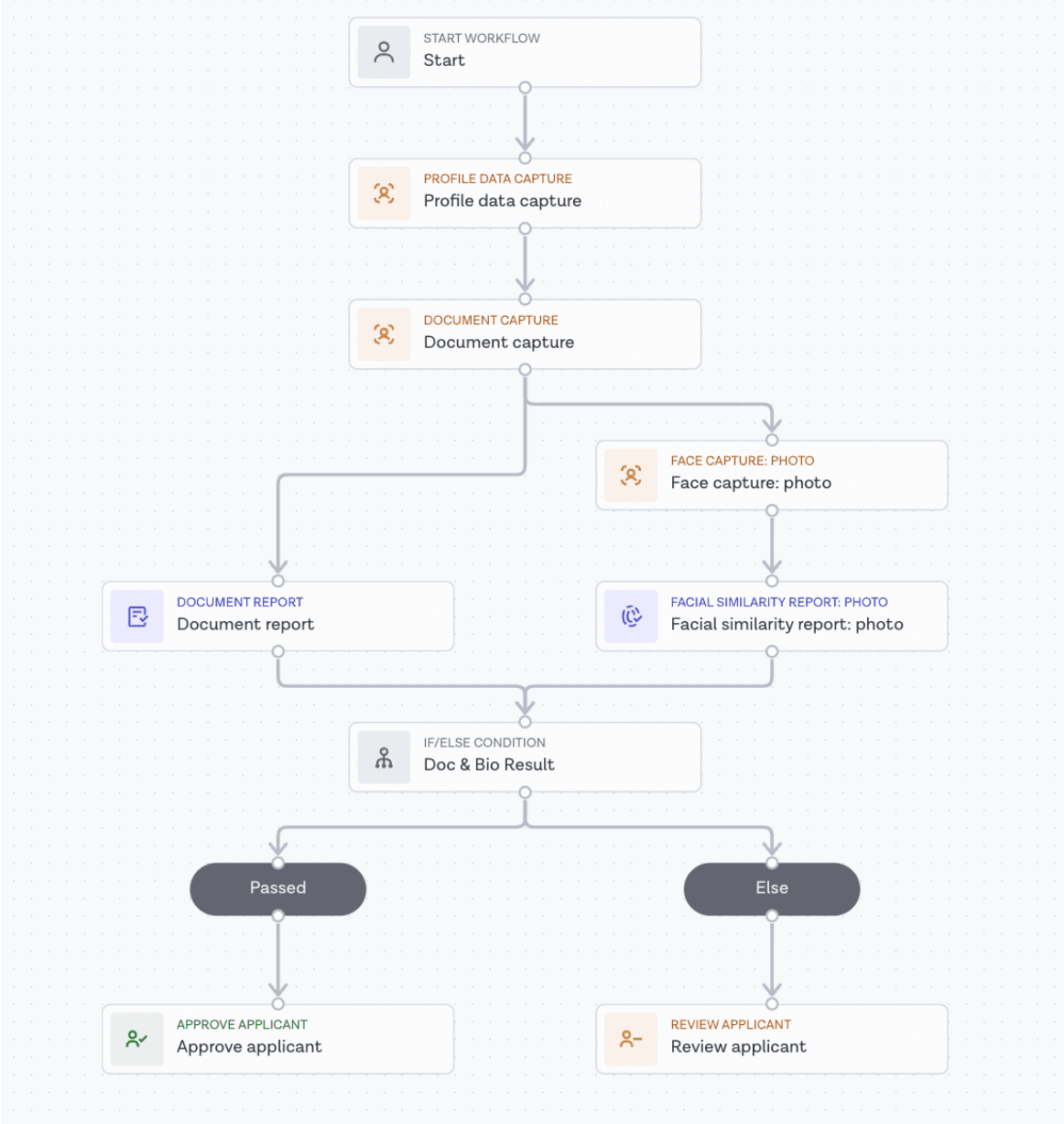


More information can be found at Onfido Real Identity Platform and Tour & Demo.

3.1. Onfido Studio

Onfido Studio enables our clients to build and manage multiple identity verification experiences to meet user and market requirements. Onfido Studio allows clients to orchestrate verification flows using the entire verification suite and flexible, no-code workflows.

Below is an example of a simple workflow in our Studio Builder tool:



Automated tailored experiences
Trigger the right experiences for every user with workflows that respond to changing market conditions.

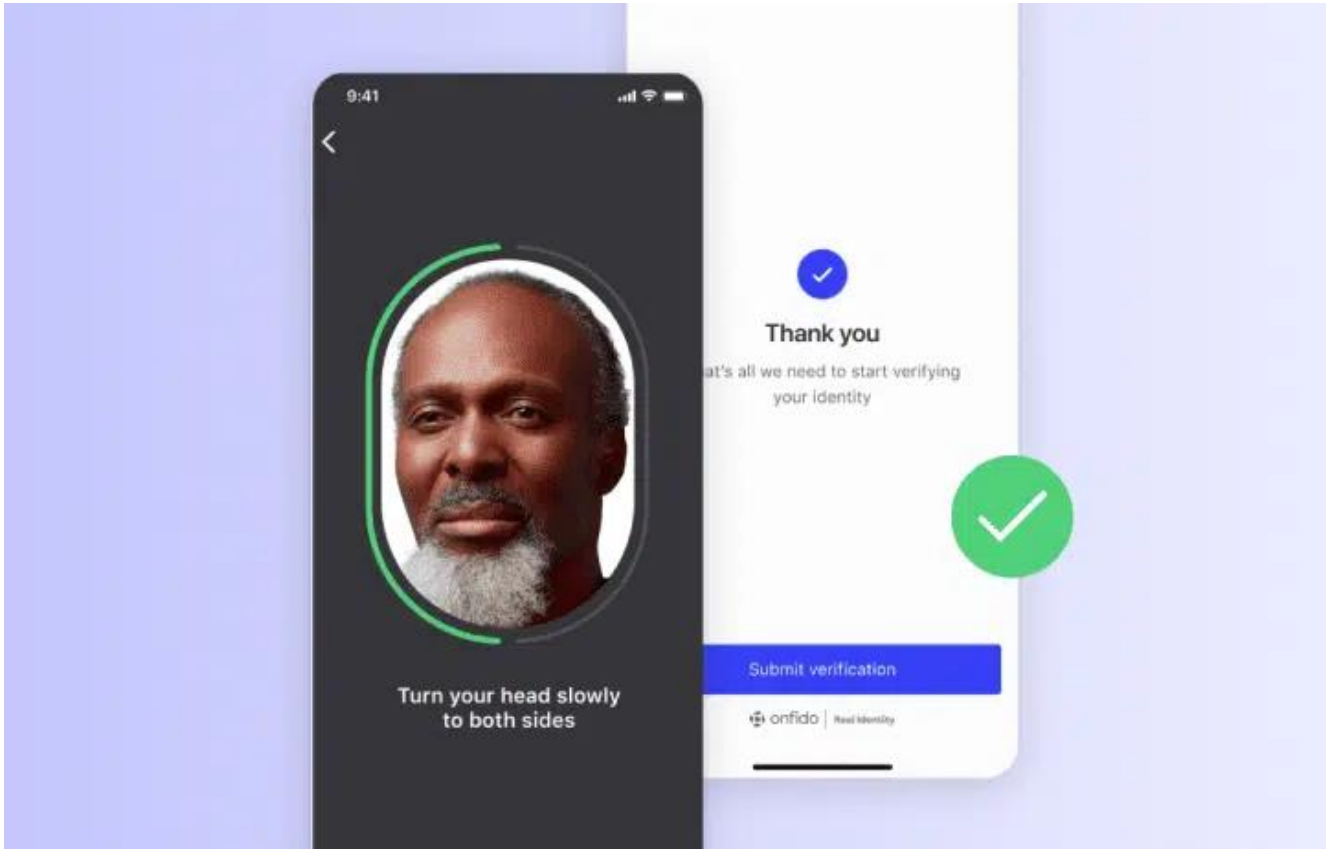
Build no-code workflows
Simply drag and drop document, biometric, and data verifications, and fraud detection signals into the user IDV journey.

Navigate KYC & AML Compliance
Easily introduce new verification methods, data sources, and fraud signals to address global regulatory compliance needs at scale.

More information can be found at Onfido Studio | Mission Control for Identity Verification.

3.2. Smart Capture SDKs

Onfido Smart Capture SDKs provide a **responsive capture experience** by communicating directly with Onfido's back-end services to execute the IDV attribute and evidence collection processes as well as transmit the on-device signals for fraud assessment.



Onfido supports the following platforms:

- **Web SDK** (guide)
- **Mobile SDKs**: iOS (guide), Android (guide), React Native (guide) and Flutter (guide)

More information can be found at Smart Capture SDK for digital onboarding.

3.3. Smart Capture Link

Smart Capture Link is a low- to no-code front-end solution complementing Onfido Studio, allowing clients to verify individuals with or without engineering effort.

Rather than clients integrating the user experience into their system or application using our Smart SDKs, Onfido hosts the verification journey on their behalf.

More information can be found at Smart Capture Link | Onfido Developer Hub

3.4. Onfido Verification Suite

A library of global verifications and signals to verify identities with minimum friction, catch sophisticated fraud attacks, and address compliance needs at scale.

By combining verification tasks into a Studio workflow, clients can increase the overall assurance that a given user:

- is a real person
- presenting genuine authoritative evidence of their own identity through government-issued ID (and/or genuine supplementary evidence)
- and is using a trusted device, network & Onfido SDK to capture all required attributes and evidence.

Document Verification
Verify identity documents such as a government–issued photo ID. Onfido's automated analysis, powered by Atlas AI, classifies documents in milliseconds and supports over 2,500 documents in 195 countries.

Biometric Verification
Ensure identity documents are presented by their rightful owners. Onfido's biometric verification matches a photo ID to facial biometrics captured in the same flow. Clients can choose verification using Selfie, Video or Motion. Selfie requests a static photo and passively checks for liveness. Video & Motion request a video selfie to protect against more sophisticated attack methods.

Data Verification
Fulfil compliance regulations such as AML with a suite of financial crime and compliance signals — from PEPs and sanctions, to adverse media and proof of address. Clients can choose trusted data sources that make sense for them and convert users in seconds.

Fraud Detection
Unleash the power of phone and device intelligence to accurately distinguish between trusted and fraudulent behaviour at onboarding. Harness intelligence related to devices, locations, identities and threats without impacting the experience of genuine users.

More information can be found at Verification Suite

3.4.1 Qualified Electronic Signature Report

Qualified Electronic Signatures are a special type of digital signature under the European Union's eIDAS regulation. As long as the signature has been created with a qualified certificate issued by another member state or Qualified Trust Service Provider (QTSP), it must be recognised by all EU Member states, and has the same legal status as a hand-written signature.

Using Qualified Electronic Signatures as part of an onboarding process may be used within specific EU member states in order to meet local AML regulations that require the highest levels of assurance (E.g. KYC in France).

Onfido has integrated directly with a QTSP that is responsible for issuing a temporary qualified certificate in the user's name. This certificate is then used immediately to sign a

document provided by the client as part of the onboarding process (E.g. the terms and conditions for a bank account).

Before a Qualified Electronic Signature can be used, users must first 1) Verify their identity through a high assurance ETSI Certified IDV process, accept the terms and conditions of the QTSP that will issue the qualified certificate and complete an additional One-time Password authentication step.

This report is only available when using Onfido SDKs and Onfido Studio. Our QTSP partner is Namirial.

More information can be found at Qualified Electronic Signature report | Onfido Developer Hub.

3.5. Onfido Atlas AI

Onfido Atlas™ AI is our bespoke technology that helps our clients to identify and react to fraud, while empowering them to onboard more genuine users, with AI that is fair, fast, and accurate.

More information can be found at Atlas AI | Onfido Real Identity Platform.

3.6. Compliance Suite for High Assurance IDV under standards or regulations

The EU regulatory landscape is challenging for organisations to navigate, with a patchwork of regulations, IDV standards, sector-specific guidelines and the evolving threats of fraud.

Onfido's all-in-one identity verification solution, Compliance Suite, empowers fast-growth businesses to expand seamlessly into new markets and meet local regulatory needs for onboarding users.

These solutions have been certified by accredited conformity assessment bodies, demonstrating that they adhere to the highest security, interoperability and assurance standards, and that Onfido is a mature, reputable and established provider.

For more information see Onfido Compliance Suite and EU KYC requirements guide.

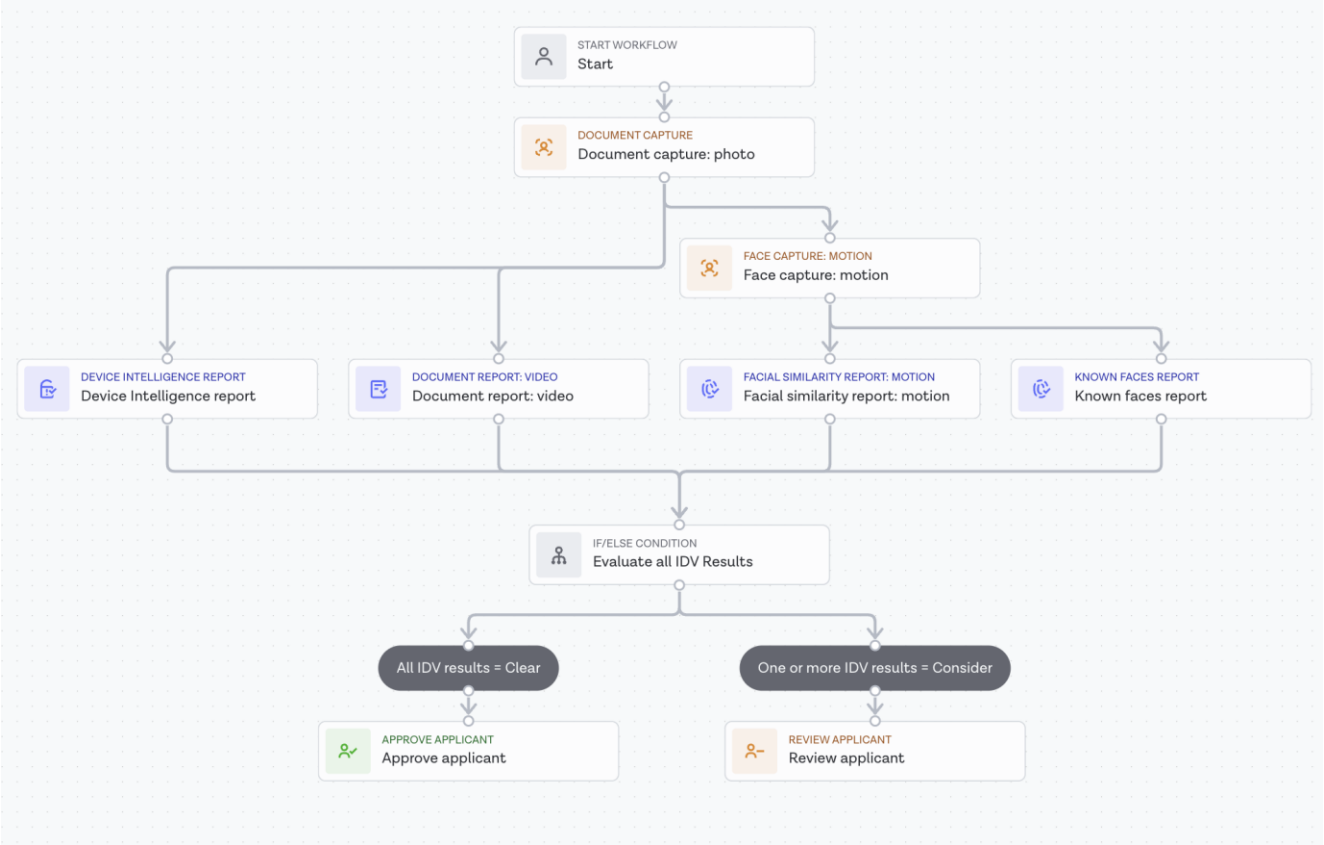
3.6.1. ETSI-Certified IDV

This solution targets the following assurance levels:

- ETSI TS 119 461 (V1.1.1): "**Baseline Level of Identity Proofing**"
- EIDAS: Level of Assurance "**Substantial**"

The following remote IDV workflows and integration options are supported:

Remote IDV Workflow	Required configuration to meet target assurance level
1. Collecting & validating **Physical ID** as **authoritative evidence** AND binding evidence to user with **facial biometrics**	Integrated via Onfido Studio with: ● Document Video Report ● Facial Similarity Report - Motion OR Facial Similarity Report - Video ● Device Intelligence Report ● Known Faces Report *(optional but recommended)* + Onfido Smart Capture SDKs (Mobile or Web) or Smart Capture Link; and download all required Evidence Files (Evidence Summary File and all Captured Media)
2. Collecting & validating **Electronic ID (eMRTD)** as **authoritative evidence** AND binding evidence to user with **facial biometrics**	Integrated via Onfido Studio with: ● Document Video Report (with NFC) ● Facial Similarity Report - Motion OR Facial Similarity Report - Video ● Device Intelligence Report ● Known Faces Report *(optional but recommended)* + Onfido Smart Capture SDKs (Mobile or Web) or Smart Capture Link; and download all required Evidence Files (Evidence Summary File and all Captured Media)



ETSI Certified IDV - Example Workflow

Onfido provides workflow templates from the Template modal in the Workflow Builder. The templates have been designed for use in different countries, therefore select the template that best suits the customer's needs - for example the "ETSI Certified IDV for Romania RO" template.

More information can be found at [ETSI certified identity verification | Onfido Developer Hub]

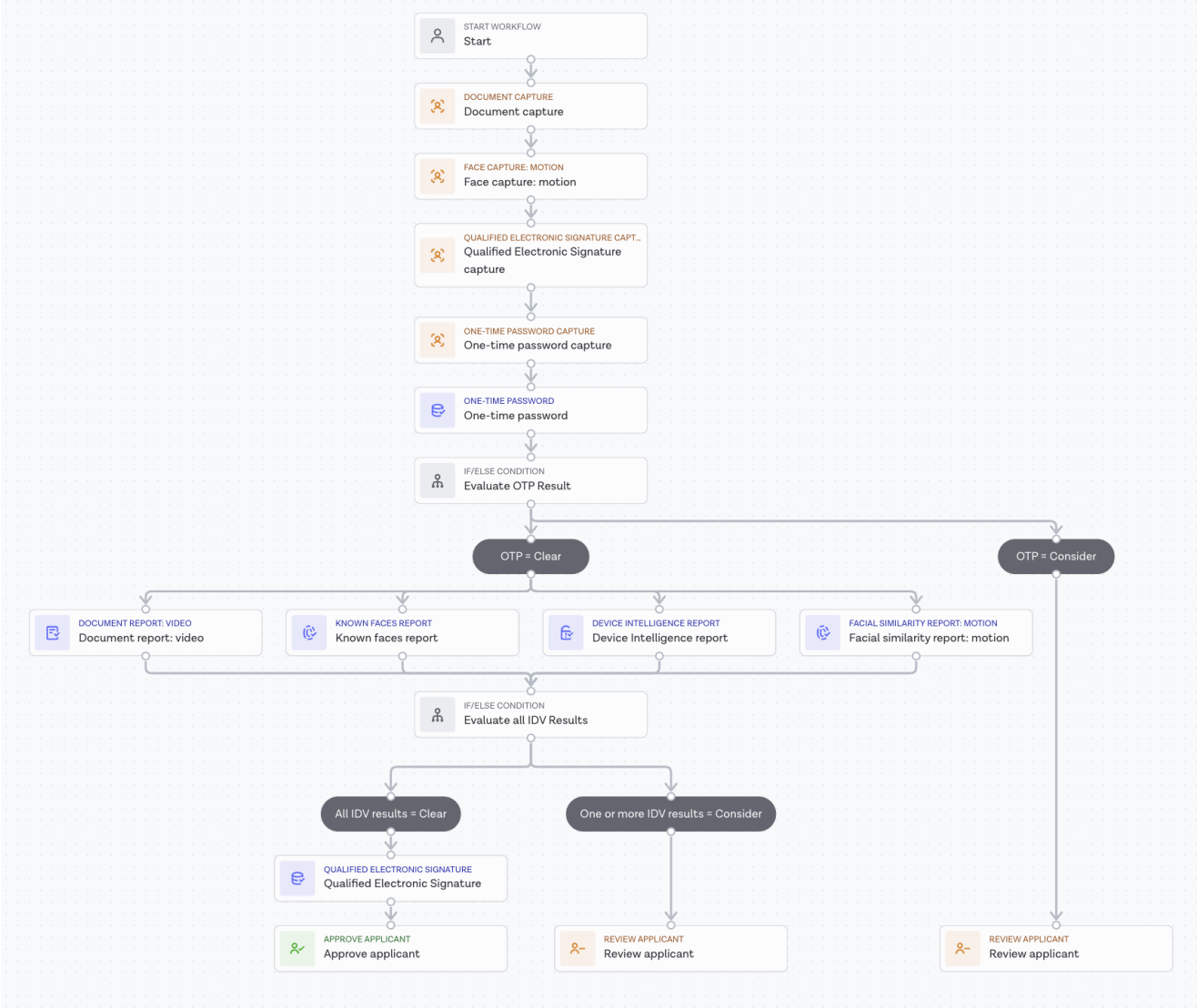
3.6.2. ETSI-Certified IDV with Qualified Electronic Signature

This solution targets the following assurance levels:

- ETSI TS 119 461 (V1.1.1): "**Baseline Level of Identity Proofing**"
- EIDAS: Level of Assurance "**Substantial**"

The following remote IDV workflows and integration options are supported:

Remote IDV Workflow	Required configuration to meet target assurance level
1. Collecting & validating **Physical ID** evidence Binding evidence to user with **facial biometrics** AND THEN using a **Qualified Electronic Signature** as **authoritative evidence**	Integrated via Onfido Studio with: ● Document Video Report ● Facial Similarity Report - Motion OR Facial Similarity Report - Video ● Device Intelligence Report ● Qualified Electronic Signature Report ● One-time Password Report ● Known Faces Report *(optional but recommended)* + Onfido Smart Capture SDKs (Mobile or Web) or Smart Capture Link (light integration); and download all required Evidence Files (Evidence Summary File, all Captured Media, Certificate Documents and Signed Documents)
2. Collecting & validating **Electronic ID (eMRTD)** evidence Binding evidence to user with **facial biometrics** AND THEN using a **Qualified Electronic Signature** as **authoritative evidence**	Integrated via Onfido Studio with: ● Document Video Report (with NFC) ● Facial Similarity Report - Motion OR Facial Similarity Report - Video ● Qualified Electronic Signature Report ● One-time Password Report ● Device Intelligence Report ● Known Faces Report *(optional but recommended)* + Onfido Smart Capture SDKs (Mobile or Web) or Smart Capture Link (light integration); and download all required Evidence Files (Evidence Summary File, all Captured Media, Certificate Documents and Signed Documents)



ETSI Certified IDV with Qualified Electronic Signature - Example Workflow

More information can be found at [ETSI certified IDV with Qualified Electronic Signature | Onfido Developer Hub]

3.6.3. Workflow templates

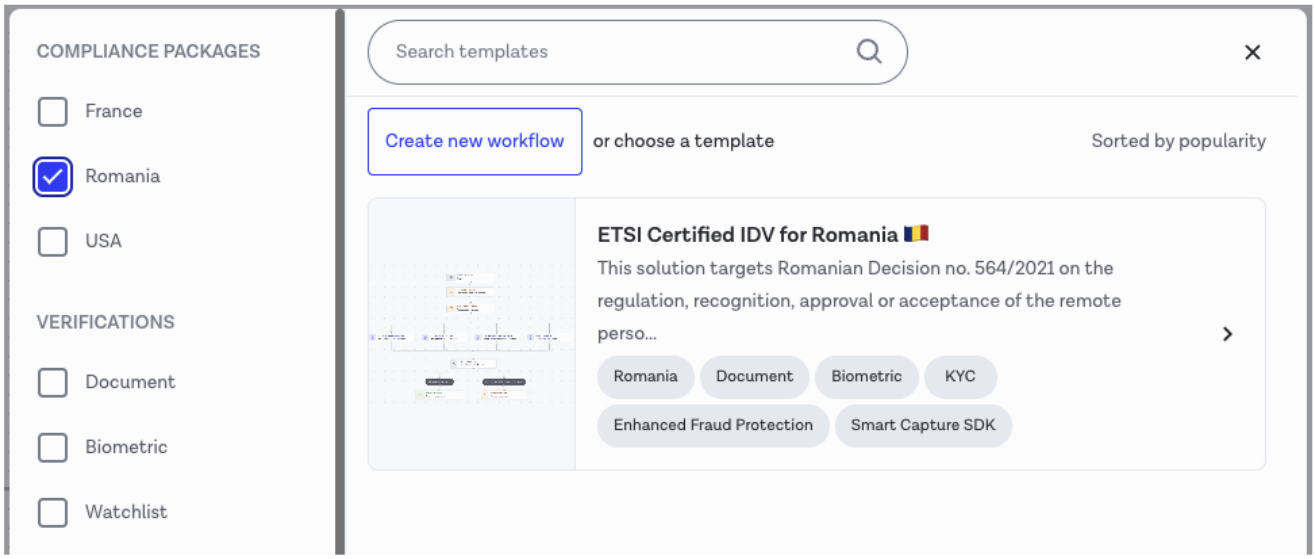
Studio is used to build compliant workflows for the different regulatory contexts required.

Onfido generally recommends that clients configure and maintain separate workflows for each regulated IDV context as requirements tend to differ from one country to the next.

This will make it easier to maintain, analyse and optimise your workflow performance over time while making the necessary changes to remain compliant.

To start, the customer chooses a template from the Template modal in the Workflow Builder. The templates have been designed for use in different countries, therefore select

the template that best suits the customer's needs - for example the "ETSI Certified IDV for Romania RO" template.



Please note: Templates are provided for guidance and informational purposes only.

3.6.4. Compliance Policy Validation task

For the "ETSI Certified IDV with QES & OTP for France FR" and "ETSI Certified IDV for Romania RO" Studio workflows, customers can validate at design-time that the minimum set of requirements in the policy have been met and understand if/where there are any errors.

This is done with a Compliance Policy Validation task that is included in the workflow templates.

The design-time validations include:

- Task presence
- Task configuration requirements
- Task input presence and semantic type requirements

Any policy requirements that cannot be validated at design-time will be validated at runtime instead. This includes task input/output values and whether the task results are cleared.

3.7. Certifications

Clients who require confirmation of our certifications for audit or regulatory application purposes can request this via their Customer Success Manager or Account Manager. Alternatively, contact Client Support.

3.7.1. Trust Frameworks (Product Platform)

Name	Scope	Assurance levels
ETSI standards for Identity Proofing	Role: Identity Proofing Service Provider (IPSP) ETSI TS 119 461 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects. ETSI EN 319 401 v2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. eIDAS Regulation (UE) 910/2014 Art. 24.1d Remote identification service component.	ETSI TS 119 461: “Baseline Level of Identity Proofing” EIDAS: Level of Assurance “Substantial” for ETSI Certified IDV
UK Digital Identity and Attributes Trust Framework (UK DIATF)	Role: Identity Service Provider (ISP) Sub Role: Identity Verification Services - i.e. we offer a point in time verification, and the user may or may not have an account. Public Sector Schemes / use cases supported: ● Right to Rent (Home Office) ● Right to Work (Home Office) ● Disclosure and Barring Service (Standard & Enhanced)	Identity profiles supported: ● M1A - Medium confidence, 1 piece of evidence, profile A ● H1A - High confidence, 1 piece of evidence, profile A ● H2B - High confidence, 2 pieces of evidence, profile B

3.7.2. Product-specific

Name	Scope	Assurance levels
ISO 30107-3 Presentation Attack Detection (PAD) for Biometrics	Products: Facial Similarity - Selfie Platforms: iOS and Android	Level 1 PAD with 0% False Acceptance Rate
	Products: Facial Similarity - Motion Platforms: iOS and Android	Levels 1 and 2 PAD with 0% False Acceptance Rate
Web Content Accessibility Guidelines	Products: Smart Capture SDKs Platforms: Web, iOS and Android	WCAG 2.1 Level AA

3.7.3. Information Security

Name	Scope
SOC2 Type II - Security, Availability & Confidentiality Report	SOC 2 defines criteria for managing client data based on five “trust service principles”—security, availability, processing integrity, confidentiality and privacy. There are two types of SOC reports: ● Type I describes a vendor’s systems and whether their design is suitable to meet relevant trust principles. ● Type II details the operational effectiveness of those systems. Onfido holds a **Type II** certification
ISO27001 - Information Security	ISO/IEC 27001 is the international standard for information security. It sets out the specification for an effective ISMS (information security management system). ISO 27001's best-practice approach helps organisations manage their information security by addressing people, processes and technology.

3.7.4. Country-specific

Void.

4. Remote IDV Practices

Onfido's remote IDV practices proceed along 5 stages:

1. Initiation of Remote IDV Process
2. Attribute and Evidence Collection
3. Attribute and Evidence Validation
4. Binding Evidence to User
5. Issuing of Remote IDV Result

Before describing each of these steps, the wider threat landscape is considered.

4.1. Threat landscape

The following high level attack vectors are considered within the context of identity theft, identity fraud and Onfido's remote IDV practices:

(A) Falsified or counterfeited evidence

1. The IDV Process is compromised by the use of evidence of insufficient quality
2. The IDV Process is compromised by counterfeited and/or manipulated evidence
3. The IDV Process is compromised by use of evidence that is terminated, revoked or reported as lost/stolen

(B) Impersonation

1. The IDV Process is compromised by an imposter claiming the legitimate identity of another person

(C) For all remote IDV use cases

1. The IDV Process is compromised by manipulation of image capturing systems or transmission channels

4.2. Initiation of Remote IDV Process

Onfido **clients** decide when to initiate the IDV Process. Under the terms of the Onfido's Services Agreement, Onfido **clients** are responsible for taking all steps required to ensure that Onfido may lawfully process the personal data of users for the purpose of providing the clients' requested IDV services.

In particular, clients are responsible for obtaining all necessary consents from, and providing all necessary notices to, users in accordance with applicable privacy laws. In practice, this may entail:

- Informing users, in a clear and comprehensive manner, of the purpose of the identity verification and the related terms and conditions as required by the IDV context.

- Providing users with guidance on how the process will be carried out with regards to the data collected, the evidence the user is required to present, and any tool that user is required to use.
- Where consent is required, ensuring that users accept the purpose of the identity verification and the related terms and conditions ***before*** proceeding with the IDV process and allowing users to select an alternative IDV process.

Where Onfido **clients** have users located in the USA, the terms of the Onfido Services Agreement will also require the client to:

- Ensure its interface either directs users to certain Onfido policies (including the Onfido Facial Scan and Voice Recording Policy) or to the client's own policies and legal agreements which must meet the requirements of the Onfido Services Agreement; and
- Submit an API consent parameter which confirms that consent has been granted to collect biometric data.

Further information on Onfido's privacy notices and consent requirements for the collection and processing of biometrics of users located in the USA is available at Onfido privacy notices and consent (US).

4.3. Attribute and Evidence Collection

Different verification tasks have different requirements for user data. They will also collect different attributes and evidence to be able to perform their respective validation steps.

All attributes and evidence collected across verification tasks are required for attribute and evidence validation and are included in the final identity verification result.

Onfido's Privacy Policy explains the attributes and evidence we collect and process to provide our different identity verification services.

4.4. Attribute and Evidence Validation

4.4.1. Validation of Identity Documents

Our Document Reports protect against the following types of document fraud:

- Forged documents
- Counterfeit documents
- Blank stolen documents
- Fantasy or camouflage documents
- Imposter or 'look-a-like' documents
- Publically compromised documents

The first step of the verification process is to classify the document to the sub-version level (E.g. GBR Passport 2020) which will determine:

- Whether the document is supported by Onfido for IDV purposes.
- The attributes we can extract and the verification checks that can be performed against the document.

4.4.1.1. Quality of ID Evidence

***Context 1 and 2**: Collecting & validating **Physical ID** or **Electronic ID (eMRTD)** as authoritative evidence. **Attack vector A1**: IDV Process compromised by the use of evidence of insufficient quality*

Government-issued IDs have different levels of robustness based on their inherent features and characteristics. Within Onfido and the IDV context, each document can be classified into a sophistication tier based on its unique collection of features that enable remote verification.

These features also influence the specific capabilities Onfido can build to extract a document's data and verify its authenticity, which directly impacts a document's real-world attack vector coverage and overall performance.

Onfido currently classifies documents into 1 of 5 sophistication tiers

- Tier 1 documents are not supported by Onfido
- Tier 2 documents are supported by Onfido but only for the purposes of Data Extraction, not full verification.
- Tier 3-5 documents are supported by Onfido for IDV use cases but document quality, capabilities and performance will differ between these tiers.

Within Onfido Studio workflows, clients can configure the accepted document rules to match their identity proofing context, and decline any users who do not provide an accepted document.

4.4.1.2. Physical ID Validation (Document and Document Video Reports)

***Context 1:** Collecting & validating Physical ID as authoritative evidence. **Attack vector A2**: IDV Process compromised by counterfeited and/or manipulated evidence*

Document verification leverages multiple techniques, including specially trained Machine Learning powered algorithms, to classify documents, extract their data and verify their authenticity through specific Data Integrity and Visual Authenticity checks. When required, document verification is supported by a team of highly trained analysts.

Document verification performs static image analysis of the front and back of the document depending on the document type being verified. Additionally, for the **Document Video Report**, our SDK records a 1.5-second video of an user's document, available for download via API or directly from the Client Dashboard. If a video isn't successfully recorded or there are signs that it was digitally tampered, the Document Video Report will be flagged.

Document verification implements a hybrid verification workflow by default:

- All automated processes and verifications run first with any detected anomalies triggering a review by trained analysts. Once the analyst assessment is complete, a final result is issued.
- Documents where no anomalies are found by automation or where automation has high confidence on the anomalies that were found are returned with their final results without further human review.
- Any documents with low overall automation coverage will fallback to being processed by trained analysts performing classification, data extraction and visual authenticity and data consistency checks as required.

- Data validations and database lookups are only performed by automation, not analysts.
- The final result is either “clear” or “consider” with more detailed breakdowns provided for each aspect of the verification.

High-level controls for document verification are covered below.

Control
Image Integrity Checks - Yes, see “Image Quality Controls” section further below
Data Integrity Checks
Asserts whether algorithmically validatable elements are correct. E.g. MRZ lines, barcode data and document numbers.
Data consistency between MRZ/Barcode and PII fields.
Is the document publicly compromised?
[Optional] **Data Comparison** between the data extracted via OCR from the image of the document and the attributes supplied by the user (First name, Last name & Date of Birth).
Visual Authenticity Checks Level of automation coverage for visual authenticity checks varies depending on the document type and sub-version. Documents with lower coverage that pose a higher risk are always routed to human review.
Original Document Presence (Copy Detection) - checks whether the provided image is an image of the original document or a copy (i.e. photo of screen, screenshot, photo of print out or scans).
Shape & Template - Checks whether the document matched the expected shape and template for the country, document type and sub-version.
Picture - checks if the pictures of the person identified on the document show signs of tampering or alteration .
Fonts - checks whether fonts in the document match the expected ones
Security Features - checks if the security features expected on the document are missing or wrong.
Digital Tampering - checks if the document shows signs of being tampered digitally.
Binding Physical ID to user with facial biometrics
Yes, when combined with our Biometric Verification suite. See: - Validation of Facial Biometrics and Liveness - Binding Evidence to User -> Face Comparison Between User & Physical ID

Replay & injection attack controls

Contexts 1 and 2: *Collecting/validating Physical ID or Electronic ID (eMRTD) as authoritative evidence AND binding evidence to user with facial biometrics.* ***Attack vector C1:*** *IDV Process compromised by manipulation of image capturing systems or transmission channels*

Document Report detects photos of screens which are used in replay attacks.

To ensure payload integrity, authenticity and confidentiality and protect against injection attacks, SDKs sign the uploaded video payload and the signature is verified by Onfido's platform responsible for storing media files.

Image Quality Controls

Controls: On device, during document image capture flow

Onfido's SDKs combine on-device and server-side document image quality algorithms during capture flow. We assess the document's image quality and then provide in-flow feedback and guidance to users to re-attempt the capture of a good quality image.

Our **latest SDKs** support the following image quality and document capability checks:

- Document detection
- Document side (back/front) detection
- Blur detection
- Cutoff detection
- Glare detection
- MRZ readability
- Barcode detection (USA/CAN IDs and DLs)
- Photo of Screen detection

Controls: Downstream operations when Document Report is processed

During the verification step, image quality is checked again and will directly impact the final result depending on the scenarios outlined in the table below.

Image Quality Scenarios	Onfido Processing Actions	Typical Client Actions
1. Required data points cannot be extracted due to one or more of them being completely cut off, covered or very blurry (i.e. unreadable by a human)	Flag for Image Quality with specific reasons. **Sub-result: "Rejected"**	Request user to re-attempt verification with a higher quality image
2. Required data points can be extracted but visual fraud assessment will be hampered due to IQ - typically some blur, low resolution, key security features obscured, too dark.	Extract all data Perform full Data Fraud assessment Perform **partial** visual fraud assessment (ODP only) and flag for Conclusive Document Quality with specific reasons. **Sub-result: "Caution"** (except if flagged as fraud based on	**Higher risk tolerance** Onboard as genuine **Lower risk tolerance** Request user to re-attempt verification Escalate internally / enforce alternative verification steps

	the assessment we've done, then will map to "Suspected"	
3. Required data points can be extracted and the full visual fraud assessment can be completed	Extract all data Perform full Data Fraud assessment Perform full Visual Fraud assessment (ODP, Fonts, Picture Face Integrity, etc) **Sub-result: "Clear" or "Suspected"**	Onboard as genuine (Clear) OR Deny onboarding (Suspected)

Additional information
More information can be found at Document report | Onfido Developer Hub

This report is available via the Onfido API and SDKs.

The full list of Government-issued IDs supported by the Document Check can be found on our Supported documents page. This also provides the requirements for which documents require the back to be submitted.

4.4.1.3. Electronic ID (eMRTD) Validation (Document Report with NFC)

***Context 2**: Collecting & validating **Electronic ID (eMRTD)** as authoritative evidence. **Attack vector A2**: IDV Process compromised by counterfeited and/or manipulated evidence*

eMRTD documents (most passports, newer national identity cards and residence permits) contain a chip which can be accessed using Near Field Communication (NFC) readers on mobile devices using Onfido's mobile SDKs. In this case, our Document Report or Document Video Reports can use this chip to fully validate the authenticity of the document using cryptographic methods.

NFC-based verification implements a fully automated verification workflow:

1. On compatible document types, following the capture of a photo of the document, the user is asked to initiate an NFC-based document verification by scanning their document using their mobile device.
    - If NFC is unsupported or the scanning fails, clients can decide to fall back to using the physical ID verification flow.
    - Clients can also enforce that NFC verification is performed instead of allowing users to decide.
2. Reading NFC chip data - there are two chip reading mechanisms supported:
    - Basic Access Control (BAC) - NFC chip is unlocked using data points extracted from the photo of the document through the Machine Readable Zone (MRZ).
    - Password Authenticated Connection Establishment (PACE) - NFC chip is unlocked using data points extracted from the photo of the document through the Machine Readable Zone (MRZ) AND using a pin code provided by the user. This mechanism is only supported on a subset of document types on Android.

    - Note: The chip can contain both biometric and non-biometric data. Depending on the document issuing country and sub-version, biometric data may not be accessible.
3. NFC chip data is securely transmitted from the user's device to the server for validation via the following methods:
    - Passive Authentication - NFC data integrity authenticated against signed country certificates and revocation lists.
    - Active Authentication - If supported by the document, NFC chip is also authenticated using the chip's private key to ensure it hasn't been cloned.
4. The authenticated NFC chip data is stored and returned to clients as Document Report properties. Additionally, Onfido returns a dedicated "nfc" field containing all of the extracted data.
5. The final report result is either "clear" or "consider" with more detailed breakdowns provided for each aspect of the verification (see Issuing of Proof)
6. Where possible for the given document, the photo extracted from the authenticated chip data is then bound to the user via our Facial Similarity Reports (See Face comparison between user & electronic ID (eMRTD))

High-level controls for document verification (with NFC) are covered below with the differences with standard document verification highlighted.

Control
Image Integrity Checks *- skipped when using NFC data authentication*
Data Integrity Checks
Asserts whether algorithmically validatable elements are correct. E.g. doc numbers.
~~Data consistency between MRZ/Barcode and PII fields~~ *- skipped when using NFC data authentication as only the NFC data is extracted and validated (see below).*
NFC Passive Authentication - NFC data integrity authenticated using signed country certificates and revocation lists.
NFC Active Authentication - If supported by the document, NFC chip is also authenticated using the chip's private key to ensure it hasn't been cloned.
Is the document publicly compromised?
[Optional] **Data Comparison** between the data extracted from the NFC chip and the attributes supplied by the user (First name, Last name & Date of Birth).
Visual Authenticity Checks *- skipped when using NFC data authentication*
Binding Electronic ID (eMRTD) to user with facial biometrics
Yes, when combined with our Biometric Verification suite. See: - Validation of Facial Biometrics and Liveness - Binding Evidence to User -> Face Comparison Between User & Electronic ID (eMRTD)

Additional information
More information can be found at NFC for Document report | Onfido Developer Hub

NFC-based verification is only available when using Onfido mobile SDKs.

The full list of Government-issued IDs supported by Onfido for NFC Verification can be found on our Supported Documents for NFC page. Additional documents will be supported over time.

4.4.1.4. Issuing Authority & Document Validity Checks

***Attack vector A3** - IDV Process compromised by use of evidence that is terminated, revoked or reported as lost/stolen*

An identity document can be declared lost, stolen, or revoked, but not all document issuers provide an online status service that can be used to check current status, and if an online status service exists, its availability can be restricted.

While Onfido periodically assesses the availability and feasibility of these online services, at this time we do not offer these additional validity checks.

Onfido's Police Record check, is an additional, opt-in feature that asserts whether the document has been identified as lost, stolen or otherwise compromised. Applies to all UK documents or any document that has been reported stolen in the UK.

4.4.1.5. Identify repeat users via document data

The Repeat Attempts product compares the identity document submitted by an user as part of a Document Report to other previously onboarded documents in a client's account. This helps to protect against cases where the same document is used repeatedly with minor modifications, indicating potential fraud.

Repeat Attempts does not run as a separate report, rather it analyses Document Reports, with the results returned as part of the Document Report sub-breakdown. Further Repeat Attempt details can be inspected in the Client Dashboard or retrieved through an API endpoint.

For each repeat attempt match, Onfido returns whether the document matches the personal document data used for each previous attempt:

- If the personal document data doesn't match, this indicates that one, or potentially multiple, of the documents might be fraudulent.
- A large number of repeat attempts can also signal fraudulent behaviour.

Additional information
More information can be found at Repeat Attempts | Onfido Developer Hub

4.4.2. Validation of Facial Biometrics and Liveness

***Contexts 1 and 2**: Binding Physical ID and Electronic ID (eMRTD) evidence to user with facial biometrics. **Attack vector B1**: IDV Process compromised by an imposter claiming the legitimate identity of another person*

4.4.2.1. Facial Similarity Report - Photo

Images and data are extracted from identity documents and then compared to a selfie taken by the user for lower-risk users or transactions.

Both the Photo and Photo Fully Auto reports use a photo of the user. The photo needs to be a "live photo" taken at the time of check submission, so that it can assess whether the holder of the identity document is the same person as the one on the document.

For Presentation Attack Detection (PAD), this report relies on static image analysis where the user is not required to perform any specific actions (i.e. passive liveness). We do this by running a suite of machine learning models relying on learned features (e.g. texture analysis) and hand-crafted features (e.g. presence of specific artefacts).

Facial Similarity Photo implements a hybrid verification workflow:

- All automated processes and verifications run first and, provided all verifications fall within a high confidence threshold, the final result is returned without further human review.
- When automation encounters an issue (e.g. no face detected) or is not confident in its assessment, this will trigger a review by trained analysts. Once the analyst assessment is complete, a final result is issued.
- The final result is either “clear” or “consider” with more detailed breakdowns provided for each aspect of the verification (see Issuing of Proof)

Facial Similarity Photo protects against several presentation attack vectors, for example:

- Photos of identity documents
- Photos of screens
- Photos of printed photos
- Face masks

Facial Similarity Photo is **iBeta PAD Level 1 certified** on both Android and iOS with a perfect score of 0% False Acceptance Rate and 0% False Rejection Rate.

Replay & injection attack controls

***Contexts 1 and 2:** Collecting & validating Physical ID or Electronic ID (eMRTD) as authoritative evidence AND binding evidence to user with facial biometrics. **Attack vector C1:** IDV Process compromised by manipulation of image capturing systems or transmission channels*

Facial Similarity Report (Photo) detects photos of screens which are used in replay attacks.

To ensure payload integrity, authenticity and confidentiality and protect against injection attacks, SDKs also sign the uploaded selfie payload and the signature is verified by Onfido’s platform responsible for storing media files.

Additional information
More information can be found at Facial Similarity reports | Onfido Developer Hub

This report is available via the Onfido API or SDKs.

4.4.2.2. Facial Similarity Report - Video

Facial Similarity Video provides increased assurance for higher-risk users or transactions. The user records a video of themselves repeating numbers and performing randomised head turn movements. The video includes audio recording.

The video needs to be a "live video" taken at the time of check submission, so that it can assess whether the holder of the identity document is the same person as the one on the document.

For Presentation Attack Detection (PAD), two active liveness controls are implemented:

1. The user is asked to rotate his/her head. During the verification process, an algorithm tracks the user's face and ensures that the user did rotate their head, and that they rotated it in the expected direction.
2. The user is asked to repeat a random phrase / combination of numbers. (17 languages are currently supported). During the verification process, algorithms ensure that the user pronounced the phrase / combination of numbers out loud and that these matched the initial query.

Moreover, these required actions are randomised (combination of numbers, headturn direction, different order between the actions).

Further passive liveness controls are implemented in the form of analysis via deep learning networks.

Facial Similarity Video implements a hybrid verification workflow:

- All automated processes and verifications run first and, provided all verifications fall within a high confidence threshold, the final result is returned without further human review.
- When automation encounters an issue (e.g. no face detected; spoofing detected, unsupported language spoken) or is not confident in its assessment, this will trigger a review by trained analysts. Once the analyst assessment is complete, a final result is issued.
- The final result is either "clear" or "consider" with more detailed breakdowns provided for each aspect of the verification (see Issuing of Proof)

Facial Similarity Video protects against several presentation attack vectors, for example:

- Videos of identity documents
- Videos of screens
- Videos of printed photos
- Face Masks
- Video playback

Replay & injection attack controls
Contexts 1 and 2: *Collecting & validating Physical ID or Electronic ID (eMRTD) as authoritative evidence AND binding evidence to user with facial biometrics.* ***Attack vector C1:*** *IDV Process compromised by manipulation of image capturing systems or transmission channels*

Facial Similarity Video checks for videos of screens & video playback which are used in replay attacks.

To ensure payload integrity, authenticity and confidentiality and protect against injection attacks, SDKs also sign the uploaded video payload and the signature is verified by Onfido's platform responsible for storing media files.

Video quality controls
A suite of algorithms running at time of capture guides the user in recording a high-quality video of themselves:

- Face detection and head tracking provide real-time user feedback to ensure successful recording and high clear rate.
- If the user does not say the correct combination of numbers or doesn't rotate their head, a "Consider" result will be issued for the liveness detection.

Additional information
This report is only available when using Onfido SDKs.

More information can be found at Facial Similarity reports | Onfido Developer Hub

4.4.2.3. Facial Similarity Report - Motion

Facial Similarity Motion provides increased assurance for higher-risk users or transactions with lower friction and higher performance than the Video variant. The user records a video of themselves performing head movements. By default, background audio is not recorded (but can be enabled by clients if required).

The video needs to be a "live video" taken at the time of check submission, so that it can assess whether the holder of the identity document is the same person as the one on the document.

For Presentation Attack Detection (PAD), a suite of deep learning networks analyse different regions of the video (in space and time). Their results are combined to provide a final spoofing assessment.

Facial Similarity Motions implements a fully automated verification workflow:
- The final result is either "clear" or "consider" with more detailed breakdowns provided for each aspect of the verification (see Issuing of Proof)
- When automation encounters an issue (e.g. no face detected) a final result is always issued as "consider".

Facial Similarity Motion protects against several presentation attack vectors, for example:

- Videos of identity documents
- Videos of screens
- Videos of printed photos

- Face Masks
- Video playback

Facial Similarity Motion is **iBeta PAD Levels 1 and 2 certified** on both iOS and Android with a perfect score of 0% False Acceptance Rate and 0% False Rejection Rate. See Product-specific Certifications for more information.

Repeated, replay & injection attack controls
Contexts 1 and 2: *Collecting & validating Physical ID or Electronic ID (eMRTD) as authoritative evidence AND binding evidence to user with facial biometrics.* ***Attack vector C1:*** *IDV Process compromised by manipulation of image capturing systems or transmission channels*

Facial Similarity Motion checks for videos of screens and video playback which are used in replay attacks.

To ensure payload integrity, authenticity and confidentiality and protect against injection attacks, SDKs also sign the uploaded evidence payload and the signature is verified by Onfido's platform responsible for storing media files.

Video quality controls
A suite of algorithms running at time of capture guides the user in recording a high-quality video of themselves:

- The video encoding parameters have been optimised to ensure the right balance of image quality and video payload size.
- A face tracking algorithm detects when the user's face deviates from the ideal position. In which case a prompt guides the user to reposition their face accordingly.
- An intuitive UX paired with a face headpose algorithm ensures the user is rotating his/her face in all required directions, with appropriate speed and with sufficient angle.

Together, these algorithms provide real-time user feedback to ensure successful recording and high clear rate.

Additional information
This report is only available when using Onfido SDKs.

More information can be found at Facial Similarity reports | Onfido Developer Hub

4.4.2.4. Identify repeat users via facial biometrics (Known Faces Report)

The Known Faces report compares a specific user's likeness in their most recent live photo or live video to live photos and live videos from the last 1 year of user faces processed through a Onfido client's account.

It alerts clients to faces which have already been through their identity verification flow, so they can 1) catch repeat identity fraud attempts, and 2) prevent duplicate accounts from being opened.

Additional information
More information can be found at Known Faces report | Onfido Developer Hub

4.4.3. Validation of Digital Signature with Certificate

Void.

4.4.4. Validation of Device, App and Network Integrity

***Attack vector B1**: The IDV Process is compromised by manipulation of image capturing systems or transmission channels*

4.4.4.1. Device Intelligence Report

Device Intelligence uses non-visual passive signals to identify fraudulent activity and protect our clients from bad-actors.

This includes the verification of the Device, App and Network's integrity and their connection with recent fraudulent activity.

Device and App Integrity
Device Intelligence uses passive device signals to analyse whether the device or Onfido app has been compromised, including device spoofing and SDK spoofing, without requesting the user for any additional input.

It answers questions such as:
- Has this device or app been tampered with or spoofed? Is it not a legitimate device?
- Has this device recently been flagged for fraudulent activity?

Network integrity (IP and Geolocation)
Device Intelligence gathers and analyses information including IP attributes and geolocation to detect additional fraud, including malicious traffic, risky IP's, and bot traffic, without requesting the user for any additional input.

It answers questions such as:
- Has this device location been spoofed?
- Has this IP recently been flagged for fraudulent activity?

Additional information
More information can be found at Device Intelligence | Onfido Developer Hub

4.4.5. Validation of Proof of Access

***Context**: Validating **proof of access to a phone number, bank account or email** as supplementary evidence. **Attack vector B1**: IDV Process compromised by an imposter claiming the legitimate identity of another person*

4.4.5.1. One-time Password Report

The One-time Password Report verifies that an user is in possession of the phone number, by sending a unique code to that number for validation.

Verifying a One-time Password must be included when integrating our ETSI certified IDV with Qualified Electronic Signature | Onfido Developer Hub solution.

Additional information
This report is only available when using Onfido SDKs and Onfido Studio.

More information can be found at One-time Password report | Onfido Developer Hub

4.4.6. Validation of Identity Attributes against Trusted Registers

***Context**: Validating identity data against **trusted registers** as supplementary evidence.*
***Attack vector B1**: IDV Process compromised by an imposter claiming the legitimate identity of another person*

4.4.6.1. Identity Enhanced Report

An Identity Enhanced report validates an user's address, date of birth, name, and mortality (where applicable) by cross-referencing their details against a range of verified databases.

More information can be found at Identity Enhanced report | Onfido Developer Hub

4.4.6.2. Watchlist Report

Watchlist reports allow clients to verify user records on global watchlists, including:

- Sanctions - Government and International Organisations Sanctions Lists
- Politically Exposed Persons - Proprietary database of Politically Exposed Persons sourced from government lists, websites and other media sources
- Monitored Lists - Law-enforcement and Regulatory bodies Monitored Lists (including Terrorism, Money Laundering and Most Wanted lists)
- Adverse Media - Negative events reported by publicly and generally available media sources

Available Report Types: AML; Standard; Enhanced; PEPs only; Sanctions Only; Ongoing monitoring (auto re-check + alert)

Additional information
More information can be found at Watchlist reports | Onfido Developer Hub

4.4.6.3. Driver's Licence Data Verification Report

The DLDV report verifies the authenticity of an user's driver's licence by comparing it against US state driver's licence databases to confirm whether the data submitted corresponds to a genuine driver's licence.

Onfido uses a third-party subprocessor to verify driving licence data against the American Association of Motor Vehicle Administrators (AAMVA) database, facilitated by the Department of Motor Vehicles (DMV). This allows quick and accurate verification that a given driver's licence is real, providing a strong signal against synthetic fraud.

Additional information
Only drivers licences and state ID card issued by 39 39 US states are supported.

More information can be found at Driver's License Data Verification report | Onfido Developer Hub

4.4.7. Validation of Other Documents and Attestations

***Context**: Validating **other documents and attestations** as **supplementary evidence**. **Attack vector B1**: IDV Process compromised by an imposter claiming the legitimate identity of another person*

4.4.7.1. Proof of Address Report

The Proof of Address (PoA) report allows clients to verify an user's address by reviewing an eligible uploaded document. The PoA report cross checks the address information provided by the user with the details of a PoA document (such as a bank statement or utility bill), in order to verify the authenticity of the address.

In addition, the report also asserts whether the document is supported by Onfido, as well as having a valid date of issue.

Additional information
More information can be found at Proof of Address | Onfido Developer Hub

4.5. Binding Evidence to User

***Contexts 1 and 2**: Binding Physical ID and Electronic ID (eMRTD) evidence to user with facial biometrics. **Attack vector B1:** IDV Process compromised by an imposter claiming the legitimate identity of another person*

All Facial Similarity Reports (Photo, Video & Motion) support face matching that is performed by a deep neural network trained with pairs of matching/non-matching images. According to the statistics, it currently performs much better than humans.

For Photo and Video: if a face cannot be detected, we will escalate to a highly specialised individual for review. In all cases, Onfido deploys trained super recognizers who use custom-built comparison tools. Super recognizers are the 2% of the general population that are exceptionally good at facial recognition.

For Motion: if a face cannot be detected, the “Face Comparison” breakdown is flagged with an overall result of “Consider”.

Additional information
More information can be found at Facial Similarity reports | Onfido Developer Hub

4.5.1. Face Comparison Between User & Physical ID

In the scenario where an user validates their physical ID via the Document Report or Document Video Report, face comparison will be performed between the user’s face and the main portrait of the document holder, typically located on the front or main page of the document.

This applies to all Facial Similarity Report variants (Photo, Video and Motion).

4.5.2. Face Comparison Between User & Electronic ID (eMRTD)

In the scenario where an user validates their electronic ID (eMRTD) via the Document Report (with NFC enabled), face comparison will be performed between the user's face and the photo extracted from the unlocked and authenticated chip.

This applies to all Facial Similarity Report variants (Photo, Video and Motion).

4.6. Issuing of Proof

4.6.1. Decision Procedures

4.6.1.1. Decision recommendations

All IDV results returned by Onfido and any suggested client actions are *recommendations only*.

Onfido's results and supporting documentation include recommendations and the rationale behind it, but it is the **client** who must ultimately decide how to proceed with the user after receiving Onfido's results. This may be to approve them, decline them outright, decline with the option to retry or escalate to an internal team for further checks.

By providing detailed results and recommendations, we empower clients to make their own informed decisions about their users and to support these users in passing through Onfido IDV successfully.

4.6.1.2. Workflow results configuration

The overall workflow result depends on how clients have configured their workflow using **Result tasks** which represent all possible outcomes for an user's verification journey.

The three Result task types are: "Approve applicant", "Review applicant" and "Decline applicant".

Generally speaking, Result tasks will follow the outcome of a Logic task, based on the conditions and results of the Verification tasks run on the workflow. Clients can define as many Result tasks as they wish in a workflow.

More information can be found on Result Tasks | Onfido Studio

4.6.1.3. Manual decision tasks

The Manual Decision task allows clients and their internal teams to make manual decisions within a workflow in order to dictate the outcome of a workflow run. Some examples of a manual decision could include: Was the image quality sufficient? Could I make an exception on the document type used? The workflow will then use the outcome of the decision and proceed.

When a Manual Decision task is triggered during the execution of a workflow run, clients can make the decision from the Workflow Results page in the Studio Dashboard.

More information can be found on Manual Decision Tasks | Onfido Studio

4.6.1.4. Additional client actions and retries

Onfido also provides suggested client actions based on the results returned for:

- Document reports
- Facial Similarity reports

For the user, typical suggested actions as referenced in the above links include requesting the user to re-attempt verification, such as with a higher quality image or a supported document.

Retries are therefore allowed, using the same remote IDV method, subject to controls mentioned above in this document to detect and prevent abuse such as repeated, replay and injection attacks. Client-configurable controls include Known Faces, Repeat Attempts (Document Report) and the Studio Retry Task.

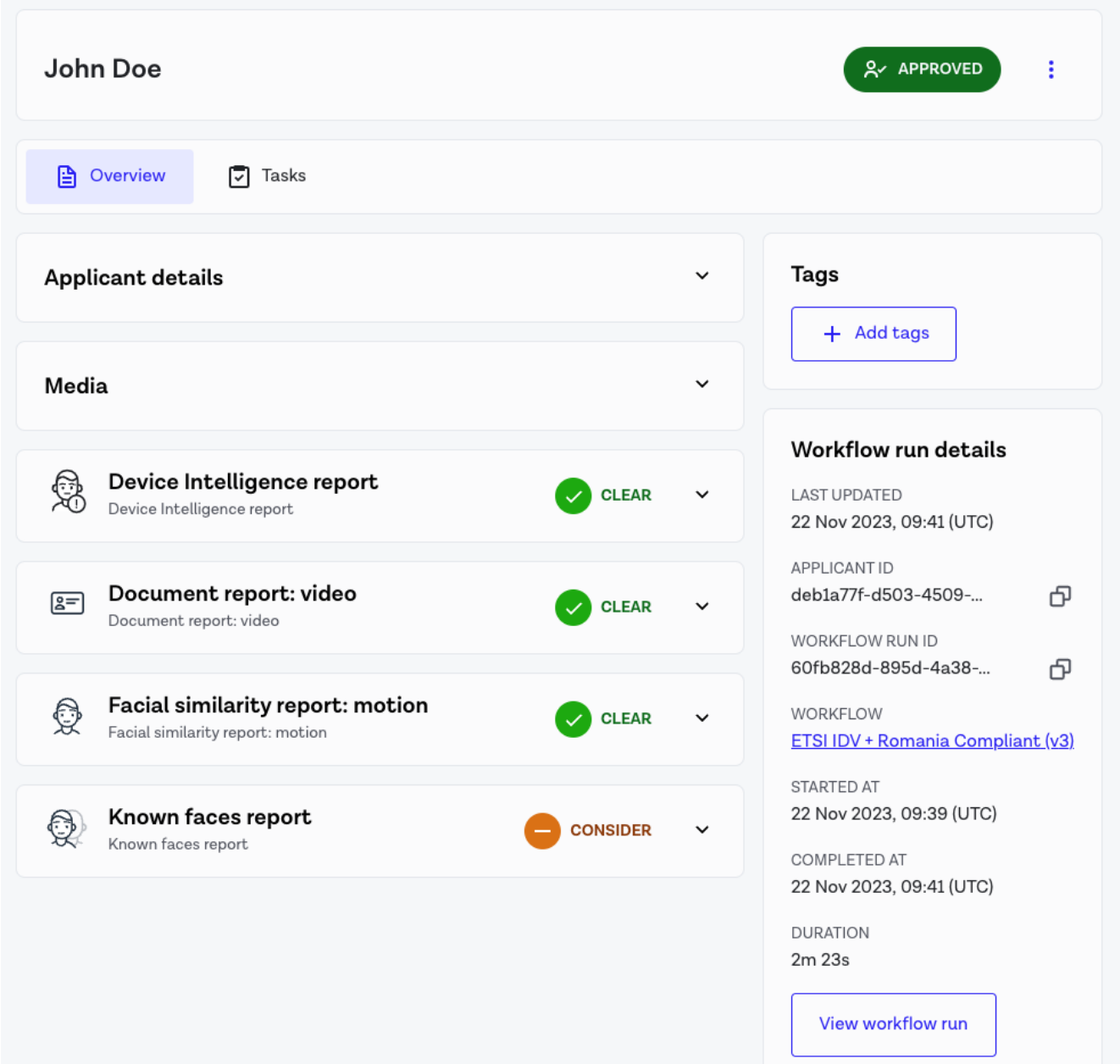
4.6.2. Results of the Remote IDV Process

All remote IDV results are made available to clients via our **Public API** and **Client Dashboard.** 4 high level categores of data can be returned:

- The **results** for each verification task (E.g. “clear” or “consider”) as well as the overall result for a given workflow run (E.g. “approved”, “declined”, “review”)
- The **breakdown results** for each verification task provide granular reasons to help with result interpretability as well as more fine-grained decision making. E.g. explaining that a document was rejected for IDV due to poor image quality.
- The **properties** (A.K.A verified identity attributes) for each verification. E.g. a first name or date of birth extracted from a document.
- Additionally, we return a number of evidence files which includes all relevant information collected and validated by Onfido during a Studio workflow.

Clients can use Studio’s Workflow Output Data feature to map the specific task data they require and then easily retrieve this subset of data via the API.

4.6.2.1. *Client Dashboard Example - Workflow Summary with Verification Tasks*



4.6.2.2. *API Example - Workflow Run and Tasks*

See Onfido API (Workflow Run Object) and Onfido API (Workflow Run Output Object) .

More information can be found on the Onfido Studio Product Guide

4.6.3. Evidence Files

Evidence Files include all relevant information collected and validated by Onfido during a Studio workflow. Depending on local regulations, clients may be required to download and retain these files so that they can demonstrate the authenticity and integrity of each remote identity verification performed through Onfido.

As part of our Compliance Suite solutions, Onfido makes the following Evidence Files available to clients:

1. **Evidence Summary File** is a PDF document containing a time-stamped audit trail of all relevant information collected and validated by Onfido during a Studio workflow. This file is signed by Onfido using a qualified certificate to ensure its authenticity and integrity and also meets the requirements of relevant standards and regulations.
    a. It is signed by Onfido using the PDF Advanced Electronic Signatures (PAdES) standard which is eIDAS-compliant and can be verified through tools such as Adobe Reader.
    b. It also includes references for each captured media, including unique identifiers and a hash based on the SHA256 algorithm. The hash can be compared to the hash of the captured media to verify that it is the same file referenced in the summary.
2. **Captured Media** includes all images/videos of the user's identity document and the images/videos of the user's face.

Additionally, for ETSI Certified IDV with Qualified Electronic Signature we provide:

3. The **Certificate Documents** which are the QTSP's terms and conditions for issuance of a qualified certificate to the user. This includes 3 PDF documents: the Application Form, General Terms and Conditions and Data Processing Notice
4. The **Signed Documents** are the PDF documents electronically signed by the User using their QES.

All Evidence Files are available to download via the API in their original, high quality format.

More information can be found at ETSI certified identity verification | Onfido Developer Hub, ETSI certified IDV with Qualified Electronic Signature | Onfido Developer Hub and API documentation.

4.6.4. Accuracy of IDV Timestamps

Onfido implements controls that ensure that the timestamps recorded throughout the IDV process and Evidence Files are accurate, and remain accurate over time.

Our infrastructure, hosted on AWS, uses the AWS Time Sync Service delivered over Network Time Protocol (NTP). The service uses a fleet of redundant satellite-connected and atomic clocks in each cloud infrastructure region to deliver a highly accurate reference UTC clock to our IDV systems and components.

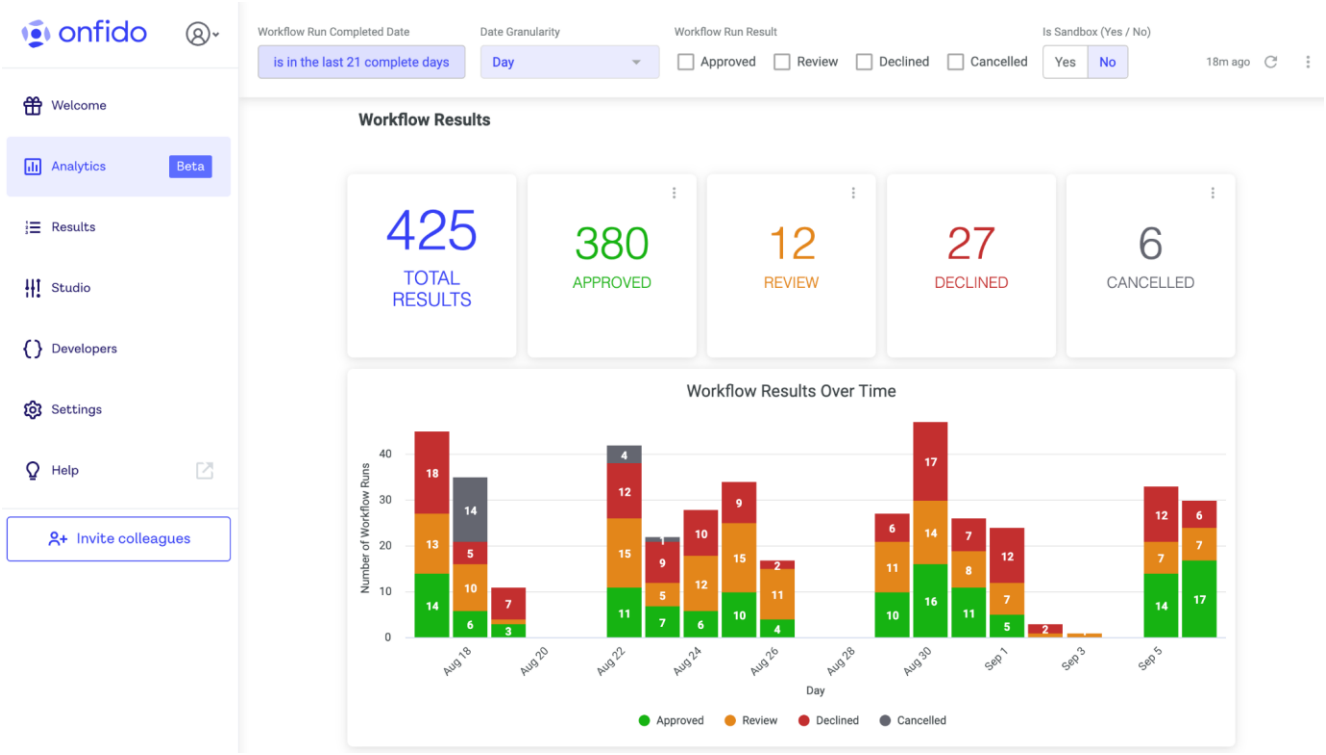
Individual clocks are continuously monitored for time deviations and are automatically synchronised multiple times per hour. All clock synchronisation events are logged.

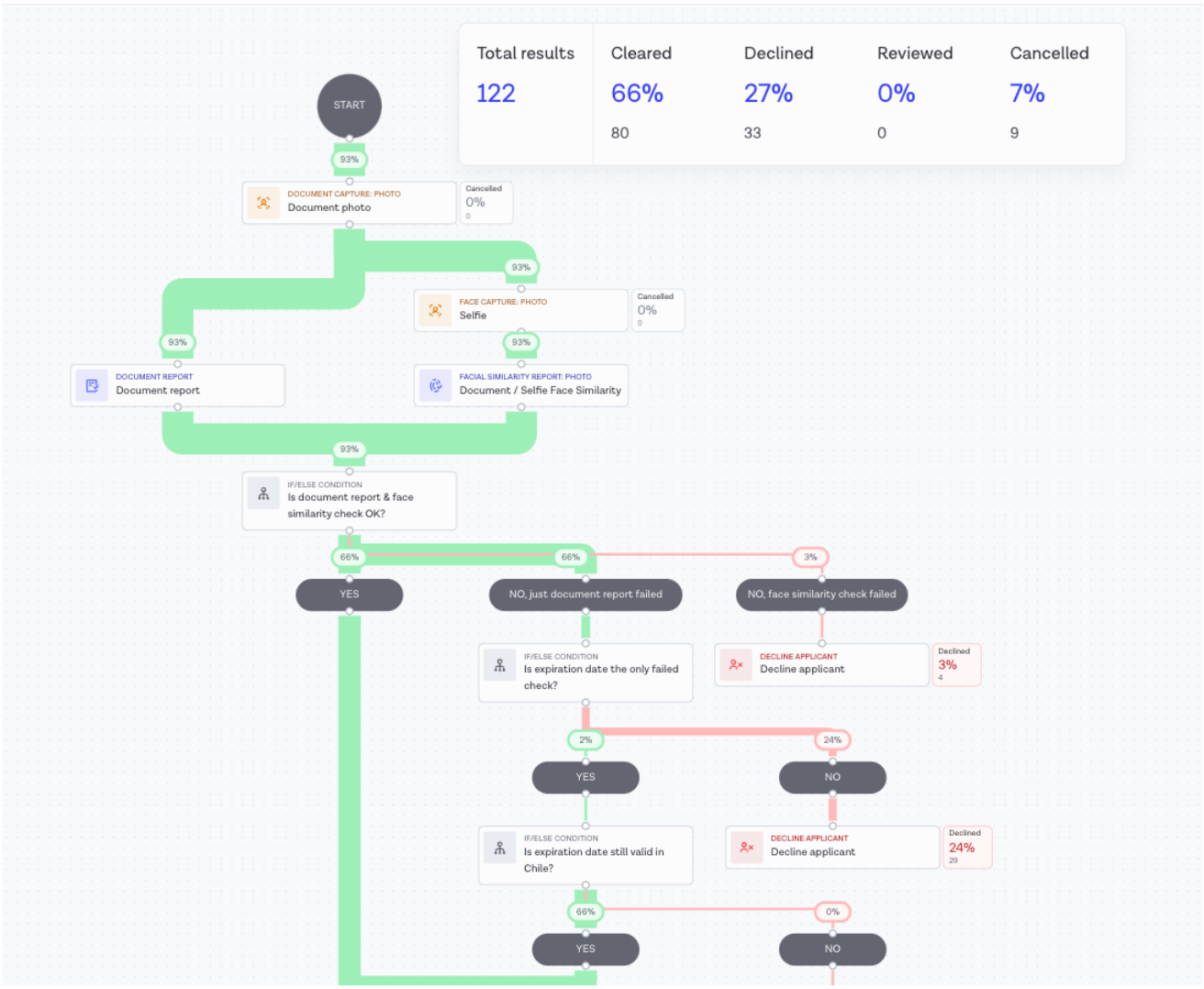
Clock accuracy when using the Time Sync Service is within one millisecond of UTC.

4.7. Analytics and Performance Monitoring

Onfido Studio provides detailed analytics that enables clients to monitor performance and optimise verification journeys.

- **Monitor Performance -** Get a snapshot of how workflows are performing across all business units, all in one place.
- **Identity Trends -** Spot trends in workflow behaviour over time, and identify opportunities for optimisation.
- **Optimise Journeys** - Get a complete look at the identity verification funnel, identify areas of drop-off, and iterate in a few clicks.



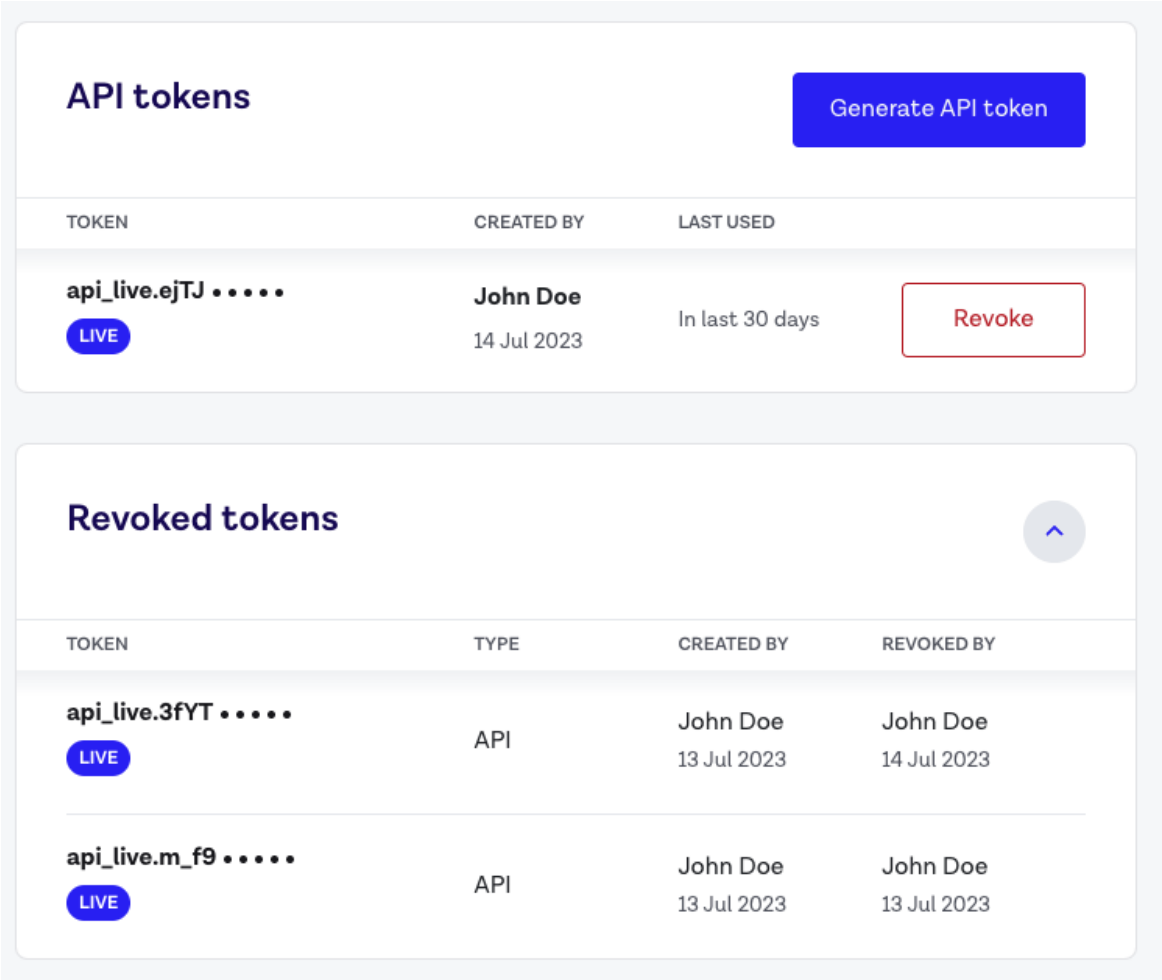

Total results
122
Cleared
66%
80
Declined
27%
33
Reviewed
0%
0
Cancelled
7%
9
START
93%
DOCUMENT CAPTURE: PHOTO
Document photo
Cancelled
0%
0
93%
FACE CAPTURE: PHOTO
Selfie
Cancelled
0%
0
93%
93%
DOCUMENT REPORT
Document report
FACIAL SIMILARITY REPORT: PHOTO
Document / Selfie Face Similarity
93%
IF/ELSE CONDITION
Is document report & face similarity check OK?
66%
66%
3%
YES
NO, just document report failed
NO, face similarity check failed
IF/ELSE CONDITION
Is expiration date the only failed check?
DECLINE APPLICANT
Decline applicant
Declined
3%
4
2%
24%
YES
NO
IF/ELSE CONDITION
Is expiration date still valid in Chile?
DECLINE APPLICANT
Decline applicant
Declined
24%
29
66%
0%
YES
NO

4.8. Account & Client Dashboard Security Controls

4.8.1. API Token Management

The Onfido API uses token-based authentication. API tokens must be included in the header of all requests made to the API.

Clients can generate new tokens and manage existing ones in the Client Dashboard shown below.

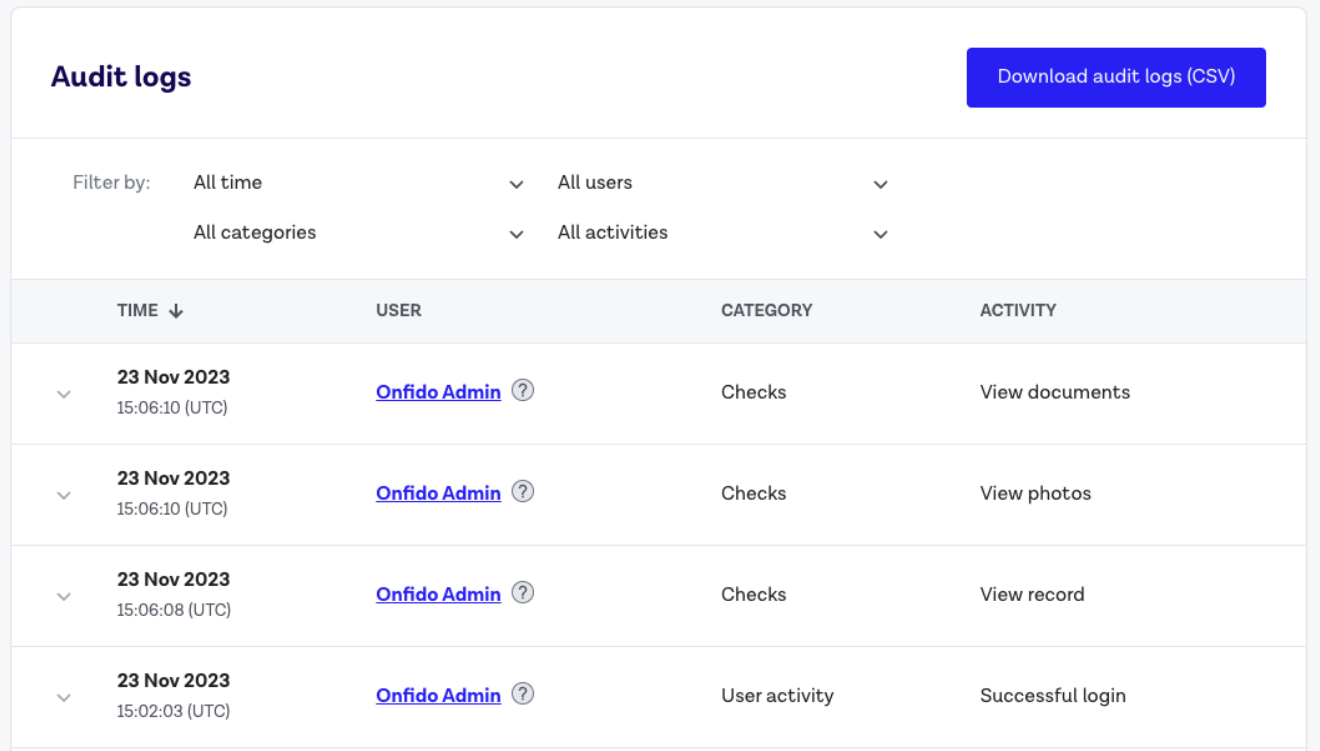


Clients can make requests using sandbox tokens to test our API before they go live.

More information can be found at [Token Authentication | Onfido API]

4.8.2. Audit Logs

If enabled on a client's account, Onfido tracks a wide range of activities related to a client's account and those performed through the Client Dashboard. Events are stored in a timestamped audit log visible only to the "Owner" user role as seen below.



The following categories of data are logged:

- User activity e.g. Successful login, Password changed, user deactivated
- Profile Changes e.g. change to user name
- Organization Changes e.g. Activate/Deactivate SSO
- Audit Log Activity e.g. View Audit Log page
- Developers Tokens e.g. Generate API Token
- Developers Webhooks e.g. Create Webhook

Audit logs can also be downloaded to a CSV file and accessed via API.

4.8.3. User Access Management

Onfido's Client Dashboard allows different user roles and permissions to be assigned to different users in an organisation.

The available roles and permissions are as follows:

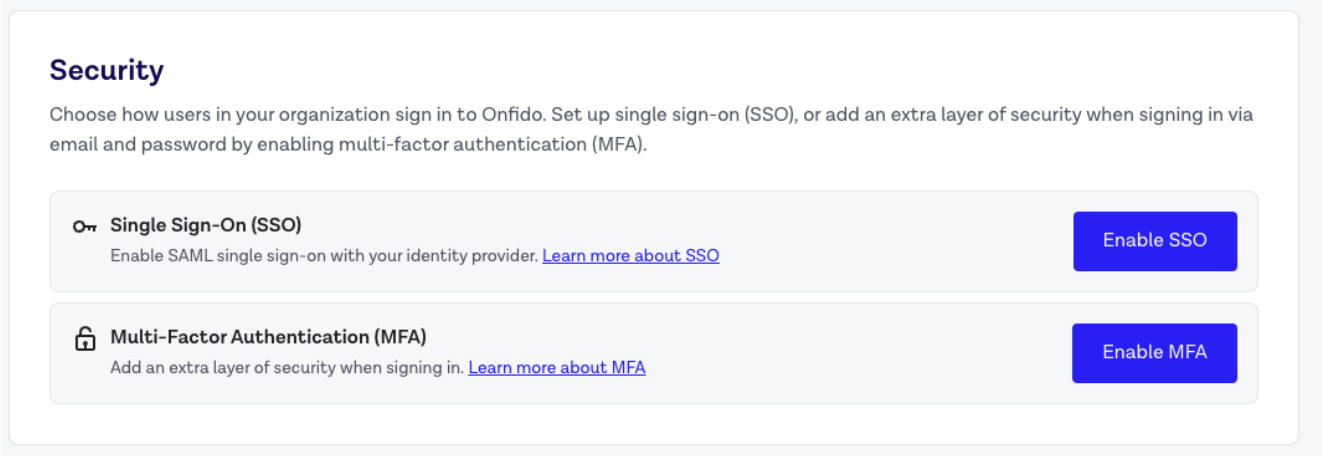
- Owner
- Admin
- Standard
- Read-only
- Developer
- Read-only Analytics

Roles and access permissions for the different areas of the Client Dashboard are documented in the following support articles:

- Dashboard - User Roles and Permissions (Studio)
- Dashboard - User Roles and Permissions Part 1 | Part 2 | Part 3

4.8.4. Single Sign-On and Multi-Factor Authentication

For added security, clients can configure both single sign-on and multi-factor authentication through the Client Dashboard.



The following support articles contain the steps on how to configure these features:

- Dashboard - Setting up Single Sign-On SSO
- Dashboard - Multi Factor Authentication

4.8.5. Data Deletion

Clients control how long Onfido retains their data (subject to maximum retention periods set by Onfido). A client can instruct Onfido to delete data relating to a particular check for any reason by either submitting an ad hoc deletion request/instruction, or enabling rolling deletion on their account.

Once data is deleted, Onfido will not be able to carry out any troubleshooting or investigate any queries raised by clients regarding that data. It is for this reason we recommend clients do not delete their data within the first thirty days following completion of a verification.

Note: Depending on local laws and regulations, clients may be required to download and store all evidence files from Onfido prior to data deletion. Once data has been deleted, these files cannot be downloaded anymore.

Ad-hoc deletion flow

Rolling Deletion Flow

More information can be found at Data deletion | Onfido Developer Hub

onfido

5. Remote IDV Security Policy

In addition to the *Remote IDV Practice Statement* above, Onfido maintains a *Remote IDV Security Policy* which includes the following topics:

- Risk Assessment
- Policies and Practices
- TSP Management and Operation
    - Internal Organisation
        - Organisation Reliability
        - Segregation of Duties
    - Human Resources
        - Pre-employment Screening
        - Trusted Roles
        - Disciplinary Processes
    - Asset Management
    - Protection of Information Assets
        - Media Handling
        - Assess Control
    - Cryptographic Controls
    - Physical and Environmental Security
    - Operation Security
    - Network Security
    - Incident Management
    - Collection of Evidence
    - Business Continuity Management
    - Termination and Termination plans
    - Compliance

5.1. Scope

This part of the document covers remote identity verification in regards to the information security policies at Onfido. We are closely aligned to the SOC2 Type II and ISO/IEC 27001:2022 standards, and hold the SOC2 Type II and ISO/IEC 27001:2022 certifications.

5.2. Reference Documents

IDV Standards

- ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI TS 119 461 V1.1.1 (2021-07) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

Onfido Public Policies

- Remote IDV Practice Statement (**sections 1-4 of this document**)

Onfido Internal Policies (only made available to auditors and clients under NDA) include but are not limited to the following:

- Risk Management Policy
- Information Security Policy
- (Security) Incident Management Policy
- IT Infrastructure and Network Policy
- Physical Access Security Policy
- External Party Management Policy
- Software Development Lifecycle Policy
- Patch Management Policy
- Secure Coding Policy
- IT Asset Management Policy
- User Access Management Policy
- Data Management Policy
- Information Classification and Handling Policy
- Business Continuity Policy
- Disaster Recovery Policy

5.3. Risk Assessment

5.3.1. Risk Assessment process and measures

Onfido carries out a risk assessment process to identify, analyse, evaluate, monitor, and escalate/report trust service risks including business and technical issues. Onfido defines the methodology for the identification, assessment and treatment of enterprise-wide risks in Onfido.

Please refer to our *Risk Management ("Assessment")* and *Information Security Policies* for more details.

5.4. Policies and Practices

5.4.1. Trust Service Practice Statement

Our *Remote IDV Practice Statement* (sections 1-4 of this document) contains the policies and the processes used for the trust service components we provide for identity proofing of trust service subjects.

5.4.2. Terms and Conditions

Onfido terms and conditions specify the service provided and the definitions applied to the service agreement. They are available as a durable means of communication, for more details please refer to the Onfido Services Agreement (OSA) on our website.

5.4.3. Information Security Policy

Onfido *Information Security Policy (ISP)* outlines the framework, rules, and principles for managing Information Security within Onfido. It defines Onfido's core procedural and organisational requirements relating to Information Security (Technical and Organisational Measures), and is communicated to clients and other stakeholders in line with contractual and ETSI EN 319 401 requirements.

Onfido's Technical and Organisational Measures defined in the ISP and summarised in this document, achieve a level of protection as defined in Article 32 of the General Data

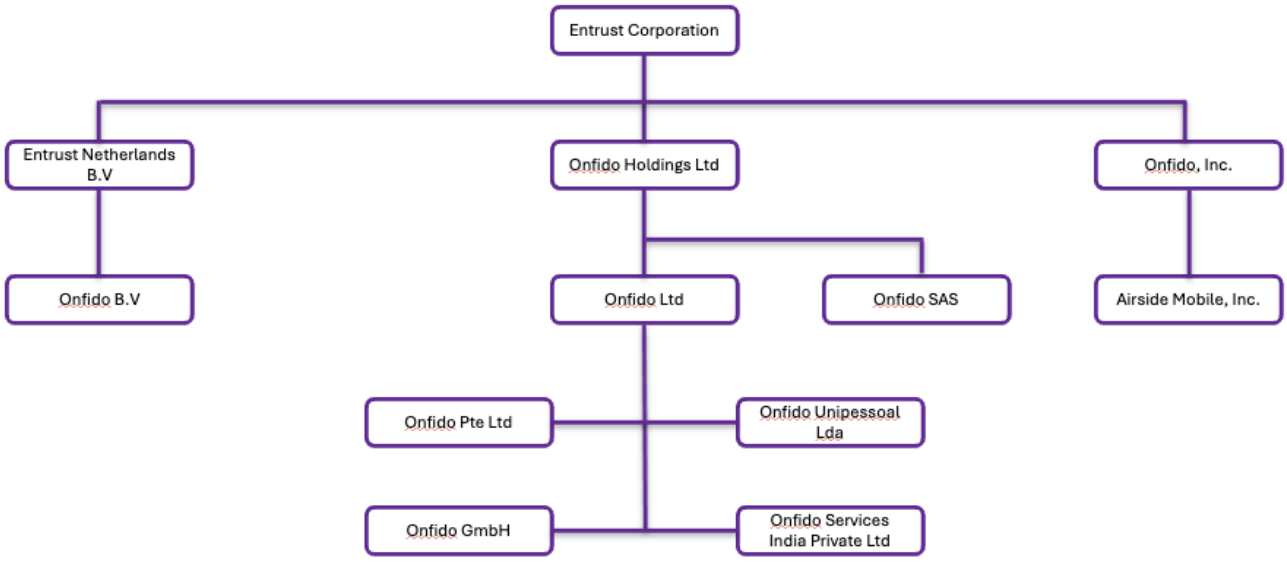
Protection Regulation (GDPR), including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

We are closely aligned to the SOC2 Type II and ISO/IEC 27001 Standards - and we hold the SOC2 Type II and ISO/IEC 27001:2022 certifications.

For more details please refer to our Information Security Policy, and our ISO 27001 Statement of Applicability and SOC2 Type II audit report.

5.5. IPSP Management and Operation

5.5.1. Corporate structure



The Onfido group was acquired by Entrust Corporation in April 2024. Onfido Ltd is the principal trading entity of the subset Onfido Group. Onfido GmbH, Onfido BV, Onfido SAS, Onfido Inc, Onfido PTE Limited and Onfido Services India Private Limited are set up as distributors of Onfido Limited.

Company registration details are provided below for relevant Onfido and Entrust entities.

Legal Entity Name	Company Number	Registered Address & Contact information
Onfido Holdings Ltd	13693711	14-18 Finsbury Square, 3rd Floor, London, England, EC2A 1AH Email: notices@onfido.com
Onfido Limited	07479524	14-18 Finsbury Square, 3rd Floor, London, England, EC2A 1AH Email: notices@onfido.com
Onfido SAS	848 016 176	1 Place Rivierre Casalis , 45400 Fleury Les Aubrais , France Email: notices@onfido.com
Onfido, Inc.	5769835	1187 Park Place, Shakopee, MN 55379 Email: notices@onfido.com
Onfido B.V.	83285490	Zijlweg 148 A 002, 2015BJ Haarlem, Netherlands Email: notices@onfido.com
Onfido GmbH	HRB 211512 B	Lütticher Straße 132, 40547 Düsseldorf, Germany Email: notices@onfido.com
Onfido PTE LTD	201915799K	100 TRAS STREET, #16-01, 100 AM, SINGAPORE (079027)

		Email: notices@onfido.com
Onfido Services India Private Limited	U74999MH2018FTC305598	Unit No 9, Corporate Park II, 9th floor, VN Purav Marg, Near Swastik Chambers, Chembur, Mumbai City, Maharashtra 400071, India Email: notices@onfido.com
Airside Mobile, Inc.	4822606	1187 Park Place, Shakopee, MN 55379 Email: notices@onfido.com
Entrust Corporation	0705421	7 Park Place, Shakopee, MN 55379
Entrust Netherlands B.V.	56686331	Zijlweg 148A 002 2015BJ Haarlem, The Netherlands

5.5.2. Internal Organisation

5.5.2.1. Organisation Reliability

Onfido operates under a non discriminatory environment, there is a governance in place that sets up a non-bias structure. Onfido has an appropriate amount of insurance to cover the risks associated with the use of the service it provides, and has the financial means necessary to cover the obligations set out in this policy.

The procedure for the resolution of complaints and disputes is covered in the Terms of Use available on our website.

5.5.2.2. Segregation of Duties

Onfido implements segregation of duties where possible to prevent users having excessive privileges in order to preserve the integrity of assets. Role-based access is also implemented.

Please refer to our *User Access Management Policy* for more details.

5.5.3. Human Resources

5.5.3.1. Pre-employment Screening

In accordance with applicable employment laws, Onfido performs pre-employment screening checks ("background checks") on employees and contractors to confirm their identity, right to work, and suitability to work based on criteria such as criminal history, international fraud and sanctions, credit check, and reference check.

Please refer to our *Pre Employment Screening Policy* for more details.

5.5.3.2. Trusted Roles

Onfido employs staff and third parties who have expertise, experiences, qualifications, and have received training on security and personal data protection to provide the service offered reliably and according to their job function.

Onfido has defined the following trusted roles:

Trusted Role	Description of role
Security Officers	The security officer is responsible for managing the implementation of the security practices and liaising with the relevant external parties in the event of a fraud cyber attack.
System Administrators	The system administrator is in charge of the administration and configuration of all the technical components of the service.
System Operators	The system operator is authorised to perform system backup and restoration as well as the day-to-day operations of the service.
System Auditors	The system auditor is responsible to keep relevant audit logs of the security system

5.5.3.3. Disciplinary Processes

Onfido has a disciplinary policy and procedure in place to report and respond to suspected instances of behaviour or conduct which fall below what is expected. This includes suspected misconduct and/or breaches of company policy. Per the policy, if possible disciplinary cases are initially responded to informally; if this is unable to resolve the issue Onfido may proceed with a formal disciplinary if necessary.

Please refer to our *Disciplinary Policy* for more details.

5.5.4. Asset Management

5.5.4.1. Protection of Information Assets

Onfido has a policy and procedure in place to prevent the loss of data or organisational assets, protect Onfido's resources on the network, and reduce risk of losing data due to poor planning. Please refer to our *IT Asset Management Policy* for more details.

In addition Onfido has relevant logs to detect possible malfunctions and attempts to illegally access information system components.

Security-critical events are logged. Security event logs for critical servers are collated, monitored, and alerted to the Security team using our Splunk SIEM system and AWS GuardDuty.

5.5.4.2. Media Handling

Onfido handles media securely in accordance with requirements of the information classification scheme. Please refer to our *Data Management* and *User Access Management* and *Information Classification And Handling Policies* for more details.

5.5.5. Access Controls

Onfido implements logical access control across its networks, internal IT systems, the Onfido service itself, to provide authorised, auditable and appropriate user access. Please refer to our *User Access Management Policy* for more details.

In addition Onfido has a policy and procedure in place to prevent the loss of data or organisational assets, protect Onfido's resources on the network, and reduce risk of losing data due to poor planning.

Please refer to our *User Access Management Policy* for more details, and below section 'Business Continuity Management' for further details on how Onfido manages the risk of losing data due to poor planning of business continuity.

5.5.6. Cryptographic Controls

Data is logically segregated with software and access policy controls. Data is encrypted both in transit and at rest. Additionally, all data at rest is encrypted with dedicated master encryption keys providing two layers of encryption and protection.

Please refer to our *IT Infrastructure and Network Policy* for more details.

5.5.7. Physical and Environmental Security

This policy enables the organisation, in as far as is reasonably practicable, to ensure the safety and security of the building, the Onfido assets contained therein, and the people using these facilities.

Please refer to *Physical Access Security Policy* for more details.

5.5.8. Operation Security

Onfido uses trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

Please refer to our *User Access Management, External Party Management, Information Security, Patch Management, Secure Coding, and Software Development Lifecycle Policies.*

5.5.9. Network Security

Onfido set out framework, rules, and principles to protect its network and system from attack.

Please refer to our *Information Security, IT Infrastructure and Network,* and *User Access Management Policies*.

5.5.10. Incident Management

The Onfido *Security Incident Management Policy* covers the process for managing security incidents enabling Onfido to respond quickly to incidents and to limit the impact of breaches of security. This policy also covers all roles and personnel who are involved to investigate the incident.

The incident management process includes the following:

- Reporting of Incident
- Containment and Recovery
- Assessment
- Breach Notification
- Notification Methods
- Collection of Evidence
- Evaluation and Response

5.5.11. Collection of Evidence

Onfido has a policy that defines the processes, controls, and roles and responsibilities relating to data management.

Data management in this context refers to the controlled:

- Collection
- Storage
- Processing (use)
- Retention
- Backup
- Quality management, and
- Deletion

of data collected and/or processed as part of Onfido's service provision.

Please refer to our *Data Management Policy* for more details.

5.5.12. Privacy & Data Protection

Onfido's identity verification services are designed using privacy by design and by default and data minimisation principles. As a UK company we have built our data handling policies, processes and overall framework on the EU/UK GDPR and to support, maintain and reflect our role as a data processor of the data submitted by users using our products ("End Users"). Please refer to the Onfido Privacy Policy for more details.

5.5.13. Business Continuity Management

Onfido has a Business Continuity Plan (BCP). The plan includes the following:

- Identification of critical Onfido applications and information assets.
- Identification of roles and responsibilities.
- Maintaining compliance with clients and data providers, security requirements and contractual agreements.
- Maintaining compliance with data protection requirements.
- Maintaining compliance with ETSI EN 319 401 and IDV requirements.
- Continued compliance with Onfido information security policies.
- Operational procedures that will ensure recovery and restoration of business
- operations and availability of information within agreed timescales.
- Education of relevant staff on agreed procedures.
- Testing and updating of plans and procedures.

Please refer to our *Business Continuity Plan Policy* and *Disaster Recovery Policy* for more details.

5.5.14. Termination and Termination plans

Terms and termination of service plans are outlined in the Client Service Agreement signed by both parties. They are issued in durable means and made available to our clients electronically. Please refer to our *Client Service Agreement template* for more details.

Onfido has an internal Services Termination Plan which sets out how Onfido will support its clients to ensure continuity and facilitate an orderly transition to another provider. This document outlines Onfido's plans relating to termination communications, transition mechanics, economic funds, and on-going monitoring / internal assessment / controls.

5.5.15. Compliance

Onfido has policies and processes to ensure that it operates in a legal and trustworthy manner, and runs annual compliance training to ensure that employees are aware of their responsibilities.

Every employee has a formal employee contract, which must be signed prior to starting employment and includes agreement to adhere to all company policies, including but not limited to:

- Anti-Corruption Policy,
- Code of Ethics,
- Anti-Harassment Policy,
- Acceptable Use Policy,
- Information Security Policy,
- Information Classification and Handling Policy,
- IT Asset Management Policy,
- Physical Access Security Policy,
- User Access Management Policy,
- Secure Coding Policy,
- Security Incident Management Policy; and
- Service Capacity Management Policy.

Onfido's Anti-Modern Slavery Statement is published on our website.