xProof Identity Proofing Service (ETSI) Practice & Policy Statement

17th September 2025

www.daon.com

Contents

Review & Approval

Revision History

Version	Date	Revision Author	Summary of Changes
0.1	4th July 2025	Eric Gilmore	Initial version for CAB
0.2	15th August 2025	Eric Gilmore	Minor updates and addition of accuracy targets
0.3	22nd August 2025	Eric Gilmore	Revisions to address Stage 1 audit findings
1.0	17th September 2025	Eric Gilmore	Revisions to address final findings. Initial published version.

Distribution

EMEA Customer Success team

VP, Cloud Services

CISO

Approval

Name	Position	Signature	Date
Clive Bourke	President, EMEA & APAC	(Signed copy on file)	18/09/2025

On Behalf Of

Daon Ltd.

IFSC House

Custom House Quay, Dublin 1

DO1 R2P9 Ireland

1 Introduction

This document is the Trust Service Practice Statement and Policy Statement for Daon's xProof-based Identity Proofing Service on the TrustX platform, aligning with the ETSI Identity Proofing Technical Specification (ETSI TS 119 461).

This document will be available on a Daon web site (www.daon.com or www.trustx.com). Sensitive information is not disclosed.

1.1 About Daon, our Products and Services

Daon, the Digital Identity Trust company, enables market-leading organizations worldwide to easily and accurately proof, verify, authenticate, and secure customer identities at every trust point across the entire customer lifecycle. With industry-leading identity proofing and biometric authentication technologies at its core, Daon's technology ensures that customer identities are accurately verified, safely secured, and easily recovered. By mitigating fraud, reducing friction, and ensuring regulatory compliance, Daon helps businesses deliver a seamless customer experience, increase customer satisfaction, and reduce costs. Daon delivers these solutions through its AI and ML-powered TrustX and IdentityX platforms, chosen by leading companies in financial services, telco, travel & hospitality, and other industries to secure and process hundreds of millions of digital identity transactions daily. Learn more at www.daon.com.

xProof, Daon's identity proofing and verification product, offers global identity validation for onboarding customers from wherever they are. Featuring patented document verification processes, advanced anti-spoofing technologies, and watchlist capabilities, xProof provides the necessary technology to ensure customers are who they claim to be, while meeting regulations including for KYC and AML.

xProof is available on TrustX, our cloud native, SaaS-based identity continuity platform, featuring a no-code orchestration layer for rapid deployment and continual customization of user journeys. TrustX is built to support identity proofing and authentication applications, as well as easy integration of third-party applications, with full insight into every customer interaction.

1.2 Scope of Service

This document describes an ETSI TS 119 461-compliant ID Proofing Service using xProof on TrustX. It includes references to other documents that include further detail but that may not be publicly available (but are available to Daon customers, CAB and other authorities as needed.)

The audience for this document is primarily TSPs and other RPs using the service. This document is also used by the CAB performing audits of the IPSP service.

The ID Proofing Service addresses ETSI TS 119 461 V2.1.1 (2025-02) and ETSI EN 319 401 V3.1.1 (2024-06). It provides LoIP Extended (High).

It supports Use Cases for *Identity Proofing of a Natural Person using an Identity Document for Unattended Remote Identity Proofing* in either *Automated* (9.2.3.4) or *Hybrid Manual and Automated* (9.2.3.3) methods.

Proofing of identity in this way is intended to comply with identity verification according to EIDAS Article 24.1a (c) and verification of the attributes listed in this document in accordance with EIDAS Article 24.1b (d).

Daon customers can work with Daon's Account and Customer Success teams to get enabled with xProof configured as an ETSI TS 119 461-compliant ID Proofing Service.

This document contains references to various other Daon policies that underly the Identity Proofing Service.

1.2.1 Identity Proofing Context

The Identity Proofing service can be used by any organisation wanting to implement an identity proofing process in conformance with ETSI TS 119 461. This could include Trust Service Providers including electronic signatures, Attribute Service Providers and others, but also other types of Relying Parties (e.g., financial services providers requiring KYC/AML ID verification).

Organisations providing Trust Services or other services depending on identity verification in accordance with EIDAS norms on can rely on Daon as an independent IPSP. Trust Services will need to meet a range of additional requirements, in addition to those met by Daon as an IPSP.

May be used by financial institutions or other subject to AML regulations. Completion of a fully AML verification will involve additional steps.

Other organisations with scenarios needing this level of identity assurance (or choosing to adhere to the specification) may also use the service.

RPs are responsible for ensuring compliance with the relevant regulations for their operating conditions (business needs, regulations, locations, etc.)

It is intended that the identity proofing can be configured within the approach specified here, e.g., to limit the types of documents further, adding additional checks, etc.

1.2.2 Attributes

The service intends to prove these identity attributes:

- Name (Surname and Given Names)
- Date of Birth
- Place of birth (if available)
- Nationality (if available)
- ID number (if available and appropriate)
- Document number (if available and appropriate)
- Document expiration date (if available and appropriate)
- Address (if available)

1.3 Terms and Conditions

Daon's publishes standard Terms and Conditions (T&Cs) and Privacy Policy.

In many cases, Daon's Identity Proofing Service will be part of our customer, the RP's service, e.g., another trust service. In this case, the RP will publish the relevant T&Cs and Policy and ensure that their end-users are aware of them and, where necessary, consent to them.

Where an RP uses their own terms and conditions, they will include Daon's data processing under GDPR (and other relevant data protection regulations) and any other relevant conditions. This is governed by Daon's contract with the RP.

1.4 Information Security Policy

Daon maintains a certified ISO 27001 Information Security Management System, which includes an Information Security Policy that is available under NDA as need to CAB and Daon customers.

To maintain a secure configuration, automated daily scans of the Service are used to identify security configuration gaps, with any alerts actioned as required.

1.5 Other Certifications and Compliance

Daon maintains other relevant certifications and compliances. These currently include the following for which Daon has been independently audited:

- Spanish National Cryptologic Centre (CCN) Security Products Catalogue – Video Identification Tools
- UK Digital Identity & Attribute Trust Framework registered Identity Verification, Attribute & Orchestration provider
- ISO 27001:2022 (information Security Management), ISO 27018:2019 (Protection of Personally Identifiable Information), ISO 27017:2015 (Cloud Data Protection) and ISO 27701:2019 (Privacy Information Security Management)
- SOC 2 Type 2
- Biometric and other similar certifications are mentioned in the relevant sections.

1.6 Responsibility and Approval

This document is reviewed and approved by the Daon senior management person responsible for our European business, who are also responsible for implementing the practices.

This document is to be reviewed at least annually.

1.7 Changes

When necessary, this document will be updated to reflect changes in the Identity Proofing Service. A new version will be created and numbered. The updated version will be reviewed and approved before being put in place. The new version of the document is to be published on www.daon.com or www.trust.com

In the event that the changes have an impact on RPs or their end-users, Daon will inform the RP with due notice so that they can in turn inform their end-users as needed.

1.8 Terminology

Applicant: as in ETSI TS 119 461, in this case an end-user of a Daon Relying Party's service.

Customer: means a Daon customer organisation, typically acting as a Relying Party for Daon's service.

End-user: means a person who is the subject of the identity proofing process (referred to as an Applicant in ETSI TS 119 461.)

Process: means an identity proofing/verification process, being operated by Daon's Service

Relying Party (RP): means an organisation using Daon's Identity Proofing service to verify the identity of their end-users (e.g., their customers or applicants for their services)

Service: means Daon's Identity Proofing service, typically the back-end/server components running in the cloud-based environment managed by Daon.

2 Risk Assessment

Daon carries out risk assessment to identify and address risks in its business and services. The relevant processes include Risk Assessment and Treatment Process, Fraud Management Policy and Digital Identity Fraud Control Plan.

3 Management and Operation

3.1 Internal Organisation

Daon operates in a non-discriminatory manner, with policies and practices in place for management and employees.

We maintain appropriate types and levels of insurance for our business.

We operate segregation of duties across our business and specifically in relation to access to systems and data.

3.2 Human Resources

Daon operates appropriate Human Resources (HR) policies including for hiring, screening and disciplinary procedures.

In addition, we have processes in place for engagement of third parties.

3.3 Asset Management

Daon operates Information Security and related Policies covering asset management and storage media.

3.4 Access Control

Daon operates a User Access Control Policy and Access Management Policy, which ensure that appropriate access control is in place for all systems and that access is restricted to those who need it.

3.5 Cryptographic Controls

Data managed within the Identity Proofing Service is logically separate from other business data and systems. Each Customer's data is encrypted and access controlled separately. Cryptography keys are stored in a Key Management System.

3.6 Physical and environmental security

Daon operates security and safety policies for its office locations.

3.7 Operation security

Daon operates trustworthy systems and products that are protected against modification that ensure the technical security and reliability of the processes they support. A number of our Information Security policies support this.

3.8 Network security

Daon operates Network Security Policy and a number of related policies to protect assets on our networks.

3.9 Incident Management

Daon operates an Incident Management Policy and maintains a series of technical measures including logging and alerting to support this. Our Customer Support and Cloud Services (and

where appropriate, Information Security) teams lead incident response, classification, reporting and review procedures.

3.10 Collection of Evidence

Daon operates a Records Retention and Protection Policy and operates its services with appropriate data retention processes.

See also Section 5 of this document.

3.11 Business Continuity management

Daon operates a number of policies for business continuity including a Disaster Recovery Policy.

3.12 Termination plan

Termination of service is covered in the contract terms with each of Daon's Customers. Daon will communicate with Customers in advance of a termination of service (allowing them to communicate with end-users if necessary), assist Customers to access any data before termination and to transition to another service provider.

3.13 Compliance

Daon operates policies and processes to ensure that it operates in a legal and trustworthy manner and provides regular training to ensure that employees are aware of their responsibilities.

4 Service Components

4.1 TrustX Platform

TrustX is Daon's SaaS identity platform. It uses an Orchestration approach to create customised identity verification processes that are compliant with regulations (and internal policies) while offering a seamless user experience. It is managed by Daon's Cloud Services team.

xProof on TrustX offers identity verification processes with a range of configurable options, including image-based checks for Passports and other ID documents; ePassport checks with NFC; Biometric Checks; extension points for trusted 3rd party checks via Cloud Functions and the option of incorporating Manual Review by trained document reviewers. It includes the "ready to go" document and biometric capture user interfaces.

We offer APIs and SDKs to allow Daon Customers to integrate identity proofing within their business systems. Back-end systems, including web/mobile application servers, line of business systems and others can access the Daon platform services via a REST web services API. We offer our Trust SDKs that can be used to easily add identity verification to iOS and Android mobile apps and our Trust Web components for browser-based identity verification.

The orchestration capabilities of TrustX allow our customers to define identity verification processes to meet a range of needs in addition to allowing configuration of the approach described in this document.

The architecture of TrustX includes:

- Mobile SDK (iOS/Android) or Web component used for evidence collection, which can be embedded in a Daon customer's own app or Daon can provide an app. In some case, a Customer may use alternative evidence collection tools in which case they must collect the information specified in Section 5.2 of this document.
- All evidence is transmitted to Daon's TrustX SaaS platform for processing
- This platform includes a range of services for:
    - ID Document quality assessment, validation, etc.
    - Biometric matching and liveness/presentation attack detection for binding
    - Process management/orchestration
    - User data management and storage
    - Analytics
    - Etc.
- The platform is running in AWS and is managed and supported by Daon staff in Daon's worldwide office locations who have limited access to systems, based on their role.
- The platform is separate from Daon's office/business systems.
- Sensitive data is stored encrypted by keys that are specific to the Daon Customer (RP). The keys are secured within AWS KMS.
- We use AWS locations in the EU (currently Ireland and Germany) for the scope of this certification.

- A web-based Back Office tool is available to authorised users with Role-Based Access Control (RBAC) for configuration and data access.
- Customers can initiate identity proofing and get access to their data via REST web services (with authentication and authorization).
- All UI and API-based data transfer is encrypted.
- The core identity verification service is supported by other components, such as an IAM for user authentication/authorisation, system monitoring tools, etc.
- The service is under the scope of Daon's ISO 27001 ISMS and its extensions.

4.2 External Organisations

Amazon Web Services (AWS) cloud service is used as a hosting platform. For AWS certifications, see https://aws.amazon.com/compliance/programs/

We may incorporate components from certain open source or third party software providers in our Service, for which Daon takes responsibility.

Optional third party services may be incorporated in an identity proofing process using our platform's integration framework. We may use third party services to verify or assess the risk of information gathered during the identity proofing process, e.g., to assess risk of or to verify a device/evidence/attribute (such as trusted sources or commercial services).

5 Identity Proofing Approach

This section describes how our platform verifies an identity following identity proofing service requirements as specified in ETSI TS 119 461. Refer to the Use Cases section for any specific configuration to be used for specific use cases.

Documentation for use in initiating; configuring collection, validation and binding; and for getting the proof issued by the solution is available at https://docs.trustx.com/trust. Daon's EMEA Customer Success team can provide guidance to those responsible for implementation in alignment with this document.

5.1 Initiation

The identity verification process is embedded in a Relying Party's mobile app or web site.

A Relying Party (RP) system must initiate an identity verification process using the TrustX REST API. They will indicate the Process that they want to initiate, which will determine the specifics of the capture and validation.

The RP determines which Use Case(s) is used by initiating the Process with the appropriate approach. The RP can offer the applicant alternative processes (e.g., if the applicant has a passport and a mobile phone, they may be able to use the Automated use case; if they only have a non-electronic ID document, they may be able to use the Hybrid use case instead.) The RP is responsible for offering any other alternatives not supported by the Service that may be available and/or required.

Optionally, the RP can include additional information (such as attributes to be verified and evidence to be collected) during the initiation process. In this case, the identity verification process definition can configure the steps of the process accordingly (e.g., set the document country and type expected and verify that these attributes match).

The API provides a token that allows an app or web site to initiate the identity verification process within their end-user-facing user interface. The Trust SDK or Trust Web then guides the end-user through the collection of the attributes in a web or mobile app UI flow.

The end-user/applicant interacts with a UI presented by the Trust SDK or Trust Web which includes guidance for each step in the identity proofing process. Guidance may be fixed or conditional. It can be supplemented by additional guidance included by the Relying Party before the identity proofing is initiated (e.g., describing the purpose of the identity proofing).

The user interface can be customized with the RP's logo, colours, fonts, etc. It is available in multiple languages.

The TrustX UI has been designed to be compliant with Web Content Accessibility Guidelines (WCAG) 2.2 AA guidelines and so allows persons with disabilities to use assistive tools to complete the identity proofing process. An RP may also offer alternative identity proofing approaches to persons with disabilities.

5.1.1 Initial Steps

Introduction (optional): In introducing the process, it can be useful to let the end-user know the steps that are involved. A UI screen may be included (configurable) to show these to the user. An RP can also opt to include this information, additional context, alternative processes, etc. in further information provided to the user before initiating the TrustX UI so that the user can make the choice to continue or not.

Switch to Mobile (optional): In the case that a user initiates the process on a desktop or laptop, the process will typically be configured to ask them to transfer to a mobile device for better capture quality, access to NFC, etc. TrustX UI can display a QR on the desktop/laptop, which the user can scan on their mobile phone to continue the process. An RP can also choose to use alternative methods at this step. When the process completes, the desktop/laptop UI refreshes and allows the user to continue. In this scenario, no evidence is captured or processed on the desktop/laptop.

Consent (optional): TrustX will display a screen where the user can consent to data collection with a link to a privacy policy and terms & conditions as the next step of the identity verification flow. Daon's maintains and publishes standard Terms and Privacy Policy in addition.

Alternatively, the terms and policies may have been provided by the Relying Party before initiating the identity proofing. Responsibilities for data protection and related topics are clarified as part of Daon's contract with each Relying Party before implementation.

Some or all of the collection steps below are then initiated, according to the Process initiated by the RP.

5.2 Attribute and evidence collection

The following paragraphs list the main data collection steps. The flow can also include guidance and transitional screens relevant to the steps in the flow. TrustX also allows Custom Forms and Pages to be incorporated into the flow if needed, e.g., to collect or display additional/optional information.

The process will allow a maximum number of attempts to complete each step. This limit must be configured by/for the Relying Party. Where this is exceeded without evidence being successfully captured or validated, the process will be ended with status failed.

The service collects these identity attributes as a minimum:

- Name (Surname and Given Names)
- Date of Birth

The service may also collect these identity attributes if available and appropriate:

- Place of birth
- Nationality
- ID number
- Document number

- Document expiration date
- Address.

No other data is collected as identity attributes.

5.2.1 Face Capture

Capture face photo/selfie: A selfie capture with a liveness check allows the system to verify that the ID document holder is present during the identity proofing. A face photo/image is captured using the front-facing camera on the device.

The user is prompted to position their face in the centre of the camera and quality checks of the video stream are done to ensure that a face is visible. Our solution can recognize when the user has positioned themselves in front of the camera and automatically capture face data; it can provide feedback where the user is not suitably positioned (this is known as a "quality check"). Additional video data/meta-data is captured to assist with liveness (physical presence) and injection attack detection.

A facial image is then submitted to the TrustX service to be processed (i.e., to verify quality, check liveness and match to the document) and if for some reason it cannot be processed, the end-user can be asked to re-try with a configurable limit of attempts in the case of failures other than quality issues.

A limited number of retries is allowed.

5.2.2 Physical Document Capture

The Service can accept passports and national identity cards from a range of countries. In some contexts, other official photo ID documents may also be accepted, e.g., residence permit cards from EU countries, driving licenses and. The RP determines which document types and from which countries can be accepted and the Service is then configured as such. For this Service, the document type must be included in the document library (for the hybrid UC) and/or the country signing certificates are available (for the automated UC). In some cases, we can work with RPs to source the required additional information in order to extend the accepted documents.

Capture ID document via video: using the rear camera of the device to capture an image of the ID document.

We typically recommend asking the end-user to say which document they will capture beforehand. This allows the system to prompt with instructions that are more specific to the kind of document (passport, driving license or ID card).

During document capture, the solution can process the video stream and recognize when a document has been correctly positioned under the camera and automatically capture a suitable image.

A video of the document can be captured. A single primary document image from the video stream is also captured. The data is then submitted to the server to be processed (i.e., to verify quality, identify/confirm the document type, extract the photo from the document,

OCR extraction of identity attributes and document checks) and if for some reason it cannot be processed, the end-user can be asked to re-try in the case of failure. A limited number of retries is allowed.

Capture other documents (optional): either upload a PDF or image OR use the rear camera of the device to capture an image of other documents, e.g., as proof of additional attributes such as address. TrustX allows RPs to define the category of documents to request from your end-users as evidence of extended aspects of identity. The documents/image(s) are then submitted to the TrustX service to be processed.

5.2.3 Digital/Electronic Document Capture (NFC)

The Service can accept national passports and identity cards that comply with the ICAO 9303 (as referenced in EU Regulation 2019/1157) and where country signing certificates are available. The RP determines which document types and from which countries can be accepted and the Service is then configured as such.

Capture ePassport details via NFC: The system uses the data from the Machine-Readable Zone (MRZ) of the passport to extract the data needed to access the data on the ePassport chip and the photograph from the passport data page (i.e., from the printed document).

The app then prompts the end-user to position their phone over the document and provides guidance on how to position the document and capture device. The SDK will automatically begin to capture the document when placed correctly and show the user the progress in capturing it. The SDK will perform the necessary access control mechanisms and any other interactions required during capture to support validation during this process.

If capture is not fully completed, the user will be asked to retry. A limited number of retries is allowed.

The data captured is then submitted to the TrustX service to be processed.

5.2.4 Completion of Capture

Once all identity verification data has been captured, validation is completed in order to reach a decision on the result of the identity verification (see following sub-section). This is orchestrated by the xProof/TrustX Server.

Where the process is completed with failed status, the Trust Web/SDK UI will typically show that the identity proofing process has been completed but will not show any further information to the user. The Relying Party can get data on the reason(s) for failure and determine appropriate next steps, including what details to inform the user and what further options for identity proofing to offer them, if applicable.

5.3 Attribute and evidence validation

The data from the identity document and any additional data (such as capture meta-data) is transferred to the TrustX server environment, which is controlled by Daon. API authentication and Transport Layer Security (TLS) are used as measures to ensure authenticity, integrity, and confidentiality of the data exchanged with the server.

A series of validation steps are included in the Process executed by TrustX.

Validation may take place as data is submitted (e.g., face liveness checks can happen as soon as the face data is captured) or at the end of the process, when all data is available.

5.3.1 Automated Validation – Digital/Electronic Documents

Automated document validation is executed using NFC verification services within the TrustX server. These validate the document and the attributes gathered from it.

- The digital identity document is first validated using Passive Authentication, to check that the issuer's digital signature on the document is correct.
- Country Signing Certificates are used to ensure that the document has been signed by the document issuer. These are maintained within the TrustX service and can be sourced and maintained by Daon or our Customer.
- Certificate Revocation Lists will be checked if available.
- If supported by the document, Active Authentication is also validated to prevent the use of a cloned document. A challenge is generated by the TrustX service and processed by the chip. Active Authentication can also be required, with documents rejected if not supported.
- See Section 5.3.4 for additional injection attack measures.
- If an online status service to confirm the document's validity exists and is practically available, the verification process must be configured to use this service to verify that the document is currently valid. Where these services are available, they are to be included as a Cloud Function in the TrustX process definition with conditional logic to ensure that they are executed for the relevant document types.

The document will be rejected and the identity proofing marked failed if the country signing certificate is not available or if the signature from the document cannot be validated.

The personal data and photo are extracted from chip when all authentication is completed successfully.

5.3.2 Automated Validation – Physical Documents

For physical documents, the following automated validation takes place within the TrustX service.

- For all documents, including ePassports, ID cards and driving licenses, checks include:
  - Document type recognition
  - Verification that the document is an accepted type
  - Scanning of front and back images and OCR/extracting all the information including photo of the holder
  - Verification that the document is valid (within its expiry date and, if appropriate, not older than allowed)
  - Cross-verification of data from available sources - visual zone, machine readable/OCR zone, barcode, RFID chip

    - Screen Detection: Detect images of documents that have been captured from a screen rather than from a live capture
    - Copy Detection: Detect images of documents that have been captured from a copy of the document rather than from the original physical document
    - Photo Substitution Detection: Detect signs of manipulation of the document around the photo.
- For documents with an MRZ (all passports and most ID cards), verification of MRZ format and check digits
- For documents with a PDF417 barcode, verification of barcode format and data (option)
- For some documents, automated verification of data formats and visual security features is also available. In this case, additional security features are assessed with manual validation.
- If an online status service to confirm the document's validity exists and is practically available, the verification process must be configured to use this service to verify that the document is currently valid. Where these services are available, they are to be included as a Cloud Function in the TrustX process definition with conditional logic to ensure that they are executed for the relevant document types.

OCR is used to extract attributes from the MRZ and visual zone (VIZ). Data from both of these sources is made available to the RP. This allows attributes to be provided in both the normalised format used in MRZ as well as the richer format printed on the VIZ which may for example include accents and non-latin characters.

For comparison of names, we use the MRZ as the basis for comparison and normalise the name(s) on the visual zone based on the rules for MRZ encoding specified in ICAO Document 9303. This addresses how accents and non-latin characters not used in the MRZ are handled. Other changes such as shortening of names may also occur during encoding in the MRZ by the document issuer. We incorporate logic for automating these checks which takes into account common approaches to this. We work with our customers to adapt the automation strategy in this area, e.g., the RP may choose not to automatically reject a document that fails the automated test and have it checked during manual review, in order to maximise acceptance rates (while also still rejecting documents with inconsistent data in the MRZ and VIZ). RPs may also ask for additional matching rules to be incorporated that may be appropriate for the types of documents that their end-users present.

5.3.3 Manual Validation

For physical documents, the identity verification process is extended to include a Review. The review is focused on verifying that the document is not counterfeited or falsified/modified.

The data is queued for review by our EU-based trained review team. Reviewers have access to a web-based tool with images and video of the document. They also have access to authoritative reference sources for the document format and security features including PRADO and others.

Manual reviewers have received training on document assessment, which was created by ID document experts, in addition to training on how to use the tools provided and on data

protection. Training and procedures are in place and are updated as needed to incorporate additional information on ID documents.

For the purpose of this document, the review will include at least (in addition to prior automated checks):

- Verification of the quality of the capture
- Examination for evidence that the document was not captured live and for tampering
- Verification of at least three security features

The reviewer will record a decision (pass/fail) and may record additional information.

5.3.4 Device Signals

The identity proofing process can capture and assess Device Signals as a risk mitigation measure. These include user device risk scoring and may include a check against a known fraud device service. It helps to detects devices that may be compromised or that were used in prior fraud, which may result in fraudulent data presentation (e.g., injection attacks).

5.4 Binding to applicant

Binding is via automated biometrics verification.

5.4.1 Face Collection

See Face Capture section above.

The TrustX UI transmits the relevant parts of the video stream is transmitted to the TrustX server. A high quality frame containing the end-user's face is extracted from the video stream for matching.

Immediately after collection, initial checks are performed:

- Face Quality Check: ensure that a suitable face image is available for attack detection and matching
- Liveness Check: a Liveness Detection/Presentation Attack Detection check is run. This uses a TrustX liveness detection service with an algorithm that has been tested by an accredited independent lab, iBeta, in accordance with ISO/IEC 30107. See https://www.ibeta.com/wp-content/uploads/2022/07/20220719-Daon-PAD-Level-2-Confirmation-Letter.pdf The results of the testing show an APCER (attack presentation classification error rate) as defined by ISO/IEC 30107-3 of 0% and BPCER (bona fide presentation classification error rate) of 0%, representing the level of industry best practice assessed by iBeta at the time of the test. This module will undergo testing under ISO/IEC 19989-3 by an accredited lab before the end of 2026 and then repeated every second year.
- Injection Attack Detection Check: this service incorporates multiple checks to detection injections and also includes a specific module for detection of artificially generated faces (deep fakes - these may be detected either as an injection or using this specific module). This module will undergo testing under CEN TS 18099 at level

High by an accredited lab before the end of 2026 and then repeated every second year.

See also Section 5.3.4 for other measures to prevent injection attacks.

The algorithms used are updated with appropriate regularity by Daon to address changes in the threat landscape and available technology.

The target operational APCER is 0.01% with an expected corresponding BPCER of <5%. As it is unlikely to be possible to verify APCER in a live system, the algorithm is re-tested on each update by Daon's Research team and where necessary a new threshold is recommended.

5.4.2 Binding to applicant (Automated Face Biometrics)

Binding to the applicant/end-user is by automated face biometric comparison of the live photo ("selfie") and the photo extracted from either the physical document or digital document's chip (or both). The comparison uses the face biometric matching service of TrustX.

Only selfie image, document reading and capture of other necessary meta-data is done on the end-user's device. For binding, the data are captured, then transferred to the TrustX server environment, which is controlled by Daon, for biometric transformation (processing), comparison (matching), data storage and decision.

Matching is only done after liveness and injection attack detection is completed successfully.

The comparison uses the face biometric matching microservice of TrustX using at least DaonFaceV6.

The DaonFace algorithm has been assessed by NIST in the FRTE 1:1 (formerly known as Face Recognition Vendor Test). Test results for the biometric face recognition show a FAR (false acceptance rate) and FRR (false rejection rate) at the level of industry best practice. See https://face.nist.gov/frte/reportcards/11/daon_000.html and https://face.nist.gov/frte/reportcards/11/daon_001.html.

The biometric algorithms and technologies are updated to cope with changes in the threats and risk situation and are systematically tested against reference datasets. Daon's tests are conducted using the relevant approach from ISO/IEC 19795. These tests are repeated before release of each new version of the face matching component containing the face biometric algorithm, i.e., before any changes are introduced in the product/service.

Biometric verification is based on a threshold which is configured in the system based on a False Accept Rate, for which Daon's Research team maintains a corresponding False Reject Rate.

The target operational FMR (False Match/Accept Rate) is 0.001% with a corresponding FNMR (False Non Match/False Reject Rate) of <1% depending on the document types that are used. As it is unlikely to be possible to verify FAR in a live system, the algorithm is re-tested on each update by Daon's Research team and where necessary a new threshold is recommended.

5.5 Issuing of proof

Completion: On completion of processing, the TrustX UI will hand back to the RP app or web site, which can take back control, receive the results via API calls or webhooks and determine the next step in the user's journey.

The RP's system can then use an access controlled, secured API to retrieve the result, attributes and data about the identity verification process including evidence used and additional metadata. Data is returned in JSON format.

An OIDC (OIDC4IA) interface is also available to get basic results.

This data is also available for authorised users to review in the TrustX Back Office UI during the period of time that the evidence is configured to be retained.

RPs are responsible for only using the data that is needed.

RPs are responsible for storing the data that is required to meet the regulations that apply to them. Personal data and detailed process data is automatically removed from TrustX after no more than 90 days.

6 Use Cases for Natural Person ID Proofing

The service provides identity proofing of natural persons in unattended remote scenarios using an identity document.

6.1 Use Case 1: Unattended Remote Automated Operation

This corresponds to Section 9.2.3.4 of ETSI TS 119 461.

This approach is based on the remote presence of the applicant with automated online communication, and validation of evidence is automated using a digital identity document, and binding to applicant is by automated face biometrics and the following requirements apply.

This approach is only available for iOS or Android mobile application clients using an SDK incorporating Daon NFC capture features.

This approach uses a digital identity document as evidence, i.e., an electronic passport or identity card, to be read using NFC with validation of the digital security features by the service. Identity data and biometric data for binding is read from the electronic chip in the document (after reading the necessary details from the physical document to unlock the details in the chip.) Any MRTD such as an ePassport or eID card that uses the relevant parts of the ICAO 9303 standard and where the issuing authority makes the relevant certificates available for Daon or the RP to access can be accepted. The RP can determine which specific set of documents is allowed to be accepted.

The Trust SDK is used to capture the necessary evidence, i.e., a live face photo (selfie), an image or other data from the physical document necessary for unlocking the chip and reading via NFC the digital document (chip). The Trust SDK guides the user through these steps.

The evidence is evaluated via Automated and Manual means as described in this document.

Binding to the applicant is by automated face biometric comparison of the live photo (“selfie”) and the photo extracted from the document.

This approach is available for iOS or Android mobile applications.

6.2 Use Case 2: Unattended Remote Hybrid Manual and Automated Operation

This corresponds to Section 9.2.3.3 of ETSI TS 119 461.

This approach uses a physical identity document as evidence, e.g., a passport, identity or residence card or photo driving license. Identity data and biometric data for binding is read from the surface of the document. This approach can be used for Photo ID documents that are in Daon’s library; the RP can determine which specific set of documents is allowed to be accepted.

The Trust SDK or Trust Web is used to capture the necessary evidence, i.e., a live face (selfie) and the physical document. The Trust SDK guides the user through these steps.

The evidence is evaluated via Automated and Manual means as described in this document.

Binding to the applicant is by automated face biometric comparison of the live photo (“selfie”) and the photo extracted from the document.

This approach is available for iOS or Android mobile applications or in a web browser.