Trust Service Practice Statement (TSPS)

& Identity Proofing Service Practice Statement (IPSPS)

for the

Identity Verification Service

Nets Passport Reader

Version 1.1
Document date: 04/01/2022
Effective date: 28/01/2022

Document Change History

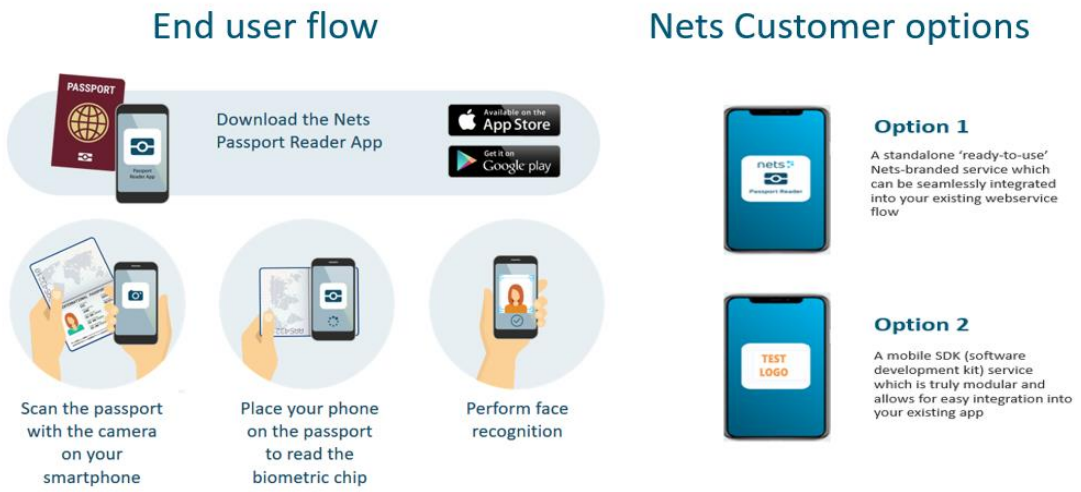
Date:	Change Description:	Version:	Author:
04.01.2022	Document creation/initial draft version	v. 1	Nets Product Management
14.01.2022	Minor changes/management review/1st version approval	v. 1.1	Nets Management

Content

1. Introduction

This document is the Trust Service Practice Statement (TSPS) of the Nets Passport Reader (from now on, Passport Reader) identity verification service. It is not a full Certification Practice Statement (CPS) because Passport Reader only cover the aspects of identity proofing for the issuance of qualified certificates and do not offer other certification services.

The Passport Reader service scans and reads machine-readable identity (ID) documents (passports, driving licenses, and residence cards) with an NFC enabled mobile phone; ensures that the person carrying out the process is the rightful owner of the document using biometrics; ensures that the information is transmitted in a secure manner. The attributes collected uniquely identify the applicant as a natural person in the identity proofing context. Please refer to the below illustration.



The purpose of this document is to serve as a base for compliance with eIDAS, the 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 and the ETSI standards ETSI TS 119 461 [1], ETSI EN 319 401, ETSI EN 319 411-2.

The mentioned eIDAS Regulation does not define identity proofing as a trust service on its own. In the present document, identity proofing is defined as a a subset of the Trust Service Component "Registration Service" as defined in the ETSI-standard ETSI EN 319411-2. The identity proofing service component can be an integral part of the Trust Service Provider's (TSP) service provisioning, but the service component can also be the task of a specialized Identity Proofing Service Provider (IPSP) acting as a subcontractor to the TSP.

For Passport Reader, the applicant is a natural person, and the identity proofing process is fully remote and automated.

1.1 Overview

Identity proofing is the process of verifying with the required degree of certainty that the identity of an applicant is correct. Nets has developed a remote identification service, the Passport Reader, for identity proofing of trust service subjects as well as for other purposes such as issuing of electronic identity, onboarding and know-your customers (KYC) processes e.g. for financial services and authentication-based signing.

In particular, Nets verifies the identity of natural persons amongst other methods in accordance with eIDAS, Article 24, paragraph 1 d) by using "other identification methods" which provide equivalent assurance in terms of reliability to physical presence. Conformance with eIDAS at assurance

level "High" allows certification service providers to use these services for identity verification in their processes of issuing qualified certificates.

In addition, in collaboration with Qualified Trust Service Providers (QTSPs) Nets enables individual users of the contracted partners to electronically sign legally binding contracts using qualified electronic signatures according to the eIDAS regulation.

1.2 Scope: Identity Proofing Service Policy (IPSP)

The present document (the 'Nets Trust Service Practice Statement') describes the applied practices employed in delivering the Passport Reader service and in meeting the applicable requirements for identity proofing.

More specifically, the practices adopted for fulling the general policy requirements given in ETSI TS 119 461 [1] and describes the policy and security requirements adopted for implementing an 'Identity Proofing Service Component' supporting identity proofing in European and other regulatory framework. This standard has been developed taking into account the following aspects:

- It is based on ETSI EN 319 401 which contains common requirements for all trust service providers (TSP) implementing best practices for use of selected means and applicable technologies that can be used for identity proofing.
- It includes specific requirements for the verification of the identity of natural persons specifying how identity proofing processes can be constructed by combining means to achieve the basic desired outcome of the identity proofing process.

The security requirements of ETSI TS 119 461 [1] cover the most common risks, which fall into two main categories: an applicant falsely claims an identity using forged means of evidence (forged evidence) and an applicant uses valid means of evidence associated with another person (impersonation). Potential operational risks and social engineering risks are also taken into account.

To summarize:
- ETSI TR 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 for the identification method: "Nets Passport Reader", providing unattended remote identity proofing, where the communication with the applicant is automated, specifically: Automated operation.

- (partial) certification of the Nets Passport Reader service provision according to ETSI EN 319 411-2 (PKI component service: Registration Service).

- confirmation of equivalent assurance to physical presence, pursuant to Regulation (EU) 910/2014 (eIDAS) art. 24.1 sub d, of the identification method: "Nets Passport Reader", based on assessment against against ETSI TS 119 461 [1] applicable requirements.

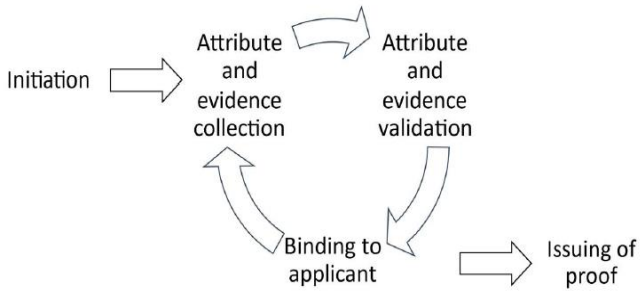
- ETSI TS 119 461 [1] applicable requirements are additionally cross-referenced against BITS[1] - Requirements for solutions for Secure digital verification of identity (2020-10) for the Norwegian market.

[1] Bits AS is the financial infrastructure company of the bank and finance industry in Norway.

1.3 Identity Proofing process

Passport Reader conforms to the following identity proofing service requirements as specified in ETSI TS 119 461 [1], Chapter 8:

- 8.1 (initiation);
- 8.2.1 (attribute and evidence collection general requirements);
- 8.3.1 (attribute and evidence validation general requirements);
- 8.4.1 (binding to applicant general requirements); and
- 8.5 (issuing of proof).



1.4 Identity Proofing context

The identity proofing context is the set of external framing conditions that an identity proofing process is subject to and that can impose requirements and restrictions on identity proofing. A core element of the identity proofing context is the regulatory requirements imposed on identity proofing for the defined purpose by the applicable legislation. Nets Customers are responsible for ensuring compliance with local regulations according to their intended identity proofing context.

Passport Reader identity proofing context will vary between purposes of identity proofing and between countries in relation to:

- The required level of assurance (e.g eIDAS High or Substantial)
- The identity attributes to collect, meaning attributes that are mandatory, prohibited, or optional (e.g in Norway, the collection of a national identity number can be mandatory for the identity proofing context, while other countries do not use such numbers).
- The country specific national legislation and government policies on applicable technologies (e.g. certain identity documents like national identity cards from selected countries can be restricted; in some countries, validation of identity attributes against a national population register can be mandatory, while other countries do not have such registers; the means to use for attribute and evidence validation and for binding to applicant, meaning that certain process steps can be mandated or prohibited; in some countries, physical presence can be mandated for certain purposes of identity proofing, or remote identity proofing can be restricted to allow only specific use cases).

When it comes to attribute and evidence collection and validation threats, the following best practices applies to Passport Reader:

- Pending on the identity proofing context, only passports and national ID cards are accepted since the attributes collected in those uniquely identify the person.
- Protection against stolen or revoked identity documents is ensured during the binding to the applicant through biometric; access to authoritative sources of information on document, e.g. TOVE register in Norway/Interpol register internationally, may be supported through Nets but is left at the discretion of Nets Customer.

2. Policy administration

2.1 Organization administering the document

Nets A.S (Nets) is a payments company specializing in digital payment. The company operates in two main business segments, merchants and banks, and provide a broad range of services within payment cards, bank account services, and payment solutions.

This document is periodically reviewed and updated in line with Nets Policy. Approval and discussions of the current scope is performed in management reviews, similarly to ISO maintenance and re-certification procedures.

2.2 Contact person

Nets Branch Norway
Haavard Martinsensvei 54
0978 Oslo
Tel: +47 22 89 89 89
Orgnr: 996 345 734
esec-vas-no@nets.eu
Nets is part of Nexi Group.

2.3 Time or frequency of publication

The latest version of this TSPS approved by management is available for download on Nets website.

2.4 Terms and Conditions

This TSPS becomes effective from the date of publication on the website.
Amendments become effective upon publication. This TSPS remains in force until it is replaced by a new version.

Applicable terms and conditions towards Nets Customer for the provision of the Passport Reader service (including e.g. termination, force majeure, dispute resolution, governing law) are regulated in the Nets Passport Reader Service Agreement.

Applicable terms and conditions towards the End user are regulated in the Nets Passport Reader Privacy Notice.

3 Definition of Terms and Abbreviations

3.1 Terms

Term:	Definition:
applicant	person (legal or natural) whose identity is to be proven
(identity) attribute	quality or characteristic ascribed to a person.
Baseline LoA	Level of Assurance (LoA) according to eIDAS Regulation (EU) 910/2014 which distinguished between High, Substantial and Low level.

binding to applicant	part of an identity proofing process that verifies that the applicant is the person identified by the presented evidence.
digital identity document	identity document that is issued in a machine-processable form though NFC (Near Field Communication) enabled technology, that is digitally signed by the issuer, and that is in purely digital form. A digital identity document can be contained in a physical identity document, e.g. an eMRTD contained n a passport or national identity card.
end user	Nets Customer's customer, signatory or other physical person with which Nets Customer has a contractual relationship regarding the Nets Passport Reader services.
(identity) evidence	information or documentation provided by the applicant or obtained from other sources, trusted to prove that claimed identity attributes are correct.
False Acceptance Rate (FAR)	proportion of verification transactions with false biometric claims erroneously accepted according to ISO/IEC 19795-1 [i.17].
False Rejection Rate (FRR)	proportion of verification transactions with true biometric claims erroneously rejected according to ISO/IEC 19795-1 [i.17].
identity	attribute or set of attributes that uniquely identify a person within a given context.
identity document	physical or digital document issued by an authoritative source and attesting to the applicant's identity.
identity proofing context	external requirements affecting the identity proofing process, given by the purpose of the identity proofing, the related regulatory requirements, and the resulting restrictions on the selection of attributes and evidence and on the identity proofing process itself.
identity proofing (process)	process by which the identity of an applicant is verified by the use of evidence attesting to the required identity attributes.
identity proofing policy	set of rules that indicates the applicability of an identity proofing service to a particular community and/or class of application with common security requirements.
Identity proofing practice service statement	Alternative name given in ETSI 119 461 [1], clause 6 for the trust service practice statement defined in ETSI EN 319 401 [1], clause 6.1
Identity proofing service provider	Subcontractor of the trust service provider.
liveness detection	measurement and analysis of anatomical characteristics or involuntary or voluntary reactions, to determine if a biometric sample is being captured from a living subject present at the point of capture according to ISO/IEC 30107-1 [i.16].
Nets Customer	the legal entity/Company subscribing to the Nets Passport Reader
Nets Passport Reader (Service)	the service provided by Nets which is in scope with this trust service practice statement.
Nets Passport Reader App	the mobile software application(s) as developed by Nets and delivered to Nets Customer.

Nets Passport Reader SDK	Passport Reader Software Development Kit (SDK) provided by Nets to Nets Customer to develop its own application(s).
Nets Passport Reader Privacy Notice	In-app terms and conditions which require consent from the End user.
Nets Security Framework (NSF)	Nets Group primary information security framework. This framework is implemented in all parts of the organization and follows the concepts provided in ISO 27001.
Nets Passport Reader Service Agreement	Nets Customer signed order confirmation for the provision of the Nets Passport Reader Service.
Nets Signing & Identification (SIS) Services	Nets product portfolio which includes Nets E-Ident broker service and Passport Reader.
physical identity document	identity document issued in physical and human-readable form.
presentation attack	presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system according to ISO/IEC 30107-1 [i.16].
Presentation Attack Detection (PAD)	automated determination of a presentation attack according to ISO/IEC 30107-1 [i.16].
qualified trust service provider	trust service provider listed in an EU Member State's Trusted List according to eIDAS regulation.
remote identity proofing	identity proofing process where the applicant is physically distant from the location of the identity proofing.
subject	legal or natural person that is enrolled to a trust service
subcontractor	Third-parties that support Nets during delivery of Nets Passport Reader
trust service	electronic service for: • creation, verification, and validation of digital signatures and related certificates; • creation, verification, and validation of time-stamps and related certificates;
trust service component	one part of the overall service of a TSP according to ETSI EN 319 403-1 [i.6].
trust service practice statement	statement of the practices that a TSP employs in providing a trust service.
trust service provider	entity which provides one or more trust services.
validation	part of an identity proofing process that determines whether or not attributes are validated by the presented evidence and whether or not the evidence is genuine, authoritative, and valid.

3.2 Abbreviations

DG data group
eID electronic Identification
eMRTD electronic Machine Readable Travel Document
FAR False Acceptance Rate
FRR False Rejection Rate
FML Face Match Level
GDPR General Data Protection Regulation
ICAO Internation Civil Aviation Organization
IPSP Identity Proofing Service Policy
ITIL Information Technology Infrastructure Library
LoA Level of Assurance
MRZ Machine Readable Zone
NFC Near Field Communication
NSF Nets Security Framework
PAD Presentation Attack Detection
PET Privacy Enhancing Technology
QTSP Qualified Trust Service Provider
SIS (Nets) Signing and Identification Services
TLS Transport Layer Security
TSP Trust Service Provider
TSPS Trust Service Practice Statement

ETSI EN 319 401 (PKI component service: Registration Service)

4 Risk Assessment

Nets' risk management follows the ISO 31000 standard for risk management. This includes the three lines of defence as a governance model to enhance the management of risk and internal controls. The model is used to structure roles, responsibility and accountability for decision making concerning risk and controls and to ensure a good relationship and effective communication between the three lines. The three lines of defence model is described in the Nets Risk Management Policy. The risk management process ensures a risk-based approach in all parts of the organization and enables the Management System to be based on factors identified as relevant for its success.

Based on this, Nets performs annual risk assessments as well as ad-hoc assessments based on identified level of risk. The risk assessments are performed per Nets service component, including e.g. SIS (Signing & Identification) services and Passport Reader, covering IT and business risks.

For Passport Reader, Nets performs regular internal assessments focused on identified high-risk level topics in scope with audit assessment and a Business Impact Analysis (BIA).

5 IT Risk management

IT risk management is part of the group-level operational risk management practices as required by Nets Risk Management Policy and hence is part of the overall group-level internal risk and control framework.

The IT risk process also includes a process for IT Service risk assessments covering all critical systems. The assessments are completed on a yearly basis or in the case of significant changes to the systems or infrastructure. The IT Service risk assessment process is based on ISO 31000 and the ISF IRAM2 framework and covers both overall IT service risks such as people, architecture, and compliance, as well as a separate information security assessment using a tailored threat catalogue, vulnerabilities and identified assets. Identified risks are mitigated in agreement with IT Service Owners and Business Owners.

6 Policies and Practices

All parts of Nets Group follow Nets Security Framework (NSF) as their primary information security framework. This framework is implemented in all parts of the organization and follows the concepts provided in ISO 27001. The scope for ISO certification is assessed, evaluated and maintained as part of the yearly Management review.

NSF covers processes, organizational units, locations and IT infrastructure for providing Nets trust services, and forms the basis for the actual Nets's ISO-27001 (information security) & ISO-9001 (quality management system) certifications issued by Nemko AS in 2020 and specifically covering the Passport Reader service.

7 Internal Organisation

The practices, which Nets operates under are non-discriminatory and revolve around segregation of duties. Nets personnel have the necessary education, training, technical knowledge and experience to provide Nets SIS (Signing & Identification) services. Segregation of duties and Identity and Access Management are done accordingly to NSF.

Nets financial and organizational reliability can be attested through publicly available annual reports. Service agreements and internal policies for vendor management, procurement, outsourcing and contractual relationships are in place.

- Passport Reader Subcontractors: Innovalor/ReadID is used for document scanning and offers own certification as eIDAS module for assurance level High issued by TUV Austria; while the comparison of the high-resolution image from the ID-document with the captured biometric sample is performed with a local installation within Nets infrastructure (Norway).
- Passports Reader applicants/data subject policy: the Nets GDPR web portal is used https://www.nets.eu/GDPR/dsr/Pages/request.aspx to exercise own rights.

Passport Reader qualifies for eIDAS compliant identity proofing and is certified by a Conformity Assessment Body, BSI (The British Standards Institution, BSI Group The Netherlands B.V.) Conformity certifications against eIDAS Regulation 910/2014, ETSI EN 319411-2 (Trust Service Component: Registration Service), including ETSI TS 119 461 on Identity Proofing of Trust Service Subjects and BITS are publicly available at: BSI eCertificate Service - Validate eCertificate (bsigroup.com)

8 Human Resource Security

Nets HR Onboarding Policy ensures the employment of personnel and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications.
Nets Security Academy offers adequate training for security and personal data protection rules as appropriate for the offered services and job function.

Trusted Roles for the Passport Reader service (such as security officer, system administrator/operator) are approved by management and issued to qualified personnel that has access to data center facilities and that can perform system/application configurations.

9 Asset Management

Nets manages its assets according to Nets Security Standard for Asset Management. This covers software and hardware asset management including data centre IT assets and end-user computing IT assets. A complete inventory of all key assets is maintained. Each asset is appropriately classified and protected according to the conducted risk assessment. Passport Reader is not classified as a "critical service".

10 Access Control

Nets Access Control Policy is part of NSF. The principle of least privilege is applied, which means that users only get access to parts/areas/systems they need to fulfil their tasks. Users are uniquely identified and there is a formal process of registration and deregistration with dual control. Users are also accountable for their actions.

For Passport Reader, the servers are not accessible from outside the data center facilities. Only monitoring information is allowed out of the room. There is no access to the internet or the corporate network from inside the data center facilities. Physical access logs are retained and reviewed monthly. Logical access logs are retained on a log server held within the data center facilities and are not removed.

11 Cryptographic Controls

To ensure consistent and secure management of cryptographic controls, these are always selected and used in accordance with Nets Data Protection and Integrity Guideline.

For Passport Reader communication protocol TLS is used and data is encrypted during transit. Between frontend and backendnd Nets Customer: the mobile app connects to the backend. It will send back parameters including a key to encrypt data and a dedicated URL as a destination (backend).

12 Physical and environmental security

The physical and environmental security is in accordance with NSF. Nets has an ISO 27001 certification and employs security controls in accordance with that standard. This means that proper entry controls, protection against external and environmental threats, cabling security, and maintenance of equipment are in place.

Passport Reader environment runs in data centers, in an active-active set-up, across multiple locations and is subject to strict access and access requirements (four eyes principle) - also including other physical measures such as 24/h security, surveillance, alarms, access cards with code.

13 Operation Security

Nets has implemented the ITIL-processes, including change Management. This ensures that operating procedures are thoroughly documented and kept up-to-date. Change management is strictly controlled and subject to board-approval. Development, test, and operational environments have been separated.

For Passport Reader, Change Management procedures are documented and changes are registered in the IT operations tool ServiceNow (note that larger and complicated changes are subject to Change Advisory Board-approval). Patches are implemented in a stages approach: test, staging, pre-production, production. Front-end servers are maintained by other teams (outside of security room). There is a monthly patch routine for these systems. Patches are on front-end servers are deployed with the tool Roadrunner.

14 Network Security

Nets infrastructure is segmented into security zones protected by multiple firewalls based on the functional, logical and physical relationship between the systems and services. The SIS (Signing & Identification) service of which the Passport Reader environment is part of, is e.g. running on a separate subnetwork for authorized personnel. Penetration tests are performed in different variants and are available upon Nets Customer reqest.

15 Incident Management

Nets Incident Management follows the ITIL-processes and includes any event which disrupts, or which could disrupt a service.
The main purpose of incident management is to restore normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the agreed upon levels of service quality are maintained.

For Passport Reader, this is regulated in the Nets Passport Reader Service Agreement. Any critical eIDAS security breach will be notified to selected Nets Customer (e.g. QTSP) for further notification to the relevant national supervisory body (e.g. NKOM in Norway) as soon as possible, and at least within 24 hours. Relevant information will also be submitted to relying parties. Any critical vulnerability not previously addressed, will be processed within a period of 48 hours after its identification.

16 Business Continuity

Nets has developed a business continuity plan to make disaster recovery possible. Multiple scenarios have been identified, some of which have been simulated during training sessions. Mitigations for each scenario are in place.

17 Termination

Nets has developed a termination plan to be executed if a decision is made to terminate Passport Reader service agreement. Termination procedures include

- notification of affected entities; and
- where applicable, transferring the TSP's obligations to other parties.

ETSI TS 119 461 (Chapter 8/Chapter 9, applicable requirements)

18. Identity proofing service requirements

18.1 Initiation

The Passport Reader is part of the Nets E-Ident identity broker service as one of several supported eIDs for remote identity proofing.

E-Ident has been operational across the Nordic countries since 2005. It provides the applicant/subject with an activation code to safely establish a unique authentication session with Passport Reader.

The applicant/subject is presented with a privacy notice prior to each identification. The subject has to read and accept its term. This includes a full overview of the captured/processed data, data storage, deletion, retention policy, applicable law incl. GDPR. Please refer to: eIDs (nets.eu)

18.2 Attribute and evidence collection

Passport Reader can return all or a subset of the data to Nets Customer. Each Nets Customer decide on what subset of data is needed according to their identity proofing context. Protected data (e.g. data read from the RFID-chip of a document) is not read according to Nets data minimisation policy.

Full list of attributes is available at: eIDs (nets.eu). Depending on the identity proofing context, unique identification can be in the form of an attribute such as a national identity number, or as one or more additional attributes that together with the full name provide unique identification. A

country attribute and serial number attribute are e.g. usually required to guarantee unique identity.

18.3 Attribute collection for natural person

NFC Technology is used to perform the reading and verification of the contactless chips in identity document that are ICAO Doc 9303 compliant, such as electronic passports, identity cards and residence cards. More specifically, the reading and interpretation of DG1 with the MRZ information, DG2 with the face image, D7 with written signature (if present), DG11 with additional personal information (if present) and DG12 with additional document information (if present).
Sample of data overall processed in Passport Reader:

- document type/number and expiration date
- issuing country
- picture
- full name of holder
- nationality
- date of birth
- gender
- optional data (including national identification number, if present)
- biometric/liveness data (collected during video selfie to prove that a person is a real human being)

18.4 Attribute and evidence validation

Optically the identity data is obtained from the Machine Readable Zone (MRZ) with Optical Character Recognition technology. The MRZ contains amongst others the family name, first name(s) and date of birth of a natural person. This set of attributes corresponds with the minimum data set as specified in eIDAS CIR 2015/1501 to uniquely identify a natural person.
Electronically the data is read from the chip via NFC technology. This information has been provided by the issuing country of the identity document, based on strict government identity verification and issuing processes. Besides providing very reliable personal information, another major advantage is that all data is electronically available. There is no manual input required, so there can be no mistakes in the data. If the country has opened DG11, Passport Reader is able to provide latin and non-latin characters. Since the data extracted may differ from its physical representation (e.g country specific/Norwegian character) and in order to prevent OCR mistakes, so called-checked digits and national characters are encoded as per ICAO DOC 9303 rules.

The validity of a document can be checked by looking at the expiration date of the identity document. The authenticity is checked by validating the digital signature of the data obtained from the chip via NFC against a list of country signing certificates. Several online databases of trustworthy Country Signing Certificates exist. For example, the French, German, Italian, Schengen, Swiss and Spanish CSCA master lists are published by each of these respective countries, specifying which certificates it considers trustworthy.

Protection against stolen or revoked identity documents is ensured during the binding to the applicant through biometric; access to authoritative sources of information on document, e.g. TOVE register in Norway/Interpol register, can be supported through Nets but is left at the discretion of Nets Customer.

18.5 Use of digital identity document as evidence

Passport Reader uses ReadID SDK to read the RFID chip of ICAO compliant documents (including physical passports and ID-cards), meaning that Nets is only using digital identity document properties.

Passport Reader only works with ICAO-compliant documents:
• passports and residence permits that meet the International Civil Aviation Organisation (ICAO) specifications for machine-readable travel documents,
• identity cards from an EU or European Economic Area (EEA) country that follow the Council Regulation (EC) No 2252/2004 standards, or,

• EU or EEA driving licences that follow the European Directive 2006/126/EC.
Note that all these identity documents are government issued with strict identity verification and issuing requirements and, as such, provide an authoritative source for identity proofing and verification.
A full list of available documents per country is available to Nets Customer upon request.

18.6 Validation of digital identity document

ReadID is used for document scanning and offers own certification as eIDAS module for assurance level High issued by TUV Austria. ReadID implements for ICAO 9303 compliant identity documents:
- the Basic Access Control security mechanism for getting access to the chip;
- the Passive Authentication security mechanism for verifying the authenticity of the read data;
- the Active Authentication security mechanism for verifying the authenticity of the chip (e.g. clone detection);
- the Chip Authentication (EAC-CA) security mechanism for clone detection; and
- the reading and interpretation of DG1 with the MRZ information, DG2 with the face image, D7 with written signature (if present),DG11 with additional personal information (if present) and DG12 with additional document information (if present)
- Password Authenticated Connection Establishment (PACE) which is a successor of BAC that uses more modern cryptography to provide an increased level of security. Note that EU mandates the implementation of PACE by its member states for newly issued travel documents. Passports that have support for PACE also support BAC to remain compatible with the ICAO 9303 standard, that requires documents that support PACE to also support the older BAC.

These security features only apply to the supported digital identity documents and do not extend to e.g attestation or additional authoritative sources.

Data in transit is encrypted using standard TLS protocol and data integrity features are in place to safeguard the integrity of stored data. All Passport Reader keys and licenses are stored in the security room. Each key is stored in duplicate at 2 different server locations. Each key is used for one operation/purpose only. Compromised, revoked, lost keys must be discarded immediately according to NSF. A new key must be generated to replace the compromised one. Keys that become invalid (corrupt, revoked or lost) can be immediately replace by new ones without interrupting the service.

18.7 Binding to applicant

A technical session identifier, also known as transaction identifier (TID), is defined to initiate a secure identity proofing process. A visual session identifier is displayed to the applicant in the form of QR code or activation code.

Besides the identity data and document verification functionality, Passport Reader also performs identity document holder verification. This proves that the applicant holding the identity document is indeed the rightful owner of the document.

Passport Reader compares the high-resolution image from the ID-document with the captured biometric sample. The face matching algorithm entails:
- Perspective distortion (zoomed and unzoomed video frames): ensures the user's face is three-dimensional.
- Liveness detection: measures up to 50 diverse attributes (light reflection, pupil dilation, blinking, subtle movements etc) to prevent face spoofing attacks.

A 3D shape-based face representation is created as a result of these techniques.

18.8 Capture of face image of the applicant

3D shape-based face representations are reverse engineered from 100+ video frames captured during the 2 second user video selfie, are always encrypted and aren't human viewable. They have been evaluated from 10.000+ devices from 170+ different countries and contain sessions from users with shadows, directional light, glare in glasses, non-neutral expressions, and low-light scenarios.

The technology in use achieved Level 1&2 PAD certifications in sanctioned third-party testing. More specifically, it was the first and only biometric to achieve a Level 1 & 2 rating in the NIST/NVLAP-certified iBeta Presentation Attack Detection (PAD) ISO 30107-3 Certification Test. It works with any camera of 0.3 - 20 megapixels and is much less dependent on the quality of the device than classic 2D engines. Resilience against other specific biometric attacks include extensive documentation against camera/video injection, passport morphing, alteration and anti-tampering.

Passport Reader mobile apps for iOS & Android are stateless/impersonal and only to be used for collection of raw data, which is sent encrypted using TLS 1.2 to Nets E-Ident service where the data is processed. Security features related to rooting, hi-jacking, jail in the mobile apps include root detection and certified pinning, manual code for repacking detection, app installation, debugging, logging fraud data and communication with Nets E-Ident backend.

18.9 Automated face biometrics

A confident score is returned for each identification as a Face Match Level. Passport Reader face recognition algorithm boasts a real-world false acceptance rate (FAR) of 1/950.000 FAR with less than a one-percent false rejection rate (FRR).

- Level 8 – 1/950.000 FAR
- Level 7 - 1/500.000 FAR
- Level 6 - 1/100.000 FAR*
- Level 5 - 1/10.000 FAR
- Level 4 - 1/1.000 FAR
- Level 3 - 1/500 FAR
- Level 2 - 1/250 FAR
- Level 1 - 1/100 FAR
- Level 0 - Non-match

*This level is the benchmark for eIDAS High configuration as a minimum, according to referenced industry best practices.

Also note that the Passport Reader matching algorithm is expected to improve over time based on continuous testing and refinement.

18.10 Issuing of proof

End user information will be returned in ID Token/SAML assertion to Nets Customers based on OIDC scope and identification parameters. A link to download images is added to the returned ID Token /SAML assertion. The images will be available for a short while after identification is complete.
In addition, the calling application can download a signed PDF with all end user info including picture. Example: PAdES.pdf

Pending on the identity proofing context, Passport Reader can support eIDAS High level of assurance (LoA). Configuration parameters are available at section 19.3 (Automated Operation) of this TSPS.

18.11 Evidence of the identity proofing process

All data read from the RFID chip (transaction data), including the high-resolution picture, is available as ID token and/or PDF/PAdES with a 90 days retention period. Liveness data collected during video selfie to prove that a person is a real human being is only valid for few minutes.

The data is stored in its original form, e.g. it is not decoded, decrypted or transcoded to a different format. The server, and database are both inside a secure computer environment in the security room. The database is integrity protected and only authorized personnel has access to read the database.

Data is deleted after 90 days, according to the defined retention policy. It is then up to Nets Customer to implement its own retention/archiving policy based on identity proofing context.
For logs and audit trail, image from video sequences can be additionally provided and processing of it is regulated in the app privacy policy/statement. All successful identifications are logged in statistics for invoicing purposes only.

Privacy Enhancing Technologies (PETs) are implemented across the solution.

19. Identity proofing use cases

Passport Reader conforms to the following use cases specified in ETSI TS 119 461 Chapter 8:
- 8.1 (initiation);
- 8.2.1 (attribute and evidence collection general requirements);
- 8.3.1 (attribute and evidence validation general requirements);
- 8.4.1 (binding to applicant general requirements); and
- 8.5 (issuing of proof).

Upon identity proofing context, country specific national legislation and government policies on applicable technology may pose requirement on the above use cases. E.g. in some countries, physical presence can be mandated for certain purposes of identity proofing, or remote identity proofing can be restricted to allow only specific use cases.

19.1 Identity proofing of natural person

Passport Reader does not require:
- physical presence
- online communication with a human registration officer

The identity proofing process is not hybrid, but fully digital and automated:
- remote presence of the applicant with unattended online communication

19.2 Remote identity proofing

The applicant receives automated guidance throughout the identity proofing process. Cross-platform accessibility ensures both desktop and in-app user guidance (assisted flow in terms of next steps). Passport Reader provides both in-app text aid to the end user (reason for failure/try again) while a list of error codes is sent to Nets Customer. A 2nd line support is provided to both the applicants and Nets Customer according to Nets standard contractual terms.

The identity verification process in Passport Reader app is user-friendly, intuitive and can be fully performed in under two minutes. The end user accepts Passport Reader app privacy policy, inputs a unique activation code, digitally scans the machine-readable zone (MRZ) of the selected document, verifies the chip through near-field communication (NFC) and performs face recognition.

Successful verification is dependent on meeting applicable requirements (e.g. usage of supported devices, environmental conditions) according to the identity proofing context (e.g. pass eIDAS High configuration parameters).

Once done with the in-app process, a live update on Nets Customer's controlled webpage informs the end user that the identity has been successfully verified or not. Nets Customer can flexibly decide on next steps:
- Failed authentication: please try again (or other - if fraud is detected)
- Successful authentication: congratulations message and next steps (e.g. KYC questionnaire/end-user self-assessment).

19.3 Automated operation

Passport Reader conforms to the following use cases specified in ETSI TS 119461 Chapter 8:
- 8.3.2 (validation of digital identity document);
- 8.4.3 (binding to applicant by automated face biometrics)

Passport Reader eIDAS High configuration is based upon:

- document scanning through NFC with no allowance for expired documents
- biometric facematch level: level 6 (1/100.000 FAR with <1% FRR) as a minimum