Digidentity

Identity Proofing @ Digidentity

Contexts & Methods

Title	Identity Proofing @ Digidentity - Contexts & Methods
Date	16 August 2023
Author	Sander Remmerswaal
Version	2023-v1
Location	https://www.digidentity.eu/en/documentation/
Classification	Public

Digidentity

Revisions

Version	Date	Author	Changes Made
2022-v1	31 January 2022	Sander Remmerswaal	Initial version
2023-v1	16 August 2023	Sander Remmerswaal	Updated contexts with UK DIATF, added verification methods and details, removed GOV.UK Verify

22 Aug 2023 19:53 +0200
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Digidentity

Contents

Digidentity

1 Introduction

Identity proofing is the process of verifying with the required degree of reliability that the claimed identity of an Applicant is correct.

Digidentity is a Qualified Trust Service Provider (QTSP) and performs identity proofing for several services. Each service is considered an identity proofing context. This document describes the evidence required, attributes collected, and validation and verification performed, for each identity proofing context.

Identity proofing policy and security requirements for trust service components providing identity proofing of trust service subjects are documented in ETSI TS 119 461. The scope of in ETSI TS 119 461 is identity proofing of applicants to be enrolled as Subscribers of a QTSP.

Digidentity carries out Identity proofing as an integral part of the trust service provisioning.

Digidentity conforms to the applicable requirements of ETSI TS 119 461 for the use cases:

- 9.2 Use cases for identity proofing of natural person
- 9.2.3 Use cases for unattended remote identity proofing
- 9.2.3.3 Use case for hybrid manual and automated operation
- 9.2.3.4 Use case for automated operation
- 9.3 Use case for identity proofing of legal person
- 9.4 Use case for identity proofing of natural person representing legal person

ETSI TS 119 461 aims to support identity proofing in European and other regulatory frameworks. Specifically, but not exclusively, ETSI TS 119 461 aims to support issuing of qualified certificates as defined in Regulation (EU) No 910/2014 (eIDAS) Article 24.1. The present document aims to meet the requirements of Article 24.1 as follows: 24.1 (a) by clause 9.2.1, 24.1 (b) by clause 9.2.4, 24.1 (c) by clause 9.2.5, 24.1 (d) by clauses 9.2.2 and/or 9.2.3 depending on the decision of the competent national authority.

Digidentity has documented identity proofing in an Identity Proofing Services Practice Statement (IPSPS) which is integrated in our Certificate Practice Statement (CPS). The CPS/IPSPS is available on our website at https://cps.digidentity-pki.com/.

Digidentity

2 Contexts

Digidentity performs identity proofing for identity proofing contexts:

[1] eIDAS Trust Services & eID
[2] Electronic Signatures
[3] eHerkenning
[4] UK Digital Identity & Attributes Trust Framework

2.1 eIDAS Trust Services & eID

Digidentity conforms to identity proofing requirements as defined in EU Regulation 910/2014 (eIDAS). The Level of Assurance of the service selected, determines the remote identity proofing method allowed:

- eIDAS High or Qualified: remote identity proofing using NFC, biometric validation and verification (liveness detection & face comparison).
- eIDAS Substantial or Advanced: remote identity proofing using NFC or video of identity document, biometric validation and verification (liveness detection & face comparison).

Sources to collect attributes for natural persons and natural persons representing legal persons:

[a] Identity documents (as defined in table "Accepted Identity Documents" in Appendix A)
[b] Selfies made by Applicant
[c] Company data from Chamber of Commerce

Sources to collect attributes for legal persons:

[a] Company data from Chamber of Commerce
[b] Company data from Value Added Tax (VAT) number (VIES check)
[c] Company data from a notary statement

Methods to verify identity evidence

[a] Biometric validation and verification (liveness detection & face comparison) of natural persons
[b] Photographic validation and verification of identity documents and personal data
[c] Cryptographic validation and verification of identity documents and personal data
[d] Legal person validation and verification for authorisations

Attributes of natural person used:	Attributes of legal person used:
[a] Full name of Applicant (Given Name and Surname)	[a] Company Name
[b] Date of Birth	[b] Company Address
[c] Gender	[c] Country of registration of company
[d] Identity Document number	[d] Company registration number at Chamber of Commerce
[e] Personal Identification Number	[e] Tax (VAT) number
[f] Date of issuance	[f] Full name of Legal Representative(s)
[g] Date of expiry	[g] Authorisation of Legal Representative(s)
[h] Issuing country	

All Digidentity services are based on eIDAS identity proofing.

2.2 Electronic Signatures

Digidentity eSignatures is our electronic signature solution based on certificates for Advanced Electronic Signature (AdES), Qualified Electronic Signatures (QES) and Qualified Electronic Seal. Identity proofing for eSignatures is based on the eIDAS context.

Digidentity uses remote identity proofing for eSignatures. The eSignature product selected, determines the remote identity proofing method allowed:

- eSignatures QES, eSignatures Seal: remote identity proofing using NFC, biometric validation and verification (liveness detection & face comparison)
- eSignatures Advanced: remote identity proofing using NFC or video of identity document, biometric validation and verification (liveness detection & face comparison).

Sources to collect attributes, verify identity evidence and attributes collected are equal to the eIDAS context.

eSignatures Seal is a product linked to a legal person (Qualified Seal for legal persons).

Digidentity links the natural person representing the legal person using the Trusted Register from the Chamber of Commerce if possible. The Chamber of Commerce retains information on legal representatives and authorisations. Digidentity uses information from the Chamber of Commerce not older than fifteen (15) days.

For legal persons that cannot be identified using Chamber of Commerce, Digidentity uses VAT validation to identify the legal person. Digidentity also support the use of a notary to state the existence of the legal person and the legal representatives of the legal person.

Requirements for digital signatures are defined and documented in EU Regulation 910/2014 (eIDAS).

2.3 eHerkenning

In the Netherlands, eHerkenning is the EU notified electronic identity scheme (eID) for legal persons. Representatives of a legal person use eHerkenning to log in at Government services and other business services. Identity proofing for eHerkenning is based on the eIDAS context.

Digidentity links the natural person representing the legal person using the Trusted Register from the Chamber of Commerce. A legal person in the Netherlands, is registered in the Chamber of Commerce. The Chamber of Commerce retains information on legal representatives and authorisations. Digidentity uses information from the Chamber of Commerce not older than fifteen (15) days.

Digidentity uses remote identity proofing to perform identity proofing for eHerkenning. The eHerkenning product selected, determines the remote identity proofing method allowed:

- eHerkenning Level 4: remote identity proofing using NFC, biometric validation and verification (liveness detection & face comparison), physical presence (for use in EU)
- eHerkenning Level 3: remote identity proofing using NFC or video of identity document, biometric validation and verification (liveness detection & face comparison)
- eHerkenning Level 2+: remote identity proofing using NFC or video of identity document

Physical presence of the Applicant or representative is mandatory for eHerkenning Level 4 outside of The Netherlands pending notification of Digidentity Remote Identity Proofing by the European Commission.

Sources to collect attributes, verify identity evidence and attributes collected are equal to the eIDAS context.

Rules for approving eHerkenning authorisations

eHerkenning defines the rules for approving eHerkenning authorisations. Each Level of Assurance has specific rules for approving authorisations depending on the authorisation of the Applicant or Legal or Authorised Representative.

eHerkenning 2+

Authorisations for eHerkenning Level 2+ require the approval(s) defined in the table below.

Authorisation in Chamber of Commerce	Condition
Legal representative with full authorisation, independent authorisation of power of attorney	N/A
Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	n.v.t.
Legal representative with joined authorisation	Minimum of two representatives with joined authorisation
Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Minimaal twee vertegenwoordigers met gezamenlijke bevoegdheid
Legal representative with limited authorisation or limited power of attorney	Minimum of two representatives with limited authorisation or limited power of attorney
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Minimaal twee vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht
Legal representative with limited authorisation or limited power of attorney related to eHerkenning	Explicit authorisation to approve eHerkenning must be in Chamber of Commerce
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

Digidentity

eHerkenning 3

Authorisations for eHerkenning Level 3 require the approval(s) defined in the table below.

Authorisation in Chamber of Commerce	Condition
Legal representative with full authorisation, independent authorisation of power of attorney	N/A
Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	n.v.t.
Legal representative with joined authorisation	Majority of representatives with joined authorisation (half plus one)
Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Meerderheid van de vertegenwoordigers met gezamenlijke bevoegdheid (helft plus een)
Legal representative with limited authorisation or limited power of attorney	Majority of representatives with limited authorisation or limited power of attorney (half plus one)
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Meerderheid van de vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht (helft plus een)
Legal representative with limited authorisation or limited power of attorney related to eHerkenning	Explicit authorisation to approve eHerkenning must be in Chamber of Commerce
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

eHerkenning 4

Authorisations for eHerkenning Level 4 require the approval(s) defined in the table below.

Authorisation in Chamber of Commerce	Condition
Legal representative with full authorisation, independent authorisation of power of attorney	N/A
Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	n.v.t.
Legal representative with joined authorisation	All representatives with joined authorisation
Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Alle vertegenwoordigers met gezamenlijke bevoegdheid
Legal representative with limited authorisation or limited power of attorney	All representatives with limited authorisation or limited power of attorney
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Alle vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht
Legal representative with limited authorisation or limited power of attorney related to eHerkenning	Explicit authorisation to approve eHerkenning must be in Chamber of Commerce
Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

Requirements for eHerkenning are defined and documented in the Dutch Trust Framework (https://afsprakenstelsel.etoegang.nl).

2.4 UK Digital Identity & Attributes Trust Framework

The UK digital identity and attributes trust framework (DIATF) is a set of rules and standards designed to establish trust in digital identity products in the UK.

Digidentity offers three identity verification services under the digital identity and attributes trust framework:

[1] Right to Work
[2] Right to Rent
[3] Disclosure and Barring Service

Digidentity is certified against the requirement of DIATF for identity profiles M1A, M1C and H1A set out in the annex to "Good Practice Guide (GPG 45) – How to prove and verify someone's identity", as published by Cabinet Office and the Government Digital Service on the gov.uk website.

	M1A	M1C	H1A
Strength	4	3	4
Validity	2	3	3
Activity history	NA	NA	NA
Identity fraud	1	NA	1
Verification	2	3	3

The strength of the evidence (maximum score is 4) is determined by:

- what security features protect it (for example a hologram or an electronic chip)
- how the person's identity was checked when the evidence was issued

The validity of the evidence (maximum score is 4) is determined by:

- is evidence valid (not expired)
- cryptographic check of the evidence

The identity fraud check (maximum score is 3) is to make sure the claimed identity is not:

- at a higher than usual risk of identity fraud
- suspected to be a synthetic identity

The verification check (maximum score is 4) is to make sure the person performing the identity proofing, is the actual person of the claimed identity:

- perform biometric matching e.g. face comparison

https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-profiles

2.4.1 Right to Work

Right to Work (RtW) is an identity verification service required to be able to work in the UK.

https://www.gov.uk/government/publications/right-to-work-checks-employers-guide

Sources to collect and verify attributes

[a] Identity documents (UK or Irish passport with NFC chip)
[b] Selfies made by Applicant

Sources to verify identity evidence

[a] Biometric validation and verification (liveness detection & face comparison) of natural persons
[b] Cryptographic validation and verification of identity documents and personal data

Attributes used:

[a] Full name of Applicant (Given Name and Surname)
[b] Date of Birth
[c] Gender
[d] Identity Document number
[e] Personal Identification Number
[f] Date of issuance
[g] Date of expiry
[h] Issuing country
[i] Photo from chip

2.4.2 Right to Rent

Right to Work (RtR) is an identity verification service required to be able to rent property in the UK.

https://www.gov.uk/government/publications/landlords-guide-to-right-to-rent-checks

Sources to collect and verify attributes

[a] Identity documents (UK or Irish passport with NFC chip)
[b] Selfies made by Applicant

Sources to verify identity evidence

[a] Biometric validation and verification (liveness detection & face comparison) of natural persons
[b] Cryptographic validation and verification of identity documents and personal data

Attributes used:

[a] Full name of Applicant (Given Name and Surname)
[b] Date of Birth
[c] Gender
[d] Identity Document number
[e] Personal Identification Number
[f] Date of issuance
[g] Date of expiry
[h] Issuing country
[i] Photo from chip

2.4.3 Disclosure & Barring Service

Disclosure & Barring Service (DBS) is an identity verification service to perform background checks the UK.

https://www.gov.uk/government/publications/dbs-identity-checking-guidelines

Sources to collect and verify attributes

[a] Data provided by Applicant manually (address)
[b] Identity documents (UK or Irish passport with NFC chip)
[c] Selfies made by Applicant

Sources to verify identity evidence

[a] Biometric validation and verification (liveness detection & face comparison) of natural persons
[b] Cryptographic validation and verification of identity documents and personal data
[c] Verification of address

Attributes used:

[a] Full name of Applicant (Given Name and Surname)
[b] Date of Birth
[c] Gender
[d] Identity Document number
[e] Personal Identification Number
[f] Date of issuance
[g] Date of expiry
[h] Issuing country
[i] Photo from chip
[j] Home address

2.5 Know Your Customer (KYC) – Identify & Delete

Digidentity provides Know Your Customer (KYC) processes to accurately identify your customers that meet any regulatory requirement. Depending on your specific needs, this process can be customised using our set of modular validation and verification methods.

Our system supports the creation of persistent identities, allowing customers to create an account that can be used for other services. Additionally, Digidentity offers an Identify & Delete (I&D) service. For this service, we perform the validation and verification processes and provide you with a metadata report detailing the necessary data, checks, and outcomes. Once the report is delivered, all relevant data and evidence are promptly deleted by Digidentity. Digidentity will soon be able to deliver data as a Verifiable Credential.

Clients have the option to either accept or reject an identity based on predetermined requirements. Alternatively, we can generate a metadata report containing the results of our validation and verification processes, supplemented with our recommendations. However, the final decision to approve or reject the identity rests solely with you.

Digidentity

3 Identity Proofing Methods

Digidentity has developed a reliable and regulatory compliant remote identity proofing method to identify a person which provides equivalent assurance in terms of reliability to physical presence. This remote identity proofing process, which is a part of the identity proofing process for qualified signatures and digital identities with eIDAS assurance level high, uses the Digidentity Wallet on a smartphone.

The identity proofing process consists of three steps which uses different methods to validate and verify the identity. The three steps of identity proofing are:

- Identity Document validation and data verification – is the document genuine and is the data correct?
- Liveness detection – is an actual 'live' person performing the identity proofing?
- Face comparison – is the person on the identity document also the person performing the identity proofing?

Digidentity is required to verify all data (personal data, organisation data, other data) provided by the Applicant and validate that a genuine identity document is presented.

3.1 Pre-Validation of Identity Documents

Digidentity performs a pre-validation of the identity document using the MRZ, and checks if the identity document is genuine, valid and allowed for the selected Product. Pre-validation makes sure that only allowed identity document are used to register. The Applicant does not have to select which identity document is used or if an NFC chip is present.

We check the MRZ to determine the type of document and issuing country to determine of the document is allowed, has an NFC chip which can be validated. We also perform checks on the MRZ data for:

- Verify issuing country & organisation
- Verify document number and check digit (is calculated with an algorithm and based on the document number)
- Verify date of birth and check digit
- Verify date of expiry (is document valid) and check digit
- Verify date of issuance and check digit
- Verify national identification number and check digit
- Verify composite check digit (check digit for the correct position of the data in the MRZ)

If the identity document passes pre-validation, the identity proofing continues using the best possible route for the selected Product. Documents that fail the pre-validation will be rejected.

Digidentity

3.2 Cryptographic Validation of Identity Documents

Digidentity supports the use of Near Field Communication (NFC) to read the NFC chip in modern identity documents (e.g. passports, identity cards and driving licenses). This chip is standardised as part of Doc 9303, Machine Readable Travel Documents (MRTD), by the International Civil Aviation Organization (ICAO). We use Digidentity or ReadID technology to read the NFC chip in the identity document.

The Identity Wallet supports NFC (iOS and Android) and allows Applicants to read the data (text and photo) from the NFC chip in their identity document. We perform an automated validation of the document and verify the data using cryptographic controls.

During the identity proofing process, real time video of the identity document is made and Digidentity extracts a photo of the front and back of the identity page of the document. We require the MRZ of the document to generate the key to access the chip. Digidentity extracts both personal details stored as text and the photo from the chip in the identity document.

Digidentity compares the data on the front of the document with the data from the chip to determine if the document has been modified. Any discrepancies are reviewed before a decision to accept or reject the document is made.

The Applicant has a maximum of three attempts to upload new photos. After three attempts, the account is blocked, and the Applicant must contact the Service Desk.

Data from the NFC chip of the identity document allows multiple validation and verification steps:

[a] Basic Access Control

During Basic Access Control (BAC) the mobile phone proves to the NFC chip that it has access to a key derived from three fields in the Machine-Readable Zone (MRZ): document number, date of birth, and date of expiry.

[b] Passive Access Control

After reading the data from the NFC chip, Passive Authentication is performed on our systems. Passive Authentication consists of three verifications:

[1] Hash Table verifies that the hashes contained in the NFC chip correspond to the hashes of the individual data groups. The signed-data structure (hash table) which contains a hash for each data group. To be able to perform this check, whole data groups must be read completely. If the Hash Table verification fails, this means one or more data groups have been manipulated.

[2] Verification of the Document Signer consists of a verification of the digital signature on the signed-data structure (hash table) using a document signer certificate. The chip contains the complete document signer certificate. This check verifies the signed-data structure in the chip was signed by the document signer.

[3] Verification of the Country Signer consists of the issuer of the document signer certificate is trusted using a list of trusted, self-signed Country Signer certificates: Country Signer Certificate Authority (CSCA) certificates, and also a list of link-certificates (intermediate certificates). This check will search the list of trusted certificates and attempt to establish a chain of certificates starting at the document signer certificate and ending in a CSCA certificate. The CSCA certificates are made available by the German Bundesamt für Sicherheit in der Informationstechnik (BSI) to maintain an up-to-date and valid list of CSCA certificates to validate identity documents.

All verifications performed during passive authentication must be successful for Digidentity to accept the document. Any failed verification will result in a rejected document.

[c] Clone Detection

Next to verifying the authenticity of the content, some documents allow to verify that the actual chip is used and not a clone. Digidentity uses two methods to detect if an NFC chip in the document is a clone:

[a] Active Authentication (AA)

For clone detection using Active Authentication (AA), a challenge-response mechanism is used. We can trust the key after successful performing the Passive Authentication on data group 15. If the signature is correct, this means the actual chip is used and not a clone.

[b] Chip Authentication (CA)

For clone detection using Chip Authentication (CA) a complicated challenge-response mechanism using a Diffie-Hellman Key Exchange. CA is a part of Extended Access Control (EAC-CA). We can trust the key after successful performing the Passive Authentication on data group 14. If the signature is correct, this means the actual chip is used and not a clone.

Digidentity accepts documents where the clone detection verification was successful (clone not detected) or not available. As the availability of clone detection is limited, older documents do not support clone detection, documents without clone detection support can continue validation and verification process. If a clone is detected, the document is rejected.

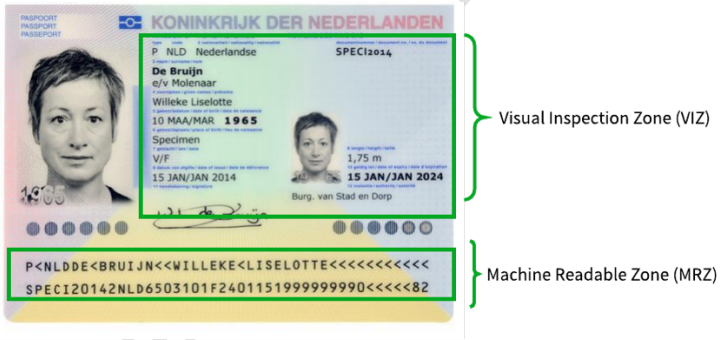
Using the data read from the NFC chip of the identity document and a verification of the cryptographic controls, provides Digidentity the guarantee that the document is 100% genuine.

3.3 Photographic Validation of Identity Documents

Identity documents that do not have an NFC chip or when the country certificate is not available, Digidentity uses photographic validation of the document. Digidentity uses photographic validation services from DataChecker and Mitek.

During the identity proofing process, real time video of the identity document is made. We extract the photos of the front and back of the identity document from the video to validate the document and verify the personal data. Digidentity only accepts photos that have been taken real time during the identity proofing process.

Digidentity performs an automated and manual verification to verify the security features of the document and detect manipulation. The validity of the document is inspected, as well as the date is issuance of the document. The data on the document from the Visual Inspection Zone (VIZ)and the Machine-Readable Zone (MRZ) is extracted. The data is compared, analysed and verified to determine the correctness and plausibility of the data.



MRZ data

- Verify issuing country
- Verify document number and check digit (is calculated with an algorithm and based on the document number)
- Verify nationality
- Verify date of birth, date of expiry and data of issuance and check digits
- Verify national identification number and check digit
- Verify composite check digit (check digit for the correct position of the data in the MRZ)

VIZ & MRZ data

- Verify font validation
- Verify photo integration

We use a combination of technologies to verify the genuineness of the identity document. This includes sophisticated artificial intelligence analytics (computer vision, machine learning and deep learning) to analyse photos of identity documents, collecting evidence for identity verification. A higher level of machine learning weighs the results from hundreds of these algorithms, making an intelligent decision about the relative importance of each piece of evidence, then predicts whether or not the document is genuine. The analysis will detect if a photo is real and not a photo of a screen or copy of an identity document.

The manual verification also includes plausibility checks in which the photo compared to the date of birth and gender stated on the identity document.
Digidentity uses an automated verification can accurately and consistently detect the following:

- inconsistencies in kinegram, hologram and multiple laser image;
- inconsistencies in the typography such as printing techniques and fonts;
- inconsistencies in the photograph including substitution;
- presence of a ghost image, guilloche structures and micro lettering;
- presence of correct watermarks and security fibers;
- presence of document number and image perforation.

After the automated verification of the identity document, a professionally trained employee will reverify the results of the automated verification and manually inspect the identity document on formal visually identifiable features that an identity document typically possesses. This includes layout, number, size and spacing of characters, as well as typography and any other relevant formal security features.

If the verification of the document fails, the document is rejected.

3.4 Lost or Stolen Identity Document Check

Digidentity checks every identity document against a lost or stolen register or Interpol which allows us to check if a document had been reported lost or stolen.

If the document number is registered as lost or stolen, Digidentity rejects the identity document.

3.5 Liveness Detection

Digidentity uses Liveness detection to determine if an actual 'live' person is performing the identity proofing process. Liveness detection of the Applicant is performed during the selfie taking process. Digidentity records a video of the Applicant and extracts two photos from the recorded video.

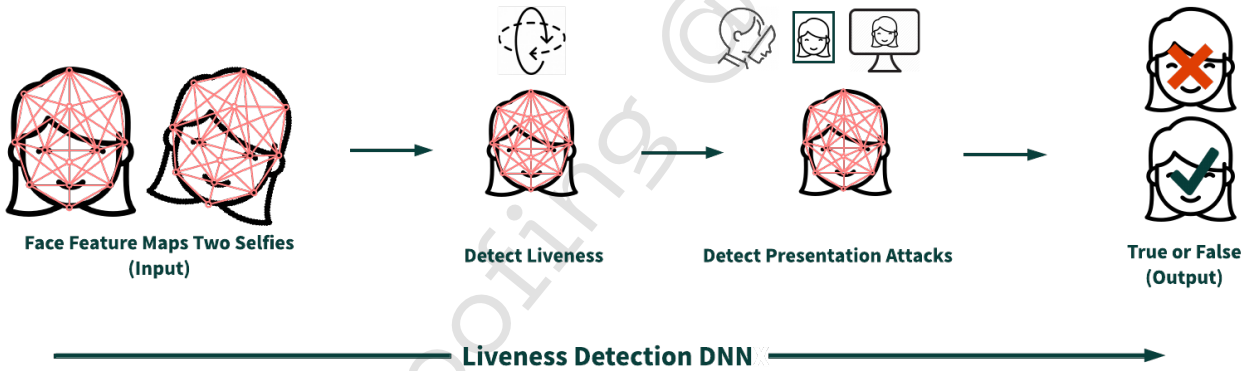
The liveness detection starts with a first selfie (#1), the Applicant is required to look straight at the camera and press the shutter button. Next, the Applicant is directed to move their head. The direction of movement is randomly selected by the system. The camera of the phone records a video stream of the Applicant and automatically captures selfies #2 and #3 from the video. This capture is not based on period of time but on detection of movement. As soon as our Wallet detects movement, two selfies are extracted.

Digidentity

Digidentity uses biometric verification services from BioID in Germany (www.bioid.com). BioID uses active liveness detection as end-user must interact (head movement) with the system. Active liveness detection:

- combines motion analysis and artificial intelligence with multiple images;
- requires user's consciousness and therefore is particularly suitable for services with a high focus on data privacy and security;
- can be combined with a challenge-response mechanism for additional security and the protection against deepfakes;

Digidentity sends selfie #2 and #3 to BioID. BioID detects natural movement of the head (also checks the photos are not taken from a screen, video or Applicant is wearing a mask). The identity proofing process continues when BioID confirm the liveness detection was successful. The Applicant is allowed to perform five liveness detection attempts. After five attempts, the identity proofing process stops, and Applicant must contact the Service Desk.



Liveness detection works with standard webcams and mobile phone cameras. This allows widely deployment of an extremely secure authentication with positive impact on the intended service in terms of convenience, cost, quality and performance.

Liveness detection can detect spoofing attacks that use video (including deep fakes) or photo replays and photos from other photos or screens. BioID uses a patented algorithm to accurately detect whether images come from a live person, or a photo or video is used. When spoofing is detected, the images are also used to train the engine to create a more robust system.

Two selfies are sufficient in the important step of liveness detection in remote identity proofing to ensure the physical presence of the applicant preventing video and still photo spoofing attacks.

The liveness detection, an industry proven technology from BioID, is used to:

[1] Ensure the physical presence of the applicant ("face-to-face")

[2] Detect spoofing attacks using video (including deep fakes) or photo replays and photos from other photos or screens

Liveness detection is based on two algorithm stages: 3D geometry analysis and resampling.

3.5.1 3D geometry analysis

First, BioID performs an optical flow analysis and detects movement between two or more frames of the camera. BioID uses the two selfies (#2 and #3) to calculate the flow field of the face area. From this flow field, BioID can tell if the movement of the face was a linear movement, and if there is a real 3D face. Using a 3D geometry analysis on the flow field, BioID can reject all kinds of printed photo attacks, as well as still images displayed on any type of screen. A 3D face moves differently from a 2D photo, which the technology can distinguish. The capture of the second and third photo can be triggered with sensitive motion detection, so that an attacker cannot simply present slightly different photos; the second and third image would be captured before the attacker's next photo was in place.

3.5.2 Resampling (texture) inspection of the selfies

Secondly, BioID inspects the texture of the facial area to find out whether the image has been resampled (any screen shows a resampled version of the original image). BioID uses methods of Deep Learning. BioID trains a Deep Neural Network (DNN) with millions of samples that are either live or fake. Fakes are taken from all kinds of display devices, as well as masks. With this second step, BioID detects photos from videos or mask attacks.

By combining these two steps, BioID reaches a higher accuracy than others who follow only one of those steps.

3.6 Presentation Attack Detection

Active Presentation Attack Detection (PAD) prevents forgery through replay attacks with videos, avatars or deep fakes and is based on texture detection and error level analysis (ELA). Image-processing algorithms analyse the texture to differentiate between the texture of skin and that of the paper a photo is printed on. The texture of a recaptured image or a video can now be detected for reliable anti-spoofing.

The BioID Liveness Detection is compliant with ISO30107-3:2017 for Level 1 and Level 2 attacks and FIDO Biometric Certification Requirements v1.1 (FIDO1.1).

For Liveness Detection, the performance of the system in protection against Presentation Attack Detection (PAD) is expressed in error rates such as Attack Presentation Classification Error Rate (APCER) and Bona fide Presentation Classification Error Rate BPCER.

Measurement		Description
Attack Presentation Classification Error Rate	APCER	Proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario
Bona fide Presentation Classification Error Rate	BPCER	Proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

As a part of the ISO30107 certification, the APCER and BPCER are determined for BioID. The auditor determined the error rates for BioID at a APCER of 4.6% and BPCER of 9.0%.

3.7 Face Comparison

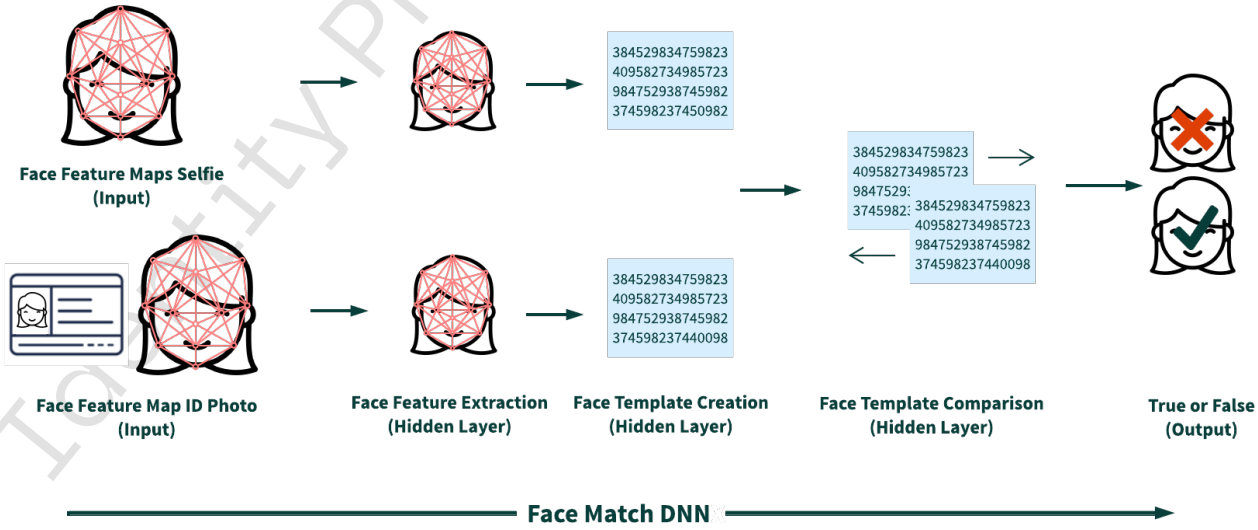
Digidentity performs a face comparison of the selfies and the photo from the identity document to determine if the person on the document is performing the identity proofing process.

Digidentity uses the BioID PhotoVerify for the face comparison. BioID uses periocular (eye) biometrics and face recognition for the comparison of the photos, as it gives the best results and performance. Periocular biometrics focuses around the human eyes, where the richest features are located. It has proven to be least affected by lighting conditions. Face recognition verifies the full face of the applicant. BioID PhotoVerify uses the fusion (face & periocular) to create the desired results.

Periocular-based biometrics refers to the automatic recognition or classification of an individual based upon features extracted from the area of the face which surrounds the eye. Typically, the facial area utilised extends from the top of the eyebrow to the cheekbone and includes the area from the midline of the nose to just inside the ear.

Potential features found in the periocular region which can be used for biometric applications include the upper/lower eyelids, the upper/lower eye folds, various skin lesions (moles, freckles), eye corners, eyebrows, as well as skin colour/texture. One of the motivations for periocular-based biometrics is that features from the periocular region can be used in situations in which the face is partially occluded (nose, mouth covered) preventing facial recognition.

Digidentity sends the high-resolution photo[1] from the NFC chip together with selfies #2 and #3 to BioID for the Face Comparison. The selfies #2 and #3 are compared again by BioID for liveness detection and both selfies #2 and #3 are compared to the photo from the identity document to achieve a more accurate result.



[1] The eMRTD (Machine Readable Travel Documents, ICAO 9303) standard mandates that the face image is a high-resolution photo, suitable for automated facial recognition.

The comparison is performed on the servers of BioID. No user profiles are created. Normally, face recognition is based on features extracted from all enrolled images will be calculated using the BioID algorithm to create and save as a "template" for later recognition use. This is a typical "enroll-verify" application scenario.

Using a combination of sophisticated artificial intelligence analytics (computer vision, machine learning and deep learning) to analyse photos from the identity document and end-users' selfies, collecting evidence for identity verification. A higher level of machine learning weighs the results from hundreds of these algorithms, making an intelligent decision about the relative importance of each piece of evidence, then predicts whether the identity document photo is genuine and belongs to the Applicant. The analysis will detect if a photo is real and not a photo of a screen or copy of a document and if the live person matches the person on the identity document.

The face/periocular in BioID PhotoVerify, create a "template on the fly" and then used to compare to the identity document photo. After the PhotoVerify operation, the images and the "templates" used are discarded. PhotoVerify is a "zero footprint" or "traceless" or "enrolment-free" biometric matching. This is the "privacy by design" principle in making BioID a GDPR-compliant Data Processor.

3.8 Biometric Performance

For Face Comparison, the performance of biometric security systems is expressed in error rates such as False Acceptance Rate (FAR) and False Rejection Rate (FRR).

Measurement		Description
False Acceptance Rate	FAR	number of times the system incorrectly accepts an unauthorised person (person should have been rejected)
False Match Rate	FMR	see FAR
False Rejection Rate	FRR	number of times the system incorrectly rejects an authorised person (person should have been accepted)
False Non-Match Rate	FNMR	see FRR

A study in 2014, researchers found that highly experienced passport officers incorrectly accepted 14% of fraudulent person-photo comparisons. This is a significantly higher false acceptance rate than can be achieved using automated biometric verification.

Study 'Passport Officers' Errors in Face Matching' (https://pubmed.ncbi.nlm.nih.gov/25133682/).

The decision if the person on the photos matches, is made according to the accuracy level. Digidentity uses the highest accuracy level (level 5) from BioID defining the number of false positives (incorrect matches). BioID achieves a FAR of 0,001% and FRR of 6,00% for accuracy level 5.

The FAR must be calculated only over the subset of comparisons that attempt fraud and not over the total amount of comparisons as the total amount also contains non fraudulent attempts.

Example:
Comparing photos of 100.000 natural persons where the number of persons who try to commit fraud is 1% (1.000 persons), a FAR of 0,1% will result in a false acceptance of one person (0,1% of 1.000). Compared to the study in 2014, passport officers will allow 14% of persons who try to commit fraud to pass the comparison (14% of 1.000 is 140 persons).

Digidentity has set the accuracy level to five (5) as the system is trained and evaluated. On level 5 (0,001%), the FAR is much lower than the FAR for identity proofing by trained professionals (14%). The BioID Services offer more accurate results than trained professionals can achieve.

The BioID biometric services uses artificial intelligence in several instances of Deep Neural Networks (DNN) to provide Digidentity with a true or false response. The DNN for face comparison and liveness detections are trained on datasets using more than five million face images.

The BioID technology is patented (https://patents.justia.com/patent/10586098).

3.9 Manual verification

Digidentity performs a manual verification in the event an identity proofing has been rejected. Our agents review all identity evidence and checks performed to confirm the rejection or to overrule the rejection and accept the identity manually.

The identity proofing requirements determine if the process is fully automated or includes a manual verification.

Digidentity

4 Attribute Handling & Sources

Identity attributes could have differences in encoding, name attributes or additional attributes.

4.1 Handling of attribute encoding

Digidentity uses the personal data from the NFC chip or the Machine Readable Zone (MRZ). If the personal data from the chip or MRZ differs from the official name as printed in the Visual Inspection Zone (VIZ), Digidentity will use the data from the NFC chip or MRZ zone.

If the NFC chip does contain national language characters (e.g. German ä, ü, ß or Norwegian æ, ø, å), these characters will be included. If the NFC chip does not contain national language characters, the transcription from the chip is used (e.g. German ae, ue, ss or Norwegian ae, oe, aa).

For Non-alphabetical scripts (e.g. Chinese or Russian) the alphabet version (from chip or VIZ) is used.

4.2 Handling of name attributes

Digidentity does not include name attributes such as prefixes (e.g. Dr) and suffixes (e.g. Jr, e/v <name>). When the identity document contains one name only, either given name or surname is empty, we will fill the empty field with a "-". Names that are longer than the 64 characters of each given name and surname field, will be truncated.

Digidentity accepts only names that are supported by the evidence provided. Nick names or synonyms are not accepted (Mike/Michael, Bill/William). Digidentity only accepts attributes verified by identity evidence.

If a name change is not reflected on the evidence, Digidentity cannot verify the changed name. Applicant must obtain new evidence confirming the name change.

4.3 Handling of additional attributes

Digidentity collects identity attributes as part of the identity proofing process. Some attributes are used during the proofing process to validate and verify identity evidence. These additional attributes will be deleted after the proofing process is completed and quality control is performed.

4.4 Rules for Identity Documents

The overview of accepted Identity Documents is in Appendix A of this document.

DDY also applies the following rules to identity document:

[1] Identity document with no issuing date is rejected

[2] Identity document with no expiry date cannot be older than ten (10) years based on the issuing date (e.g. identity document with issuing date 01-Aug-2015 (six year old) is accepted, identity document with issuing date 21-Feb-2007 (14 years old) is rejected)

[3] Identity document with expiry date longer than ten (10) years is rejected when identity document is older than ten (10) years (e.g. identity document with expiry on 31-Dec-2099 and issuing date is 01-Jun-2017 (six years old) is accepted, identity document with expiry on 31-Dec-2099 and issuing date is 15-May-2002 (21 years old in 2023) is rejected)

Issue date	Expiry Date	Calculation	Result
04 May 2019	03 May 2029	9 June 2023 in period of validity	Accept
06 Dec 2019	05 Dec 2099	2019 plus 10 years is 2029, 9 June 2023 in period of validity	Accept
29 Jul 2019	No expiry date	2019 plus 10 years is 2029, 9 June 2023 in period of validity	Accept
15 Mar 2007	14 Mar 2017	9 June 2023 outside period of validity	Reject
17 Nov 2008	16 Nov 2099	2008 plus 10 years is 2018, 9 June 2023 outside period of validity	Reject
16 Apr 2010	No expiry date	2010 plus 10 years is 2020, 9 June 2023 outside period of validity	Reject
No issue date	No expiry date	No dates to determine validity	Reject
No issue date	6 Jul 2025	No issue date to determine validity (could be issued in 2000)	Reject

Result determined using date of 9 June 2023.

4.5 Authoritative Sources & Trusted Registers

Digidentity uses Trusted Registers to validate and/or verify identity evidence provided by the Applicant.

For eHerkenning:

- Dutch Chamber of Commerce
- PROBAS

For Certificates for a Registered Profession

- Royal Netherlands Institute of Chartered Accountants (Dutch: Koninklijke Nederlandse Beroepsorganisatie van Accountants - NBA)

4.6 Supplementary evidence

Digidentity requires supplementary evidence to verify the authorisation of a natural person. For eHerkenning, Digidentity requires proof of authorisation when the Applicant is not registered as a legal or authorised representative.

The supplementary evidence is provided with a letter of authorisation signed by the legal representative(s) confirming the requested authorisation of the Applicant.

Digidentity

Appendix A — Accepted Identity Documents

Identity Document	eSGN		eH			UK Trust Framework				
	Qualified	Advanced	LoA4	LoA3	LoA2+	RtW	RtR	DBS		
Biometric passports (NFC) that comply with ICAO 9303 (e-passports) and implement basic or enhanced access control (e.g. EEA/EU/UK/US/AU/NZ/CN)	✓	✓	✓	✓	✓					
EEA/EU Government issued identity cards (NFC) that comply with Council Regulation (EC) No 2252/2004 that contain a biometric	✓	✓	✓	✓	✓					
ID with NFC that comply the ICAO9303 part 10 (Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC)) (e.g. Residence Permits)	✓	✓	✓	✓	✓					
Passports that comply with ICAO 9303 (Machine Readable Travel Documents)		✓		✓	✓					
EEA/EU Government issued identity cards that comply with Council Regulation (EC) No 2252/2004		✓		✓	✓					
EEA/EU driving licences that comply with European Directive 2006/126/EC		✓		✓	✓					
EEA/EU driving licences that comply with European Directive 2006/126/EC with NFC that comply the ICAO9303 part 10 (Logical Data Structure (LDS) for Storage of Biometrics and Other Data in the Contactless Integrated Circuit (IC))	✓	✓	✓	✓	✓					
UK Passport with NFC Chip						✓	✓	✓		
Irish Passport with NFC Chip						✓	✓	✓		

Physical documents

The use of physical identity document is defined in requirement COL-8.2.3-04:

[CONDITIONAL] If physical identity documents are used as evidence, only passports, national identity cards and other official identity documents that according to the identity proofing context offer comparable reliability of the identity shall be accepted; where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process of passport and/or identity card.

Digital documents

The use of digital identity document is defined in requirement COL-8.2.3-06:

[CONDITIONAL] If digital identity documents are used as evidence, only eMRTD digital identity documents according to ICAO 9303 part 10 [2] and other digital documents that according to the identity proofing context offer comparable reliability of the identity shall be accepted; where the judgement on comparable reliability shall be based on an assessment of the security features and issuance process of the other identity document towards the security features and issuance process required by ICAO 9303 part 10.

For both physical and digital documents: The comparable reliability of other identity documents can be based on a comparison of protection against known threats.

An identity document that contains an NFC chip is not by default ICAO compliant.

The security features and issuance of an identity document could provide comparable reliability. Acceptance of other documents must be assessed, and the results documented.