Digidentity

Identity Proofing @ DDY
Contexts & Methods

Title	Identity Proofing @ DDY - Contexts & Methods
Date	31 January 2022
Version	2022-v1
Classification	Public

Digidentity

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Revisions

Version	Date	Author	Changes Made (*)
2022-v1	31 January 2022		Initial version

(*) All changes are marked in grey highlight.

Digidentity

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

Identity proofing policy and security requirements for trust service components providing identity proofing of trust service subjects are document 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 TSP.

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 at supporting 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

Contexts

Digidentity performs identity proofing for four identity proofing contexts:

[1] eIDAS
[2] eSGN - Electronic Signatures
[3] eHerkenning
[4] GOV.UK Verify

eIDAS Trust Services & eID

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

- eIDAS High or Qualified: remote identification using NFC, biometric verification
- eIDAS Substantial or Advanced: remote identification using NFC or video of ID, biometric verification

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

[a] Identity documents (as defined in table "Accepted Identity Documents" - see last page)
[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

Sources to verify identity evidence

[a] BioID for verification of liveness and face comparison
[b] Mitek, Onfido and ReadID for validation and verification of Identity Documents
[c] Chamber of Commerce for verification of 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] Full name of Legal Representative(s)
[f] Date of issuance	[f] Authorisation of Legal Representative(s)
[g] Date of expiry	
[h] Issuing country	

All Digidentity services are based on eIDAS identification.

eSGN – Electronic Signatures

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

Digidentity uses remote identification to perform identity proofing for eSGN. The eSGN service selected, determines the remote identification method allowed:

- eSGN Qualified, eSGN Seal: see eIDAS Qualified
- eSGN Advanced: see eIDAS Advanced

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

eSGN Seal is a service 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. 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.

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

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. Identification 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 identification to perform identity proofing for eHerkenning. The eHerkenning service selected, determines the remote identification method allowed:

- eHerkenning Level 4: remote identification using NFC, biometric verification, physical presence
- eHerkenning Level 3: remote identification using NFC or video of ID, biometric verification
- eHerkenning Level 2+: remote identification using NFC or video of ID

Digidentity

Physical presence of the Applicant or representative is mandatory for eHerkenning Level 4 pending notification of Digidentity Remote Identification 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 Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	N/A
Legal representative with joined authorisation Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Minimum of two representatives with joined authorisation Minimaal twee vertegenwoordigers met gezamenlijke bevoegdheid
Legal representative with limited authorisation or limited power of attorney Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht	Minimum of two representatives with limited authorisation or limited power of attorney Minimaal twee vertegenwoordigers met beperkte bevoegdheid of beperkte volmacht
Legal representative with limited authorisation or limited power of attorney related to eHerkenning Wettelijk vertegenwoordiger met beperkte bevoegdheid of beperkte volmacht voor eHerkenning	Explicit authorisation to approve eHerkenning must be in Chamber of Commerce Expliciete autorisatie voor eHerkenning moet op KvK uittreksel staan

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 Wettelijk vertegenwoordiger met volledige bevoegdheid, zelfstandige bevoegdheid of een volmacht	N/A
Legal representative with joined authorisation Wettelijk vertegenwoordiger met gezamenlijke bevoegdheid	Majority of representatives with joined authorisation (half plus one) Meerderheid van de vertegenwoordigers met gezamenlijke bevoegdheid (helft plus een)

Authorisation in Chamber of Commerce	Condition
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	
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).

Digidentity

GOV.UK Verify

GOV.UK Verify is an identity service to access government services in the UK.

Digidentity uses remote identification to perform identity proofing for GOV.UK Verify. The GOV.UK Verify service selected, determines the remote identification method allowed:

- GOV.UK Verify Level 1 & Level 2: remote identification using NFC or video of ID, biometric verification, manual input by Applicant

Sources to collect and verify attributes

[a] Data provided by Applicant manually (address, phone number, identity document data)
[b] Identity documents (as defined in table "Accepted Identity Documents" - see last page)
[c] Selfies made by Applicant

Sources to verify identity evidence

[a] Government Document Checking Service (DCS) for validation of UK Identity Documents
[b] BioID for verification of liveness and face comparison
[c] Mitek, Onfido and ReadID for validation and verification of Identity Documents
[d] Transunion for verification of address and activity history
[e] Transunion for providing Knowledge based questions
[f] Phronesis for verification of name, address and phone number
[g] Onfido ID Record for verification of name and 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

Requirements for GOV.UK Verify scheme are defined and document in the GPG44 and GPG45.

Attribute Handling

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

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.

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.

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.

Rules for Identity Documents

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

Next to the accepted ID, DDY also applies the following rules to ID before accepting:

[1] ID with no issuing date is rejected

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

[3] ID with expiry date longer than ten (10) years is rejected when ID is older than ten (10) years (e.g. ID with expiry on 31-Dec-2099 and issuing date is 01-Jun-2017 (four years old) is accepted, ID with expiry on 31-Dec-2099 and issuing date is 15-May-2002 (19 years old in 2021) is rejected)

Digidentity

Trusted Registers

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

For eHerkenning:

- Chamber of Commerce (Dutch: Kamer van Koophandel - KvK)

For Certificates for a Registered Profession

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

For GOV.UK Verify (as approved by Government Document Service):

- Document Checking Service (DCS): validate UK identity documents

Supplementary evidence

Digidentity requires supplementary evidence to verify the authorisation of a natural person. For eHerkenning, Digidentity require 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			GOV.UK				
	Qualified	Advanced	LoA4	LoA3	LoA2+	LoA2	LoA1			
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))	✓	✓	✓	✓	✓	✓	✓			
Northern Ireland Voters Card						✓	✓			
US passport card						✓	✓			
Armed forces ID card						✓	✓			
Proof of age card issued under the Proof of Age Standards Scheme (containing a unique reference number)						✓	✓			
UK Biometric Residence Permit (BRP)						✓	✓			
NHS staff card containing a biometric						✓	✓			

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 ID 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 result documented.