

Identity Proofing @ Digidentity

Contexts & Methods

Title	Identity Proofing @ Digidentity – Contexts & Methods
Date	6 December 2025
Author	Sander Remmerswaal
Version	2026-v1
Location	https://www.digidentity.eu/en/documentation/
Classification	Public

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
2026-v1	6 December 2025	Sander Remmerswaal	Complete rewrite, in line with ETSI TS 119 461 (changes not marked)

(*) All changes are marked in grey highlight.

Identity Proofing

Contents

1	Introduction	6
1.1	Identity Proofing Services Practice Statement	7
1.2	Supported Use Cases	8
1.3	Identity Proofing Contexts	8
1.4	General Requirements	9
1.5	Level of Assurance	9
1.6	Result & Evidence of Identity Proofing.....	9
1.7	Abbreviations & Definitions	9
2	eIDAS Trust Services & eID	10
2.1	Attributes Collected for Natural Persons	10
2.2	Attributes Collected for Legal Persons	10
2.3	Validity of Collected Evidence	11
2.4	Validation & Verification	11
2.5	Accepted eID	11
2.6	Accepted documents.....	11
2.7	Binding natural person to legal person	12
2.8	Supplementary evidence.....	12
3	Electronic Signatures.....	13
3.1	Collected attributes	13
3.2	Validity of Collected Evidence	13
3.3	Validation & Verification	13
3.4	Accepted eID	14
3.5	Accepted documents.....	14
3.6	Trusted Register	14
3.7	Binding natural person to legal person	15
3.8	Supplementary evidence.....	15
4	eHerkenning.....	16
4.1	Collected attributes	16
4.2	Evidence Collection for Natural Person representing a Legal Person	16
4.3	Validity of Collected Evidence	17
4.4	Validation & Verification	17
4.5	Accepted eID	17
4.6	Accepted documents.....	17
4.7	Trusted Register	18
4.8	Binding natural person to legal person	18
4.9	Supplementary evidence.....	18

5	PKloverheid Private Certificates	19
5.1	PKloverheid Private SBR Certificates	19
5.2	PKloverheid Private TLS Server Certificates	20
5.3	Collected attributes	20
5.4	Validity of collect evidence	20
5.5	Validation & Verification Methods	21
5.6	Accepted eID	21
5.7	Accepted documents	21
5.8	Trusted Register	21
5.9	Binding natural person to legal person	22
5.10	Supplementary evidence	22
6	UK Digital Identity & Attributes Trust Framework	23
6.1	Right to Work	24
6.2	Right to Rent	24
6.3	Disclosure & Barring Service	25
6.4	Validity of collect evidence	25
6.5	Accepted documents	26
6.6	Trusted Register	26
6.7	Binding natural person to legal person	26
6.8	Supplementary evidence	26
7	Custom Identity Proofing (KYC)	27
8	Attributes & Evidence Validation	28
8.1	Attribute Collection of Natural Person	28
8.2	Attribute Collection of Legal Person	28
8.3	Attribute Handling & Sources	29
9	Is the Identity Document Genuine & Valid?	31
9.1	Pre-validation of Identity Documents	31
9.2	Lost or Stolen Check	32
9.3	Physical Identity Document	33
9.4	Digital Identity Documents	35
9.5	Identity Document Validity Handling	41
10	Is an actual 'live' person performing the Identity Proofing?	43
10.1	Capture of Face Image	43
10.2	Liveness Detection	44
11	Does the 'live' person match the person on the Identity Document?	46
11.1	Face Comparison	46
11.2	Biometric Performance	47

12	Identity Proofing Legal Person	50
12.1	Does the organisation (legal person) exist?	50
12.2	Is the natural person authorised to represent the legal person?	50
12.3	Trusted Registers	52
12.4	Supplementary evidence	52
13	Presentation & Injection Attack Detection	53
13.1	Presentation Attack Detection	53
13.2	Injection Attacks Detection	54
13.3	Security & Biometric Evaluations	56
13.4	Addressing threats to Identity Proofing	57
14	Use of AI in biometric verification	60
14.1	Deep Convolutional Neural Networks	60
14.2	Face Finder DCNN	61
14.3	Liveness Detection DCNN	61
14.4	Face Match DCNN	62
14.5	DCNN Dataset	63
14.6	Bias	64
14.7	Manual Checks	64
15	Supervisory & Audits	66
15.1	Internal Audits	66
15.2	External Audits & Certifications	66
15.3	Supervisory	67
15.4	Topics of Audits	67
	Appendix A - Abbreviations & Definitions	68
	Appendix B – Identity Proofing Process	72
	Appendix C – Supported Identity Documents	73
	European Union	73
	Europe (non-European Union)	76
	Africa	78
	Middle East	81
	South Asia	82
	Asia	83
	Oceania	85
	American Continent	87
	Caribbean	89

Identity proofing is the process of confirming or in other words verifying that a person is who they claim to be, using the required degree of reliability methods.

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

ETSI TS 119 461 specifies the identity proofing and policy security criteria requirements for trust service components. The scope of ETSI TS 119 461 is to verify the identification of applicants seeking to enrol as Subscribers of a QTSP.

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 each using different methods to validate and verify identity:

- [1]** Identity Document validation and data verification – is the document genuine and is the data correct?
- [2]** Liveness detection – is an actual 'live' person performing the identity proofing?
- [3]** Face comparison – does the person on the identity document match the 'live' person performing the identity proofing?

In addition to identity proofing of natural persons, identity proofing of legal persons is also required. The two steps of identity proofing of a legal person are:

- [1]** Legal person validation and verification – Does the organisation (legal person) exist?
- [2]** Representation validation and verification – Is the natural person authorised to represent the legal person?

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

This document "Identity Proofing @ Digidentity" describes in detail the identity proofing processes for each context.

The complete document is available on request.

Send your inquiry to sales@digidentity.com or contact your account manager.