

Security

Risk @ Digidentity

Compliance

Policies & Controls

Title	Security, Risk & Compliance @ Digidentity – Policies & Controls
Date	6 December 2025
Author	Sander Remmerswaal
Version	2026-v1
Classification	Confidential

Revisions

Version	Date	Author	Changes Made (*)
2019-v1	12 April 2019	Sander Remmerswaal	Initial version
2020-v1	22 May 2020	Sander Remmerswaal	Updated standards
2021-v1	1 February 2021	Sander Remmerswaal	Added Digidentity & GDPR
2022-v1	20 January 2022	Sander Remmerswaal	Added operational security
2022-v2	8 April 2022	Sander Remmerswaal	Updated suppliers, updated policies
2024-v1	25 April 2024	Sander Remmerswaal	Full revision and update, included information based on security questionnaires
2025-v1	1 October 2025	Sander Remmerswaal	Full revision
2026-v1	6 December 2025	Sander Remmerswaal	Minor updates

(*) All changes are marked in grey highlight.

Contents

1	Digidentity.....	6
1.1	Statement from Management.....	8
1.2	History.....	9
1.3	Digidentity Timeline	10
1.4	Abbreviations & Definitions	10
2	Product Descriptions	11
2.1	Identity Proofing of Natural Person	11
2.2	Identity Proofing of Legal Person.....	11
2.3	eHerkenning	12
2.4	Qualified Electronic Signatures	12
2.5	Know-Your-Customer (KYC)	13
2.6	Outsourced Functions	13
2.7	Product Customisation	13
3	Information Security	14
3.1	Information Security Management System.....	14
3.2	Information Security Policy.....	14
4	Privacy @ Digidentity	15
4.1	Privacy Information Management System	15
4.2	Privacy Policy.....	15
4.3	Processing Personal Data on behalf of End-User (Data Subject)	16
4.4	Processing Personal Data on behalf of Controller.....	16
4.5	Processing of biometric data	16
4.6	Deletion of Personal Data.....	17
4.7	Data Subject Access Rights.....	17
4.8	Location of Processing	17
4.9	Processors	18
5	Business Continuity @ Digidentity.....	19
5.1	Business Continuity Management System	19
5.2	Business Continuity Policy	19
6	Quality @ Digidentity	20
6.1	Quality Management System.....	20
6.2	Quality Policy.....	20

7	Management System	21
7.1	Scope.....	21
7.2	Risk Management & Risk Treatment.....	21
7.3	Roles & Responsibilities.....	22
7.4	Policies & Procedures	24
7.5	Controls & Governance	25
7.6	Documentation Overview.....	25
7.7	Digidentity Publications	25
8	Organisational Controls.....	26
8.1	Operations	26
8.2	Change & Release Management.....	26
8.3	Asset Management	27
8.4	Incident Management	28
8.5	Supplier & Supply Chain Management	30
8.6	Human Resource Security.....	32
8.7	Acceptable Use	33
8.8	Security & Privacy Awareness.....	34
8.9	Compliance.....	34
9	Technical Controls	35
9.1	Product & System Overview.....	35
9.2	Access Management.....	35
9.3	Configuration Management.....	37
9.4	Data Management	38
9.5	Data Protection.....	40
9.6	Network Security	42
9.7	Cryptographic Controls & Encryption.....	44
9.8	Cloud	46
9.9	Threat & Vulnerability Management	46
9.10	Logging, Monitoring & Alerting	48
9.11	Physical Security.....	50
9.12	System Maintenance	51
10	Development.....	52
10.1	Software Development Lifecycle	52
10.2	Security in Development	53
10.3	Software Testing & Quality Assurance.....	55
10.4	API Security	56

11	Digidentity Wallet - Mobile Device Security	58
11.1	Application Protection	58
11.2	Data Protection	61
11.3	Communication Protection	62
11.4	Presentation Attacks	62
11.5	Man-in-the-middle Attacks, Eavesdropping or Hijacking	62
11.6	Additional controls	64
11.7	Penetration tests & Vulnerability Scans	67
11.8	Threat & Mitigation Summary	67
12	Business Resilience @ Digidentity	68
12.1	Business Continuity Plan	68
12.2	Crisis Management Plan	68
12.3	High Availability	69
12.4	Backup & Restore	69
12.5	Recovery Time Objectives & Recovery Point Objectives (RTO & RPO)	70
12.6	Disaster Recovery	70
12.7	Business Continuity Tests	70
13	Compliance	71
13.1	Standards, Schemes & Regulations	71
13.2	Laws & Regulations	72
13.3	eIDAS - EU Regulation 910/2014 – Electronic Identification & Trust Services	72
13.4	Directive (EU) 2022/2555 - Measures for a High Common Level of Cybersecurity (NIS2)	73
13.5	Regulation (EU) 2022/2554 - Digital Operational Resilience (DORA)	74
13.6	Contractual requirements (DORA)	76
13.7	AI Act - EU Regulation 2024/1689 – Artificial Intelligence Act (AIA)	77
13.8	Other Assurance Statements (Digidentity does not have)	78
14	Supervisory, Audits & Penetration Tests	79
14.1	Internal Audits	79
14.2	External Audits & Certifications	79
14.3	Supervisory Bodies	80
14.4	Topics of Audits	80
14.5	Penetration Testing	81
14.6	Resolving Non-Conformities	82
	Appendix A - Abbreviations & Definitions	83
	Appendix B - System & Network Diagram	87
	Appendix C - Organisational Chart	88
	Appendix D – Documentation Overview	89
	Appendix E – Regulations & Standard	90

Digidentity B.V. was founded in 2008 by Marcel Wendt and has since developed into a leading provider of secure, self-service digital identity solutions. In the same year, the company's digital identity platform was introduced in collaboration with the Dutch government through DigiD, facilitating secure online communication between citizens, organisations, and public authorities. Building on this success, Digidentity expanded its services in 2009 with the launch of eHerkenning, enabling trusted digital access for organisations interacting with government institutions.

In 2015, Digidentity expanded to the United Kingdom as digital identity provider for the GOV.UK Verify programme, Digidentity also delivered the identity platform for the Post Office.

Digidentity is a Qualified Trust Service Provider and Identity Provider as defined in the EU Regulation 910/2014 (eIDAS). Digidentity, as part of the Dutch eID system, has been notified against eIDAS to provide digital identities throughout the European Union as well as electronic certificates for qualified, and advanced digital signatures and qualified seals for our electronic signature products.

Digidentity develops products focused on a unique digital identity, where the user and their privacy are key. We currently operate in several countries providing national digital identity solutions to the Dutch governments, as well as solutions for a large variety of international organisations. Our technology supplies digital identities and identity proofing products such as Know-Your-Customer (KYC) to more than 20 million people across 190 different nationalities. Digidentity provides more than 300 million secure online transactions per year between people, organisations, and governments.

This document describes policies, procedures and controls that Digidentity has implemented to protect our business, products, and data (both personal data as well as business data). Based on risk, experience, and industry standards, we have implemented a multi-layer security model that meets the highest security requirements for our industry.

The complete document is available on request.

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