Digidentity

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.

06 Dec 2025
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Digidentity

Contents

1 Digidentity 6

1.1 Statement from Management 6
1.2 History 7
1.3 Digidentity Timeline 8
1.4 Abbreviations & Definitions 8

2 Product Descriptions 9

2.1 Identity Proofing of Natural Person 9
2.2 Identity Proofing of Legal Person 9
2.3 eHerkenning 10
2.4 Qualified Electronic Signatures 10
2.5 Know-Your-Customer (KYC) 11
2.6 Outsourced Functions 11
2.7 Product Customisation 11

3 Information Security 12

3.1 Information Security Management System 12
3.2 Information Security Policy 12

4 Privacy @ Digidentity 13

4.1 Privacy Information Management System 13
4.2 Privacy Policy 13
4.3 Processing Personal Data on behalf of End-User (Data Subject) 14
4.4 Processing Personal Data on behalf of Controller 14
4.5 Processing of biometric data 14
4.6 Deletion of Personal Data 15
4.7 Data Subject Access Rights 15
4.8 Location of Processing 15
4.9 Processors 16

5 Business Continuity @ Digidentity 17

5.1 Business Continuity Management System 17
5.2 Business Continuity Policy 17

6 Quality @ Digidentity 18

6.1 Quality Management System 18
6.2 Quality Policy 18

7 Management System 19
7.1 Scope 19
7.2 Risk Management & Risk Treatment 19
7.3 Roles & Responsibilities 20
7.4 Policies & Procedures 22
7.5 Controls & Governance 23
7.6 Documentation Overview 23
7.7 Digidentity Publications 23

8 Organisational Controls 24
8.1 Operations 24
8.2 Change & Release Management 24
8.3 Asset Management 25
8.4 Incident Management 26
8.5 Supplier & Supply Chain Management 28
8.6 Human Resource Security 30
8.7 Acceptable Use 31
8.8 Security & Privacy Awareness 32
8.9 Compliance 32

9 Technical Controls 33
9.1 Product & System Overview 33
9.2 Access Management 33
9.3 Configuration Management 35
9.4 Data Management 36
9.5 Data Protection 38
9.6 Network Security 40
9.7 Cryptographic Controls & Encryption 42
9.8 Cloud 44
9.9 Threat & Vulnerability Management 44
9.10 Logging, Monitoring & Alerting 46
9.11 Physical Security 48
9.12 System Maintenance 49

10 Development 50
10.1 Software Development Lifecycle 50
10.2 Security in Development 51
10.3 Software Testing & Quality Assurance 53
10.4 API Security 54

11 Digidentity Wallet - Mobile Device Security 56
11.1 Application Protection 56
11.2 Data Protection 59
11.3 Communication Protection 60
11.4 Presentation Attacks 60
11.5 Man-in-the-middle Attacks, Eavesdropping or Hijacking 60
11.6 Additional controls 62
11.7 Penetration tests & Vulnerability Scans 65
11.8 Threat & Mitigation Summary 65

12 Business Resilience @ Digidentity 66
12.1 Business Continuity Plan 66
12.2 Crisis Management Plan 66
12.3 High Availability 67
12.4 Backup & Restore 67
12.5 Recovery Time Objectives & Recovery Point Objectives (RTO & RPO) 68
12.6 Disaster Recovery 68
12.7 Business Continuity Tests 68

13 Compliance 69
13.1 Standards, Schemes & Regulations 69
13.2 Laws & Regulations 70
13.3 eIDAS - EU Regulation 910/2014 – Electronic Identification & Trust Services 70
13.4 Directive (EU) 2022/2555 - Measures for a High Common Level of Cybersecurity (NIS2) 71
13.5 Regulation (EU) 2022/2554 - Digital Operational Resilience (DORA) 72
13.6 Contractual requirements (DORA) 74
13.7 AI Act - EU Regulation 2024/1689 – Artificial Intelligence Act (AIA) 75
13.8 Other Assurance Statements (Digidentity does not have) 76

14 Supervisory, Audits & Penetration Tests 77
14.1 Internal Audits 77
14.2 External Audits & Certifications 77
14.3 Supervisory Bodies 78
14.4 Topics of Audits 78
14.5 Penetration Testing 79
14.6 Resolving Non-Conformities 80

Appendix A - Abbreviations & Definitions 81
Appendix B - System & Network Diagram 85
Appendix C - Organisational Chart 86
Appendix D – Documentation Overview 87
Appendix E – Regulations & Standard 88

1 Digidentity

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.

1.1 Statement from Management

Digidentity is an international company, providing qualified trust services and digital identities to individuals, organisations and governments. To provide qualified trusted services to our customers, we are committed to information security, privacy, quality and compliance to applicable laws and regulation.

Digidentity is therefore committed to protecting data including personal data and customer data and supporting information technology to make sure that the confidentiality, integrity and availability of these assets are maintained.

To ensure the quality, continuity, integrity, and availability of our products, all appropriate measures will be taken to meet our customer needs in every aspect of the business.

Digidentity will establish, implement, operate, monitor, review, maintain and continually improve the Security, Privacy, Quality, and Business Continuity within the context of the organisation's overall business activities and the risks it faces. The management system includes and should reflect the organisational structure, culture, policies, planning activities, responsibilities, practices, procedures, processes and resources necessary to successfully execute this policy.

Management of Digidentity

Fred Slikker
Marcel Wendt

1.2 History

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.

Digidentity is the technical market leader in Europe. In the Netherlands, Digidentity is officially recognised by the Dutch government as a broker and supplier of eHerkenning (Dutch Trust Framework). In the United Kingdom, we are certified to provide identification for Right to Work, Right to Rent and Disclosure and Barring Service within the UK's Digital Identity and Attributes Trust Framework. Digidentity is the authentication service (Trust Center) for SERMI (standardised access to security-related vehicle Repair & Maintenance Information - RMI). Our software performed 300 million authentications and protected the digital identity of more than 17 million people.

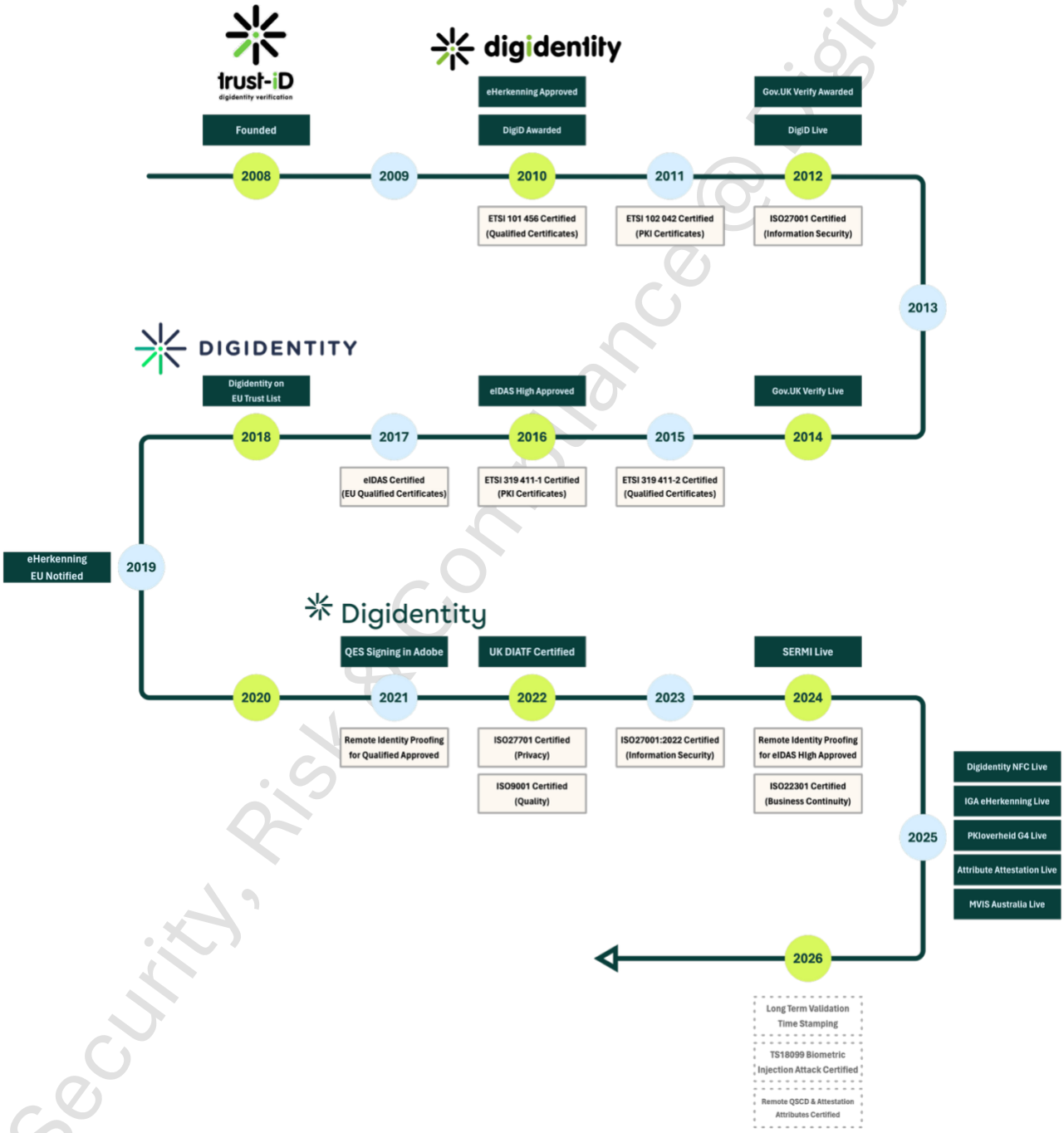
Digidentity is part of the EU Digital Identity Wallet Consortium (EWC) together with 41 partners and 28 associated partners from the EU. This consortium is working on the development of a digital wallet based on the requirements of the European Commission. The EU Wallet is one of the new services defined in eIDAS.

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.

Security is never a 100% absolute guarantee as this is impossible to realise and maintain. Digidentity has found a balance in providing an efficient user experience with the highest level of security to protect the digital identity of our customers.

1.3 Digidentity Timeline

The timeline of Digidentity's milestones:



1.4 Abbreviations & Definitions

See Appendix A - Abbreviations & Definitions for the table with abbreviations and definitions.

2 Product Descriptions

Digidentity delivers standard products for authentication and electronic signatures such as eHerkenning and Qualified Electronic Signatures (QES). All products comply with the applicable requirements necessary for the provisioning of these products. Digidentity cannot implement customer specific requirements for these standard products as this may violate the applicable requirements.

2.1 Identity Proofing of Natural Person

Digidentity verifies the identity of each registrant by checking a valid identity document (ID). We use the personal data from the ID (authoritative source) to confirm the end-users identity. The use of an official document is required. Subsequently, the user is asked to take selfies to ensure an actual person is registering. The selfie is then compared with the photo on the ID to bind the person to the identity document.

These steps answer the questions:

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

A detailed description of our identity proofing process is available in our Identity Proofing Practice Statement (document “Identity Proofing @ Digidentity”)

All our products are based on the Identity Proofing product.

2.2 Identity Proofing of Legal Person

For any product involving the identity of a legal person, Digidentity is required to verify the legal person itself as well as all authorised legal representatives.

The end-user provides the organisation registration number from an authentic source (National Trade Registers). Digidentity verifies the existence of Digidentity verifies the existence of the organisation using this source and confirms whether the end-user is authorised to act on behalf of the organisation by checking the registered legal representatives. If the end-user is not registered as a legal representative, they must obtain authorisation from one or more legal representatives. Once the legal representative(s) approve the authorisation, the product is issued to the end-user.

In the Netherlands, the National Trade Register serves as the authentic source. For company registers in other countries, we rely on our supplier Kyckr to provide organisation details.

An authentic source means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice (definition from Regulation EU 910/2014, Article 3(47)).

2.3 eHerkenning

eHerkenning is the identity and access system of the Dutch government to allow organisations to access government services such as tax office or justice department (known as Service Providers).

The requirements for eHerkenning are defines in the Dutch Trust Framework (Dutch: Afsprakenstelsel Elektronische Toegangsdiensten - eTD). These requirements are published on: https://afsprakenstelsel.etoegang.nl/Startpagina/v3/?l=nl

Only organisations that have been notified in the European Union by the Dutch Ministry of Economic Affairs (EZ) are allowed to issue authentication services for eHerkenning. Participants of the Dutch Trust Framework as Digidentity must comply to the requirements set by the Dutch government and are annually inspected by the supervisory body, the Dutch Authority for Digital Infrastructure (Dutch: Rijksinspectie Digitale Infrastructuur - RDI). Participants that successfully pass government inspections, are authorised to provide digital identities and authentication services.

Digidentity is one of the official participants (Deelnemers) of eHerkenning. We offer authentication products that enables access to Service Providers. as well as broker products (connecting Service Providers to eHerkenning).

First, the end-user 's identity is verified using our Identity Proofing product. Secondly, Digidentity verifies the organisation and whether the end-user is authorised to act on behalf of the organisation. This is achieved through the identity proofing of a legal person.

Digidentity is responsible for the authentication of the end-user. Any disruption at the Service Providers in eHerkenning is out of scope of our product.

Digidentity has documented how eHerkenning works (document: eHerkenning @ Digidentity) which is available on our website: https://www.digidentity.eu/documentation

Digidentity provides an authentication product (Dutch: middel) within the eHerkenning framework. This allows end-users to log into government services or insurance services on behalf of their organisation. The product consists of two parts; first identity proofing, authorisation and issuance i.e. verifying the Applicant and their authority to act on behalf of the organisation. Second, use of the authentication product (enabling secure access to connected Service Providers).

2.4 Qualified Electronic Signatures

Qualified Electronic Signatures and Qualified Electronic Seals are a Qualified Trust Service under EU Regulation 910/2014 (eIDAS). In accordance with this regulation, Digidentity issues qualified electronic certificates that enable the use of both electronic signatures and seals.

For Qualified Electronic Signatures (QES), we start with the identity proofing of the user (natural person). The identity proofing must be at eIDAS level High. After the identity is verified, we issue the qualified certificate to the Digidentity wallet on the mobile phone of the user. The user can digitally sign documents with the QES.

For Qualified Electronic Seal (QESe), after the identity proofing of the natural person, Digidentity verifies the organisation and if the end-user is allowed to act on behalf of the organisation using the identity proofing of a legal person process.

In 2026, Digidentity will add Long Term Validation and Time Stamping to our eSGN platform. We are also investigating the Trust Service of Preservation and Validation of Qualified Certificates to extend our signing platform.

2.5 Know-Your-Customer (KYC)

With our KYC product, the result of the identity proofing is an Identity Verification Report of the identity of the user. The Identity Verification Report contains the identity evidence provided and the results of the validation and verification steps.

The Identity Verification Report is available for download for a period of three days. Digidentity deletes the identity evidence and report after 72 hours erasing all data, both personal data and non-personal data from our systems.

2.6 Outsourced Functions

Digidentity has outsourced parts of the product to external service providers. A list of service providers used, is documented in our Privacy Statement available on our website: https://www.digidentity.eu/documentation

Digidentity delivers standard products for millions of customers. Supplier selection follows a defined process based on risk and will be reported to our supervisory body and external auditor. Digidentity will inform customers but will not ask for permission to change a supplier. With millions of customers, it is impossible to obtain approval from all customers. This would interfere with our business and competitive advantage.

2.7 Product Customisation

Digidentity provides standard products for Identity Proofing, eHerkenning and QES. These products are aligned with the applicable requirements from the Dutch Trust Framework (eHerkenning) and EU Regulation 910/2014 (eIDAS) for QES.

To ensure compliance with these regulatory frameworks Digidentity does not support customisation of these products as this would jeopardise compliance to the requirements.

However, Digidentity does allow customisation within identity proofing process. Additional validation and verification steps may be integrated to support the use of further identity evidence, while maintaining compliance with the relevant standards.

3 Information Security

Digidentity is an international company, providing qualified trust services and digital identities to individuals, organisations and governments. To deliver the products to our customers, information security and compliance to laws and regulation are fundamental to our operations.

Digidentity is therefore committed to protecting all data, including personal data and customer data and supporting information technology that ensure the confidentiality, integrity and availability of these assets are maintained.

To guarantee the continuity, security, and availability of our services and resources, Digidentity will take all appropriate technical, organisational, and procedural measures to safeguard the privacy and integrity of data assets in line with recognised standards and regulatory requirements

3.1 Information Security Management System

Digidentity has implemented and maintains an Information Security Management System (ISMS) based on requirements in ISO27001:2022. The ISMS is established to control risks regarding data and systems that process this data. The scope of the management is defined in section 7.

3.2 Information Security Policy

Information Security Policy requirements are documented in ISO27001:2022 - Section 5.2 & Annex A.5.1-5.6 and ETSI EN 319 401 - REQ5.03

The management system includes and should reflect the organisational structure, culture, policies, planning activities, responsibilities, practices, procedures, processes and resources necessary to successfully execute this policy.

Digidentity establishes information security based on the principles:

- Risk-based: controls are based on risks to data and systems
- Everyone: is responsible for correct and secure use of assets and authorisations
- Always: security is in Digidentity's DNA
- Security by Design: security is a starting point of every change and project
- Security by Default: all systems are secure, and access is allowed on necessity

4 Privacy @ Digidentity

Digidentity processes personal data of end-users and customers to deliver our identity proofing, electronic identities and trust services as digital signature products. All personal data collected by Digidentity and the lawful basis of processing is described in the public Privacy Statement available on our corporate website (https://www.digidentity.eu/documentation).

Digidentity has appointed a Data Protection Officer responsible for protection of personal data and compliance with GDPR. The Data Protection Officer reports directly to the CEO of Digidentity.

4.1 Privacy Information Management System

Digidentity has implemented and maintains a Privacy Information Management System (PIMS) based on ISO27701:2019. The PIMS is designed to manage risks related to personal data and systems that process this data. The scope of the management is defined in section 7.

4.2 Privacy Policy

In addition to our Information Security policy, Digidentity has a documented Privacy Policy to ensure that appropriate controls are implemented to protect personal data.

Digidentity establishes privacy or protection of personal data based on the principles:

- End-user is the owner of their own data
- Privacy by Design: privacy is built into our systems and the starting point of every change and project
- Privacy by Default: all personal data is secure, and access is only allowed on necessity
- Data minimalisation: only process data that is needed for the defined purpose, delete data that is no longer required
- Process only verified personal data

Digidentity performs Data Privacy Impact Analysis (DPIA) on processing of personal data when significant changes to the processing of personal data is involved. We maintain a centralised register of processing activities.

Privacy by Design aims to integrate privacy as the “default mode of operation”. The concept can be applied to all kinds of systems, such as IT systems, apps, business practices and network infrastructure.

4.3 Processing Personal Data on behalf of End-User (Data Subject)

Digidentity offers products where each individual Applicant (after identity proofing the Applicant becomes the Subscriber) accepts the Terms & Conditions and agrees with the Privacy Statement personally when creating an account. The Applicant consents to processing of photos (ID and selfies - biometric data) when uploading identity evidence. Digidentity acts as a data controller, as defined in the GDPR, and processes personal data of the account holder. The Subscriber has access to the account and is authorised to execute all rights such as viewing, modifying, and deleting personal data themselves (see Section 4.7). The Subscriber can use the account to acquire products for personal use and products for business use.

When the Subscriber is an employee of an organisation, the Subscriber can use the personal account/identity to acquire products related to an organisation. The Subscriber enters the business registration number of the organisation or a coupon code indicating that the invoice must be sent to the organisation. The organisation can authorise the Subscriber to act on behalf of the organisation. The Subscriber is in control of the account; the organisation is in control of the authorisations.

Digidentity does not process personal data on behalf of the organisation and does not receive personal data from the organisation for such processing. Digidentity defines the purpose for processing as the execution of contract for a digital identity or signature. Since is no processing is carried out on behalf of an organisation, a data processing agreement is not required.

4.4 Processing Personal Data on behalf of Controller

Digidentity offers Know-Your-Customer (KYC) products where Digidentity acts as the processor on behalf of a controller (the Organisation). These products follow the "Verify & Delete" principle where Digidentity performs identity proofing of individuals for the controller. This is done by validating and verifying the identity of the individual. We provide an identity verification report containing the required personal data to the controller. After the controller receives the identity verification report, Digidentity immediately deletes all personal data of the individual.

4.5 Processing of biometric data

In accordance with Article 9, sub 1 of GDPR, biometric data for the purpose of uniquely identifying a natural persons fall in the special category of personal data.

Digidentity processes biometric data (photos) of Applicants when they are registering for a product.
As part of the identity proofing process, the Applicant must submit identity evidence to complete their registration. This evidence consists of photos of front and back of identity documents and selfies of the Applicant.

In compliance with GDPR article 9 sub 2a, Digidentity asks explicit consent from the Applicant to process their biometric data. When the Applicant creates an account, the Terms & Conditions, Privacy Statement must be accepted as well as consent given to process biometric data (photos).

The explicit consent is registered in the account of the Applicant. If the Applicant does not give explicit consent, registration for a product is not possible as Digidentity is not able to perform the identification. The Applicant can revoke their consent by deleting their account.

4.6 Deletion of Personal Data

Subscribers are in control of their own data. By deleting their account and all associated personal information, the Subscribers can exercise their right to be forgotten.

For customers that use our KYC product, all personal data of their Applicants is deleted after the identity verification report is received.

Our personal data deletion rules are documented in our Privacy Statement on our corporate website: https://www.digidentity.eu/documentation

4.7 Data Subject Access Rights

Data Subject Access Rights are described in GDPR articles 15-22.

Digidentity has implemented controls to allow data subject to execute their access rights as defined in GDPR. See document "Data Subject Access Rights @ Digidentity" on our corporate website.
https://www.digidentity.eu/documentation

4.8 Location of Processing

Digidentity processes all personal data in the European Economic Area (EEA) and the United Kingdom (UK). All sub-processors (suppliers) must process personal data in the UK and the EEA. Personal data can be processed in the customer's preferred location.

Digidentity uses the processing capacity of Amazon Web Services (AWS). Digidentity has complete authority over the configuration and management of the systems in AWS. AWS does not have access to these systems and the data these systems hold. Our access management ensures that only authorised employees have access to the systems and data. Accessing data is logged and monitored. Digidentity uses regional settings to make the data inaccessible outside the EEA.

All locations for processing personal data are described in the public Privacy Statement available on our corporate website (https://www.digidentity.eu/documentation).

4.9 Processors

Digidentity has contracted suppliers to perform specific processes. Digidentity has Data Processor Agreements (DPA) with all suppliers that process personal data on our behalf. Digidentity requires all processors to obtain and maintain accredited ISO27001 certification. All suppliers and their sub-processors are required to process personal data within the EEA or UK. For our MVIS products in Australia, we process the data in Australia, the Netherlands, Germany and the UK.

Activity	Organisation	Location Data Processing
Production systems - Europe	Amazon Web Services (AWS)	Ireland, Germany
Production systems - MVIS	Amazon Web Services (AWS)	Australia
Liveness detection & Face Comparison	BioID	Germany, Netherlands
Certificate Authority systems	North-C (Data Centers)	Netherlands
Validation of identity documents (optical) - EU	DataChecker	Netherlands
Validation of identity documents (optical) - MVIS	Onfido	United Kingdom
Verification of addresses (UK addresses)	Onfido	United Kingdom
Identity Fraud Check (UK)	CIFAS	United Kingdom
Politically Exposed Person (PEPs) & Sanctions	Ardent	United Kingdom

5 Business Continuity @ Digidentity

Digidentity is committed to providing the best possible experience to its customers and the best possible relationships with employees, shareholders and suppliers. To ensure the consistent availability and delivery of its products, Digidentity has developed the following Business Continuity policy in support of a comprehensive program for Business Continuity, Disaster Recovery and overall business survivability.

Digidentity, like any other firm, is exposed to potential risks that could disrupt or destroy critical business functions and/or the production and delivery of Digidentity's products. The strategy for the continuation of business in the event of an incident, is to ensure the safety and security of all employees, and to continue critical business functions, production and delivery of products from predefined alternative sites.

5.1 Business Continuity Management System

Digidentity has implemented and maintains a Business Continuity Management System (BCMS) based on ISO22301:2019. The BCMS is established to control risks regarding business continuity, disaster recovery and overall business resilience. The scope of the management is defined in section 7.

5.2 Business Continuity Policy

Digidentity has a Business Continuity Policy to ensure that a framework of systems and processes are implemented to set continuity objectives. The Business Continuity Policy is to ensure that a framework of controls is implemented to ensure the continuity of business processes and products.

Digidentity establishes a framework for business continuity based on the principles:

- Resilient by Design – plan for failure as part of normal operations
- Continuity by Design – redundancy, fail over, recovery
- Adaptability by Design – flexibility to scale workload
- Safeguard employees, clients, and stakeholders
- Protect critical business functions and operations
- Ensure timely and effective communication
- Minimise financial losses and reputational damage
- Enable the recovery of business operations as soon as possible

Any local law that supersedes this policy should be respected.

It also applies to the management of the supply chain and requires those negotiating contracts to ensure appropriate Business Continuity and Information Security measures are included in contracts, where possible, so that the supplier is able to deliver acceptable levels of service.

6 Quality @ Digidentity

Digidentity has established a framework of controls, policies, and standards, as laid out in the Quality Management Systems (ISO: 9001:2015) to monitor and improve the quality of our products.

6.1 Quality Management System

The Quality Management System (QMS) of Digidentity is certified against the requirements in the international standard ISO9001:2015 by DNV in the Netherlands. The scope of the management is defined in section 7.

6.2 Quality Policy

Digidentity has a Quality Policy to ensure that a framework of systems and processes are implemented to set quality objectives. This policy outlines a set of standards for all Digidentity employees to follow in order to preserve and enhance the quality of the products delivered while improving customer satisfaction and experience.

The Quality Policy ensures that a framework of controls is implemented to manage quality by:

- Build a mutually profitable relationship with our corporate customers, ensuring their long-term success
- Achieve our objectives for quality, cost, and planning
- Enhance the systematic research and use of best preventive practices at all levels and ensure reliable risk management
- Drive continual improvement and innovation based upon efficient business processes, well-defined measurements, best practices, and customer surveys
- Develop employee competencies, creativity, and accountability through appropriate development programs and show strong management involvement and commitment

All Digidentity employees are responsible for the quality of their own work. Digidentity provides training and has established systems to assist all personnel to achieve the standards required. Only by providing an outstanding service and product quality will we achieve our aims of long-term success and sustained improvements.

7 Management System

Digidentity has implemented, maintains and improves a management system for information security (ISMS), privacy information (PIMS), quality (QMS) and business continuity (BCMS).

7.1 Scope

The scope of the management system is defined as:

Processing (validation, verification and issuance of) data of natural and legal persons to deliver digital identities, Wallet, electronic signing services, and attribute attestation. Register, generate, disseminate, revoke and provision digital certificates and develop and manage broker identity services as defined by management and in accordance with the Statement of Applicability version 2025-v1, dated 1 July 2025.

7.2 Risk Management & Risk Treatment

Risk Management requirements are documented in ISO27001:2022 - Section 8 and ETSI EN 319 401 - Section 5.

Risk Management is an integral part of Digidentity's the strategic management. The risk management process is designed to identify potential threats and vulnerabilities that may affect the business, and to manage risk within the risk appetite.

The objective of performing risk management is to:

[1] Make a conscious effort towards securing and managing the organisation's information assets, both from external and internal threat sources

[2] To ensure there is a common, consistent and unambiguous understanding of information risks, assets, threats, vulnerabilities and mitigating controls

[3] Keep the management informed, and to closely track or monitor the information risks which prevail within the organisation's environment

[4] Assist management to make well-informed risk management decisions, and to allocate the desired level of resources in mitigating those information risks which have been identified

Risk management is a continuous process that should be reviewed at least annually, or whenever significant changes occur within the organisation or its processes. Digidentity ensures that all risk assessments are properly documented.

The risk assessment method is based on the ISO 27005:2022 standard. Risk Management is the process of identifying threats and vulnerabilities, evaluating and assessing the risks, and taking the necessary steps to reduce the risks to an acceptable level. Digidentity conducts risk assessments at least annually to account for changes in the context of the organisation, changes in security requirements and overall risk landscape. Risk assessment involves threat and vulnerability identification, risk analysis, and risk evaluation.

After determining the threat and vulnerabilities, the risk can be defined. The steps of the risk analysis are:

[1] List all information security-related assets relevant to information security, the associated threats, vulnerabilities, and consequences (in terms of confidentiality, integrity, and availability)
[2] Estimate the impact of the risk
[3] Estimate the likelihood of the risk
[4] Calculate the qualitative risk based on the formula: Risk Level = Impact x Likelihood
[5] Assess the effectiveness of current controls
[6] Identifying implemented controls and their effect on either Impact or Likelihood or both

A list of incident scenarios along with their potential impact on assets and business processes and their likelihood of occurrence should be assessed. Risk analysis assigns values to the likelihood and the impact of a risk providing a structured evaluation based on the assessments.

The objective of identifying the existing safeguards or controls within the information processing environment is to correctly assess whether a given threat source may impact the organisation. For the effectiveness, it is important to consider that the controls are in line with the standards and that these controls are operating effectively. These controls are not limited to just technical controls, but also include organisational controls, such as policies, procedures and guidelines.

Risks that cannot be accepted are treated to reduce them to an acceptable level. Based on the assessed risk value, the risk level determines whether a risk can be accepted, requires treatment, or needs a management decision regarding acceptance or mitigation.

The risk assessment is documented, and all risks are registered in a risk register.

7.3 Roles & Responsibilities

Roles and responsibilities requirements are documented in ISO27001:2022 - Section 8 and ETSI EN 319 401 - REQ-7.2-06.

To support the Management System, Digidentity has defined the roles and responsibilities.

7.3.1 Management

Management holds overall responsibility for the management system. It maintains a customer focus approach ensuring that the customer requirements, as well as all applicable laws and regulations are identified, understood and met. Management shall support, facilitate, and promote information security, privacy, and quality. It is responsible for approving all policies, and risk assessment, accepting residual risk, approving important changes and improvements to the overall security, business continuity and quality of the products of Digidentity.

7.3.2 Chief Security Officer

The Chief Security Officer (CSO) is responsible for the maintenance of the ISMS and information security for Digidentity.

7.3.3 Quality Manager

The Quality Manager (QM) is responsible for ensuring that the products delivered by Digidentity are continuously improving and of excellent quality. The QM promotes a customer-oriented approach to make sure the focus on enhancing customer satisfaction is maintained.

7.3.4 Data Protection Officer

The Data Protection Officer (DPO) is responsible for the maintenance of the PIMS, the security and compliance regarding processing of personal data by Digidentity and subcontractors acting on behalf of Digidentity. The DPO handles personal data breach incidents.

7.3.5 Business Continuity Manager

The Business Continuity Manager (BCM) leads the development, maintenance, training, testing and execution of the Business Continuity Plan.

7.3.6 Security, Risk & Compliance

Security, Risk & Compliance (SRC) is responsible for the monitoring of security, risk, compliance and quality assurance within Digidentity. This responsibility includes security support, business continuity management and disaster recovery, security training, risk management and security incident management.

SRC is the contact for all employees regarding security and compliance. SRC provides a quality assurance role to make sure policies, procedures and general documentation meet the requirements of the organisation.

7.3.7 Service Delivery Manager

The Service Delivery Manager (SDM) monitors the overall performance of service-related processes and manages the service desk to ensure that an optimal level of support is maintained. The SDM assesses and enhances the customer satisfaction.

7.3.8 Service Desk Quality Assurance

Service Desk Quality Assurance (SDQA) is responsible for monitoring and improving the quality of the Service Desk. SDQA aims to observe every agent across all support channels. A feedback meeting is held to assess every agent's performance, covering areas of improvements and competencies. This is an indicator of general performance. There are separate QAs for the Dutch and English Service Desk.

7.3.9 Software Quality Assurance

Software Quality Assurance (SQA) is responsible for evaluating whether a certain item has met the business requirements and achieved the opportune level of quality to be released into production. Throughout the software development cycle, SQA refines and plans items with the team; writes and performs (regression) tests and maintains the related documentation.

7.3.10 Customer Success

Customer Success (CS) is accountable for building trust with key stakeholders and customers. CS anticipates challenges and participates in the risk mitigation process to answer issues and provide effective solutions to customers. CS thus, contributes to improving components of the overall experience of the customer.

7.3.11 Employees

Employees are responsible to comply to Digidentity policies and procedures. They are required to participate in security, privacy, quality and business continuity training from Digidentity. Employees must always consider security, privacy and quality of their work.

See Appendix C - Organisational Chart for the Digidentity organisation structure.

7.4 Policies & Procedures

Digidentity has documented policies and procedures covering information security, privacy, quality, cloud, and business continuity. Each policy has an assigned owner and is reviewed at least annually, as well as whenever significant changes occur. All policies are approved by Management prior to publication.

Digidentity adheres to the principle of "comply or explain". Exceptions to any policy must be requested in writing with a clear business justification. All exceptions must be approved by management.

Any wilful breach of any policy, supporting policies and procedures could be subject to disciplinary processes and procedures that could result in sanctions including first warning up to and including dismissal and legal actions.

Policies and procedures are available for:

- Access & Authorisation Management (Section 9.2)
- Acceptable Use Policy (Section 8.7)
- Asset Management (Section 8.3)
- Backup & Restore Policy (Section 12.1)
- Business Continuity (Section 12)
- Change Management (Section 8.2)
- Cloud Policy (Section 9.8)
- Cryptography Policy (Section 0)
- Cyber Security (Section 9.9)
- Data Management & Protection (Section 0)
- Human Resource Security (Section 8.6)
- Incident Management (Section 8.4)
- Network Security (Section 9.6)
- Physical Security (Section 9.11)
- Privacy & Data Protection (Section 4)
- Quality Policy (Section 6)
- Secure Development Policy (Section 10)
- Supplier Management (Section 8.5)

7.5 Controls & Governance

Digidentity has implemented technical and organisational controls to protect personal data of customers. In case of an incident, the account holder will be informed. Digidentity is audited annually by independent auditors and government supervisory bodies to verify compliance to GDPR.

Digidentity protects personal data and has implemented a management system for security and privacy which has been certified against ISO27001:2022, ISO27017:2015, ISO27018:2019 and ISO27701:2019. See Section 13 for detailed description of our certificates.

Our certificates are available on our corporate website https://www.digidentity.eu/certifications.

7.6 Documentation Overview

An overview of our documentation is available in Appendix D – Documentation .

7.7 Digidentity Publications

Digidentity has published several documents related to our products and technology.

Title Document	Description
Identity Proofing @ Digidentity	describes how Digidentity verifies your identity
eSignatures @ Digidentity	describes the difference between digital and electronic signatures and the legal value of the signature
eSignatures FAQ @ Digidentity	answers question about electronic signatures
eHerkenning @ Digidentity (in Dutch)	describes the Dutch Trust Framework for organisations

These documents are available on our corporate website: https://www.digidentity.eu/documentation or available on request.

8 Organisational Controls

8.1 Operations

Operations requirements are documented in ISO27001:2022 - Annex A8, and ETSI EN 319 401 - Section 7.7.

The IT Operations team is responsible for the maintenance and organisation of the application platform. In accordance with. Change management procedure, all major changes are subject to review and require approval from the Change Advisory Board (CAB). Changes on the infrastructure in AWS, as well data centres are formalised due to the requirements of the certifications: changes need to be planned, documented and are audited.

The overall strategy of the IT Operations team is towards a Continuous Delivery. To achieve that, and to ensure traceability of changes, the majority of changes follow the principles of GitOps and infrastructure-as-code:

- Describe the entire system declaratively
- Version the canonical desired system state in Git
- Automatically apply approved changes to the desired state
- Ensure correctness and alert on divergence with software agents

Digidentity provides a real time dashboard on the status of our products https://ddy.statuspage.io/.

IT Operations and Security Team maintain an operational planning that encompasses all the activities required to maintain the management system. These activities consist of recurring (mandatory) tasks and processes such as document reviews, review of logging, internal audits, external audits, backup and restore tests, penetration tests, firewall reviews, access control reviews and other operational tasks.

8.2 Change & Release Management

Change Management requirements are documented in ISO27001:2022 - Annex A8.32 and ETSI EN 319 401 - Section 7.9).

Digidentity has implemented a change management process for changes to application code, network and systems. This process is designed to enable employees to adequately consider the impact of a change and the associated risks. The process provides guidelines for approval of changes.

The guidelines to identify these risks are the following:

[1] What is the issue?
[2] What is the proposed solution?
[3] What are the requirements for this change?
[4] What is the impact (time, security, legal) of the change?

All changes must be registered in the Digidentity ticketing system. The assessment of the change considers how the event could impact costs, schedule, criteria. As part of this process the documentations must be updated. The CAB evaluates and approves the release of major changes. Approval is documented in the applicable change ticket.

Emergency changes are used to restore disrupted products or repair a high priority incident immediately and must be communicated to the Emergency Change Advisory Board (ECAB) for approval.

Please note: Changes which require downtime on the customer's end are always considered as high impact.

All changes must be tested in the pre-production environment and reviewed before release to the production environment. Changes that have an effect on corporate customers are communicated in advance.

Release management within Digidentity is based on a two-week release cycle. At the beginning of the sprint, the acceptance criteria are defined. At the end of the sprint, a release scope meeting is held to validate the acceptance criteria. When the criteria are met, the tickets are approved in Jira.

8.3 Asset Management

Asset Management requirements are documented in ISO27001:2022 - Annex A5.9-5.13, A7.10-7.11, A8.1-8.5, and ETSI EN 319 401 - Section 7.3.

Digidentity maintains a register of all assets (both information assets and information processing assets) including a description, identification (e.g. serial number), owner and if applicable, risk classification.

The assets include, but are not limited to:

- Hardware (laptops, servers, printers, mobile phones)
- Software (licenses, applications)
- Cloud assets (computing instances)
- Data (databases, registrations, contracts, documents, procedures, log files)

Digidentity must ensure that both company data and customer data are used for defined purposes only. Data within Digidentity is classified in three categories, each with a specific handling policy. Personal data is processed to deliver the products to customers and maintain business operations. All personal data must be protected and handled according to the risk level.

The acceptable use of Digidentity assets (resources) are defined in the Acceptable Use Policy (see Section 8.7). This policy includes use of computer equipment, clean desk, working in the office, remotely, travelling or from home, internet, and social media behaviour.

Digidentity has implemented a device management system to manage company assets. The device management system continuously verifies operating system updates, enforces security settings, and notifies IT Operations of the use of unauthorised software.

Destruction of storage media containing confidential data is performed by specialised external companies under supervision of IT Operations. Evidence of destruction is retained.

Digidentity does not allow access to production systems and data from non-Digidentity devices. Access to production systems require VPN connectivity which is only installed on Digidentity-issued hardware. Digidentity also has the capability to remotely wipe company devices.

8.4 Incident Management

Incident Management requirements are documented in ISO27001:2022 - Annex A5.24-5.28, A6.8, and ETSI EN 319 401 - Section 7.9.

An Incident Management process is implemented to ensure an effective and consistent approach in the management, handling, recording and follow up of all incidents which occur within the business activities of Digidentity. The term “incident” is used to describe incidents which are related to products, data and information security.

In the case of an incident, Digidentity has a procedure which is to be followed by all employees, contractors or external parties working with the organisation. The framework for each incident consists of: Identification, reporting, classification, investigation and evaluation. Incident Managers have been appointed to handle and monitor incidents. If required, an escalation procedure is available to ensure timely resolution of the incident.

Digidentity recognises four types of incidents:

[1] Incident — an unplanned interruption to a service or reduction in the quality of a service

[2] Security Incident — an unwanted or unexpected security event that compromises the security of data or systems and weaken or impair business operations, causing damage.

[3] GDPR Incident — a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[4] Event — Something happened that should not have happened, but no damage occurred.

Incidents must be reported immediately upon detection. The individual that identifies the incident is required to complete the online Incident Registration Form to create a ticket and call one of the Incident Managers to inform them about the incident. The Incident Manager will classify the incident and inform the other Incident Managers. Depending on the type and classification, the relevant Incident Manager(s) will be assigned.

An incident ticket shall be registered for each P1 (Critical), P2 (Major) and P3 (Minor) incident and shall contain the following:

- Reporting (user) contact (phone) information
- Approximate date and time incident started
- Approximate date and time incident was detected
- The impact to the reporting organisation
- The follow up actions being requested at this time
- Description of the current status or resolution of the incident
- Evidence collected to analyse the incident
- Notification of customers and/or supervisory bodies as required and if applicable, time of notification
- Corrective actions taken, Root Cause Analysis and future actions/recommendations

The steps required for handling an incident are:

[1] Event detection
[2] Incident classification
[3] Immediate fix to resolve problem
[4] Communication
[5] Root Cause Analysis
[6] Resolution Plan
[7] Resolution Implementation
[8] Collection of Evidence
[9] Incident Reporting
[10] Incident Closure

For each incident or nonconformity, a resolution time is defined. The table below provides an overview of the resolution time.

Priority	Resolution Time
P1 Critical	Immediately
P2 Major	Within 60 days
P3 Minor	Within 120 days
P4 Event	Not Applicable

Digidentity has an incident management procedure implemented as required by applicable laws, regulations and standards. The incident management process is part of the annual inspections by the government as well the annual audits by an external auditor.

Resolution of incidents is documented in our Service Level Agreement.

8.5 Supplier & Supply Chain Management

Supplier Management requirements are documented in ISO27001:2022 - Annex A5.19-5.23, ISO27017:2015 – Clause 15, and ETSI EN 319 401 - REQ-7.14

Digidentity has multiple suppliers to support delivery of its products. Maintaining effective operational relationships with all suppliers is essential to ensure uninterrupted service levels to its customers. Suppliers are subject to a risk assessment covering security, privacy, continuity and quality.

The Supplier Management process allows Digidentity to manage the performance of its suppliers. During the contracting phase, requirements (technical, organisational, legal) are defined to make sure that Digidentity can fulfil its obligations to its customers as well as comply to applicable laws, regulations and standards.

Operational procedures include change management, incident management and performance management. Digidentity evaluates the performance of each supplier and discusses the performance on a regular basis.

Digidentity has defined requirements for suppliers. The objective of these requirements is to ensure that the supply chain of Digidentity's products is protected.

Digidentity reviews suppliers at least once per year or when significant changes occur, with all review evidence certifications documented.

8.5.1 General Requirements

Supplier must:

[1] forward Digidentity requirements to subcontractors that are part of the service or product delivered to Digidentity
[2] verify that subcontractors comply to the Digidentity requirements
[3] inform Digidentity on changes to the product or service provided

8.5.2 Security & Privacy Requirements

Supplier must:

[1] have an ISMS which is certified against the requirements from ISO27001:2022
[2] have an ISO27001 certificate that is under accreditation
[3] provide the ISO27001 Statement of Applicability in scope of the ISMS to Digidentity
[4] Supplier must inform Digidentity on changes to certification, scope of the ISMS and selected controls.
[5] Suppliers that process personal data on behalf of Digidentity are required to:
- **[a]** store personal data of Digidentity in the EEA or UK and not export data outside the EEA or UK
- **[b]** ensure that personal data is only accessed and processed from within the EEA or UK
- **[c]** delete personal data within 28 days after processing
- **[d]** implement data protection measures to protect personal data
- **[e]** implement multi-factor authentication (MFA) to access personal data
- **[f]** do NOT make backups of personal data

[6] Suppliers that use cloud services to deliver the product/service to Digidentity.
  [a] Ensure that no personal data of Digidentity is exported outside EEA (including failover or other redundancy sites)
  [b] Implement least privileged access controls
  [c] Restrict access to Digidentity data, instance, and source code
  [d] Ensure that software, libraries and other components are kept up to date
[7] Vulnerability & Continuity Management
  [a] Perform a penetration test on the service or product provided to Digidentity at least once per year or in case a significant change to the service or product is made
  [b] Perform regular vulnerability scans on the endpoints used by the service or product provided to Digidentity at least once every three months
  [c] Perform regular planned business continuity exercises of the service or product provided to Digidentity

8.5.3 Service Delivery Requirements

Supplier must:

[1] Deliver products and services within the agreed-upon timelines to ensure continuity and efficiency
[2] Provide periodic performance reports (monthly, yearly) that detail service delivery metrics, including adherence to service level agreements and usage of the product or service
[3] Participate in regular performance reviews to assess service delivery against agreed-upon metrics and standards
[4] Meet the quality standards specified in the contract for all products and services supplied, including any relevant certifications
[5] Maintain open and regular communication with Digidentity, providing updates on service delivery and any potential issues that may arise
[6] Provide adequate training and support for Digidentity staff to ensure effective use of the products or services provided
[7] Maintain accurate documentation related to service delivery, including service agreements, invoices, and compliance records
[8] Inform Digidentity without due delay of any changes to their services, processes, or personnel that may impact service delivery.

8.5.4 Reporting requirements

Supplier must:

[1] Provide information describing the software components used in product or service (to determine vulnerable or malfunctioning components - such as libraries used)
[2] Provide information describing the implemented security measures of their product and the configuration required for its secure operation (e.g. certification of the product or component)
[3] Provide assurance that critical components and their origin can be traced throughout the supply chain
[4] Provide assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features
[5] Ensure that components from suppliers are genuine and unaltered from their specification

[6] Report all incidents involving any type of security or data privacy breach or unauthorised access to the Digidentity's information assets within 12 hours of detection
[7] Provide sufficient support during investigation of such incident
[8] Report on the results (summary) of the penetration test and resolution of findings if applicable
[9] Report quarterly on the results (summary) and follow up of the vulnerability scans
[10] Report on the results (summary) of the business continuity tests and resolution of findings if applicable

8.6 Human Resource Security

Human Resource requirements are documented in ISO27001:2022 - Annex A6, ETSI EN 319 401 - Section 7.2.

Digidentity has implemented and maintains security controls related to human resources including employee selection, onboarding, employment, and offboarding.

8.6.1 Before employment

New employees will be selected based on a screening, depending on the role in the organisation. Job descriptions are available for each role in Digidentity.

Digidentity screens candidates using interviews and assignments (for developers) at the second stage of an application. After passing the second selection round, the candidate is requested to provide references.

Employment contracts include confidentiality and intellectual property rights clauses.

8.6.2 Starting employment

Digidentity has developed and implemented the documented onboarding procedure for all new employees. The onboarding procedure starts after the candidate has signed the contract.

The declaration from the Dutch Ministry of Justice (Declaration of Good Conduct) is requested. All employees are required to provide this declaration stating there is no objection for this person to act in the specified role at Digidentity. A positive declaration is mandatory for all employees and external contractors.

On the first day of employment, required assets such as a computer and access badge are issued. A record of all issued assets is maintained in the employee's personnel file. Along with the assets, the Acceptable Use Policy is provided, which defines the proper use of Digidentity resources, including laptops, phones, internet, offices, and other company assets. New employees are informed about all relevant policies, and security and PKI registration training are scheduled.

8.6.3 During employment

Service Desk agents receive and must pass a specialised training on face comparisons and identity document validation before they are allowed to perform as a Registration Officer (Trusted Role appointment).

Service Desk agents are required to attend an annual refresher training, delivered by an external trainer with experience in document validation and face comparisons.

Documented disciplinary actions are available in the event an employee wilfully breaches any policy, supporting policy or procedure. This could result in sanctions including ranging from first warning up to and including dismissal, as well as legal actions.

8.6.4 Ending employment

Employees that leave Digidentity will follow the documented offboarding procedure. Digidentity confirms the end of employment and sends the employee the steps of the offboarding process.

On the last day of employment, the employee is required to return all Digidentity assets as laptop, access badge, phone and other issued items. All access to systems and locations are revoked. The employee is informed that confidentiality clauses are applicable until two years after employment.

8.7 Acceptable Use

The Acceptable User Policy is intended to improve the security and confidentiality of information and to reduce the risk of unauthorised access, loss, theft, or damage to information.

The policy seeks to encourage a supportive, positive, efficient, and effective work environment for Digidentity personnel (including contractors), reduce workplace accidents and minimise risks associated with existing vulnerabilities.

Digidentity resources are provided for legitimate business purposes. The following are examples of prohibited uses of these resources:

[1] Use of Digidentity resources to access, upload, view, create, send, forward, post, publish, display, or distribute any content that may be considered defamatory, harassing, threatening, indecent, obscene, profane, or that would likely offend someone based on race, gender, national origin, sexual orientation, religion, age, disability, or any characteristic protected by law

[2] Use of Digidentity resources that would be in violation of any Digidentity policy, or to access, upload, create, send, forward, post, publish, display, or distribute any unlawful or unlawfully obtained information or material

[3] Unauthorised disclosure or distribution of sensitive information outside of Digidentity is considered as gross misconduct

8.8 Security & Privacy Awareness

All employees receive regular security awareness training. Digidentity specific security awareness training delivered in person, as well as a quarterly specific security training (e.g. phishing, passwords) via an online training platform. The security awareness training includes recognising phishing messages, social engineering, safe internet behaviour, privacy, password security, clean desk policy and relevant certifications.

8.9 Compliance

Compliance requirements are documented in ISO27001:2022 - Annex A5.31, A5.32, A8.10, and ETSI EN 319 401 - Section 7.13.

The products of Digidentity are subject to laws, regulations and other requirements such as standards and contractual requirements. Digidentity is compliant to GDPR and eIDAS and is assessed on these regulations as part of the regular external audits from BSI, DNV and Government agencies (e.g. Dutch Authority for Digital Infrastructure — RDI).

A wide variety of controls are implemented to verify technical compliance to the internal policies and standards. Next to the overall internal audit plan, internal penetration tests are performed, regular vulnerability scans are executed, and real time active system file monitoring is implemented.

See Section 13 for detailed information on Audit & Compliance.

9 Technical Controls

Digidentity has implemented several technical controls to secure systems and data. All controls are subject to regular internal audits to measure the effectiveness of the measures and make improvements where applicable. As the technical controls are part of security standards, annual external certification audits are performed by an independent auditor to evaluate measure effectiveness.

9.1 Product & System Overview

Digidentity provides products as Identity as a Service (eHerkenning), Identity Proofing as a Service (KYC) and Signing as a Service (eSGN, Seal). We offer standard products that can be configured to meet specific customer requirements. The Digidentity platform operates as a multi-tenant environment.

Our platform is almost completely cloud based using Amazon Web Services (Ireland). High-risk services such as Certificate Authority (CA) services, HSM, Authenticators (Virtual Smart Cards) and CA processes are hosted in data centres in The Netherlands.

AWS gives Digidentity products the scalability and flexibility needed to guarantee performance and availability to our customers.

We have separated our system based on functionality. Systems are created for customer accounts, account authorisations, identity systems, evidence, smart card management, certificate management, logging, archiving, monitoring and system management.

Digidentity uses pseudonyms to mask and secure personal data. We store personal data in one encrypted system. Other systems use the pseudonym, so personal data is not directly available in those systems.

For a system overview, see Appendix B - System & Network Diagram.

9.2 Access Management

Access Management requirements are documented in ISO27001:2022 - AnnexA5.15-5.18, A8.18, A8.19, A8.23, ETSI EN 319 401 - Section 7.4 and CA/B Forum Network Security - Section 2.

Digidentity grants access rights based on the following Access Management principles:

[1] Least privileged access
[2] Role based access
[3] Personal accounts only
[4] Multi-factor authentication unless not possible
[5] Dual control on high-risk systems

9.2.1 Logical Access

Access to systems and data is restricted to authorised personnel. Following the principle of least privileged, access is granted only to systems, applications, functions and information resources necessary to perform assigned duties. We apply a role-based access system, ensuring that access rights are granted according to the role of the employee or contractor.

All employees have a unique personal account to access applications and systems. Digidentity does not allow shared accounts. All account activities are logged, and privileged access activities are both logged and monitored.

Access rights are revoked within eight hours of an employee leaving Digidentity or re-issued when an employee changes role within Digidentity.

Access rights are reviewed and the implemented access rights to the documented role-based access are verified. This review is performed on a regular basis.

9.2.2 Privileged Access

Digidentity uses accounts with privileged access for management of users, systems, applications and data. These accounts have full access. The number of privileged accounts is kept to a minimum and a list of privileged accounts is maintained. Each user who requires a privileged account, has a separate account to perform system management tasks.

Accounts with privileged access use Multi Factor Authentication (MFA) and encrypted connections. Privileged access rights are reviewed every quarter.

9.2.3 Authentication (Password) Management

Digidentity uses multi-factor authentication (MFA) to access systems. Internal systems containing personal data require MFA to login, using an eIDAS High (Level of Assurance 4) identity with our authenticator in our Digidentity Wallet. High-risk systems and data require dual control access. Under the principle of dual control, two employees each hold part of a complete password, and both parts are required to gain access.

End-user accounts require MFA. When creating a Digidentity account via the Digidentity Wallet, a passwordless account using an authenticator is created. End-users can access their account by scanning a QR code with the Wallet and confirm login with the pin code of the Authenticator. Digidentity is planning to stop using passwords and give all end-users a passwordless account (Multi-Factor Authentication - MFA).

Digidentity requires all default passwords on accounts for systems and services to be changed.

Digidentity uses passphrases with multi-factor authentication. Password rotation is not applicable with the use of MFA.

9.2.4 Session Time Out

Digidentity has implemented session time out on all platforms (servers, Wallet) after 15 minutes. Any established session will be timed out and the user will be logged out after 15 minutes of inactivity. The end-user must authenticate themselves to log back in after a session time out.

9.2.5 Physical Access

The Digidentity office is secured with both physical and electronic key systems. A limited number of employees have a physical key. All employees have a key card for access to the office.

9.2.6 Access Logging, Monitoring & Alerting

All access requests, both logical and physical are logged. All account activities are logged and monitored. Privilege access requests will generate an alert to IT Operations.

Digidentity monitors access on unexpected behaviour. When detected, an alert is generated and send to IT Operations for further investigation.

9.3 Configuration Management

Systems and applications require a correct configuration to operate properly and to be secure. Default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use – not security. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, and pre-installation of unneeded software can be exploitable in their default state.

Digidentity uses the CIS Controls as a baseline for secure configuration of systems, devices and applications. We have developed a strong, secure baseline configurations for all systems and applications.

Digidentity adheres to the following configuration principles:

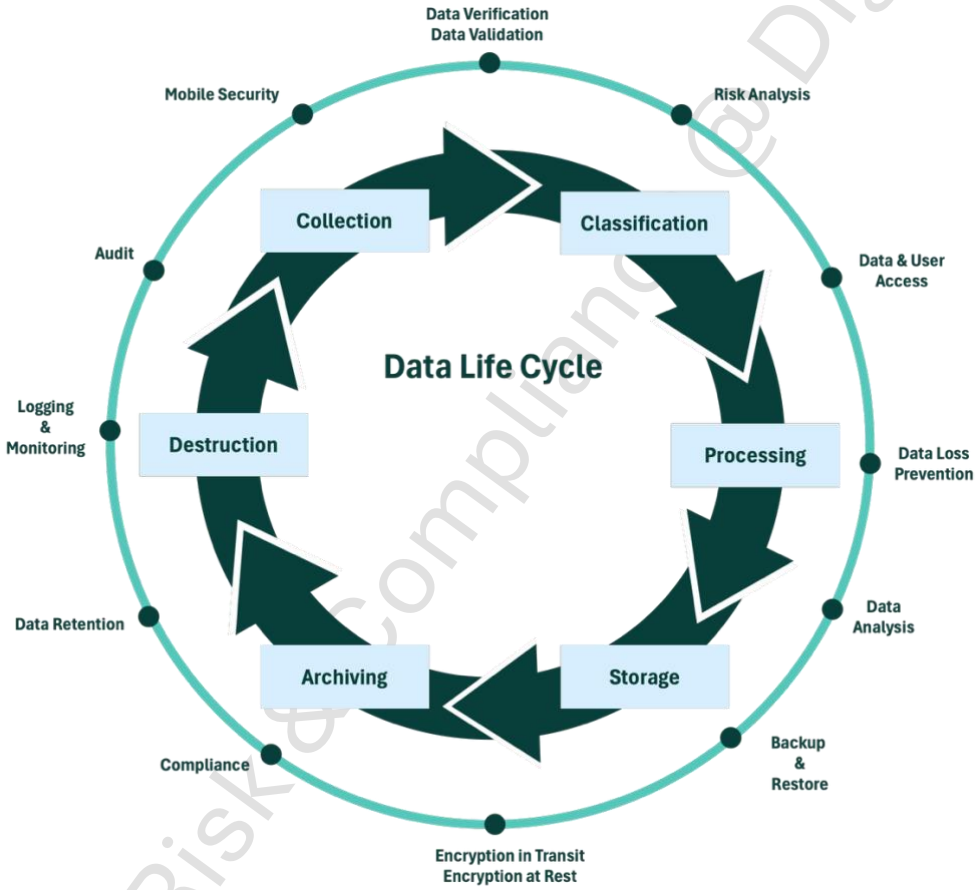
- Always change default passwords
- Always change default accounts
- Remove or disable unrequired services, protocols and functions
- Uninstall unrequired software or functions (if possible)
- Systems must be configured to only perform the functions required

Baseline configurations are reviewed at least once per year or when major updates of the software are released.

9.4 Data Management

Digidentity is an organisation where data is used in our products. We have implemented measures to manage the life cycle of data; including the collection, classification, processing, storage, archiving and destruction of data.

Our data management policy ensures that all data collected and generated is handled in a consistent manner and all data is protected against loss and modification.



9.4.1 Collection

Collection & Protection of Records requirements are documented in ISO27001:2022 - Annex A5.33, and ETSI EN 319 401 - Section 7.10.

Digidentity collects data required to deliver the products to our customers. We verify the accuracy of the data and validate its authenticity. As we provide attributes to relying parties, the data must be trustworthy.

A detailed description of the data collection is documented in the document “Identity Proofing @ Digidentity”.

9.4.2 Classification & Handling

Classification, handling and destruction of data requirements are documented in ISO27001:2022 - Annex A5.12, 5.13, and ETSI EN 319 401 - Section 7.3.1, 7.3.2).

Digidentity has three classifications of data:

[1] Confidential: all personal data and data where access is on need-to-know basis
[2] Internal: all data which does not clearly fit into either of the other classifications
[3] Public: data that has been explicitly approved by management for release to the public or that is already publicly known data

All data must be labelled according to the classification if possible. Document templates are provided which includes data classification. Data must be handled according to the handling policy (use, storage, printing, transfer and deletion) for the applicable classification. Digidentity prohibits the use of removable media.

9.4.3 Processing

Digidentity processes personal data to deliver the services to customers and to maintain business operations. All personal data shall be protected and handled according to the risk level.

The processing of data is documented in section 4.

9.4.4 Storage & Archiving

Digidentity is required to store and archive data according to the applicable laws, regulations and standards.

Digidentity archives all events related to the life cycle of keys it manages, including any key pairs generated, for a period of seven (7) years.

User accounts are archived for at least seven (7) years starting when the account is deleted (either by the user or by Digidentity).

9.4.5 Data Destruction

Careless disposal of any asset could result in security incidents compromising the safety of Digidentity systems and its confidential information.

Destruction of storage media containing confidential data such as hard drives, solid-state drives, USB drives, and magnetic tape must only be performed with approved methods and by IT Operations. These include the use of shredders, degaussers, or other equipment. Evidence of destruction shall be kept.

Employees must ensure that all printed media are shredded or disposed of in the confidential wastepaper bins located around the office.

9.5 Data Protection

Digidentity protects all data (personal data and non-personal data) based on the data classification policy. We have implemented data loss prevention controls to protect data against intentional and unintentional loss. Our privacy policy (see Section 4.2) defines the principles for personal data.

9.5.1 Data Verification & Validation

Digidentity must verify and validate all data collected. A detailed description of data verification and validation is available in the document "Identity Proofing @ Digidentity".

9.5.2 Data Access & User Access

Data must be securely maintained to prevent unauthorised access, alteration, damage or deletion. Data must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents. Access to records is granted based on job roles and need-to-know principles.

Systems containing records must have appropriate security controls (encryption, backups, authentication).

9.5.3 Data Loss Prevention

Digidentity protect its data against loss or exposure. Digidentity protects communication channels and restricts transmission of confidential data using corporate e-mail services, online cloud storage services and external storage devices.

Digidentity should implement and maintain measures to protect against:

[1] Malware protection
[2] Insider risk
[3] Cyber attack
[4] Ransomware
[5] Phishing
[6] Accidental exposure

Digidentity has implemented measures to:

- Monitor and alert on data access, usage, volume and destination
- Access to personal data is restricted after identity proofing is completed
- Detect and block suspicious activity
- Access to public cloud (e.g. Dropbox) is blocked
- System does not allow for downloading or exporting of personal data

Sharing or communicating data is restricted and based on the classification of data. This policy defines how employees must handle data i.e. label, e-mail, print, store, encrypt, archive, destroy.

9.5.4 E-mail protection

Digidentity uses an advanced e-mail protection designed to stop a wide variety of e-mail fraud. Our system detects and blocks malicious payload but also sophisticated attacks such as payment redirects and invoicing fraud which requires advanced detection techniques. Our detection engine uses artificial intelligence and machine learning to analyse every detail of messages and stop e-mail attacks. Digidentity enforces e-mail authentication, as SPF, DKIM, and DMARC.

9.5.5 Data Masking

Data masking is the process of obscuring sensitive information in order to protect it from unauthorised access. This technique is commonly used in testing and development environments to ensure that sensitive data is not accidentally exposed. For Digidentity masking is anonymising data, the process is irreversible.

The process on data masking is:

[a] Identify which data should be masked (social security number, BSN, personal identification number)
[b] Define guidelines for masking data (replace all character except last two character with 'X')

Currently, the social security or personal number collected from identity documents are masked as soon as the product registration is completed.

9.5.6 Data in Transit (Encryption)

Data in transit concerns all data that is transmitted over networks or on portable storage. Digidentity protects data in transit by using encrypted network communication channels (using TLS 1.2 or TLS 1.3). Removable storage includes all laptops (full hard disk encryption using 256-bit Advanced Encryption Standard - AES keys) and external disks (full disk encryption using 256-bit AES keys).

All laptops use full hard disk encryption. Digidentity policy states that no personal data of customers should be stored on employee laptops. External disks are only used by IT Operations and Security for backup purposes.

9.5.7 Data at Rest (Encryption)

Data at rest concerns all data that is backed up or archived. All data at rest is encrypted using AES 256-bit or equivalent. Access to encrypted data at rest is restricted to specific users.

9.5.8 Data Retention

Digidentity retains data as required by applicable laws and regulations. Details on data retention for specific data is documented in our Data Retention Policy which is available in our Privacy Statement available on our corporate website (https://www.digidentity.eu/documentation).

9.5.9 Data Analysis

Digidentity analyses the data to improve our products, detect issues, and perform business analysis. Data analysis is performed on anonymised data.

Section 12.4 describes the Backup & Restore policy.

Section 9.10 describes Logging & Monitoring.

Section 14 describes Audits.

Section 11 describes Mobile Security.

9.6 Network Security

Network Security requirements are documented in ISO27001:2022 - Annex A8.20-8.22, ETSI EN 319 401 - Section 7.8 and CA/B Forum Network Security - Section 1.

Digidentity has implemented network security controls to mitigate risks related to networks.

9.6.1 Network Segmentation

Digidentity has implemented controls to secure its network. Network segmentation is implemented with access controls on each network (VLAN). Different network zones are created, with specific equipment placed accordingly to the associated risk. Networks are protected by firewalls and use high secure zones, secure zones, office zones, a guest zone and other segments to protect systems (internet facing systems are in a De-Militarised Zone - DMZ).

The High Secure Zone contains the high-risk system such as Certificate Authority systems supporting certificate issuance. Access to the High Secure Zone is under dual control and must be from our office via a wired internet connection. In the Secure Zone all systems except 'high-risk' are located. The Secure Zone is dedicated to IT Operations members and Development team leads.

The Office Zone is available to all employees working in our office. The Office Zone contains the Digidentity internal wireless network. This wireless network is only accessible for Digidentity devices. The Office Zone offers virtual networks to separate departments.

The Guest Zone is a wireless network in our office for guests and personal devices of our employees. This zone is only connected to the internet.

9.6.2 Network Protection

Digidentity uses a reverse proxy that protects our systems and maintains the availability of our products. Our reverse proxy server provides functionality such as:

[1] load balancing: a "traffic cop" located in front of our servers and distributing client requests across a group of servers to maximise speed while ensuring no server is overloaded

[2] web application firewall: intercepting requests to our servers protecting their identities and acts as a defence against attacks

[3] web acceleration: compress inbound and outbound traffic, as well as caching commonly requested content to increase throughput between clients and servers

Digidentity has automated scanning on vulnerabilities of systems and network components. Network traffic from outside Digidentity to Digidentity is encrypted to protect the communication between employees and our systems.

9.6.3 Intrusion Detection & Prevention

Digidentity uses network intrusion detection and prevention systems to detect and prevent attacks on our systems. We use real time traffic analysis and packet logging on IP networks to detect and block attacks. Our system performs protocol analysis, content searching and matching. Alerts are sent when suspicious traffic is detected.

Digidentity has implemented threat and vulnerability management controls (see section 9.9).

9.6.4 Remote Access

VPN access is necessary to connect to Digidentity servers and data from any location even within our office. Each Digidentity device is configured in the VPN server. The VPN access is segmented to restrict access to systems and data. When employees connect to the VPN from outside the EEA or UK, an alert is generated, and access is blocked to prevent access to personal data from outside the EEA or UK.

9.6.5 Network Management & Monitoring

Our networks are monitored for unknown devices or access points. Internet connections are redundant to address the risk of failure of our primary provider and fail over to our secondary provider. Our internet connections are protected against Denial of Service (DDoS) attacks using a scrubbing service to detect attacks and makes sure there is no disruption of our Products.

All changes to the network (new devices, ports, firewall rules) are handled via the Change Management process and must be approved. Firewall rules are reviewed every quarter.

9.7 Cryptographic Controls & Encryption

Cryptographic Control requirements are documented in ISO27001:2022 - Annex A8.24 and, ETSI EN 319 401 - Section 7.5.

Digidentity uses cryptographic controls on multiple levels of the infrastructure. All communication channels are encrypted using Transport Layer Security (TLS) 1.2. This applies to Digidentity's websites, mobile application(s), and all API connections. Sensitive data is encrypted both in transit and at rest.

Access to Digidentity systems is based on smart card authentication. The pin code to authenticate login or signing is hashed. If username and password is used, the credentials are hashed and salted.

Documents which are signed using esgn.com, are encrypted while on Digidentity systems. If documents are signed using third party signing applications such as Adobe Sign, DocuSign or Seal sign, Digidentity only receives a hash that needs to be signed.

Digidentity is a Certificate Authority and complies to the requirements for certificate generation, issuance, revocation and key life cycle management.

9.7.1 Encryption

Digidentity has implemented cryptographic controls to protect confidential data (during transmission or stored).

The encryption principles that Digidentity uses, are:

[1] Data on mobile storage devices (laptops, flash drives, external hard disks) must be encrypted
[2] Encryption should never be deactivated
[3] Data at rest (backups, archive) must be encrypted
[4] Stored passwords must be hashed and encrypted
[5] Encryption should be used to establish trusted connections, ensuring data only goes where it is intended to go
[6] All encryption mechanisms must align with industry standards at a minimum
[7] Symmetric encryption requires the AES using 256-bit keys or equivalent
[8] Asymmetric encryption requires RSA and Elliptic Curve Cryptography (ECC) algorithms using 256-bit keys or equivalent
[9] Encrypted channels should use TLS 1.2 or newer
[10] Algorithm requirements must undergo an annual review and be upgraded as technology advances
[11] All keys should be managed within EEA or UK

9.7.2 Trustworthy Systems

Digidentity manages systems that are labelled as Trustworthy Systems (TWS). According to article 24.2 of the EU Regulation 910/2014 (eIDAS), Trust Service Providers (TSP) issuing qualified certificates are required to use trustworthy systems and products that are protected against modification and ensure the technical security of the processes they support.

Trust Service Providers need to use Trustworthy Systems (TWS) for securely providing the component services:

[1] Registration Service: to verify the identity and any specific attributes of a subject
[2] Certificate Generation Service: to create certificates
[3] Dissemination Service: to provide certificates and policy information to subjects and relying parties
[4] Revocation Management Service: to allow the processing of revocation requests
[5] Revocation Status Service: to provide certificate revocation status information to relying parties
[6] Subject Device Provision Service: to prepare and provide a Signature Creation Device (SCDev) to subjects. This includes Qualified electronic Signature and Seal Creation Device (QSCD) provision.

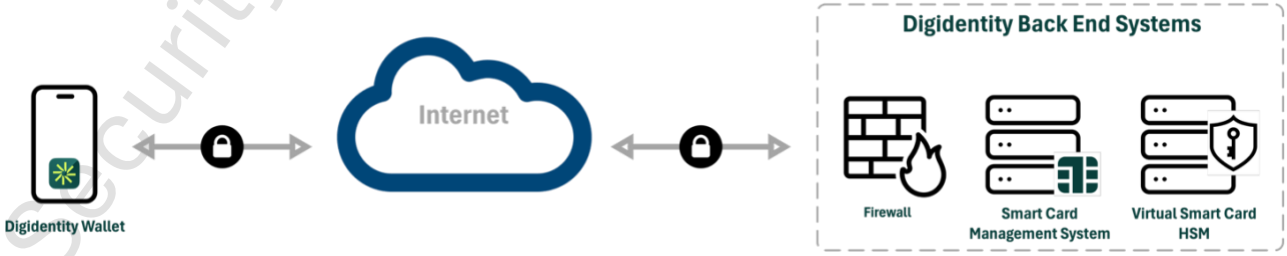
Security requirements for Trustworthy Systems are documented in CEN/TS 419 461 (Security requirements for trustworthy systems managing certificates and timestamps). Digidentity's Trustworthy Systems meet the requirements of CEN/TS 419 461.

9.7.3 Digidentity Authenticator (Virtual Smart Card)

Digidentity has designed, developed and implemented an authenticator based on certificates stored on a Virtual Smart Card. The Virtual Smart Card (VSC) uses centralised Hardware Security Modules (HSM) and the mobile phone to replace the physical smart card using improved protection of cryptographic material and multi-layered security controls.

The VSC is stored on Digidentity HSMs and contains the cryptographic keys used for authentication and signing. The Digidentity Wallet acts as a remote control to the VSC. Access to the VSC on the HSM is only possible when the user enters the memorised pin code (stored as hash in the HSM) in the Digidentity Wallet.

The Digidentity Wallet uses the Security Environment of the mobile phone to generate encryption keys to communicate securely with the authenticator (VSC on the HSM).



Digidentity has no access to the contents of the VSC. The user has sole control over the cryptographic keys on the VSC. The Digidentity VSC is patented (number EP2414983A1).

9.8 Cloud

Cloud Security requirements are documented in ISO27001:2022 – Annex A5.23

Digidentity uses public cloud services to provide products to customers. Our cloud policy is to ensure that a framework of controls is implemented to manage systems and data in the cloud.

Digidentity establishes a framework for cloud computing based on the principles:

- Process services from the cloud if possible and/or allowed
- Use scalable and flexible processing capacity
- Process services globally

Digidentity uses cloud services as virtual machines (EC2), storage (S3), databases (RDS and Content Delivery Network (CloudFront) from AWS to deliver our products.

9.9 Threat & Vulnerability Management

Threat & Vulnerability requirements are documented in ISO27001:2022 - Annex A5.7, A8.7-8, ETSI EN 319 401 - Section REQ-7.7-05, and CA/B Forum Network Security – Section 4

Digidentity has implemented an extensive set of controls to address threat and vulnerabilities. Our threat and vulnerability management program consists of system hardening, patch management, vulnerability detection, malware protection, penetration testing and security awareness program (see section 8.8).

Additionally, to the technical controls to battle threats and vulnerabilities, Digidentity receives information on new threats and vulnerabilities from the Dutch National Cyber Security Center (NCSC) and monitors the updates from US Cyber Security & Infrastructure Security Agency (CISA) and other sources.

The remediation timelines for vulnerabilities are based on severity, with critical vulnerabilities addressed within 72 hours, high risk vulnerabilities addressed within 7 days and medium/low issues resolved within 30 to 90 days. If immediate remediation is not feasible, temporary mitigations shall be implemented to reduce risk until a permanent corrective action is deployed. Digidentity documents exceptions.

9.9.1 System Hardening

System Hardening requirements are documented in ISO27001:2022 - Annex A8.8, 8.9, 8.16, 8.19, ETSI EN 319 401 - Section 7.7, and CA/B Forum Network Security - Section 1.

Digidentity applies system hardening to secure systems by minimising its surface of vulnerability, and potential attack vectors. Digidentity uses hardened operating systems. Unnecessary items such as services, protocols, applications, users and access rights are removed. This reduces vulnerabilities and a potential compromise of the entire system.

For system hardening, the Centre for Internet Security (CIS) Benchmarks are used as a reference. Monitoring on updates of the baseline will alert Operations regarding any possible issues. The security hardening standards are reviewed annually.

Systems are actively monitored on system changes and any change to system files will generate an alert to IT Operations.

Digidentity uses clock synchronisation for computing devices with publicly accessible stratum-1 time server including fallback servers.

9.9.2 Patch Management

Patch Management requirements are documented in ISO27001:2022 - Annex A8.8, ETSI EN 319 401 - Section 7.7, and CA/B Forum Network Security - Section 3.

Digidentity monitors the security updates for all systems continuously e.g. vulnerability scanning and vendor notifications. Supporting systems and workstations are updated automatically. Updates for customer services systems are assessed for impact, risk and applicability before implementing to avoid disruptions.

Critical security patches will be installed in accordance with the Emergency Change Process.

Digidentity is part of the vital infrastructure of The Netherlands and has therefore a direct link with the National Cyber Security Centre (NCSC) of the Dutch government. NCSC informs Digidentity on known weaknesses and threats.

9.9.3 Vulnerability Detection

Vulnerability Detection requirements are documented in ISO27001:2022 - Annex A8.8, ETSI EN 319 401 - Section 7.8, and CA/B Forum Network Security - Section 4.

Digidentity has implemented Continuous Vulnerability Scanning on all end points of its products. The vulnerability scans include port scans, end points of the Trustworthy Systems, customer services systems and supplier end points. All target end points are scanned at least once every two weeks.

Vulnerability scans will automatically create tickets to resolve for all CVSS (Common Vulnerability Scoring System) of 4.0 and higher (medium, high, and critical).

Digidentity requires suppliers to perform vulnerability scans on their systems, networks and processes that are used by Digidentity.

9.9.4 Malware Protection

Protection against Malware requirements are documented in ISO27001:2022 - Annex A8.7, and ETSI EN 319 401 - Section 7.7.

Digidentity has implemented a wide variety of technical and organisational controls to protect against malware.

All systems have active malware protection software installed. The software will detect and protect against all forms of malware such as viruses, worms, trojan horses, spyware, rootkits, botnet software, keystroke loggers, ransomware, adware and malicious mobile code.

Server systems are monitored on system file changes and alerts are generated when unauthorised system changes are detected. The Digidentity e-mail server is protected against spam, malware and phishing attacks.

All locations have firewalls that monitor, track and control outgoing and incoming data and network traffic. Firewall firmware and configuration are checked on a routinely basis.

Digidentity uses reverse proxy servers. The reverse proxy server is behind the firewall in a private network and directs client requests to the appropriate backend application. A reverse proxy provides an additional level of abstraction and control to ensure the smooth flow of network traffic between clients and applications.

These include:

- Load balancing – distributing client requests across a group of application instances in a manner that maximises speed and capacity utilisation, while ensuring no one instance is overloaded, which can degrade performance.
- Security and anonymity – reverse proxy servers protect their identities and act as an additional defence against security attacks. It also ensures that multiple application instances can be accessed from a single record locator or URL.

9.10 Logging, Monitoring & Alerting

Logging & Monitoring requirements are documented in ISO27001:2022 - Annex A8.15/16, ETSI EN 319 401 - Section 7.9, ETSI EN 319 411 - section 6.4.5 and CA/B Forum Network Security - Section 3.

9.10.1 Logging & Audit Logging

Logging has been implemented on all Digidentity systems. Digidentity has implemented a system that continuously monitors, detects, and alerts personnel to any modification and access to identity proofing systems, identity evidence systems, certificate systems, certificate issuing systems, certificate management systems, security systems, and application and support systems unless the modification has been authorised through the change management process.

Digidentity logs security events to monitor successful and unsuccessful login of authorised users, and unsuccessful changes to access privileges.

Digidentity logs all events related to the life cycle of keys and certificates as well as events related to certificate generation, dissemination, and revocation.

The logging system records the following types of events:

[1] Key Lifecycle Events:
- **[a]** Key generation, backup, storage, recovery, archival and destruction
- **[b]** Cryptographic device lifecycle management events

[2] Certificate Lifecycle Events:
- **[a]** Certificate requests and revocation
- **[b]** Verification data and activities
- **[c]** Date, time, phone numbers, contact persons, and their verification
- **[d]** Acceptance and rejection of certificate requests
- **[e]** Issuance of certificates
- **[f]** Generation of CRLs

[3] Events:
- **[a]** Access & authorisation attempts
- **[b]** System actions performed
- **[c]** Profile changes
- **[d]** System activity
- **[e]** Database activities & events
- **[f]** Transactions
- **[g]** Firewall and router activity
- **[h]** Entries to and from Digidentity controlled areas

All log entries provide the date and time, the identity of the person and a description of the event.

9.10.2 Log Review

All logs are periodically reviewed. Digidentity IT Operations performs a manual monthly review of the logs and logging measures to ensure the integrity and functionality of the logs.

Evidence of the reviews is documented in a monthly report stating whether the logging tools are functional.

9.10.3 Protection of logs

All logs are protected against modification and deletion. Each log event is digitally signed to protect each event against modification (modification of the event will make the signature invalid).

The logging system creates block of events covering all events in a period of the last five minutes. This block of events is digitally signed to protect log events against deletion (if a log event is deleted the signature of the block will be invalid).

Verification of the signatures is performed at the creation of the blocks (verification of signature of each log event). Verification of the signatures of the signed blocks is performed every 24 hours. Any failure of the verification will trigger an alert to IT Operations.

9.10.4 Monitoring

Digidentity continuously monitors the performance of the systems. All logging is monitored to detect selected events. Monitoring of the logging is implemented based on CIS guidelines.

Digidentity monitors:

- Uptime of applications, endpoints and servers
- Web and mobile applications performance
- Application errors
- API usage and performance
- Security events
- Vulnerabilities detection
- Modification of servers, firewall, access policies and operating systems
- Cloud performance and configurations
- All access (both user and privileged), remote access, data access and MFA access
- Network performance and traffic
- Performance and availability of supplier services

Digidentity has configured monitoring to alert on specific events or threshold.

9.10.5 Alerting

Alerts are set on specific events or thresholds that indicate medium or high-risk issues. Alerts are sent to relevant departments and employees via e-mail, collaboration and communication software and SMS. If alerts are not addressed within the defined response time, alerts are sent to fall-back employees or departments to make sure the alert is addressed in time. Alerts are monitored 24x7.

Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network are detected and alerted.

9.11 Physical Security

Physical Access requirements are documented in ISO27001:2022 - Annex A7, and ETSI EN 319 401 - Section 7.6.

Digidentity's office in Den Haag is a shared office building. Digidentity has a dedicated floor which is secured with electronic locks. The logs of the electronic lock system are periodically reviewed. We have installed CCTV cameras monitoring the entrances of the office outside opening hours. Recordings are deleted after 24 hours.

Visitors of the Digidentity office are required to show a government issued identity document to verify their identity. Visitors will be issued a visitor badge that must be visibly worn.

The Digidentity office does not host any customer systems. Only employee laptops are in the office during opening hours. Employees are required to take their device home after work.

Digidentity uses two data centres from North-C (https://www.northcdatacenters.com/en/) in The Netherlands for high-risk systems such as HSM which are not allowed in the cloud. These data centres are secured, and only authorised employees have access to the data centres. The data centres provide fail over mechanisms in case of disruption of service in one of the data centres. Digidentity uses data centres that are ISO27001 certified.

All other services are provided from AWS from the Amazon data centre in Dublin (Ireland) and fail over site in Frankfurt (Germany).

9.12 System Maintenance

Digidentity has setup our production systems in such a way that maintenance can be performed without disruption to our customers. Our redundant systems allow Digidentity to perform maintenance on one part of the system and let the production systems operational on the other part of the system.

10 Development

Development requirements are documented in ISO27001:2022 - Annex A8.25-8.33.

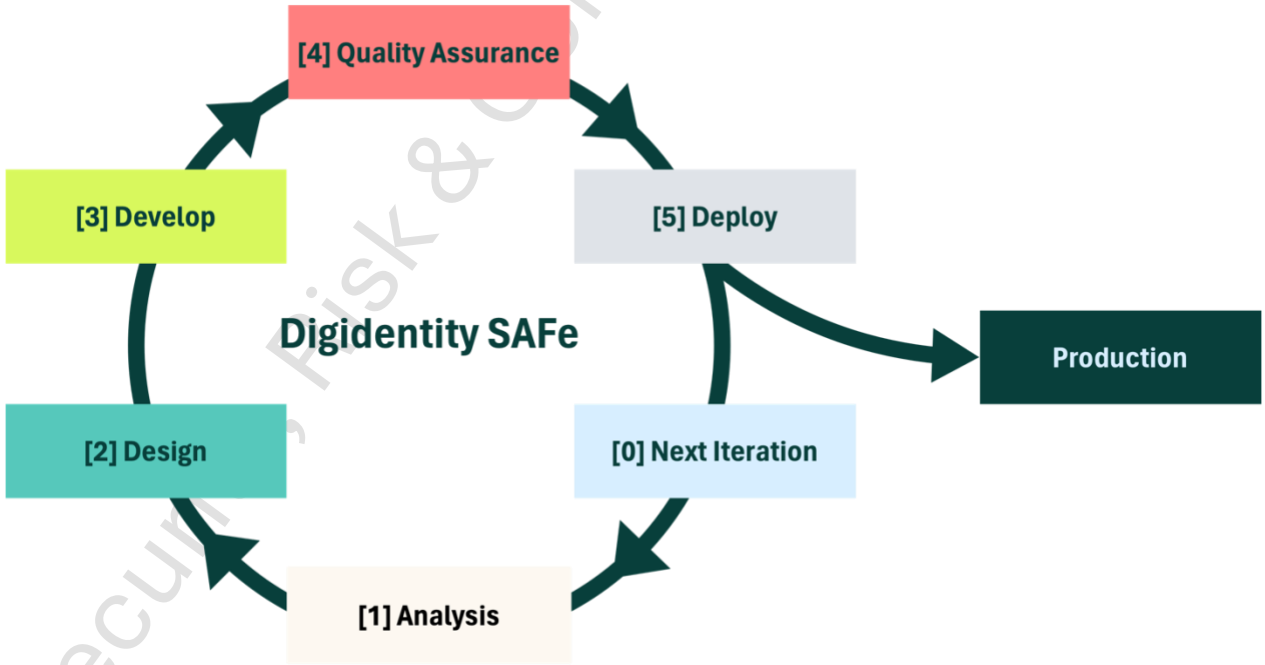
Digidentity designs, develops and maintains software to support our products. We develop full-stack back-end systems and a mobile app to allow customers to register and use our products. Digidentity has defined a software development policy to provide principles and guidelines to develop our software.

10.1 Software Development Lifecycle

Digidentity uses SAFe (Scaled Agile Framework) methodology in its development process. SAFe provides flexibility to respond quickly to changes as well as improve the quality of products. SAFe makes sure that all stakeholders are involved in the development process. All disciplines, such as Service Desk, Sales, Development, Operations, Compliance and Security are involved in the process.

Digidentity uses a development policy in the development of its products. Development is based on the principles of:

[1] Security by Design: security is a starting point of every change and project
[2] Security by Default: all systems are secure, and access is allowed on necessity
[3] Privacy by Design: privacy is a starting point of every change and project
[4] Privacy by Default: all personal data is secure, and access is allowed on necessity



Using the SAFe method, changes are submitted, refined, assessed, developed, tested and released. At each stage, the requirements are verified to ensure accuracy and completeness. Digidentity uses development sprints of three weeks, providing a consistent rhythm for delivering improvements.

Digidentity Development is organised to develop:

- Small changes
- Iterate quickly
- Deploy often
- Simple, well written, documented, and readable code

Documentation, like flow and sequence diagrams and manuals, are part of the process within the planning phase of a new feature and are provided by the architecture team.

All development changes follow the documented change and release management process (see Section 8.2).

10.2 Security in Development

Digidentity always takes security into account when developing software. We have developed a multi-layer security architecture in our software to prevent or detect security breaches in our software.

10.2.1 Security by Design & Security by Default

At Digidentity, we believe that preventing security issues is always better than fixing them afterward. That is why we adhere to the principles of Security by Design and Security by Default.

As a Trust Service Provider, Digidentity must deliver trust to our customers and relying parties. To uphold this responsibility, we develop our software with security as a foundation, embedding protective measures from the design stage through to changes in operational systems.

Digidentity uses a multi-layer approach for security designs to address or protect against threats or to reduce vulnerabilities. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection measure will not leave the system unprotected.

10.2.2 Security Principles & Rules

Digidentity has implemented several security principles for software development:

- External systems are insecure
- Protect data during processing, in transit, in storage and at rest
- Implement multi-layer security controls
- Implement audit mechanisms to analyse performance and security
- Keep it simple
- Implement least privilege

Next to security principles, Digidentity set rules for the development process:

[1] Comply to Secure systems practices
[2] Perform security risk analyses when designing systems
[3] Perform regular vulnerability scans
[4] Perform penetration tests at regular intervals and with major changes
[5] Implement data validation
[6] Perform regular secure code reviews

Technical rules:

- Encrypt communication channels
- Use TLS 1.3 or higher
- Session management (session terminates after 10 minutes of inactivity)
- Run the application as a non-root user
- Store no data in the Wallet (mobile app) or on the phone
- No clear-text passwords (only save a hash) in back-end systems
- Use a salt when hashing passwords
- Use HTST header to require HTTPS in production
- Filter confidential data from logs
- Encrypt any production secrets or database credentials
- Do not use environment variables for secrets
- Implement lockouts for users with too many failed access attempts
- Check the code for issues as Cross Site Scripting, Denial of Service and SQL Injection

10.2.3 Source Code Security

Digidentity stores all source code in a central code repository (GitHub). Developers must check out code they work on. After completing the work, code is submitted to the repository.

The development teams review all submitted changes. All security changes (as identified in the planning, refinement) are reviewed by other developers (four-eye principle). Code can only be merged after a positive review and comprehensive testing.

10.2.4 Continuous Delivery

Digidentity uses continuous delivery (CD) in which teams produce software in short cycles, ensuring that the software can be reliably released at any time and following a pipeline through a "production-like environment".

CD aims at building, testing, and releasing software with greater speed and frequency which helps reduce cost, time, and risk of delivering changes by allowing for more incremental updates to applications in production.

10.2.5 Environments (DTAP)

Digidentity has implemented a four-tier architecture for software development. These four tiers are:

[1] Development (DEV)
[2] Test (TEST)
[3] Acceptance (ACCEPT)
[4] Production (PROD)

Development (DEV)

Digidentity uses two development environments (Spade and Heart) for application development, design, programming and debugging. Two separate environments are used by different teams to prevent code conflicts.

Test (TEST)

Our test environment, called Staging, is used for regression testing. All finished development code is released to staging for testing by our QA Engineers. The test environment is to verify the quality of the software. Any issues identified will be reported to the developers to be resolved.

Acceptance (ACCEPT)

Digidentity Preproduction (acceptance environment) is used as a sandbox by customers before final release to production. Digidentity uses Preproduction also for demonstrations and Proof-of-Concepts.

Production (PROD)

The production environment is the actual environment our end-users and customers use their products and management tools.

All environments run on our cloud platform. Digidentity does not use production data in other environments other than Production. Test and Acceptance only use fictional data.

10.3 Software Testing & Quality Assurance

Digidentity has developed a data set for testing. This data set contains fictional personal data. Testing with production data is not allowed.

Every development team has a dedicated tester (Quality Assurance – QA). The QA focuses on improving software development processes, preventing defects, and guarding operational functions in production. QA monitors regression testing, smoke testing, integration testing and API testing. Scripted automated tests use open-source software test tools.

Our QA are involved early and often in the development process to help developers design testable features by working on test criteria from the beginning. Our testing is running continuous integration every day, to ensure immediate feedback between development and testing.

Digidentity performs various tests:

[1] Performance Testing

This allows developers to measure the performance of our applications. Several aspects of our application (e.g. page load speeds, input processing, stability and reliability) are tested.

[2] System Integration Testing (SIT)

Digidentity performs system integration tests to check if all components, such as code, individual applications, mobile applications and client and server applications, can communicate with each other as per their dependencies.

[3] User Acceptance Testing (UAT)

Corporate customers perform user acceptance testing to check if the application meets the requirements.

[4] Quality Assurance (QA)

Quality assurance testing ensures that the application developed is of the highest quality possible for end users. In this environment, computer programmers test the new software against the previous version to verify that the new product meets the specified parameters.

[5] Security Testing

Security tests are performed by specialised testers to examine how secure the application is from malicious programs, viruses, threat actors, injection, and manipulation. Security tests include the authorisation and authentication features.

10.4 API Security

Digidentity uses Application Programming Interfaces (API) to connect with suppliers and customers. API security is an important part of our security architecture.

Digidentity assesses API security on network and system level security risks, message and transport security, authentication and authorisation protocols, and continuous vulnerability testing. Digidentity assesses risks regarding data exposure, customer confidentiality, regulatory requirements, and deployment infrastructure.

Digidentity uses REST API using an access token retrieved via OAuth2 or OpenID Connect (OIDC). The OAuth client credentials necessary for the API will be provided by Digidentity's Implementation team.

Digidentity has implemented security measures such as:

- Integrate OAuth or OpenID Connect
- IP whitelisting
- Encrypt data
- Use rate limits and throttling to regulate access and protect against brute-force attacks
- Security testing

We follow the Zero-Trust Policy principle, validate and verify all data that is received via our API connections. The Digidentity Wallet contains a Digidentity signed API key to establish a secure connection to our backend systems.

More information on Digidentity API is available on: https://docs.digidentity.com/

11 Digidentity Wallet - Mobile Device Security

Digidentity has developed a mobile app (Wallet) for iOS and Android. This Wallet contains the digital identities, credentials and authenticators of the user.

Digidentity regards mobile phones as non-secure and potentially hostile devices, since we neither control nor intend to control them. We have implemented a multi-layered security architecture in our Wallet to protect the digital identities of our users.

All processing is performed on Digidentity systems and data including private keys are stored on Digidentity systems, not on the phone. The phone is a "remote control" for the digital identities on our systems.

This section provides details on the measures Digidentity has implemented to protect the Wallet.

11.1 Application Protection

Our Wallet is only available for download from the official Google Play Store and Apple App Store.

Digidentity Wallet requests the user for permission to access the system camera, the NFC antenna and push notifications. Access to the camera is needed to scan identity documents, take selfies and scan QR-codes. The NFC antenna is used to read the NFC chip of identity document. Push notifications are needed to notify the user on login attempts and sign requests. No other permission is needed.

11.1.1 Application Shielding

Hackers could reverse engineer the Wallet to access and analyse the source code. The objective of the hacker is to obtain knowledge of the way the application works, look for vulnerabilities, if present extract sensitive information as credentials, discover algorithms, authentication methods, key (API, encryption keys), communication logic and more.

Digidentity has developed the Wallet using the principle that we do not store secrets in the mobile application or API code. Digidentity uses application shielding to make it as difficult as possible for hackers to reverse engineer or modify the Digidentity Wallet and find information on the way the Wallet works.

Techniques used for application shielding are:

[1] Source code obfuscation
[2] Binary obfuscation
[3] Code hardening
[4] Runtime Mobile Application Self-Protection (RASP)

11.1.2 Code Obfuscation (Source Code & Binary)

Digidentity implemented code obfuscation for the Wallet. Code obfuscation makes our code unreadable without affecting the functionality. Its purpose is to prevent hackers from accessing and gaining insight into the logic of our mobile application, to prevent extracting data, code tampering, and exploiting unknown vulnerabilities.

To protect the Wallet from reverse engineering, Digidentity uses code obfuscation to make the application difficult or nearly impossible to decompile or disassemble. Code obfuscation regenerates the project and changes all meaningful names (name obfuscation), static strings in the application and modification of the logical structure of the code to make it less predictable and traceable (control flow obfuscation). Digidentity also converts simple arithmetic and logical expressions into complex equivalents (arithmetic obfuscation).

Binary obfuscation is performed after compilation and obfuscates binary representations, generated bit code, arithmetic operations and meaningful names and static strings.

Digidentity's code obfuscation strategy includes:

- Renaming classes, fields, methods, libraries etc.
- Altering the structure of the code
- Transforming arithmetic and logical expressions
- Encryption of strings, classes etc.
- Removing certain metadata
- Hiding calls to sensitive APIs, and more

11.1.3 Code Hardening

Digidentity applies code hardening techniques to make our application code unreadable for hackers without affecting the functionality. Hackers often use reverse engineering such as decompiling applications to analyse the code. This can the hacker to modify the code to compromise security systems, manipulate data and redirect data flows.

Code hardening makes our code difficult to interpret when decompiled. Digidentity's code hardening includes removing metadata, static string encryption of secrets and constant strings, renaming classes and variables, adding ancillary code, and altering the structure of the code.

11.1.4 Runtime Mobile Application Self-Protection (RASP)

Digidentity Wallet uses runtime application self-protection (RASP) that enables the Wallet to monitor for suspicious behaviour at runtime. When a runtime threat is detected, the RASP features help defend against hackers attempting to tamper with the Wallet or perform a dynamic analysis.

With dynamic analysis, hackers use several techniques as jailbreaking and rooting (see section 11.5.3), and hooking (see section 11.5.4) to analyse, reverse engineer and modify the app to steal keys, intercept communications, inject fake data and more.

11.1.5 App Attestation

Digidentity uses app attestation to verify the integrity and authenticity of the Digidentity Wallet on the user's mobile phone. App attestation ensures that only the trusted and unmodified Wallet runs on the mobile phone of the user and communicates with Digidentity servers.

The app attestation services from Apple and Google provide responses that confirm if the app (Wallet) is:

[1] Genuine app binary: determine the app binary is unmodified
[2] Genuine install: determine the installed app is from the official App Store or Play Store
[3] Genuine device: determine the app is installed on a genuine Apple or Android device

Digidentity uses app attestation App Check from Google Firebase. Firebase uses the attestation services from Apple (iOS) and Google (Android) to attest that the Digidentity Wallet is not modified, installed from official store and installed in genuine hardware.

Firebase App Check:	https://firebase.google.com/docs/app-check
Android Play Integrity API:	https://developer.android.com/google/play/integrity
Apple App Attest:	https://developer.apple.com/documentation/devicecheck

In short, app attestation uses several test and measurements to verify the Wallet's integrity. Using cryptographic tokens from attestation servers from Apple and Google, the Digidentity servers can verify the integrity of the Wallet, and the data sent every time the Wallet communicates with the Digidentity server. Each time the Wallet wants to send data to Digidentity, the attestation token is checked, and the sent data is signed. The Digidentity server verifies the token and signature to determine the integrity of the Wallet and validity of the data sent.

App attestation confirms the Wallet is not modified by hackers and data is not manipulated. In case the app attestation fails (Wallet is modified), the Digidentity servers will reject all evidence send by the Wallet.

11.1.6 Input & Output Validation

In order to use correct data, Digidentity collects and uses only verified data. The use of disposable e-mail addresses is detected and rejected. All personal data must be verified using authoritative sources such as identity documents and company registrations.

To minimise input errors (and user error), we ask the user a minimal amount of data to enter. All personal data and company data is extracted from authoritative sources such as identity documents and registers such as National Trade Register. We aim to configure our products, so the end user does not have to enter personal data manually.

We ask the user to enter an e-mail address which we check on syntax. The user must verify the e-mail address (prove control over the mailbox) by entering the confirmation code we send to the e-mail address. All data that is uploaded to our system which is uploaded through the Wallet. The user does not have to upload documents or photos themselves.

11.1.7 Forced App update

Digidentity can force the update of the Wallet on the mobile phone. A forced update requires the users to update the Wallet to the latest version. Previous versions of the Wallet will not work anymore. This allows Digidentity to exclude version of the app and make sure that the latest version is used.

11.1.8 QR-code protection

We use QR-codes to authenticate Subscribers. We prevent QR-code injection with the implementation of Universal Links. QR-code payloads are fetched from Digidentity servers and we sign each payload and our wallet will validate the signature when the QR-code is scanned.

11.2 Data Protection

Digidentity uses the Wallet to collect data to verify the identity of the end-user. Identity evidence (personal data and organisational data) is collected and sent to Digidentity for validation and verification.

Digidentity has implemented controls to mitigate risks related to storage of data, communication between Wallet and back-end systems, authentication and other threats.

11.2.1 Limit local data storage

Digidentity uses local storage of the mobile phone during registration and operation. During registration, the Wallet temporarily stores personal data and photos (of selfies and identity documents) on the mobile phone. When the identity evidence collection is completed, all data and photos are sent to Digidentity and deleted from the mobile phone.

During use, the Wallet only accesses limited personal data, such as your full name and email address, to display in the app. All other personal data, such as your profile photo, is stored on Digidentity systems and displayed in the Wallet without being stored on the phone. This data is not available in the Wallet when there is no internet connection.

We do not store passwords, pin codes or private keys on the mobile phone as we consider the mobile phone a hostile environment.

11.2.2 Encrypted data in local storage

All data sent to Digidentity Systems is encrypted using RSA keys of 2.048 bits generated by the Secure Environment (SE) of the mobile phone during registration or account recovery. The Wallet asks the SE of the mobile phone to store and encrypt the keys making the keys only accessible for the Wallet. The user's memorised PIN code is encrypted using the public key of the Digidentity HSM.

On iOS devices, all photos captured during the registration process are stored temporarily in the device's secure memory (RAM). Due to strict security measures in iOS, the secure memory cannot be accessed by an attacker to change or replace the photos.

On Android devices, all photos are encrypted and stored locally. If an attacker attempts to modify or replace the photos, the Wallet can no longer decrypt the photo making these photos unusable.

The Wallet creates one package which contains all photos, data and device attestation token and sends it to Digidentity across an enforced secure TLS connection.

Personal data (full name) in the Wallet stored on the mobile phone, is encrypted on local storage and in cache.

11.2.3 Secure pin code

The user's secure Identity Vault is stored on the Digidentity HSM and can only be accessed using a five-digit pin code. The pin is stored in the Identity Vault in a hashed and salted form. It is not stored on the user's mobile phone and must be memorised by the user.

The Wallet uses the secure keyboard function of the operating system of the mobile phone. No third-party keyboard can be used which prevents key logging. The memory of the mobile phone is blocked so the pin code cannot be eavesdropped, captured from the screen or read from memory.

11.3 Communication Protection

Digidentity encrypts all communication between the mobile phone of the user and Digidentity systems with a TLS certificate (see Section (0). We have implemented certificate pinning to make sure only our certificate is used (see Section 11.5.2).

11.4 Presentation Attacks

Digidentity has taken several measures to address presentation attacks. A detailed description of our presentation attack measure is available in our document "Identity Proofing @ Digidentity" on our website.

https://www.digidentity.eu/documentation

11.5 Man-in-the-middle Attacks, Eavesdropping or Hijacking

Digidentity has implemented measures to address man-in-the-middle attacks, eavesdropping or hijacking attacks. The measures are explained in the next paragraphs.

11.5.1 Hostname Verification

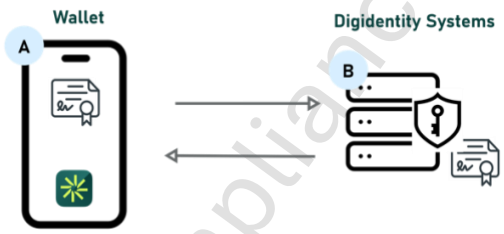
The Digidentity Wallet uses hostname verification. Hostname verification is a part of HTTPS that checks the identity of a server to ensure that the Wallet is communicating to the correct server, and data is not redirected by a Man-in-the-Middle attack to a server under control of the hacker. If a hacker tries to redirect traffic to other host, communication will fail.

The certificate contains the domain name "api.digidentity.com". The app uses hostname verification by matching the domain name in "api.digidentity.com" with the domain name "api.digidentity.com" in the certificate. After the hostname is verified (domain names match), the app communicates with the Digidentity server. If the match fails, the app will not connect to the server.

Hostname verification plays an important role in protecting the integrity and confidentiality of data transmitted over secure communication.

11.5.2 Certificate Pinning

Digidentity has implemented certificate pinning in the Wallet. Certificate pinning is a technique that ensures the Wallet only trusts a specific SSL/TLS certificate. The server certificate that proves the identity of the Digidentity server, is pinned in the Wallet. When the Wallet (A) contacts the server (B), the Wallet checks that the server's certificate matches the pinned certificate.



The Digidentity server sends the certificate with evidence of the identity. Wallet checks the pinned certificate in the Wallet with the certificate sent by the server. When the certificates match, the app communicates with the Digidentity server. If the match fails, the app will not connect to the server.

Certificate pinning requires regular maintenance as certificates are valid for one year. Digidentity updates the certificate in the Wallet when required. Users are required to update the app if the installed version contains an expired or invalid certificate.

11.5.3 Detect rooted or jailbroken mobile devices

Jailbreaking or rooting of the phone is the first step a hacker will take. When a mobile phone is jailbroken, the hacker can circumvent security measures such as SSL pinning and hostname verification. The hacker can analyse the app including traffic to the servers. Jailbreaking a device makes it possible to insert false evidence.

The Digidentity Wallet detects if a mobile device is jailbroken (Apple devices) or rooted (Android-based devices). When a jailbreak is detected, the Wallet will notify the user that the device is not supported. Digidentity has implemented jailbreak or root detection software that is kept up to date with the latest information on jailbreaking and rooting.

11.5.4 Detect application hooking

Hooking is a tool for Man-in-the-Middle attacks and allows a hacker to change the behaviour of the application when the end-user is interacting with the application.

Hooking covers a wide range of code modification methods such as intercepting function calls, messages, or events passed between the software components.

Digidentity detects modification of the Wallet using RASP (see section 11.1.4) and App Attestation (see Sections 11.1.5).

11.6 Additional controls

Digidentity has implemented several additional security controls to address threats to the Wallet and our identity proofing process.

11.6.1 Private Keys on Hardware Security Module

Digidentity uses a Hardware Security Module (HSM) to store the private keys instead of a physical smart card. The user (Account Holder) has access to the private key on the HSM using a VSC in the Wallet on the mobile phone. The Digidentity HSM is certified against Common Criteria in conformance with Protection Profile defined in prEN 419 221-5 and resistance against attack potential high. The Digidentity HSM is registered as a Qualified Signature Creation Device (QSCD) on the EU list for QSCD.

11.6.2 Only supported operating systems allowed

Digidentity only supports mobile operating systems (Android and iOS) which are actively supported by the developer (Google or Apple). When no more security updates are provided for the mobile OS, the Wallet will not work on the unsupported OS.

As of September 2025, the Digidentity Wallet only supports iOS version 18 (support of iOS version 16 and 17 stops in March 2026) and higher and Android version 11 and higher (support of Android version 10 stops in March 2026). These minimum OS versions are updated periodically based on the following:

[1] The announcements and releases of new OS versions
[2] The announcements of OS versions excluded from support by manufacturers
[3] The number of users that have upgraded to the most recent OS versions

Digidentity uses an "allowed list" containing the supported OS versions. The use of list of supported versions ensures that deprecated, insecure OS versions are excluded by default while maintaining compatibility. When an OS version is deemed insecure or out of support, the version is removed from the list.

11.6.3 No direct access to HSM

The user does not have direct access to the Digidentity HSM. When the hashed pin code is received from the Wallet, the Digidentity Smart Card Manager (SCM) communicates with the HSM and sends the hashed pin to the HSM for comparison and access to the authenticator. The HSM returns the response to the SCM. The private keys never leave the HSM.

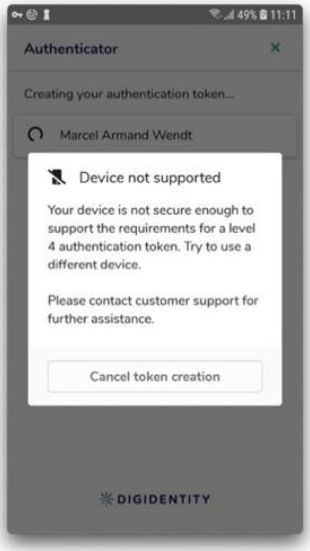
11.6.4 Authenticator (Virtual Smart Card) not transferrable

The Wallet on the mobile phone is uniquely linked to the secure vault on the HSM. The Wallet generates a unique device identifier which is stored in the secure vault. The device identifier ensures that the authenticator cannot be transferred, cloned, or replayed on another device. Each time a new certificate is issued, a new device identifier is generated. If the user has a new mobile phone, the user will receive a new authenticator (with new certificates) and the previous authenticator will be deactivated.

11.6.5 Only mobile phone with Secure Environments allowed

The Digidentity Wallet only works on mobile phones with a hardware-based Security Environment (SE). Digidentity maintains a list of approved or certified SE. When a mobile phone does not have an SE which is on the list, the Digidentity app cannot be used.

A mobile phone that does not have a trusted hardware-based SE will receive a message that the device is not supported (see screenshot).



Digidentity uses the Secure Environment, a hardware-based key manager that is isolated from the main processor, to provide an extra layer of security. Digidentity uses symmetric keys (AES) generated by the SE to secure the communication between the Digidentity Wallet and the Digidentity servers. Keys are generated and stored in the SE, making it nearly impossible for the keys to become compromised. Instead, you instruct the SE to create the key, securely store it, and perform operations with it. An SE also cannot import pre-existing keys. Keys must be created directly inside the SE. Not having a mechanism to transfer key data into or out of the SE is fundamental to its security.

Digidentity performs various checks to detect the presence of an SE such as extracting information from the device, which is then sent to and processed in the backend to mitigates attempts to tamper with the device.

These checks include (but are not limited to) whether an Android device contains an attestation key signed by a third party such as Google (ensuring the key is located in an SE). All supported Apple iPhones contains a secure environment.

Similar to devices without an SE, devices with a publicly compromised and exploitable SE cannot register digital identities for eIDAS level Substantial and High. Digidentity uses a 'block list' to excluded devices with a compromised and exploitable SE. The message shown above is presented on devices which are on the "block list".

11.6.6 Out-of-bounds notifications

Digidentity uses out-of-bounds notification systems from a third party to send authentication notifications to the mobile device to prevent Man-in-the-Middle attacks. These notifications are sent when a transaction using the authenticator is requested. The user will always see the notification when the smart card is used, and confirmation is needed using the memorised pin code to approve the authentication request. If a hacker wants to use the smart card, the user can cancel the request and revoke the certificates.

11.6.7 No use of mobile device biometrics

Digidentity does not support any biometric functions of the mobile phone. Most mobile phones provide biometric authentication using fingerprint or face recognition to unlock the mobile phone, make payments, unlock applications or confirm authentication. The Wallet does not allow the use of mobile phone biometric functions to replace the pin code. The user must always use the pin code to confirm the request.

11.6.8 Mandatory Re-identification

In the event the user loses their mobile phone, deletes the Digidentity wallet from their phone or their phone has been stolen access to their VSC is lost, the user can then start the recovery process. The recovery process requires the user to provide identity evidence by uploading the identity document and performing liveness detection and face comparison. After the mandatory remote identification is performed, the user can create a new smart card.

11.6.9 System Camera

To successfully complete the remote identification process, the Wallet requires consent from the Applicant to access the system camera of the mobile device. This will allow the Applicant to scan the QR-codes, take photos of identity document or take selfies. The Wallet does not allow access to the camera roll of the mobile device to prevent the Applicant to add previously taken photos or videos.

11.7 Penetration tests & Vulnerability Scans

The Digidentity VSC solution is subject to regular audits and security tests such as penetration tests and vulnerability scans on the authentication solution based on mobile phone in combination with the Wallet, the website and the back-office systems and trustworthy systems. A recently performed penetration test with attack potential **High** against on the complete system was performed by an experienced international external party (clients: public organisations, healthcare, financial institutions, etc).

The following topics were in scope of the penetration tests:

[1] Eavesdropping
[2] Tampering
[3] Guessing
[4] Replay attacks
[5] Man-in-the-Middle
[6] Duplication
[7] Counterfeit
[8] Disclosure of the cryptographic keys

The result of the penetration tests show that all of the above topics have passed the test, and no major findings have been registered. Low risk findings are already handled in the change management process to be resolved. Penetration tests are performed at least annually and, in the case, where significant changes of components have been made. This is a requirement from the eIDAS regulation and ETSI standards for Qualified Trust Service Providers. Digidentity uses external expertise to perform penetration tests and vulnerability scans on all systems including the Wallet and identity registration flows.

11.8 Threat & Mitigation Summary

The table below contains a summary of the threats and mitigation.

	Man-in-the-Middle	Injection	Presentation Attacks	Reverse Engineering	Dynamic Analysis	Replay Attacks
Jailbreak/Root detection	✓	✓	✓	✓	✓	✓
App Attestation	✓	✓	✓	✓		✓
Code Hardening				✓	✓	
Code Obfuscation				✓	✓	
Data encryption	✓				✓	✓
Communication encryption	✓	✓				
Certificate Pinning	✓	✓				✓
Hostname verification	✓	✓				✓
Application Shielding	✓	✓		✓	✓	

12 Business Resilience @ Digidentity

Digidentity is committed to providing the best possible experience to its customers and the best possible relationships with employees, shareholders and suppliers. To ensure the consistent availability and delivery of its products, Digidentity has established a comprehensive Business Continuity policy. This policy supports an integrated program encompassing Business Continuity, Disaster Recovery, and overall business survivability, ensuring the organisation can maintain operations under a wide range of adverse conditions.

Digidentity, like any other firm, is exposed to potential risks that could disrupt or destroy critical business functions and/or the production and delivery of Digidentity's products. The strategy for the continuation of business in the event of an incident, is to ensure the safety and security of all employees, and to continue critical business functions, production and delivery of products from predefined alternative sites.

12.1 Business Continuity Plan

Business Continuity requirements are documented in ISO27001:2022 - Annex A5.29-A5.30, and ETSI EN 319 401 - Section 7.11.

Digidentity has developed and implemented a Business Continuity Plan (BCP) to address risks that could disrupt or destroy critical business processes. We perform and document business impact analysis (BIA) to determine the effect of disruptions to our products and processes. The BIA are used as a basis for the BCP.

During the BIA, we determine the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for our systems. The Recovery Time Objective (RTO) of the authentication and signing services is four (4) hours. As products are real time processes and there is no data to restore, Recovery Point Objectives are not applicable for authentication and signing products.

All business continuity procedures are documented and reviewed at least annually or in the event a significant change will be implemented.

12.2 Crisis Management Plan

The Crisis Management Plan (CMP) defines the Crisis Management Team (CMT), its members and responsibilities. It provides definitions of crisis types and scenarios of a major incident as well as an escalation line for critical situations. This plan should be used along-side the Incident Management Process.

The CMP defines the Top Management authorities in terms of incident invocation, business recovery, warning and communication with customers and internal teams. This plan will help senior management with their decision-making process; by testing this plan on an annual basis they will become familiar with their roles and all the circumstances to be considered in case of a disaster.

The plan covers only the disaster coordination and certain details on company level, for departmental specific details, please see the BIAs and BCP.

The plan expands to all business processes, employees and contractors outlining the management and coordination of the sites/building in case of a business disruption. It provides documentation methods and forms to be filled out, suggests scenarios and instructions for a standing down process.

12.3 High Availability

Availability requirements are documented in ISO27001:2022 - Annex A8.14, and ETSI EN 319 401 - Section 7.11.

Digidentity has implemented high availability solutions to make sure customer systems are available 24x7.

The cloud provider (AWS Dublin) maintains three Availability Zones (AZ). Each zone is a fully isolated partition of Digidentity's infrastructure. All applications and products are configured across multiple AZ to achieve high availability and isolate any issue within a single AZ without affecting the application and service in other AZ. In case AWS Dublin is unavailable, products can be moved to AWS Frankfurt to guarantee availability of products.

Digidentity has multiple internet providers which allows us to use several routes for each process that supports our products. When one provider experiences downtime, we are able to switch to alternative routes to guarantee availability of our processes.

Digidentity product systems are based on lightweight Kubernetes and set-up as a micro-cloud system that runs in active-active mode to guarantee high availability of customer products.

Critical services such as HSM cannot be provided from the cloud and are redundantly set up in an active-active configuration in data centres located in The Netherlands. All systems are implemented with sufficient redundancy to meet availability requirements. All systems are divided across two data centres to maintain availability of critical services.

Digidentity has an availability of 99,8% 24x7 as defined in the Service Level Agreement. We calculate our availability on an annual basis. Our availability numbers are:

- Last 3 months: uptime 99.99% (including unplanned outages)
- Last year: uptime 99.99% (including unplanned outages)
- Last 3 years: uptime 99.85% (including unplanned outages)
- Average availability is 99.99% (minus the unplanned outages)

12.4 Backup & Restore

Backup & Restore requirements are documented in ISO27001:2022 - Annex A8.13, and ETSI EN 319 401 - Section 7.11.

Digidentity ensures that all data for which it is responsible, is securely and routinely backed up.

Digidentity has a responsibility to ensure that data which has been backed up, can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances. Regular restore tests are performed to establish the effectiveness of the backup and restore procedures by restoring data from backup copies and analysing the results.

All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration.

Wherever practicable:

[1] Backup media must be encrypted and appropriately labelled

[2] Any system used to manage backed-up media should enable storage of date(s) and codes/markings. This enables easy identification of the original source of the data and the type of backup used on the media

[3] All encryption keys should be securely kept at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster

12.5 Recovery Time Objectives & Recovery Point Objectives (RTO & RPO)

The Recovery Time Objective (RTO) of the authentication and signing services is four (4) hours. As services are real time processes and there is no data to restore, Recovery Point Objectives are not applicable for authentication and signing services.

Disaster Recovery Plans (DRP) are written to meet the RTO requirements. Digidentity performs annual disaster recovery testing to verify compliance to the requirements.

12.6 Disaster Recovery

Disaster Recovery requirements are documented in ISO27001:2022 - Annex A5.29/30, and ETSI EN 319 401 - Section 7.11.

Digidentity is prepared for disaster and has defined and implemented controls to anticipate major disruptions. As a part of the BCP and DPR have been developed to address service recovery.

Disaster recovery plans are written for business-critical systems to meet the RTO requirements. Digidentity performs annual disaster recovery testing to verify compliance to the requirements.

12.7 Business Continuity Tests

The BCP and DRP are tested annually to determine if it's complete and will fulfil its intended purpose. The BCM is tested once a year by performing either a table-top exercise, structured walk-throughs or simulations.

13 Compliance

Digidentity is a Qualified Trust Service Provider (QTSP) under the EU Regulation 910/2014, also known as eIDAS. As a Qualified Trust Service Provider and Identity Provider, Digidentity is required to comply with a range of regulatory, standards and schemes requirements.

13.1 Standards, Schemes & Regulations

Digidentity is compliant to the applicable requirements of the following standards, schemes, and regulations:

- ISO27001:2022 Information Security Management System (ISMS)
- ISO27701:2019 Privacy Information Management System (PIMS)
- ISO27017:2015 Information Security in the Cloud
- ISO27018:2019 Securing Personal Data in the Cloud
- ISO9001:2015 Quality Management System (QMS)
- ISO22301:2019 Business Continuity Management System (BCMS)
- ETSI EN 319 401 General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 1: General requirements
- ETSI EN 319 411-2 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for Trust Service Providers issuing certificates – Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI TS 119 461 Electronic Signatures and Infrastructures (ESI) - Policy and security requirements for trust service components providing identity proofing of trust service subjects
- eIDAS Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Chapter III – Trust Services
- GDPR Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- DORA Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector
- NIS2 Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity
- CA/Browser Forum Network and Certificate System Security Requirements
- PKIoverheid Program of Requirement for issuance of PKIoverheid certificates – Requirements of Dutch government for issuance PKI certificates from Dutch government Root Certificate Authority
- UK Trust Framework Requirements of the UK government for Identity and Attribute Providers including requirements GPG45 (How to prove and verify someone's identity) for Right to Rent, Right to Work and Disclosure and Barring Service

13.2 Laws & Regulations

Digidentity continuously monitors the development of new laws and regulation applicable to Digidentity and our customers.

13.3 eIDAS - EU Regulation 910/2014 – Electronic Identification & Trust Services

EU Regulation 910/2014 (eIDAS) establishes a common framework for electronic identification (eID) and trust services for electronic transactions across the European Union.

Electronic Identification (eID)

Digidentity issues electronic identities for eHerkenning that allows for the mutual recognition of national electronic identification systems across EU Member States, enabling citizens and businesses to securely access online services in other countries. eHerkenning is notified under eIDAS for use in the European Union.

Trust Services

Digidentity provides trust services as defined in the regulation. These trust services include qualified electronic signatures (creating legally binding signatures for electronic documents) and qualified electronic seals (used by legal persons to guarantee the integrity and authenticity of their electronic documents). Qualified electronic signatures have the same legal effect as a handwritten signature.

Digidentity is a Qualified Trust Service Provider (QTSP) as defined in EU Regulation 910/2014, also known as eIDAS. As a Qualified Trust Service Provider and Identity Provider, the requirements in eIDAS are applicable to Digidentity. Where a reference is made to Regulation (EU) 910/2014, the amended version including 2024/1183 is referenced. To show compliance to eIDAS, the European standards ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI TS 119 461 are available. Digidentity is certified against these standards.

Implementing Acts

The European Union published the implementation acts for applicable eIDAS articles:

- Article 5a(23) Personal identification data and electronic attestations of attributes 2024/2977
- Article 5a(23) Core Functionalities Wallet 2024/2979
- Article 5a(23) European Digital Identity Framework 2024/2982
- Article 5b(11) Registration of Wallet Relying Parties 2025/848
- Article 5c(6) Certification Wallet 2024/2981
- Article 5e(5) Security Breaches EU Identity Wallet 2025/847
- Article 8(3) Levels of Assurance 2015/1502
- Article 24(1c) Identity and recipients of qualified certificates 2025/1566
- Article 28(6) and 38(6) Qualified certificates 2025/1943
- Article 29a(2) and 39a - Remote QCSD - 2025/1567
- Article 31(3) and 39(2) Certified QSCD 2025/1570
- Article 33(2) and 40 Recognition of qualified validation services 2025/1942
- Article 34(2) and 40 Qualified preservation services 2025/1946
- Article 42(2) Qualified electronic time stamps 2025/1929
- Article 45d(5), 45e(2), 45f(6) and 45f(7) Verification of electronic attestation of attributes 2025/1569

13.4 Directive (EU) 2022/2555 - Measures for a High Common Level of Cybersecurity (NIS2)

The Directive (EU) 2022/2555 on measures for a high common level of cybersecurity also known as Network and Information Security Directive (NIS2) came into force on 16 January 2023. NIS2 is applicable to any company operating in the EU. Article 2.1.ii specifically applies NIS2 to Trust Service Providers as Digidentity. Dutch Implementation Directive article 4(1) Essential entities which is defined in article 8(1.a) Qualified Trust Service Providers.

The Directive (NIS2) covers risk management, incident management, business continuity, threat and vulnerability management and supplier management. Digidentity has already implemented measures regarding these topics as part of compliance to ISO27001:2022. The measures of NIS2 are defined in Article 21.2. In the table below the measures are listed and matched with the relevant requirements in ISO27001:2022 and ISO22301:2019.

21.2	NIS 2 Measure	ISO27001:2022 Reference
[a]	policies on risk analysis and information system security	Information Security Policy (ISO27001:2022 Section 5.2, A5.1-5.6) and Risk Management (ISO27001:2022, Section 8)
[b]	incident handling	Incident Management (ISO27001:2022, A5.24-5.28)
[c]	business continuity, such as backup management and disaster recovery, and crisis management	Business Continuity Management (ISO27001:2022, A5.29-5.30, A8.14) ISO22301
[d]	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Supplier Management (ISO27001:2022, A5.19-5.22, A8.14)
[e]	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Security in Network and Information System acquisition (ISO27001:2022, A5.23-5.26)
[f]	policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Risk Management (ISO27001:2022, Section 8)
[g]	basic cyber hygiene practices and cybersecurity training	Security Awareness (ISO27001:2022, A6.3)
[h]	policies and procedures regarding the use of cryptography and, where appropriate, encryption	Cryptography (ISO27001:2022, A8.24)
[i]	human resources security, access control policies and asset management	HR Security (ISO27001:2022, A6), Access Management (ISO27001:2022, A5.15-5.18, A8.18-8.19) and Asset Management (ISO27001:2022, A7.10-7.11, A8.1-8.5)
[j]	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate	MFA (ISO27001:2022, A8.5)

Digidentity has implemented a management system for information security (ISMS) and business continuity (BCMS). These systems have been certified against the requirements of ISO 27001:2022 and ISO 22301:2019. Based on the measures outlined in the Directive, Digidentity also meets the applicable requirements of NIS2.

13.5 Regulation (EU) 2022/2554 - Digital Operational Resilience (DORA)

The Regulation (EU) 2022/2554 also known as Digital Operational Resilience Act (DORA) has entered into force on 16 January 2023. DORA is applicable to financial entities.

DORA addresses the components of operational resilience. DORA defines rules for protection, detection, containment, recovery and repair in case of IT-related incidents. The Regulation (DORA) covers ICT risk management, incident management, resilience testing, threat and vulnerability management and third-party risk management.
DORA is not directly applicable to Digidentity as we are not directly working in the financial sector.

However, Digidentity has financial entities as customers. Those customers require their suppliers to comply to DORA. Digidentity has implemented measures to comply to the Regulation. This document describes Digidentity's response to contractual requirements and operational resilience.

Digidentity is not part of the core products of financial entities. **Digidentity provides identity proofing, authentication and signing products which are non-critical.**

Digidentity has implemented measures to comply to the Regulation. These measures are described in the next sections.

Digidentity demonstrates its commitment to operational resilience and compliance with the Digital Operational Resilience Act (DORA) by aligning its practices with the internationally recognised ISO22301:2019 standard for BCMS.

The ISO22301 certification ensures that Digidentity has implemented robust policies, procedures, and controls to prevent, manage, and recover from disruptions that may affect the availability and integrity of critical services. These measures align with DORA's core objectives, including ensuring operational continuity, minimising the impact of disruptions, and safeguarding the resilience of ICT services.

Key elements of compliance include:

[1] Business Continuity Management System:

Our ISO22301-certified BCMS ensures a structured and proactive approach to identifying and mitigating risks to our operations and ICT systems, a fundamental requirement of DORA.

[2] Disaster Recovery & Incident Management:

Digidentity has established disaster recovery plans, incident response procedures, and redundant systems to ensure the resilience of our operations in line with DORA's expectations for managing operational disruptions.

[3] Third-Party Risk Management:

By incorporating DORA-aligned processes into our BCMS, we actively monitor and mitigate risks associated with third-party service providers, ensuring compliance with supply chain resilience requirements.

[4] Annual Audits & Continuous Improvement:

Digidentity is audited annually by DNV - Business Assurance (Certificate C707812) to maintain its ISO22301 certification, ensuring ongoing compliance and continuous enhancement of resilience capabilities.

The Digital Operational Resilience Act (DORA) addresses the key components of operational resilience. It establishes rules for the protection, detection, containment, recovery, and repair of IT-related incidents, ensuring that financial and digital service providers can maintain continuity and mitigate risks effectively.

DORA requires organisation to implement measures for:

- ICT risk management
- Incident reporting
- Operational resilience testing
- ICT third-party risk monitoring

The Regulation (DORA) covers ICT risk management, incident management, resilience testing, threat and vulnerability management and third-party risk management.

Digidentity has already implemented measures regarding these topics (based on requirements from ISO27001:2022 and ETSI EN 319 401). To determine the impact of the Regulation, measures for implementation will be defined by the Member States.

Digidentity has achieved certification of our BCMS against the requirements within ISO22301:2019. ISO22301:2019 contributes to Digidentity's compliance to DORA.

13.6 Contractual requirements (DORA)

Article 30 of EU Regulation 2022/2554 defines the key contractual requirements applicable to relevant entities, establishing a framework for obligations and responsibilities under the Regulation.

13.6.1 Locations of products provided

Digidentity delivers products from locations in the European Economic Area (EEA). Details on the locations that Digidentity uses are published in our Privacy Statement available on our website: (https://www.digidentity.eu/documentation).

If Digidentity changes the location of processing, we will inform customers of changes to the locations. Digidentity will not ask permission the change the processing location. Digidentity does not seek individual customer approval for such changes, as our products are standard offerings used by millions of customers, making individual consent impractical. Waiting for approval from all customers would limit the flexibility and scalability of our products. Any change in processing location is reported to the supervisory authority as a significant change.

13.6.2 Right to Audit

Customers want the right to audit. Our products eHerkenning and QES are standard products based on requirements from Dutch Trust Framework (eHerkenning) and EU Regulation 910/2014 (eIDAS). Digidentity is inspected annually by the Dutch government (RDI) for eHerkenning and QES. Digidentity is only allowed to provide these products if the supervisory body has evidence of compliance.

Digidentity does not have the resources to support audits from customers (that would result in thousands of audits per year).

Digidentity has been certified against the requirements from several security, quality, privacy, identity and business continuity standards, frameworks (eHerkenning) and regulations. Customers must rely on the results of the independent certification audits that cover our products.

Digidentity will support audits by supervisory bodies.

13.6.3 Processing of Personal Data

Processing of Personal Data is covered in the EU Regulation 2016/679 also known as GDPR. These requirements are not a part of DORA. Information on processing of Personal Data is documented in our Privacy Statement available on our website: (https://www.digidentity.eu/documentation).

13.6.4 Return of data

Digidentity process data on behalf of the end-users and not on behalf of corporate customers. No data can be returned when the contract is terminated as we do not have data of corporate customers.

13.6.5 Service Levels

The Service Level Agreement (SLA) applies to Digidentity's standard products. Customised service levels cannot be accommodated for these products, as doing so would impact all customers. Only when updating service levels benefit the majority of customers, will Digidentity update the standard SLA.

See document "SLA @ Digidentity".

13.6.6 Participation in training

Digidentity has millions of customers using standard products. Digidentity cannot participate in training from each customer regarding security awareness and resilience.

Digidentity has an extensive security awareness and operational resilience training program for our employees. These programs are required by laws, regulations and standards and are verified annually by external auditors and supervisory bodies.

The fact that Digidentity has certificates for several standards is evidence that our awareness and operations resilience programs are implemented and effective.

13.7 AI Act - EU Regulation 2024/1689 – Artificial Intelligence Act (AIA)

Digidentity uses artificial intelligence from BioID in Germany for liveness detection and face comparison as biometric verification to confirm that the person is the person he or she claims to be.

The definition of 'remote biometric identification system' (article 3.41) is an AI system for the purpose of identifying natural persons, without their active involvement, typically at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database.
The BioID AI does not meet this definition if the AI used for biometric verification used photos that have been actively taken by the natural person. The BioID AI does not compare the biometric data to a reference database but only compares the photos provided by the user.

Article 5 of the AIA defines the prohibited practices of AI. Both article 5.1h and article 5.2 prohibits AI to be used for real-time biometric identification in publicly accessible space with the purpose of law enforcement. The BioID AI is not used for biometric identification for law enforcement and is therefore not prohibited.

Article 6 of the AIA define the classification of high-risk AI. The BioID AI for biometric verification is not listed in Annex I of the AIA. Article 6.2 refers to Annex III of the AIA. Annex III of the AIA refers to AI systems that are considered high-risk.

Annex III, article 1 lists AI to be used for biometrics. Article III.1(a) lists 'remote biometric identification systems' as high-risk. Article III.1(a) also contains the exemption for "This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be."

The BioID AI that Digidentity uses for biometric verification meets the definition of the exemption and is therefore not high-risk AI and the requirements for high-risk AI are not applicable. Digidentity and BioID have implemented measures to achieve the appropriate level of accuracy, robustness and cybersecurity.

13.8 Other Assurance Statements (Digidentity does not have)

Digidentity does not have an ISAE3402 Type II (International Standard on Assurance Engagements) report nor a SOC2 (Service Organisation Control) report. A Type II statement documents management of controls over a period of time (typically 12 months). ISAE3402 or SOC2 reports by service organisations to their customers assurance that the implemented security controls are effective. ISAE3402 or SOC2 reports are often required when outsourcing financial processes to a service organisation. Digidentity does not perform financial processes or transactions for our customers. Digidentity offers standard products for digital identities and digital signatures. These products are standardised for all customers.

To deliver our digital identity and digital signature products, Digidentity must comply to several detailed security standards as ISO27001 and ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2. Digidentity products also comply to European regulations as EU Regulation 910/2014 also known as eIDAS (Regulation defining Trust Services and Electronic Identities) and EU Regulation 679/2016 also known as GDPR. Digidentity must comply to all these standards and regulations to be allowed to provide our products and services as a Certificate Authority and Qualified Trust Service Provider. Digidentity is audited against the requirements in the standards and regulations annually by an independent external auditor and are under supervision by the Dutch government (Dutch Authority for Digital Infrastructure).

An ISAE3402 or SOC2 report is not applicable to Digidentity as we do not execute financial processes for customers. Our existing certifications offer assurance on information security, privacy and controls of our processes and systems.

14 Supervisory, Audits & Penetration Tests

Digidentity is subject to government inspections and external audits to assess compliance to regulations, standards and schemes.

14.1 Internal Audits

Digidentity carries out regular internal audits to continuously verify compliance with laws, regulations, policies, procedures, and other requirements. All internal audits are conducted at least annually for high-risk processes and at least once every two years for low-risk processes, following an approved schedule that is subject to external audit. As part of the internal audit program, Digidentity also performs the Trustworthy Systems audit.

All findings of internal audits are registered as tickets in our ticketing system. Audit tickets are assigned, and resolution tickets are linked. Digidentity monitors the resolution of audit tickets to make sure findings are resolved in a timely manner.

All audits, internal and external, are planned to minimise disruptions to operational processes.

14.2 External Audits & Certifications

Digidentity is audited annually by Attestic B.V. for the ETSI certifications to assess compliance with national laws, regulations and standards mentioned. Attestic B.V. is accredited by RvA (Dutch Accreditation Body) for assessments under ISO17065 and the requirements defined in ETSI EN 319 403. Attestic B.V. is bound by law, government regulation, or professional code of ethics.

ATTESTIC CERTIFIED — Public Key Certificates ETSI EN 319 411-1

ATTESTIC CERTIFIED — Public Key Certificates ETSI EN 319 411-1; Qualified Certificates Regulation (EU) 910/2014 ETSI EN 319 411-2

eIDAS

Digidentity is certified against the ISO27001:2022, ISO27017:2019, ISO27018:2015, ISO27701:2019, ISO22301:2019 and ISO9001:2015 standard. DNV Business Assurance carries out audits for ISO certifications to assess compliance with national laws, regulations and standards mentioned. DNV Business Assurance is accredited by RvA for assessments under ISO17021 (Certification of Management Systems).

INFORMATION SECURITY MANAGEMENT SYSTEM — DNV — ISO/IEC 27001 WITH EXTENSION OF ISO/IEC 27017 • ISO/IEC 27018

PRIVACY INFORMATION MANAGEMENT SYSTEM — DNV — ISO/IEC 27701

BUSINESS CONTINUITY MANAGEMENT — DNV — ISO 22301

QUALITY SYSTEM CERTIFICATION — DNV — ISO 9001

External auditors are independent and have no business interests in Digidentity. No external auditor has any business affiliation with Digidentity. Detailed description of our certifications can be found at the Digidentity website on our certification page.

14.3 Supervisory Bodies

Digidentity is inspected by the Dutch Authority for Digital Infrastructure for compliance with EU Regulation 910/2014 eIDAS on Trust Services (qualified electronic signatures) and electronic identities. Digidentity is registered on the EU Trust List (https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL/2)

14.4 Topics of Audits

The internal and external audits cover the requirements from the standards and regulations, internal policies and procedures. the topics addressed during audits are:

▪ Registration Service	Registration of new customers and verification of data
▪ Certificate Generation Service	Secure generation of PKI certificates for authentication, encryption and non-repudiation
▪ Revocation Management Service	Revocation of PKI certificates
▪ Revocation Status Service	Publication of revoked PKI certificates
▪ Dissemination Service	Publication of Certificate Authority documentation
▪ Network Security	Network security controls to protect data and systems such and network segmentation, firewall, intrusion detection, IP filtering, VPN segments, VLAN configurations, load balancing and network access controls
▪ Identity Proofing	Requirements for identity evidence and proofing methods
▪ Logical and Physical Access	Logical access to access systems and data. Two factor authentication on critical systems. Physical controls of office building and data centres
▪ Logging, monitoring & alerting	Logging of multiple events such as system access, system changes, certificate life cycle, monitoring and alerting on high risk/impact events
▪ Compliance	Security controls based on compliance to laws and regulations, monitoring on compliance changes and issues
▪ Human Resource Security	Screening of employees, security awareness training
▪ Business Continuity Management	Controls to guarantee continuity of business processes. Fail over mechanisms, redundancy, business continuity plan and exercises
▪ Threat & Vulnerability Management	Controls to protect against malware, vulnerabilities and other threats
▪ Organisational controls	Segregation of duties, four-eye principle, dual control access on high secure systems
▪ Development	Secure development of applications
▪ GDPR	Mandatory documentation, compliance to date retention, informing customers on processing personal data, principles of Privacy by Design and Privacy by Default, security controls, privacy awareness

14.5 Penetration Testing

Penetration Testing requirements are documented in ISO27001:2022 - Annex A8.34, ETSI EN 319 401 - Section 7.8, and CA/B Forum Network Security - Section 4.

Digidentity performs penetration tests on all systems, services, processes, internet facing systems, API and mobile applications. A focussed penetration test is performed when a significant change (new feature or major change to an application) will be implemented.

The penetration test on the full scope of our platform is performed annually. The focussed penetration test is plan on demand.

The full scope of the penetration test is:

- Web applications: internal applications and external, user applications
- Mobile applications: Digidentity Wallet on iOS and Android
- API (Application Programming Interfaces): message and transport security, authentication and authorisation protocols, input validation
- Internal infrastructure: servers, systems, network, firewalls
- External infrastructure (internet facing systems) - website, user applications
- Wifi: networks

The penetration tests use a combination of black box (no access, no knowledge), crystal box (live access, full knowledge), and grey box (limited access, partial knowledge) testing. The type of testing is in agreement with the company performing the penetration tests.

Digidentity has contracted an independent specialised company, Bureau Veritas Cyber Security (formerly Secura) (https://cybersecurity.bureauveritas.com/), to perform several security tests including penetration tests, code reviews and security testing on all systems, networks, applications, API's and end-points of Digidentity. Secura has the knowledge, skill, tooling, proficiency and experience to perform these tests.

Next to penetration tests initiated by Digidentity, the systems are also part of penetration tests performed by the Dutch government for PKIoverheid and eHerkenning. Occasionally, customers request to perform their own penetration tests.

For all penetration test, the tester must:

- Execute within the defined scope
- Perform the tests within the agreed-upon time windows
- Maintain logs of test activities
- Avoid causing disruption that impact production and denial of service
- Report critical and high-risk findings immediately

Any findings identified during a penetration test are recorded as an audit ticket and is monitored for corrective actions. High and Critical findings are addressed immediately and retested to provide evidence of mitigation.

Digidentity has contracted the accredited laboratory Cabinet Louis Reynaud (CLR) to perform a security evaluation on level High of our mobile applications. This evaluation will be in accordance with the requirements and procedures in the European standard EN 17640 Fixed-time Cybersecurity Evaluation Method (FITCEM).

The security evaluation will contain:

- Completeness check
- Review of security functions
- Security target assessment
- TOE installation assessment
- Compliance testing
- Review of vulnerabilities
- Vulnerability testing
- Penetration testing
- Extended cryptographic analysis

Digidentity aims to obtain formal certification against EN 17640 in 2026.

14.6 Resolving Non-Conformities

In case the auditor registers a non-conformity during an audit, Digidentity addresses the non-conformity in a Corrective Action Plan (CAP). In the CAP the actions and planning are documented to resolve the nonconformity.

For each nonconformity (from internal audit, external audit, penetration test or security assessment), a resolution time is defined. The table below provides an overview of the resolution time.

Priority	Resolution Time
Major Nonconformity	Within 60 days
Minor Nonconformity	Within 120 days
Observation	Within 180 days

Appendix A - Abbreviations & Definitions

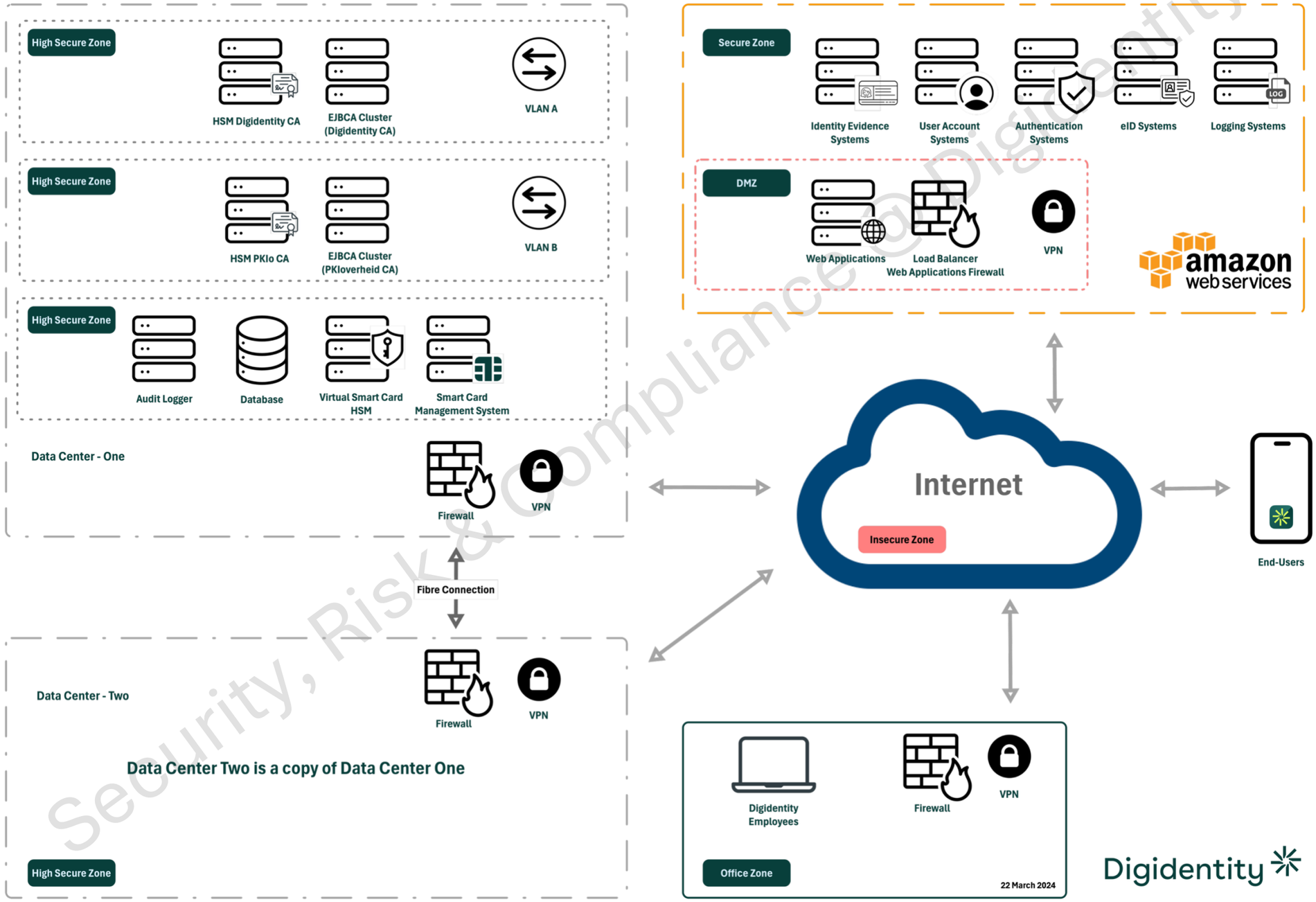
Term	Description
AA	Active Authentication
AdES	Advanced Electronic Signature
AML	Anti-Money Laundering
APCER	Attack Presentation Classification Error Rate The rate at which a given system fails to properly detect a presentation attack, similar to False Accept Rate (FAR) in biometric accuracy testing.
API	Application Programming Interface
APNRR	Attack Presentation Non-Response Rate The rate at which a given system fails to provide a response of any kind when an attack (spoof) is presented.
Applicant	Person (legal or natural) whose identity is to be proven. After identity is verified, Applicant becomes a Subscriber.
BAC	Basic Access Control
BPCER	Bonafide Presentation Classification Error Rate The rate at which a given system fails to properly detect a bona fide image (e.g. a real face), similar to False Reject Rate (FRR) in biometric accuracy testing.
CA	Chip Authentication
CC	Common Criteria
Certificate Holder	The entity stated in the subject field of the certificate, and the holder of the private key. Holders of personal certificates are natural persons. Holders of server certificates are organisations or natural persons.
CP	Certificate Policy
CRL	Certificate Revocation List
Cryptographic Key	A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. A cryptographic key is the core part of cryptographic operations.
CPS	Certificate Practice Statement
CS	Country Signer
CSCA	Country Signer Certificate Authority
CSP	Certificate Service Provider
CSR	Certificate Signing Request A request by a PKI user for their certificate to be signed by the CA. This signing means that the CA confirms the identity of the requester according to the PKI regulations.
DCNN	Deep Convolutional Neutral Network
DG	Data Groups

Term	Description
DIATF	UK Digital Identity and Attributes Trust Framework
DNN	Deep Neutral Network
DS	Document Signer
EAC	Extended Access Control
eID	Electronic Identity
eIDAS	Electronic Identification Authentication and Trust Services – EU 910/2014
eMRTD	Electronic Machine Readable Travel Documents
FAR	False Acceptance Rate Number of times the system incorrectly accepts an unauthorised person (person should have been rejected)
FITCEM	Fixed-time Cybersecurity Evaluation Method
FMR	False Match Rate (see FAR)
FNMR	False Non-Match Rate (see FRR)
FRR	False Rejection Rate Number of times the system incorrectly rejects an authorised person (person should have been accepted)
FIPS	Federal Information Processing Standards
FTA	Failure to Acquire
FQDN	Fully Qualified Domain Name (e.g. digidentity.com)
HT	Hash Table
HSM	Hardware Security Module Special equipment which generates and stores digital keys securely.
ICAO	International Civil Aviation Organisation
ID	Identity Document (e.g. passport, national identity card, driver's license)
IPSPS	Identity Proofing Services Practice Statement
KYC	Know Your Customer
LDS	Logical Data Structure
LEI	Legal Entity Identifier
MRTD	Machine Readable Travel Documents
MRZ	Machine-Readable Zone
NFC	Near-Field Communication
NCP	Normalized Certificate Policy
NTR	National Trade Register
OCR	Optical Character Recognition

Term	Description
OCSP	Online Certificate Status Protocol
OIN	Organisation Identification Number
PACE	Password Authenticated Connection Establishment
PAD	Presentation Attack Detection
PAI	Presentation Attack Instrument
Phishing	The fraudulent practice of sending e-mails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.
PKI	Public Key Infrastructure - a combination of processes and systems for the allocation and management of digital certificates.
PoR	Program of Requirements PKIoverheid
Private Key	The private key of the asymmetric key pair that is used to digitally sign or decrypt data. The private key may not be distributed.
Professional Body	an organisation with individual members practicing a profession or occupation in which the organisation maintains an oversight of the knowledge, skills, conduct and practice of that profession or occupation.
PROBAS	Protocollaire Basisadministratie (English: Protocollaire Administration)
Pseudonym	The use of a unique string of characters (numbers and letters) to identify a specific user. A name substitute.
Public Key	The public key of an asymmetric key pair used to digitally sign or decrypt data. The public key can be distributed.
PTC	Publicly Trusted Certificates
QCP	Qualified Certificate Policy
QCP-l-qscd	Qualified Certificate Policy for legal persons stored on qualified signature creation device
QCP-n-qscd	Qualified Certificate Policy for natural persons stored on qualified signature creation device
QES	Qualified Electronic Seal
QR-Code	Quick Response Code
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RA	Registration Authority - within PKI secure environment the control of client's personal details via the CA.
RDI	Rijkinspectie Digitale Infrastructuur (Dutch Authority for Digital Infrastructure)
Registration	The process of a user signing up and the subsequent verification of their identity and/or entity (organisation).
RtR	Right to Rent
RtW	Right to Work
SBR	Standard Business Reporting

Term	Description
SDK	Software Development Kit
SE	Secure Environment
Subscriber	Legal or natural person bound by agreement with a trust service provider to any subscriber obligations. When the Applicant has successfully completed the registration, they become a Subscriber
SSL	Secure Sockets Layer
Subject	The subject of a certificate is the party named in the certificate as the holder of the Private Key associated with the Public Key given in the certificate. The subject can be a; ▪ natural person ▪ legal person (e.g. Organisation) ▪ device or system operated represented by a natural or legal person
TLS	Transport Layer Security
TSP	Trust Service Provider
Validation	To confirm that something meets the requirements, is genuine and valid. Example: DDY uses cryptographic controls (NFC) to validate an Identity Document is genuine
Verification	To confirm that something is true or false using authoritative source(s). Example: DDY verifies the name of an Applicant using a validated ID
VIZ	Visual Inspection Zone
VSC	Virtual Smart Card

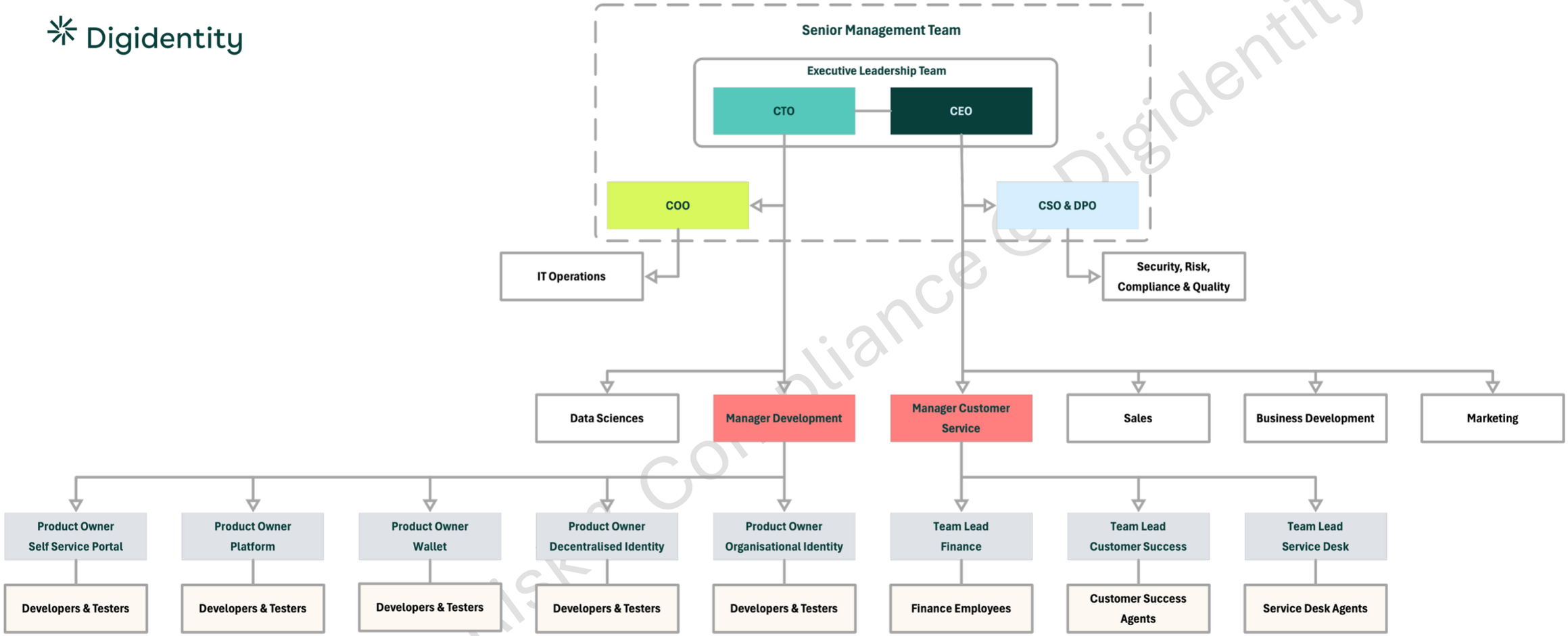
Appendix B - System & Network Diagram



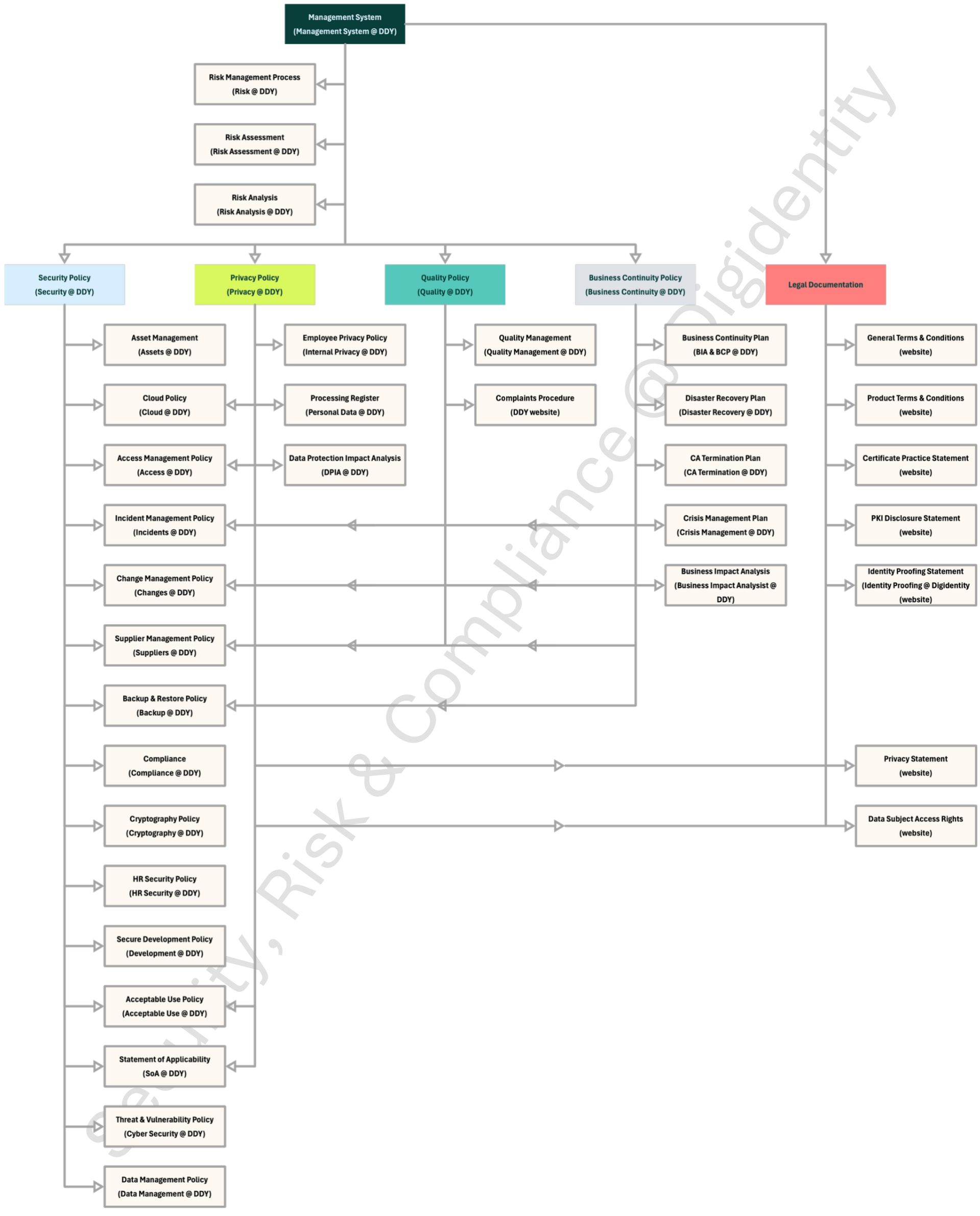
Digidentity

Appendix C - Organisational Chart

Digidentity



Appendix D – Documentation Overview



Appendix E – Regulations & Standard