Digidentity

DORA @ Digidentity

Compliance to DORA

Public

Title	DORA @ Digidentity – Compliance to DORA
Date	10 January 2025
Author	Sander Remmerswaal
Version	2025-v1
Location	website: https://www.digidentity.eu/documentation
Classification	Public

Revisions

Version	Date	Author	Changes Made (*)
2025-v1	10 January 2025	Sander Remmerswaal	Initial version

(*) All changes are marked in grey highlight.

20 Mar 2025 08:52 +0100
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Digidentity

Contents

1 Introduction 4

1.1 DORA Applicability 4

1.2 Product description 4

1.3 Digidentity & DORA 6

2 Contractual requirements 7

2.1 Functions of the product 7

2.2 Locations of products provided 7

2.3 Right to Audit 7

2.4 Processing of Personal Data 7

2.5 Return of data 8

2.6 Service Levels 8

2.7 Incident Management 8

2.8 Participation in training 8

2.9 Termination of contract 8

3 ISO22301 & DORA compliance 9

1 Introduction

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.

1.1 DORA Applicability

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.

1.2 Product description

Digidentity delivers standard products for authentication and electronic signatures. All products meet the applicable requirements to be allowed to provide these products. Digidentity cannot accept customer specific requirements for these standard products as this may violate the applicable requirements.

1.2.1 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).

DORA is not applicable to eHerkenning according to consideration 63 of the Regulation: "*To address the complexity..... should also be considered to be ICT third-party service providers under this Regulation, with the exception of central banks when operating payment or securities settlement systems, and public authorities when providing ICT related services in the context of fulfilling State functions.*"

Where Digidentity provides eHerkenning services as an ICT third-party service provider on behalf of public authorities providing ICT related services in the context of fulfilling State functions.

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 as Digidentity must comply to the requirements and are annually inspected by the supervisory body, the Dutch Authority for Digital Infrastructure (Dutch: Rijksinspectie Digitale Infrastructuur - RDI). Only participants that pass the government inspections, are allowed to provide authentication services.

Digidentity is one of the participants (Deelnemers) of eHerkenning providing authentication products (access to Service Providers and broker products (connecting Service Providers to eHerkenning). Digidentity has documented how eHerkenning works (document: eHerkenning @ Digidentity) which is available on our website: https://www.digidentity.eu/documentation

Authentication Product

Digidentity offers an authentication product (Dutch: middel) of eHerkenning to end-users to login government services or insurance services on behalf of an organisation. The product is a two-part product, first identification, authorisation and issuance. Second, use of the authentication product (access to Service Providers).

First, Digidentity must verify the identity of the person registering by checking identity document (valid ID). We use the personal data from the ID (autorotative source) to verify the personal data of the end-user. The use of an official document is required. Next, we ask the user to take selfies to make sure an actual person is registering, and we compare the face on the selfie with the photo on the ID to bind the person to the identity document.

These steps answer the questions:

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

When the identity of the end-user is verified, Digidentity must verify the organisation and of the end-user is allowed to act on behalf of the organisation.

First, the end-user provides the organisation registration number from an autorotative source (Chamber of Commerce, VAT, LEI). Digidentity verifies the existence of the organisation with the autorotative source and checks if the end-user is allowed to act on behalf of the organisation by checking the legal representatives. If the end-user is not registered as a legal representative, the end-user must obtain an authorisation from one or more legal representatives. After the legal representative(s) approve the authorisation, the eHerkenning products is issued to the end-user. The end-user can use the eHerkenning product to access government services.

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.

1.2.2 Outsourced Functions

Digidentity has outsourced parts of the product to external service providers. A list of service providers used and their location is documented on 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.

1.2.3 Product Customisation

Digidentity provides standard products for eHerkenning and QES. These products are based on the applicable requirements from the Dutch Trust Framework (eHerkenning) and EU Regulation 910/2014 (eIDAS) for QES.

Digidentity does not support customisation for these products as this would jeopardise compliance to the requirements.

1.3 Digidentity & DORA

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.

2 Contractual requirements

In article 30 of EU Regulation 2022/2554 key contractual requirements are defined.

2.1 Functions of the product

See Section 1.2 Product description.

2.2 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. As Digidentity provides a standard product used by millions of customers, it is not feasible to wait for all customers to approve this change. This would limit the flexibility of our products. Change of location is reported to the supervisory body as a significant change.

2.3 Right to Audit

Customers have the right to audit as defined in the master agreement. 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 does not have the resources to support audits from customers (that would result in thousands of audits per year). Hence the accredited certifications by independent auditors (BSI and DNV).

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 both eHerkenning as QES. Digidentity is only allowed to provide these products if the supervisory body has evidence of compliance.

Digidentity will support audits by supervisory bodies.

2.4 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).

2.5 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.

2.6 Service Levels

See document "SLA @ Digidentity".

Service level agreement applies to our standard products. Digidentity cannot accept customised service levels for these products as this will affect all customers. Only when updating service levels benefit the majority of customers, Digidentity will update the standard SLA.

2.7 Incident Management

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.

2.8 Participation in training

Digidentity has millions of customers using the 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.

2.9 Termination of contract

Exit and termination agreements should be part of the contract.

3 ISO22301 & DORA compliance

Digidentity demonstrates its commitment to operational resilience and compliance with the Digital Operational Resilience Act (DORA) by aligning its practices with the internationally recognised ISO 22301:2019 standard for Business Continuity Management Systems (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 (BCMS):
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.

By achieving and maintaining ISO22301 certification, Digidentity provides customers and stakeholders with assurance that our business continuity practices meet both the rigorous requirements of ISO22301, and the resilience requirements mandated by the DORA regulation. This dual alignment underscores our dedication to secure, reliable, and compliant digital services.

Detailed description of our certifications can be found at the Digidentity website on our certification page.