Peer Review Report – Netherlands

Document information

Version:	v. 1.0
Status:	FINAL VERSION FOR COOPERATION NETWORK
Dissemination Level:	Coordination Network
Due date of peer review report:	29 May 2019
Actual submission date:	29 May 2018
Organisation name of lead partner for this peer review report:	Federal Ministry of the Interior, Building and Community (DE)
Coordinator:	Björn Metzler (DE)
Rapporteurs:	Christine Mahieu (BE), Erik van de Wynckel (BE), Lionel Antunes (LU), Ismaël Cissé (LU), Samantha Lawler (UK), Livia Ralph (UK), Julian White (UK)
Active Members:	AT, CZ, DE, FR, IT, NO, SE
Observers:	BG, EE, FI, HR, MT, SI, SK

Abstract

This peer review report provides technical observations on the Dutch Trust Framework for electronic identification, “eHerkenning”. In accordance with the eIDAS Regulation, a group of reviewing Member States formulated an opinion on the compliance of the Dutch eID scheme with the eIDAS regulation. This opinion has been formed by examining documentation about the scheme and interacting with Dutch experts on the scheme. Various aspects have been studied in depth to come to a well-founded conclusion on the reliability of the Dutch Trust Framework for electronic identification in relation to the eIDAS infrastructure. These aspects include the following elements: enrolment, electronic identification means management and authentication, and management and organisation. Participating Member States (MS) of this peer review have concluded that:

The Dutch Trust Framework for electronic identification complies with the Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market in the following ways:

- **Platform 1 - KPN, Reconi; for the levels of assurance “Substantial” and “High”,**
- **Platform 2 - Connectis, Unified Post, iWelcome and QuoVadis; for the levels of assurance “Substantial” and “High”, and**
- **Platform 3 - Digidentity; for the level of assurance “Substantial”**

for the topics of enrolment, electronic identification means management and authentication and management and organization.

Concerns have been raised by some Member States on whether the requirements for level of assurance “High” for Platform 3 have been met for electronic means management and authentication. These concerns relate to the current implementation of Digidentity’s virtual smart card solution.

History

Version	Date	Changes made	Modified by
0.1	25 April 2019	First draft: structure of the document	Coordinator

0.2	13 May 2019	First complete draft	Coordinator, Rapporteurs
0.3	21 May 2019	Second complete draft	Coordinator, Rapporteurs, Active Members
0.4	28 May 2019	Pre-final version	Coordinator, Rapporteurs, Active Members
1.0	29 May 2019	Final version, published on CEF Cooperation Network space	Coordinator, Rapporteurs, Active Members

List of Abbreviations

Abbreviation	**Explanation**
CC	Common Criteria
eIDAS Attributes	eIDAS Technical Subgroup: eIDAS Technical Specifications – Attribute Profile
eIDAS CN	European Commission COMMISSION IMPLEMENTING DECISION (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of 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
IdP	Identity Provider
ISO	Information Standardization Organization
PIN	Personal Identification Number
PUK	Personal Unblocking Key
QTSP	Qualified Trusted Signature Provider

Countries and country codes

Austria	(AT)	Estonia	(EE)	Malta	(MT)	Slovakia	(SK)
Belgium	(BE)	France	(FR)	Netherlands	(NL)	Finland	(FI)
Bulgaria	(BG)	Croatia	(HR)	Norway	(NO)	Sweden	(SE)
Czech Republic	(CZ)	Italy	(IT)	Slovenia	(SI)	United Kingdom	(UK)
Germany	(DE)	Luxembourg	(LU)				

Table of content

Table of content 5
Executive Summary 7
1 Introduction 8
1.1 Scope and Objective of Peer Review Report 8
1.2 Methodology of Work 10
1.3 Relations to the CN Environment 13
1.4 Relations to External Environment: outside CN 13
1.5 Legal Issues 13
1.6 Structure of the document 14
2 Topic 1: Enrolment 15
2.1 Application and registration 15
2.2 Identity proofing and verification (natural person) 16
2.3 Identity proofing and verification (legal person) 17
2.4 Binding between the electronic identification means of natural and legal persons 19
2.5 Conclusions on Topic 1 19
3. Topic 2: Electronic identification means management, authentication and interoperability 21
3.1 Scope and Questions 21
3.1.1. Electronic identification means characteristics and design 22
3.1.2. Issuance, delivery and activation 23
3.1.3. Suspension, revocation and reactivation 24
3.1.4. Renewal and replacement 26
3.1.5. Authentication mechanism 26
3.2 Conclusions on Topic 2 28
4. Topic 3: Management and organisation 30
4.1 Scope and Questions 30
4.1.1 Active members contributing to this topic 30
4.1.2 Scope 30
4.1.3 Questions 31

4.1.4 General provisions 31
4.1.5 Published notices and user information 33
4.1.6 Information security management 33
4.1.7 Record keeping 33
4.1.8 Facilities and staff 34
4.1.9 Technical controls 34
4.1.10 Compliance and audit 35
5 Conclusion 37
References 38
Documents are available on the pre-notification page of NL on the Cooperation network wiki. 38
Pre-Notification Documents provided on 4 December 2018 38
Documents provided between February and April 2019 and during the Peer Review Meeting 38
Additional Documents 39

Executive Summary

In line with the European Commission’s aims to set up a Digital Single Market and to increase trust in digital services, the eIDAS Regulation 910/2014 seeks to enable European citizens to carry out transactions electronically and adopt new services. This peer review report provides observations on the Dutch Trust Framework for electronic identification from participating Member States.

The eIDAS Regulation 910/2014 seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities. The Regulation will increase the effectiveness of public and private online services, electronic business and electronic commerce in the European Union.

1 Introduction

1.1 Scope and Objective of Peer Review Report

Objective

Peer review is a mechanism for cooperation between Member States that is designed to ensure interoperability and security of notified electronic identification schemes. The specific objective of the present peer review process is to enable the Cooperation Network to provide an opinion on the Dutch electronic identification scheme i.e. the Dutch Trust Framework for electronic identification “eHerkenning”.

The Netherlands are the first Member State to pre-notify an eID scheme for legal persons, thus initiating the notification process for the business domain.[1]

The peer review process should be seen as a mutual learning process that helps to build trust between Member States. Since trust in the eIDAS will be based on the confidence of MS in European eID schemes, it is vital to have a successful notification of each member states national eID scheme. Experts from participating MS have identified areas of interest and reported their observations in this document. Based on those observations, information has been gathered by rapporteurs on each topic and an overview of interesting matters has been provided. The Dutch Trust Framework for electronic identification has been discussed in depth and the input of Dutch experts / Identity Providers (IdPs) have been required to answer questions about the eID scheme.

This peer review aims to form observations on the level of trust that other Member States have in the assurance level of the Dutch scheme. In other words, this peer review report aims to indicate how the Dutch Trust Framework with its eID means complies with the eIDAS Regulation and to discuss the acceptance of the level of assurance of the Dutch Trust Framework for electronic identification.

Scope

The security and interoperability of the Dutch Trust Framework for electronic identification with the eIDAS Regulation are in scope for this peer review. This implies that matters that are an issue only on a national level are out of scope for this peer review.

[1] The Dutch Trust Framework also includes the citizen's domain (private persons), however, it is temporarily excluded.

Description of the scheme and its concepts

- Only the Dutch Trust Framework for the business domain (eHerkenning) is part of this notification, though all Means in eHerkenning (the Framework) are issued to natural persons and could theoretically be used to identify a natural person. Based on Mandates in the Mandates Registry, eHerkenning (the Framework) can also provide attributes about a legal person.
- An Identity Provider (IDP) is a means issuer + an authentication provider. The authentication provider (provides the login means for users) is the same party as the means issuer (issues login means). The authentication provider issues declarations to the service provider at various levels of assurance, confirming that the user is who they claim to be. In the Dutch Trust Framework, the authentication providers are interoperable with all recognition brokers.
- Mandates are specified by services and Mandate Registers make use of a service catalogue to receive this information. The legal representative is able to mandate powers to certain users per service in the catalogue. The service provider determines the granularity of its registered services in the service catalogue. Most of the times the service providers do register multiple different services, or in some cases they register a single service, or a portal. Users are explicitly mandated to make use of services; this is done via the mandate register.
- A user can buy and use different login means, from different means issuers/authentication providers, to access a service provider.
- With the consent of the user, the authentication provider can also supply attributes such as name, address, identification numbers etc. These attributes are supplied in an encrypted form to the service provider.

The list of IDPs and their means in the scope of this pre-notification are summarized in the table below. Several IDPs have joined together in the same platforms:

Platform of identity provider(s)	**LOA Substantial (matching to level EH3 of the Dutch Trust Framework)**	**LOA High (matching to level EH4 of the Dutch Trust Framework)**
Platform 1 - KPN, Reconi	• Enrolment: face to face identification • Authentication: Username/password + OTP by SMS	• Enrolment: face to face identification • Authentication: PKI Overheid qualified certificate stored on a CC certified SSCD (issued in the Dutch PKI scheme for the government) + pin code
Platform 2 - Connectis, Unified Post, iWelcome and QuoVadis	• Enrolment: face to face identification • Authentication: ▪ Strong password combined with 2-factor SMS ▪ Strong password combined with 2-factor OTP device	• Enrolment: face to face identification • Authentication: Any qualified certificate combined with strong password (a minimum of 3 types are necessary in the length of at least 8 characters. The types are

	(Token) - lifetime of 3 years for the OTP device.	lowercase, uppercase, numbers, special characters.)
Platform 3 - Digidentity	• Enrolment: Using remote identification. • Authentication: applicants will use the Digidentity App for 2FA	• Enrolment: Using face to face identification. • Authentication: applicants will use the Digidentity App for 2FA

The Dutch Trust Framework can be used by everyone, not only by Dutch citizens, but the legal person (the company) needs to be registered in the Dutch Chamber of Commerce and the user needs to be registered in the Dutch Personal Records Database.

The means have to be purchased by the user from the means issuers. The (public) service provider signs a contract with a recognition broker and pays for its services. These are not free-of-cost in The Netherlands. In accordance with the eIDAS Regulation, the users of the notified means outside of The Netherlands are not charged any costs.

1.2 Methodology of Work

The scope of the peer review was determined using Article 10, paragraph 3 of the Commission Implementing Decision (EU) 2015/296 which states "peer reviewing may include, but is not limited to, one or more of the following arrangements: (a) the assessment of relevant documentation; (b) examination of processes; (c) technical seminars; and (d) consideration of independent third-party assessment."

As such it was set out in the 12th Cooperation Network meeting on 30 January 2019 that the peer review of the Dutch Trust Framework for electronic identification would be led by a team of coordinators, who would then organize Member States around topics of interest. Rapporteurs have been appointed to lead each topic and their observations would be based on:

- a description of the Dutch Trust Framework for electronic identification provided by the Netherlands,
- a self-assessment of the eID scheme by the Netherlands and the current (initial) set of IdPs / means issuers (see below) against the relevant requirements of the eIDAS Regulation and underlying implementing acts,
- discussions with technical experts from the Netherlands and the IdPs and
- a visit to The Hague on 20 and 21 March 2019 to participate in a technical peer review meeting.

Several Member States have indicated they would like to work across several topic groups, or desired to participate in one topic, and provide input in to other topics. Member States could indicate if they wanted to play an active or a passive role. 'Active' indicates that a MS wishes to contribute actively to

the topic in the creation of questions and writing the report. An ‘observer’ status means that a MS wished to follow the proceedings and offer comments on the report.

As noted in Article 7, paragraph 2 of (EU) 2015/296, “Participation of the peer Member States [is] voluntary. The Member State whose electronic identification scheme is to be peer reviewed may not refuse the participation of any peer Member State in the peer reviewing process”. Germany agreed to participate in the review as the coordinator, Björn Metzler has taken up this role.

In this role the coordinator organized the practical aspects of process. He acted as the contact point for both the European Commission and the Netherlands. The European Commission has facilitated the creation of a collaborative working space on the CEF pages to assist with the peer review. The coordinator also coordinated the production of this report and ensured that the rapporteurs and active members were satisfied with the observations made in this report. The face-to-face technical meeting on 20 and 21 March was facilitated by the Netherlands.

In terms of topics and areas of interest, three topics were proposed and rapporteurs assigned. These were arranged as follows:

Topic 1: Enrolment

- Rapporteurs: Lionel Antunes, Ismaël Cissé (LU)
- Active members: AT, BE, CZ, DE, FR, IT, NO, SE, UK
- Observers: BE, BG, DE, EE, FI, FR, HR, IE, IT, MT, SI, SK

Topic 2: Electronic identification means management and authentication and interoperability

- Rapporteurs: Christine Mahieu (BE), Erik Van de Wynckel (BE)
- Active members: AT, CZ, DE, FR, IT, NO, SE, UK
- Observers BE, BG, DE, EE, FI, FR, HR, IE, IT, LU, MT, SI, SK

Topic 3: Management and Organization

- Rapporteur: Samantha Lawler (UK), Livia Ralph (UK), Julian White (UK)
- Active members: AT, BE, DE, FR, SE
- Observers: BE, BG, CZ, DE, EE, FI, FR, HR, IE, IT, LU, MT, NO, SI, SK

The coordinator team set up two weekly conference calls

- with the rapporteurs and active members and
- with the rapporteurs and the Dutch experts

to discuss progress, technical questions, answers and organizational issues. The conference calls also provided a feedback mechanism to ensure all MS could agree on the outputs and format of the peer review document. The weekly conference calls started:

- with the rapporteurs and active members on 11 February 2019 and
- with the rapporteurs and the Dutch experts on 18 February 2019

and concluded on 27 May. During this time the peer review was also conducted, as well as preparation of the peer review report (in May).

Overall, four separate question rounds took place. The main communications channel between the peer review group and the Netherlands was email which was used to distribute information on pre-releases, releases and updates of questions. These questions were collected by the rapporteurs via email. Questions were sent to the Dutch peer review team who, together with the IdPs, provided answers. Active members analyzed the answers, gave feedback and asked additional follow-up questions.

As part of the peer review, a face to face meeting took place in The Hague on 20 and 21 March 2019. At the meeting, several presentations by Dutch national experts were given. On the second day of the meeting, three presentations by the initial set of IdPs to the Dutch framework were given:

- A presentation by members of platform 1, consisting of several identity providers, namely KPN and Reconi with the claimed levels of assurance ''Substantial'' and ''High''.
- A presentation by members of platform 2, consisting of several identity providers, namely Connectis, Unified Post and QuoVadis with the claimed levels of assurance ''Substantial'' and ''High''.
- A presentation by members of platform 3, consisting of the identity provider Digidentity with the claimed levels of assurance ''Substantial'' and ''High''.

The IdPs were also available for additional questions on a confidential basis.

The meeting was particularly useful and insightful and aided the topic groups to understand in depth and discuss in detail the subject matter in hand.

This report will be submitted to the Cooperation Network prior to its meeting to discuss the compliance of the Dutch Trust Framework for electronic identification to the eIDAS regulation and, in particular, the levels of assurance it claims to have: substantial and high.

1.3 Relations to the CN Environment

This peer review process must be seen in the spirit of cooperation between Member States, with the exchange of information and sharing of best practices aimed at achieving the mutual recognition that will facilitate “cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.” (EU) No 910/2014 Recital 9).

The Netherlands are in the fifth group of Member States (together with the Czech Republic and Italy) to pre-notify their eID scheme and, in doing so, paved the way toward achieving the benefits of the eIDAS Regulation. It is vital to note that this report should not be seen in isolation, but instead as a step towards achieving the Regulation’s overarching aims.

The participating member states have not only gained experience of the Dutch eID solution, but also in conducting a peer review.

1.4 Relations to External Environment: outside CN

The executive summary of this peer review report can be considered as a means to communicate findings of interesting aspects of the Dutch Trust Framework for electronic identification in relation to eIDAS. Decision makers, the media and any other stakeholder can use this summary as a source of information regarding the security and interoperability of this eID scheme. It can be seen as a result of an intensive investigation of the eID scheme to support the opinion of the Cooperation Network.

The information provided in the summary of this document will be the foundation of trust of the EU and EEA-countries in the Dutch Trust Framework for electronic identification.

1.5 Legal Issues

When conducting the peer review and producing the report, the following legal issues had to be borne into consideration. As stated in Art. 7, paragraph 4 of the Commission Implementing Decision (EU) 2015/296:

“Any information obtained through the peer reviewing process shall be used solely for this purpose. Representatives of the Member States conducting the peer review shall not disclose any sensitive or confidential information obtained in the course of the peer review to third parties.”

As such, the peer review members have treated such information sensitively and with due confidence. This peer review report does not contain any sensitive or confidential information.

Equally all experts from Member States had to flag any possible conflict of interest as mandated in Art.7, paragraph 5, Commission Implementing Decision (EU) 2015/296 where it cites “Peer Member States shall reveal any possible conflict of interest which representatives nominated by them to take part of the peer review activities might have.”

Finally, when determining the scope and arrangement of the peer review, Art. 10, paragraph 3 of the Commission Implementing Decision (EU) 2015/296 was consulted, which posits:

“Peer reviewing may include, but is not limited to, one or more of the following arrangements: (a) the assessment of relevant documentation; (b) examination of processes; (c) technical seminars; and (d) consideration of independent third-party assessment.”

1.6 Structure of the document

This peer review has been divided into three topics. During the 12th Cooperation Network meeting on 30 January 2019, the CN decided on the scope of the peer review by agreeing on what topics and subtopics should be considered while conducting the peer review. Each topic has covered several interesting features of the Dutch Trust Framework for electronic identification. The topics are dealt with by providing a summary of the observations per area.

This report gives an overall description of the main subjects that were discussed within the following three topics, but does not intend to provide all the details given by the Netherlands.

Each chapter summarizes the questions and answers in a narrative style to provide context to the proposed conclusions.

The topics of the peer review are the following:

1. Enrolment.
2. Electronic identification means management and authentication.
3. Management and organisation.

As the Netherlands is the first member state to pre-notify an eID scheme for legal persons, additional sections of the Annex of the Commission Implementing Regulation (EU) 2015/1502 were applicable and had to be taken into account.

By combining the information that has been gathered in the topics a conclusion was formed.

2 Topic 1: Enrolment

This chapter addresses the peer review outcomes regarding the enrolment topic, and more specifically the following sections of the Annex of the Commission Implementing Regulation (EU) 2015/1502:

- 2.1.1 Application and registration
- 2.1.2 Identity proofing and verification (natural person)
- 2.1.3. Identity proofing and verification (legal person)
- 2.1.4. Binding between the electronic identification means of natural and legal persons

In the context of the Dutch Trust Framework, several identity providers have joined together in platforms, as described below:

- **Platform 1: KPN, Reconi**
- **Platform 2: Connectis, Unified Post, iWelcome and QuoVadis**
- **Platform 3: Digidentity**

These three platforms provide eID means with the claimed Levels of Assurance “Substantial” and “High”.

2.1 Application and registration

In the context of the Dutch Trust Framework, for both LoAs “Substantial” and “High”, the terms and conditions and recommended security precautions related to the electronic identification means (hereafter the “eID means”) are made available, through the application forms, through the user agreements and/or online on the means issuers’ websites.

In the context of KPN and Reconi, for both LoAs “Substantial” and “High”, the applicable terms and conditions and recommended security precautions are part of the user agreement signed by the applicant.

In the context of Connectis, Unified Post, iWelcome and Quovadis, for both LoAs “Substantial” and “High”, the applicant signs to demonstrate that they are aware of the applicable terms and conditions which contain the recommended security precautions.

In the context of Digidentity, for both LoAs “Substantial” and “High”, the registration process requires the applicant to agree with the applicable terms and conditions and privacy statement before starting the registration.

In addition, in all three cases, the information necessary to supply the Minimum Data Set is collected online and / or on paper via the application forms.

The processes ensure that the applicant is aware of the terms and conditions, as well as the recommended security precautions, and that the relevant identity data required for identity proofing and verification are collected.

2.2 Identity proofing and verification (natural person)

In the context of the Dutch Trust Framework, for both LoAs “Substantial” and “High”, the identification of the applicant is performed based on a legal identification document containing at least the applicant’s photograph, their signature and personal data such as first name, family name, date of birth and place of birth.

All legal identity documents related to a natural person (including foreign ones) must be registered by the Dutch authorities in the Dutch Personal Records Database, which is an authoritative source.

The identity document’s validity is verified against national or international databases. In particular, to check that identity documents are neither lost nor stolen the Identity Providers use, either national authoritative sources such as the National Police Force database, or international databases, such as Interpol.

The identification document’s genuineness is verified based on the document’s security features in comparison with templates in the PRADO database. The authenticity of foreign documents is verified by specially trained personnel.

In the context of KPN and Reconi, for both LoAs “Substantial” and “High”, a face-to-face identification of the applicant is performed.

During the face-to-face identification processes, security features are verified on the identity documents, such as hologram, kinegrams, watermarks, 3D-pictures and relief. Specific electronic checks such as active authentication, signature validation (passive authentication) and MRZ digit checks are also performed.

The applicant’s identity document is verified by a certified supplier for identity verification, certified for ETSI QTSP services.

In the context of Connectis, Unified Post, iWelcome and Quovadis, for both LoAs “Substantial” and “High”, the applicant can start registration by using an online or an offline registration process. During the registration process, a face-to-face identification of the applicant is performed by a certified subcontractor.

During the face-to-face identification processes, security features are verified on the identity documents, such as hologram, kinegrams, watermarks, 3D-pictures and relief. Specific electronic checks

such as active authentication, signature validation (passive authentication) and MRZ digit checks are also performed.

The applicant’s identity document is verified by a certified supplier for Identity verification, certified against ETSI (EN 319 411) and ISO27001.

In the context of Digidentity, for LoA “Substantial”, the registration process includes remote identification performed via the Digidentity application.

During remote identification, the applicant must present a legal identity document, which is verified in order to ensure its validity and genuineness.

In order to reduce the risk of fraud, the following security measures are in place:

- Anti-spoofing liveness detection: the applicant’s motion triggers the facial photos (selfies) which are taken.
- Visual comparison performed by an agent between the photo of the identity document and the facial photos (selfies) which are taken.
- Document genuineness checks are performed both automated and manually, and including verification of, MRZ (Machine-Readable Zone) for Passports, photographs, font type and quality, holograms, laminate integrity, spelling mistakes, print quality.
- Document validity is checked using the Interpol database.

For LoA “High”, the applicant is required to attend a face to face meeting with a Digidentity agent. During this meeting, the ID and physical appearance/details of the applicant are checked against the applicant’s ID document.

The processes of identity proofing and verification for natural persons for the three cases ensure that the applicants are in possession of recognized, genuine and valid identity documents and that steps have been taken to minimize the risk that the person’s identity is not the claimed identity, in accordance with the respectively claimed Levels of Assurance.

2.3 Identity proofing and verification (legal person)

In the context of the Dutch Trust Framework, for both LoAs “Substantial” and “High”, the identity of the legal person is verified, either online in the Trade Register of the Chamber of Commerce (which is considered as an authoritative source), or based on a recent original copy from the Trade Register (not older than 14 days).

For specific licensed professions (e.g. accountants, lawyers, civil law notaries), identification is also performed against relevant professional registers.

At the least, the following information is verified: the legal person's business name and legal name, at least one location address, the legal person's identification numbers and the legal person's correspondence address.

In addition, a legal representative or an authorized representative of the legal person must sign and submit an application form and a copy of their identity document. The signature, name and surname on the application form are verified against the information on the copy of the legal representative's identity document.

In the context of KPN and Reconi, for both LoAs "Substantial" and "High", the financial status of the organisation is also checked against the online insolvency register.

For LoA "High", the process for validating the identity of the legal representative includes face-to-face identification against their legal identification document.

In the context of Connectis, Unified Post, iWelcome and Quovadis, for both LoAs "Substantial" and "High, the identification process of the legal person includes verification that the legal person is not bankrupt.

For LoA "High", the process for validating the identity of the legal representative includes face-to-face identification against their legal identification document.

In the context of Digidentity, for both LoAs "Substantial" and "High", the applicant self-registers on Digidentity's platform which includes an API interconnected to the Trade Register of the Chamber of Commerce. This registration is performed using the company registration number and the business email address. Based on this information, the list of legal representatives or authorized representatives is extracted from the Trade Register of the Chamber of Commerce.

If the applicant is one of the listed representatives or authorized representatives, the applicant's identification process as described in Section 2.2 applies.

If the applicant is not listed as a legal representative, they are required to obtain authorization from all the representatives, and then submit 1) authorization letters signed by the legal representatives, 2) copies of their identity documents and 3) a set of facial photos (selfies) for each legal representative. Verification of these documents is performed by trained service desk agents.

For LoA "High", the process for validating the identity of the legal representative includes face-to-face identification against their legal identification document.

The processes of identity proofing and verification for legal persons for the three cases ensure that the claimed identity of the legal person is demonstrated based on recognized, genuine and valid documents.

In addition, these processes ensure that steps have been taken to minimize the risk that the legal person's identity is not the claimed identity, in accordance with the respectively claimed Levels of Assurance.

2.4 Binding between the electronic identification means of natural and legal persons

In the context of the Dutch Trust Framework, for both LoAs "Substantial" and "High", the identification of the natural person acting on behalf of the legal person is performed as described in section 2.2 for the applicant.
The binding between the natural person and the legal person is achieved using the Trade Register of the Chamber of Commerce. In particular,

- The involvement of the natural person with the legal person is verified
- The identity features of the natural person are verified against those of the applicant in the Trade Register
- The status (i.e. legal powers) and the position of the natural person in the legal person's organisation is verified (including verification that there is no restriction for this natural person to represent the legal person)

In addition, the natural person must submit:

- A signed document confirming their position within the organization.
- A declaration that they are authorized to file an application for the legal person

In the context of KPN and Reconi, for both LoAs "Substantial" and "High", the specifics described in Section 2.2 for the identification of the applicant apply.

In the context of Connectis, Unified Post, iWelcome and Quovadis, for both LoAs "Substantial" and "High", the specifics described in Section 2.2 for the identification of the applicant apply.

In the context of Digidentity, for both LoAs "Substantial" and "High", the specifics described in Section 2.2 for the identification of the applicant apply. In addition, the employment of the applicant within the legal person's organization is also verified via a company authorization.

The processes of binding between the electronic identification means of natural and legal persons for the three cases ensure that the identity proofing of the natural person is performed in accordance with the respective claimed Levels of Assurance, and that the binding has been established on the basis of recognized procedures and verified against authoritative sources.

2.5 Conclusions on Topic 1

Member States actively involved in reviewing this topic conclude that the notified scheme complies with the requirements of section 2.1 Enrolment, of the ANNEX of the Commission Implementing Regulation (EU) 2015/1502 for levels of assurance “Substantial” and “High”.

3. Topic 2: Electronic identification means management, authentication and interoperability

This chapter addresses the peer review outcomes regarding the topics of electronic identification means management, authentication and interoperability, and more specifically the sections of the Annex of the Commission Implementing Regulation (EU) 2015/1502. It assesses to what extent the pre-notified scheme fulfils the eIDAS requirements and clarifies elements queried by the reviewers.

The documentation relating to the content of topic 2 provided by The Netherlands describes in detail the Trust Framework for electronic identification and its IDPs. Once requested, each IDP provided a document describing the mapping of its solution with the eIDAS requirements for LoAs. Peer reviewers asked specific questions on different aspects of this topic (29 questions were posted for the 1st round of questions, followed by another 22 for the 2nd round, 23 on the 3rd round, and 4 additional questions during a 4th round). During the face to face meeting of 20-21st of March 2019, simultaneous round tables of 1 hour with each of the 3 platforms were organized. Each peer reviewer had the opportunity to discuss and ask questions of each IDP.

More clarification documentation was asked for after these round tables, but the Netherlands could not provide all the required documents, for example, descriptions of the architectural designs and network diagrams of the IDPs in the Dutch Trust Framework (as it is company confidential information). This is the main reason why some MS found it difficult to confirm that all the requirements of the eIDAS Regulation are fulfilled.

3.1 Scope and Questions

The questions can be clustered according to sections 2.2 and 2.3 of eIDAS 2015/1502 on this topic:

- 2.2.1. Electronic identification means characteristics and design
- 2.2.2. Issuance, delivery and activation
- 2.2.3. Suspension, revocation and reactivation
- 2.2.4. Renewal and replacement
- 2.3.1. Authentication mechanism

The next sections summarize if and how the pre-notified scheme fulfils the eIDAS requirements and provide further clarification by the Netherlands to questions asked by the reviewers.

To qualify for admission to the Dutch Trust Framework, the pre-notified authentication means and mechanisms must undergo a conformity assessment demonstrating that they are resistant to the attack potential “moderate” for LoA Substantial and attack potential “high” for LoA High as defined in the Common Criteria method. The Conformity Assessment Guideline provides participants (the IDPs) in the Dutch Trust Framework and conformity assessors with guidance on how to carry out the conformity assessment. Each IDP has to conduct a risk assessment annually regarding the security of their eHerkenning means. The risk assessments are evaluated by the supervisory body.

3.1.1. Electronic identification means characteristics and design

All electronic identification means in the scheme consist of two authentication factors (for both levels Substantial and High). The participating IDPs from Platforms 1 and 2 mostly fulfil these requirements using a username, password and OTP (via SMS or an OTP device), or a qualified certificate stored on a smart card. Digidentity from Platform 3 offers an app (for both LoA Substantial and High). During the process of creating a Digidentity account it is necessary to secure the account with a 2nd factor - in this case a virtual smartcard (including PIN code).

Questions were asked by reviewers about whether users can be mandated for multiple companies and have multiple accounts with a single IDP or across IDPs – it was explained that this is possible. The user has to choose the company to log in with during the login process. However, each account will have its own unique identifier and mandate registers. There is no consolidation of the different mandate registers; the user selects the mandate register to which they are linked to with their means.

Concerning SMS OTP, the reviewers asked for evidence of the resistance of SMS OTP against moderate attack potential. In response, the NL team explained that the Dutch Trust Framework has implemented several measures to mitigate the risks of using SMS as an out-of-band channel for OTPs. In detail, the following answers were given by the NL team:

- The Supervisory Body monitors the use and risks of SMS OTPs of the participating IDPs in the Dutch Trust Framework on a regular basis. At the moment the Supervisory Body sees no reasons for deprecation at level Substantial. If this changes, then the Supervisory Body will act accordingly and require the participants to stop using SMS as an out-of-band channel for OTPs.
- The user is informed by the participant about all its authentication transactions enabling the user to identify unauthorized authentications.
- Attacks by means of SIM swapping are difficult in The Netherlands, because mobile providers have introduced various security measures such as sending a verification SMS to the original SIM before the telephone number is issued and only issuing replacement SIM cards in person. Moreover, the IDPs have various monitoring and detection processes in place to mitigate against some of the risks when using SMS, thus making the attack less 'attractive' for attackers.
- For SS7 attacks, access to the internal telecom network is required. This is not trivial and requires specialized knowledge and, therefore, is not considered viable for attackers with a moderate attack potential.

- Hijacks via the exploitation of technical flaws (SS7) or through social-engineering (SIM-swap) do not scale; this observation makes these attacks less 'attractive' for attackers. Consequently, attackers with high attack potential will show less interest in executing these types of attack, let alone attackers with moderate attack potential.
- All authentication transactions are logged and made available by the authentication provider to the user: in the portal of the authentication provider the user can see what authentication transactions have been logged when and for which service provider. So, this allows the user to raise an alarm if something is wrong, which makes the attack less attractive for an attacker.

Given these answers, it was the peer reviewers' opinion, that the Dutch Trust Framework for electronic identification fulfils the requirements for resistance against attackers of moderate attack potential. High attack potential is out of scope, because SMS-OTP is not allowed at LoA High in the Dutch Trust Framework.

Regarding the app-based solution provided by Digidentity, the binding of a user's mobile phone to an account gave rise to concerns for some Member States as to whether this platform fulfils the eIDAS requirements for LoA high (resistance against "guessing, eavesdropping, replay or manipulation of communication" for attacker with high attack potential). Other Member States considered that the solution meets the eIDAS LoA high requirements.

3.1.2. Issuance, delivery and activation

The Dutch Trust Framework is the issuer of the electronic identity, but this is in conjunction with each IDP. After issuance, the electronic identification means are delivered via a mechanism that is meant to ensure that it is delivered only to the person to whom it belongs. In practice, the IDPs create an account and associate it with authentication credentials, then proof the user's identity, thereby binding them to that account. Once the binding is done, the identification means is activated.

For participating IDPs from platforms 1 and 2, activation typically takes place via an e-mail with an activation link or an SMS OTP. When reviewers queried this, the IDPs indicated that these activation credentials have a limited lifetime (i.e. several minutes) or can only be used once.

For platform 2, after registration of the qualified certificate at level High, the user will receive an email indicating that he/she can use the qualified certificate and the strong password as their identification means. The email is sent to the email address that is registered in the certificate and that was provided by the representative.

For platform 1, peer reviewers asked how it is ensured that the means are delivered to the person to whom they belong. Platform 1 uses two channels, SMS and email, to deliver the means. During registration they validate if the user has access to their email address by sending a link by email. The user has to click the link to a website and must enter the code that has been sent via SMS to their mobile number. After validating this, the account is activated. After/during activation an email is used to

deliver the username, and SMS is used to deliver the password. The password needs to be changed at first login.

For platform 3, Digidentity, once the process of registration is complete; the full product virtual smartcard is delivered to the applicant and can be used as a login means. The virtual smartcard is protected by a PIN CODE (5 digits) that is only available to the applicant. During the process of creating a Digidentity account, it is necessary to secure the account with a second factor authenticator - in this case a virtual smartcard (including PIN code).

The solutions provided by all platforms in this respect, were deemed sufficient by the reviewers for level Substantial, and the solutions provided by platforms 1 and 2 were deemed sufficient by the reviewers for level High. Platform 3, Digidentity, stated that the virtual smartcard is stored on an HSM (which is not in possession of the citizen, but of Digidentity), that authentication does not take place on the mobile device, and that no sensitive data is stored on the mobile device. Taking this in to consideration, some peer reviewers found it difficult to understand how the requirements of LoA high for the possession-based factor are fulfilled. For other reviewers no such concerns were given as certification as a QSCD was provided and explanations given to describe how the solution meets LoA high requirements.

3.1.3. Suspension, revocation and reactivation

Suspension and/or revocation of an electronic identification mean is done in a timely and effective manner.

The implementation of this situation may differ per means issuer (the IDPs):

- There are issuers who do not support suspension and reactivation. For instance, if users do not pay for the eID means, there is a violation of the terms and conditions that the user agreed to during the enrolment phase. In this situation the means issuer will revoke the means, typically after 30 days.
- Others issuers do support suspension. In that case, if the means are not paid for, they will typically be suspended for 30 days before they will be revoked. Therefore, there is a business incentive for the means issuer to encourage the user to pay for their means and consequently, shorten the suspension time as much as possible. Mechanisms used for reactivation of suspended means are:
    - By entering the PUK code that was obtained during enrolment.
    - By sending an activation link via email; note that during this process the second factor always has to be used.
    - By sending an activation code to the address of the user.

There is no minimum time period during suspension and re-activation of eID means. There is a maximum lifetime of 10 years for each eID means; this may change due to risk assessment outcomes.

Revocation can always be enforced by the participant (the IDP) or another authoritative body.

Platform 3, Digidentity, offers various options to revoke accounts and any associated certificates (smartcard), all of which render the account useless:

- Revoke Certificates: The subscriber is able to log into their account and click “Revoke certificates”. The subscriber is able to view their virtual smartcard which contains their certificates. By deleting a specific virtual smartcard, all three (3) associated certificates (authentication, encryption and non-repudiation) will be revoked. Revocation occurs immediately.
- Deactivate Account: The subscriber is able to log into his/her account and click “Deactivate my account”. The subscriber will receive a notification informing them that their account is deactivated for 30 days. After confirmation (of deactivation on the website) by the subscriber, the account is deactivated. If the subscriber logs into their account within 30 days after deactivation, the account is reactivated and all certificates registered to the account can be used. If the subscriber does not reactivate their account after 30 days the account is deleted and all certificates associated with the account are revoked immediately.
- Delete Account: The subscriber is able to log into their account and click “Delete my account”. The subscriber will receive a notification informing them that their data will be deleted and all certificates registered to the account will be revoked immediately. After confirmation by the subscriber all certificates are revoked and the account is deleted.
- Revocation via Digidentity: If an applicant requests their account to be removed and is unable to login or recover the account login credentials then Digidentity will action the request for the applicant. Revocation requests will be processed immediately upon receipt - within any framework/operations manual guidelines of 4 hours.
- Authorisation revocation: The organization that provides authorisation may request revocation of the authorisation they gave to an applicant. This means the authorisation is removed, rendering the account into an unusable and pending state.
- Authorisation revocation via Self Service Portal: The company admin can add/remove authorizations for their own listed applicants.

Platform 2: The suspension can last as long as the mandate manager or legal representative wants. The mandate manager or legal representative can revoke mandates via the Means and mandate management tool and then revoke the mean on paper. The delay for revoking the mean is not important anymore when there are no valid mandates. To prevent unauthorized suspension, revocation and/or reactivation, Unified Post only suspends, revokes and/or reactivates when the request is received from the mandate manager or legal representative. The user and the mandate manager receive a notification when mandate / means are suspended, revoked or reactivated. Revocation/suspension on paper will be conducted immediately after receiving the papers. Reactivation after revocation/suspension is possible. For reactivation, the process is the same as for activation.

Platform 1 does not support suspension neither reactivation. Online revocation is possible by the user 7*24.

The solutions provided by all platforms in this respect, were deemed sufficient by the reviewers for levels Substantial and High.

3.1.4. Renewal and replacement

To mitigate the risks of a change in personal identification data, renewal or replacement of electronic identification means, the same assurance requirements as initial identity proofing and verification apply. Alternatively, renewal or replacement is based on valid electronic identification means of the same or higher assurance level. Typically, a user may request a renewal when the mean is broken or lost.

Platforms 1 and 2: Renewal/replacement follows the same process as an initial application.

For platform 3, Digidentity, there are several processes in place for this:

- Lost applicant name: Email address is used in conjunction with 2FA.
- Lost password: the account recovery code (ARC) is used in conjunction with the 2FA and the applicant will be required to answer a security question.
- For a lost applicant name and password, the email address is used as the applicant name and recovery is not possible.
- If an applicant loses access to the 2FA, the applicant name, password, account recovery code (ARC) & security question are required. The applicant will then be prompted to add a new 2FA.
- If an applicant has lost their applicant name and 2FA, recovery will not be possible.
- Finally, if an applicant loses their Smartcard (underlying PKI Certificate), recovery is only possible through the Digidentity Service desk; the applicant will need to provide their legal identification document (and/or selfies) again.

After 5 years the virtual smartcard certificates will expire. This implies that the smartcard will become useless as a means to log in with after this time. After 5 years the applicant must reapply in the same way as their first registration.

The solutions provided by all platforms in this respect, were deemed sufficient by the reviewers for levels Substantial and High.

3.1.5. Authentication mechanism

Personal identification data is released to relying parties only after successful identity proofing has been completed to the level required by a relying party. Currently, only the minimum dataset, as specified under eIDAS, is provided and no optional data. Before an identity provider can implement an authentication credential, it is audited by the Radio Communications Agency (RCA) to ensure it meets the requirements.

The Netherlands described the authentication process followed by each IdP in the Dutch Trust Framework and where personal data is stored, as well as how this information is securely transmitted between the participants in the Dutch Trust Framework. The strength of the protective measures that are enforced during the internal processing of identity information by the participants in the Dutch Trust Framework is covered by ISO27001 certification that all participants have. Each IDP stores all relevant identity information (typically the eIDAS minimum dataset) that is obtained and verified during enrolment in a database (typically LDAP/Active Directory based). All identity information - whilst in the database - is encrypted. The Mandate Register (MR) maintains an overview of mandates; each mandate specifies per eID mean what services can be accessed. Based on the mandates, the Mandate Register can check and will decide whether or not the user is allowed to access the service requested. If the user is not entitled to do so, the process will stop. During authentication, the Recognition Broker (RB) redirects the SAML authentication request of the Relying Party (RP) / Service Provider (SP, in this case the foreign eIDAS connector) to the IdP. Subsequently the IDP authenticates the user and returns a SAML response to the RB. This response includes, amongst others, the eIDAS minimum dataset that is fetched from the LDAP/AD database. The RB forwards the SAML assertion to the RP/SP.

All SAML communications between stakeholders in the framework are two-sided TLS-secured with qualified certificates (issued under the root of the Kingdom of the Netherlands). All these certificates can be found in the (SAML) metadata files of the framework that is managed by the Management Organisation. An overview of the SAML metadata and a description of the interface specifications are publicly available (https://afsprakenstelsel.etoegang.nl/display/as).

The active MS asked which measures are in place to mitigate "guessing, eavesdropping, replay or manipulation of communication" in the context of SMS-OTPs and the app-based solutions. Answers were given regarding the overview of the secrets used by the IDPs (for SMS-based and App-based systems) in terms of the minimum lengths of PINs and OTPs, their maximal period of validity, and the maximum value of the retry counters.

Regarding all platforms, it has to be highlighted that some reviewers found it difficult to get the information they requested (e.g., on the specific authentication mechanisms by each IdP) during the peer review process. Some questions were not sufficiently answered. Consequently, this made it difficult for some peer reviewers to be able to reach a conclusion.

Regarding Platform 3, Digidentity, clarification documents were provided. Most Member States taking part in the peer-review consider that it fulfils level "High". Arguments mentioned by some Member States are that:

- There is no virtual smartcard on the mobile device;
- The virtual Smart card is stored in the HSM and is not transferred to the mobile device;
- AES keys are stored using only SE or TEE for secure communication between the app and the HSM. A mobile device that does not have a secure enclave cannot use the Digidentity app;
- Digidentity has identification of the device;

- The identification process is a full push model – cannot be initialized from the mobile device.

Other Member States still have concerns regarding the duplication and tamper resistance of Digidentity's mobile solution. The following arguments were mentioned:

- Digidentity's premises where the HSM are operated have been audited against a standard (EN 419 241-1) which allows authentication means below LoA high.
- The proprietary authentication protocol was not disclosed to the reviewers and no security proof was provided.
- The scope and the evaluation methodology used for pen testing the whole solution has not been disclosed.
- The resistance of an SE against an attacker is highly dependent on the SE's hardware, the SE's OS, the application running on the SE, and the correct usage of all provided interfaces. As there are faulty implementations in the field an appropriate certification with a reasonable evaluation depth is crucial for LoA high.

Consequently, some Member States think that the pre-notification documentation and the information provided during the peer review did not sufficiently demonstrate that the solution provided by Digidentity fulfils all requirements for LoA High.

3.2 Conclusions on Topic 2

Member States actively involved in reviewing Topic 2 in general concluded that the notified scheme complies with the requirements of section 2.2 and 2.3 of the ANNEX of the Commission Implementing Regulation (EU) 2015/1502 for:

- **Platform 1:** KPN, Reconi for levels of assurance "Substantial" and "High",
- **Platform 2:** Connectis, Unified Post, iWelcome and QuoVadis for levels of assurance "Substantial" and "High",
- **Platform 3:** Digidentity for level of assurance "Substantial".

Some Member States consider that they did not receive the requested information regarding the internal processing of identification/authentication from all platforms and IdPs. Consequently, one Member State feels they did not have enough information in order to be able to reach to a conclusion for Topic 2 for any platform.

Regarding **Platform 3**, most Member States consider that it fulfils level “High”, but some Member States are of the opinion that the pre-notification documentation and the information provided during the peer review did not sufficiently demonstrate that the solution provided by Digidentity fulfils all requirements for LoA “High”.

4. Topic 3: Management and organisation

This chapter addresses the peer review outcomes regarding the topic of management and organisation, and more specifically section 2.4 of the Annex of the Commission Implementing Regulation (EU) 2015/1502. The documentation provided by the Netherlands for the peer review of topic 3 and the questions asked by active members are summarised in this document, under section 4.1.

The documentation provided by Netherlands that is most relevant for this topic includes:

- Appendix 1 - White Paper: Introduction to the Dutch Trust Framework for Electronic Identification
- UK 3-04_v1.0 - this is a summary and overview of the governance structure for the NL scheme
- Accession procedure
- UK 3-04 (R2-2-08 Operational handbook)
- Accession requirements
- Exit procedure
- R2-03-03 on Dutch liability law
- UK 3-04 Participant Agreement Template
- Accession, exit and termination overviews

A study by the University of Birmingham was also provided. This took the form of a security review of the Dutch Trust Framework which has previously been commissioned by the Netherlands.

4.1 Scope and Questions

4.1.1 Active members contributing to this topic

Topic 3: Management and Organization

- Rapporteur: Samantha Lawler (UK), Livia Ralph (UK), Julian White (UK)
- Active members: AT, BE, DE, FR, SE
- Observers: BE, BG, CZ, DE, EE, FI, FR, HR, IE, IT, LU, MT, NO, SI, SK

4.1.2 Scope

The Netherlands chose to notify their whole trust framework rather than individual IDPs. As such the focus under this topic was on the governance of the whole trust framework ‘General Provisions’ in order to understand how individual IDPs are governed, audited and comply with the necessary requirements as specified by the trust framework. The scope of the peer review and whether individual IDPs should be notified was discussed between active members and with the Netherlands peer review team at the face

to face meeting in The Hague. It was decided that this conversation should be further discussed at the eIDAS cooperation network with all member states, rather than as part of topic 3. Therefore, the degree of governance and compliance was considered during the peer review, but no recommendation is given here as to the implications of that governance on whether the Netherlands notify the entirety of the Dutch Trust Framework, individual IDPs, or a combination of the two.

4.1.3 Questions

During the four question rounds, the peer review group asked 17 questions focused on the topic of management and organisation.

These questions can be clustered according to section 2.4 of the commission implementing Regulation (EU) 2015/1502:

- General provisions
- Published notices and user information
- Information security management
- Record keeping
- Facilities and staff
- Technical controls
- Compliance and audit

The next sections summarise the questions asked, how the pre-notified scheme fulfils the requirements of the eIDAS Regulation, and discusses the answers provided by the Netherlands in response to questions asked by reviewers.

4.1.4 General provisions

The majority of discussions on topic 3 focused on general provisions, particularly during the face to face meeting. Written questions on general provisions related to: how the Dutch Trust Framework ensures providers meet their commitments; liability; outsourcing by providers of their commitments to other entities; and the rules placed on providers for legal versus natural person identity proofing (note this notification covers legal persons only).

In response to questions from peer reviewing member states on how a provider’s compliance to the scheme policy is ensured, the Netherlands peer review team provided information on governance of the Dutch Trust Framework. This was in the form of supporting documentation, explanations during the face to face meeting in The Hague and an overview provided in response to further questions by member states. It was explained that this governance consists of:

- an Owner - Ministry of Interior and Kingdom relations
    - is accountable for the trust framework

    - signs an agreement with the providers which legally binds them to meeting its requirements
- a Supervisory body - the Radio Communications Agency
    - supervises providers in the Dutch Trust Framework to check they are meeting its requirements
    - is a public-private partnership
- Requirements and specifications - the Dutch Trust Framework
    - the Dutch Trust Framework is a set of legal requirements and specifications
    - many of these are essential requirements of EU and national law
    - other requirements include specifications for providers e.g. how they must issue means, audit requirements, technical requirements for infrastructure used by providers
- Participants - providers of eID and authentication means and ‘brokers’ who provide technical infrastructure to send eIDs between providers and services (details of more specific role breakdowns were provided during the peer review)
    - must meet the rules of the Dutch Trust Framework to be able to issue eID and authentication means
    - are governed by the Owner and the Supervisory Body

The Netherlands also provided documentation to demonstrate that during the accession procedure, providers that want to be part of the Dutch Trust Framework are assessed by a Committee of Experts. This committee determines whether or not the provider meets the required rules for issuance and registration of eID and authentication means.

In response to questions from member states about the procedures used when a provider outsources some of its requirements, it was explained that outsourcing is assessed by the Supervisory Body and responsibility for meeting these commitments remains with the provider. Proof must be given by the provider to the Supervisory Body to demonstrate that the outsourced requirements remain compliant. Outsourcing by providers can be refused if it does not meet Dutch Trust Framework rules, such as if:

- processing of personal data is occurring outside of Europe
- the third party is not ISO27001 certified
- there is no GDPR agreement for data processing

In response to questions about the liability scheme in place, a short summary was provided on Dutch liability law. It was indicated that Dutch Law lays out five elements that must be met to determine ‘negligence’ for which a party can be deemed liable. These rules are set out in Dutch law and as such all participants within the Dutch Trust Framework are bound by it. All participants in the Dutch Trust Framework are liable for their own services/actions. The Ministry of the Interior and Kingdom Relations is responsible for and subsequently liable for the eIDAS node in accordance with national law.

Supporting documentation was also provided that demonstrated termination plans are in place if a provider were to leave the Dutch Trust Framework and cease to issue or maintain eID and authentication means.

Questions were raised about the relationship between natural and legal person eID under the Dutch Trust Framework. It was clarified that whilst the legal person eIDs provided by eHerkenning is constructed of a natural person eID and associated information about the legal entity they represent, there is no current liability agreement in place with providers for its use as a natural person eID only. Therefore, only legal person eIDs will be part of this notification.

4.1.5 Published notices and user information

It was outlined by the Netherlands during the face to face meeting in The Hague that information about eHerkenning for users is published on official pages that outline the differences between providers so that users can choose to create a legal person eID with an organisation that is right for them. This also has all information about costs; fees and what the user will have to do to protect their account e.g. not give away their password to a third party. When creating their eID users must sign up to terms and conditions.

Information is also made available to all potential participants in the Dutch Trust Framework that outlines requirements on them - the Operational Handbook.

Following questions from the peer review team, it was clarified by the Netherlands that there were no possible situations where it might be a necessity for providers to deviate from GDPR. No further questions were asked on this section.

4.1.6 Information security management

No questions were raised by peer reviewers on the area of Information Security Management.

The Netherlands outlined in their supporting documentation that: *"all participants must have an Information Security Management System that covers their requirements on the Trust Framework and that this must be configured in compliance with the ISO/IEC 27001:2013 standard and certified, or the Participant and the Management Organisation must hold a Third Party Statement (TPS) with an equivalent conformity certificate from an independent registered EDP auditor."*

4.1.7 Record keeping

Within the Dutch Trust Framework, records must be archived for the purposes of *"tracing and combating fraudulent information transactions and the protection of the User in case of misuse of his digital or real life identity. "*

All records must be kept in accordance with national law and GDPR and in line with the record-management requirements of the Dutch Trust Framework.

The amount of information kept for these purposes varies between the eHerkenning levels of assurance 1&2 and levels of assurance 3&4. At levels of assurance 3&4 more information is retained, rather than just the assertion of identity, in order for this information to be used in potential fraud investigations.

There were no questions raised by the peer review group on this section.

4.1.8 Facilities and staff

Questions were raised in the face to face meeting in The Hague about the type of staff who work in the Supervisory Body, their training and experience. The peer review team met many of these staff and presentations were given about their roles, responsibilities and previous experience.

The Netherlands provided an outline of the procedures that exist to ensure staff and subcontractors are sufficiently skilled and trained. It is explained that the requirements of IS027001 are considered sufficient to ensure appropriate facilities and staff are maintained by participants in the Dutch Trust Framework.

No further questions were asked by the peer review group on this section.

4.1.9 Technical controls

The Netherlands provided an overview of the technical controls in place at different levels of assurance within the Dutch Trust Framework for electronic identification. These controls are proportionate to the level of assurance and associated risk level. All technical connections must take place in SSL/TLS and trust framework rules must be met. The Supervisory Body is responsible for oversight of incidents, responding to security incidents and taking the appropriate steps to make any necessary updates to technical controls as a result.

Access to sensitive cryptographic information is limited at levels of assurance 1&2, whilst at levels of assurance 3&4 it must be protected against unauthorised manipulation. Under the eIDAS Regulation levels of assurance 1&2 would, therefore, only meet the technical controls requirements for Low.

However, as part of the trust framework all providers must also hold ISO27001 certification to deliver any level of assurance, therefore it was considered that providers delivering levels of assurance 1&2 also meet the requirements for level 'High' of the eIDAS Regulation.

Questions were raised on how it was tested that access to this sensitive cryptographic information is protected from manipulation. The Netherlands explained that they investigate this on accession of a

participant and then every 3 years afterwards using a method derived from common criteria evaluations.

4.1.10 Compliance and audit

Audit of the providers of eID and authentication means on the Dutch Trust Framework is conducted by the Supervisory Body. This body is external to the provider’s organisation, but internal to the Dutch Trust Framework. The peer review group asked questions on the scope of audit carried out by the Supervisory Body. It was explained that this audit includes all responsibilities of participants on the trust framework, specifically:

- technical
- legal
- organisational
    - information security
    - privacy
    - GDPR compliance
    - liability

It was also explained that in addition, certification to ISO27001 must be achieved by providers and evidence of this given to auditors from the Supervisory Body. Participants are also required to pen test their solutions and provide the results of this to the Supervisory Body.

The Supervisory Body is responsible for auditing the provider at the point of accession to the trust framework or when there is a significant change. Questions were raised about what constitutes a significant change and what happens in the instance that a non-conformity is found. It was clarified that significant changes refer to changes in process or technology used for the issuance of eID or authentication means and that non-conformities are managed in relation to their severity. The more severe a non-conformity, the faster a participant is required to fix it. Participants can be fined or forced to cease issuing eID or authentication means if deemed necessary.

4.2 Conclusions on Topic 3

The majority of questions and clarifications in this topic centred on the General Provisions section under the eIDAS Regulation. The Netherlands provided extensive material to help explain the structure and governance of their Dutch Trust Framework for electronic identification, though as the scheme is complex it took time for the eIDAS peer review team to fully understand it and form suitable questions on this topic. The face to face meeting in The Hague was particularly important to provide clarity and understanding of the scheme.

The answers provided by the Netherlands resolved outstanding concerns and queries from the eIDAS peer review team on topic 3. Subsequently, the experts in this peer review group conclude that the Dutch Trust Framework satisfies the necessary requirements of the eIDAS Implementing Regulation 2015/1502 for section 2.4, Management and Organisation, at LOAs Substantial and High.

It is highlighted that this finding is separate to any considerations on whether or not the governance of this eID scheme is extensive enough to allow it to be notified as a trust framework without the inclusion of its IDPs. The peer review group recommends that this is discussed further at the eIDAS Cooperation Network in June 2019.

Member States actively involved in reviewing Topic 3 conclude that the Dutch Trust Framework satisfies the necessary requirements of the eIDAS Implementing Regulation 2015/1502 for section 2.4, Management and Organisation, at levels of assurance “Substantial” and “High”.

5 Conclusion

In the context of the Dutch Trust Framework for electronic identification, several identity providers have joined together in three platforms. For each platform, the peer review report came to a conclusion on the claimed Level of Assurance.

Member States actively involved in in this peer review find that the Dutch Trust Framework for Electronic Identification “eHerkenning” complies with Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market for

- **Platform 1:** KPN and Reconi for levels of assurance “Substantial” and “High”, for
- **Platform 2:** Connectis, Unified Post, iWelcome and QuoVadis for levels of assurance “Substantial” and “High”, and
- **Platform 3:** Digidentity for levels of assurance “Substantial”

for the topics of enrolment, electronic identification means management and authentication and management and organization.

Concerns have been raised by some Member States on whether the requirements for level of assurance “High” for Platform 3 have been met for electronic means management and authentication. These concerns relate to the current implementation of Digidentity’s virtual smart card solution.

The next step is for the Cooperation Network to present the peer review report on the Dutch Trust Framework for electronic identification for the Cooperation Network.

References

Documents are available on the pre-notification page of NL on the Cooperation network wiki.

Pre-Notification Documents provided on 4 December 2018

- Accession overview.pdf
- Accession procedure.pdf
- Accession requirements.pdf
- Appendix 1&2 Hyperlinks.pdf
- Appx-1_Whitepaper_Introduction_to_the_Dutch_Trust_Framework.pdf
- Appx-2_Standards_Framework_for_Levels_of_Assurance.pdf
- Appx-3_Dutch_eIDAS_Architecture.pdf
- Appx-4_Glossary_and_abbreviations.pdf
- Best practice registratie en verstrekking op afstand RFC2016.pdf
- Exit procedure overview.pdf
- Exit procedure.pdf
- Letter_Dutch_notification_eID_scheme_eTD_stelsel.pdf
- Mapping requirements eIDAS - DTF Standards Framework LoA.pdf
- Notification_Form_Dutch_Trust_Framework_for_Electronic_Identification.pdf
- Termination overview.pdf

Documents provided between February and April 2019 and during the Peer Review Meeting

- The polymorphic eID scheme.pdf
- Security Review of the Polymorphic eID scheme.pdf
- Accession procedure - page 4.pdf
- Exit procedure - page 2.pdf
- Exit procedure - page 7.pdf
- Documentation and references v1.1.xlsx
- Supervision - Inge van der Aart, Frank van den Braber.pptx
- Introduction to the peer review team, The Dutch landscape - Jean Paul Bakkers.pdf
- Architecture of the Dutch Trust Framework - Frans de Kok.pdf
- Authentication sources (PRD) - Frans Rijkers.pdf
- Mandate register and commercial register - Johan van den Bosch.pdf
- Introduction to the Dutch Trust Framework - Marije Jurriens.pdf
- Governance - John Borst.pdf
- Standards Framework - Geert-Jon Jepkes.pdf

- Round 2 Answer R2-2-06.pdf
- Round 2 Best Practice Registration and Remote Issuance RFC2016.pdf
- Round 2 R1-1-followup1 0-1.pdf
- Round 2 R2-0-02 Mapping table eIDAS DTF.pdf
- Round 2 R2-2-08 Operational handbook.pdf
- Round 2 Topic 2 - R2-2-06 Normen informatiebeveiliging ISO27001.pdf
- Round 2 Topic 2 R1 -2-followup3.pdf
- Round 2 Topic R2-03-03.pdf
- Notification_Form_Dutch_Trust_Framework_for_Electronic_Identification with IDPs.pdf

Additional Documents

- Minutes of Peer Review Meeting
- Minutes of Conference Calls with Rapporteurs and Active Members / NL Peer Review Team
- Answers by NL to four questions rounds between February and April 2019