Ministry of the Interior and Kingdom Relations

Dutch Trust Framework for Electronic Identification

Notification Form

Ministry of the Interior and Kingdom Relations
Postbus 20011 | 2500 EA | The Hague | The Netherlands
Contact: jean-paul.bakkers@minbzk.nl; marleen.stolze@logius.nl
September 2018

NOTIFICATION FORM FOR ELECTRONIC IDENTITY SCHEME UNDER ARTICLE 9(5) OF REGULATION (EU) No 910/2014

The Kingdom of the Netherlands hereby notifies the European Commission of an electronic identification scheme to be published in the list referred to in Article 9(3) of Regulation (EU) No 910/2014 and confirms the following:

- the information communicated in this notification is consistent with the information which has been communicated to the Cooperation Network in accordance with Article 7(g) of Regulation (EU) No 910/2014, and
- the electronic identification scheme can be used to access at least one service provided by a public sector body in *the Kingdom of the Netherlands*.

1. General information

Title of scheme (if any)	Level(s) of assurance (low, substantial or high)
Trust Framework for Electronic Identification (*Afsprakenstelsel Elektronische Toegangsdiensten*)	Substantial and High

2. Authority(ies) responsible for the scheme

Name(s) of authority(ies)	Postal address(es)	Email address(es)	Telephone No
Ministry of the Interior and Kingdom Relations	Postbus 20011, 2500 EA, The Hague, The Netherlands	Rogier.Dokkum@minbzk.nl	+31 70 426 6426

3. Information on relevant parties, entities and bodies (where there are multiple parties, entities or bodies, please list them all, in accordance with Article 3(2) and (3)

3.1. Entity which manages the registration process of the unique person identification data

Name of entity which manages the registration process of the unique person identification data

The registration of the unique person identification data is managed by the Means Issuers within the notified Trust Framework. The current means issuers are:

- Connectis
- Digidentity
- KPN
- QuoVadis
- Reconi
- Unified Post
- iWelcome (in the role as Recognition broker).

The scope of this role will be explained in Appendix 1. The registration of the unique person identification data is managed by the authentication means providers within the notified scheme.

3.2. Party issuing the electronic identification means

Name of the party issuing the electronic identity means and indication of whether the party is referred to in Article 7(a)(i), (ii) or (iii) of Regulation (EU) No 910/2014

The Means Issuer. The scope of this role will be explained in Appendix 1.		
Article 7(a)(i) ☐	Article 7(a)(ii) ☐	Article 7(a)(iii) ☒

3.3. Party operating the authentication procedure

Name of parties operating the authentication procedure

The Authentication Provider. The current Authentication Providers are listed in section 3.1. The scope of these roles will be explained in Appendix 1.

3.4. Supervisory body

Name of the supervisory body (provide the name(s) where applicable)

The Ministry of the Interior and Kingdom Relations, the Committee of Experts and the Radiocommunications Agency Netherlands (AT). The scope of these roles will be explained under 4.1.

4. Description of the electronic identification scheme

Document(s) may be enclosed for each of the following descriptions.

(a) Briefly describe the scheme including the context within which it operates and its scope

The Trust Framework for Electronic Identification *(Afsprakenstelsel Elektronische Toegangsdiensten)* is a uniform set of standards, agreements and provisions for authorised access to digital services. The agreements apply between parties that have a recognised role in providing and using access services, management and continued development, guidance and supervision. The Ministry of the Interior and Kingdom Relations has political responsibility for this Trust Framework.

Within the Trust Framework, various accredited private providers (listed in section 3.1) offer services as part of a network, using the brand names eHerkenning (literally: eRecognition) for businesses and Idensys for citizens. In essence, the network enables users to confirm their identity and authorisation digitally. This allows users to perform transactions on their own behalf or on behalf of an organisation, while the government can be confident that the user is who he claims to be, and that this person is authorised to act. The citizen's domain is temporarily excluded to prevent unnecessary interference with a parallel European tender procedure that first has to be completed successfully.

More information about the Trust Framework for Electronic Identification can be found in the introduction to the Trust Framework in Appendix 1.

(b) Where applicable, list the additional attributes which may be provided for natural persons under the scheme if requested by a relying party

This concerns supplementary attributes from the minimum data set for a natural person:

- first name(s) and family name(s) at birth;
- place of birth;
- current address;
- gender.

All service providers are able to receive these attributes. However, different attributes will be sent for each authentication service.

(c) Where applicable, list the additional attributes which may be provided for legal persons under the scheme if requested by a relying party

This concerns supplementary attributes from the minimum data set for a legal person:

- current address;
- VAT number;
- tax reference number;
- the identifier intended in Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council of 16 September 2009 on coordination of safeguards which, for the protection of the interests of members and third parties, are required by Member States of companies within the meaning of the second paragraph of Article 48 of the Treaty, with a view to making such safeguards equivalent (1);
- the Legal Entity Identifier (LEI) intended in Commission Implementing Regulation (EU) No 1247/2012 of 19 December 2012 laying down implementing technical standards with regard to the format and frequency of trade reports to trade repositories according to Regulation (EU) No 648/2012 of the

European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories (2);
- the Economic Operator Registration and Identification Number (EORI-No) intended in Commission Implementing Regulation (EU) No 1352/2013 of 4 December 2013 establishing the forms provided for in Regulation (EU) No 608/2013 of the European Parliament and of the Council concerning customs enforcement of intellectual property rights (3);
- the excise duty number intended in Article 2(12) of Council Regulation (EU) No 389/2012 of 2 May 2012 on administrative cooperation in the field of excise duties and repealing Regulation (EC) No 2073/2004 (4).

All service providers are able to receive these attributes. However, each authentication service will receive different attributes.

4.1 Applicable supervisory, liability and management regime

4.1.1 Applicable supervisory regime

Describe the supervisory regime of the scheme with respect to the following:

(where applicable, information shall include the roles, responsibilities and powers of the supervising body referred to in point 3.4, and the entity to which it reports. If the supervising body does not report to the authority responsible for the scheme, full details of the entity to which it reports shall be provided)

(a) supervisory regime applicable to the party issuing the electronic identification means

The minister of the Interior and Kingdom Relations is the Supervisor of the Trust Framework for Electronic Identification (hereinafter: Supervisor). The minister of the Interior and Kingdom Relations has political responsibility (hereinafter: Owner) for this Trust Framework. The Supervisor is advised on accessions and actions to be taken with regard to supervision and enforcement by an independent Committee of Experts. The Committee is temporary and will be dissolved as soon as supervision of the Trust Framework is safeguarded under public law. The intention is to do this through the proposed eGovernment Act *(Wet Digitale Overheid)*. The legislative proposal was sent to the Dutch Parliament (House of Representatives) in June 2018. The Act is expected to come into force in July 2019. For the legislative proposal (in Dutch), see: https://zoek.officielebekendmakingen.nl/dossier/34972/kst-34972-2

Once the Digital Government Act has come into force and the Committee has been dissolved, the Radiocommunications Agency Netherlands *(Agentschap Telecom),* currently acting as Secretariat to the Committee of Experts, will become the main advisor to the Supervisor.

More information about the supervisory regime can be found in the Whitepaper introduction to the Trust Framework in Appendix 1.

(b) supervisory regime applicable to the party operating the authentication procedure

See 4.1.1 a). The supervisory regime applicable to the party operating the authentication procedure is identical to that applicable to the party issuing the electronic identification means.

4.1.2 Applicable liability regime

Describe briefly the applicable national liability regime for the following scenarios:

(a) liability of the Member State under Article 11(1) of Regulation (EU) No 910/2014

With regard to Article 7(1)(f) of the Dutch eIDAS Implementing Law on the functioning of the eIDAS messaging service, the minister of the Interior and Kingdom Relations can be held responsible for the eIDAS Messaging Service on the basis of national liability law. In accordance with the agreements recorded in the Trust Framework for Electronic Identification, the participants are liable for their specific role in the issuance process. In its role as Owner and Supervisor of the Trust Framework for Electronic Identification, the Member State safeguards the provisions of Article 7(d) of the Regulation.

(b) liability of the party issuing the electronic identification means under Article 11(2) of Regulation (EU) No 910/2014

All participants who take part in the Trust Framework for Electronic Identification are liable for their own actions and/or negligence within their own role. Liability is subject to the general provisions of Dutch law on the substance and scope of legal obligations regarding compensation. Participants may be able to limit their liability in the agreements they conclude with customers or service providers. However, they are still bound to the general provisions of Dutch law with regard to liability and compensation.

In outline, the following applies on the basis of these provisions.

Dutch law distinguishes two kinds of liability:

1. liability on the basis of not fulfilling an agreement (non-performance);
2. liability on the basis of an illegitimate action.

A number of criteria needs to be met to constitute a case of liability on the basis of non-performance or on the basis of an illegitimate action. Whether these criteria are met depends on the specific circumstances of the case at hand. For this reason, it is not possible in general terms to indicate when a party shall be liable. In the Trust Framework for Electronic Identification, liability is described in the Legal framework and in the Trust Framework's Terms of use.

In accordance with the Civil Code, each party is liable for its own part.

(c) liability of the party operating the authentication procedure under Article 11(3) of Regulation (EU) No 910/2014

See 4.1.2 b). The party carrying out the authentication procedure is part of the Trust Framework for Electronic Identification.

4.1.3. Applicable management arrangements

Describe the arrangements for suspending or revoking of either the entire identification scheme or authentication, or their compromised parts

If the integrity of parts of the Trust Framework or of the entire Trust Framework has been compromised, the minister responsible (Ministry of the Interior and Kingdom Relations) can, in the public interest, suspend or revoke parts and/or participants of the Trust Framework or the entire Trust Framework. A central component (the aggregator) is used to create the network and is provided by the Ministry of the Interior and Kingdom Relations. There are procedures in place to grant access or to revoke access to this network. See https://afsprakenstelsel.etoegang.nl/display/as/Proces+uittreden

4.2 Description of the scheme components

Describe how the following elements of Commission Implementing Regulation (EU) 2015/1502 (1) have been met in order to reach a level of assurance of an electronic identification means under the scheme the Commission is being notified of:

This information is provided in the Standards Framework for Assurance Levels (Appendix 2), which forms part of the Trust Framework for Electronic Identification.

4.2.1 Enrolment

(a) Application and registration

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.1.1 (Appendix 2).

(b) Identity proofing and verification (natural person)

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.1.2 (Appendix 2).

(c) Identity proofing and verification (legal person)

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.1.3 (Appendix 2).

(d) Binding between the electronic identification means of natural and legal persons

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.1.4 (Appendix 2).

4.2.2 Electronic identification means management

(a) Electronic identification means characteristics and design (including, where appropriate, information on security certification)

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.2.1 (Appendix 2).

(b) Issuance, delivery and activation

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.2.2 (Appendix 2).

(c) Suspension, revocation and reactivation

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.2.3 (Appendix 2).

(d) Renewal and replacement

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.2.4 (Appendix 2).

4.2.3 Authentication

Describe the authentication mechanism including terms of access to authentication by relying parties other than public sector bodies

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.3.1 (Appendix 2).

4.2.4 Management and organisation

Describe the management and organisation of the following aspects:

(a) General provisions on management and organisation

This information is provided in the Whitepaper, Chapter 2.2 (Appendix 1) and in the Standards Framework for Assurance Levels, Chapter 2.4.1 (Appendix 2).

(b) Published notices and user information

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.4.2 (Appendix 2).

(c) Information security management

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.4.3 (Appendix 2).

(d) Record keeping

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.4.4 (Appendix 2).

(e) Facilities and staff

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.4.5 (Appendix 2).

(f) Technical controls

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.4.6 (Appendix 2).

(g) Compliance and audit

This information is provided in the Standards Framework for Assurance Levels, Chapter 2.4.7 (Appendix 2).

4.3 Interoperability requirements

Describe how the interoperability and minimum technical and operational security requirements under Commission Implementing Regulation (EU) 2015/1501 (2) are met. List and attach any document that may give further information on compliance, such as the opinion of the Cooperation Network, external audits, etc.

Article	Requirement	Elaboration
Article 4 (2015/1501)	**Mapping of national assurance levels** The mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502. The results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1505 (2).	See Chapter 1 of the Standards Framework for Assurance Levels (Appendix 2).
Article 5 (2015/1501)	**Nodes** 1.A node in one Member State shall be able to connect with nodes of other Member States. 2.The nodes shall be able to distinguish between public sector bodies and other relying parties through technical means. 3.A Member State implementation of the technical requirements set out in this Regulation shall not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the	See Chapter 2 of the Dutch eIDAS architecture (Appendix 3).

	implementation adopted by the first Member State.	
Article 6 (2015/1501)	**Data privacy and confidentiality** 1.Protection of privacy and confidentiality of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices. 2.The nodes shall not store any personal data, except for the purpose set out in Article 9(3).	See Chapter 6 of the Dutch eIDAS architecture (Appendix 3), particularly Sections 6.6 and 6.7.
Article 7 (2015/1501)	**Data integrity and authenticity for the communication**. Communication between the nodes shall ensure data integrity and authenticity to make certain that all requests and responses are authentic and have not been tampered with. For this purpose, nodes shall use solutions which have been successfully employed in cross-border operational use.	See Chapter 6 of the Dutch eIDAS architecture (Appendix 3), particularly Sections 6.3 and 6.4.
Article 8 (2015/1501)	The nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment. The syntax shall allow: (a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person; (b) proper processing of the assurance level of the electronic identification means; (c) distinction between public sector bodies and other relying parties; (d) flexibility to meet the needs of additional attributes relating to identification.	See Chapter 5 of the Dutch eIDAS architecture (Appendix 3).
Article 9 (2015/1501)	**Management of security information and metadata** 1.The node operator shall communicate the metadata of the node management in a standardised machine processable manner and in a secure and trustworthy way. 2.At least the parameters relevant to security shall be retrieved automatically. 3.The node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with national requirements and, as a minimum, shall consist of the following elements: (a) node's identification; (b) message identification; (c) message date and time.	See Chapter 6 and Section 3.3 of the Dutch eIDAS architecture (Appendix 3).
Article 10 (2015/1501)	**Information assurance and security standards** 1. Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability	The following elements are managed by DICTU (*Dienst ICT Uitvoering*, the information and communication

	framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with national legislation. 2. Node operators shall deploy security critical updates without undue delay.	technology shared-services organisation within the Dutch Ministry of Economic Affairs and Climate): • connector • proxy • messaging service DICTU has been ISO 27001:2013-certified by DEKRA. Item two is monitored in the framework of the ISO-certification.
Article 11 (2015/1501)	**Person identification data** 1. A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border context. 2. A minimum data set for a natural person representing a legal person shall contain the combination of the attributes listed in the Annex for natural persons and legal persons when used in a cross-border context. 3. Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters.	See Chapter 2 of Dutch eIDAS architecture (Appendix 3), particularly Sections 2.4 and 2.5.

4.4 Supporting documents

List here all supporting documentation submitted and state to which of the elements above they relate. Include any domestic legislation which relates to the electronic identification provision relevant to this notification. Submit an English version or English translation whenever available.

Appendix 1: Whitepaper: Introduction to the Dutch Trust Framework for Electronic Identification

Appendix 2: Dutch Trust Framework for Electronic Identification: Standards Framework for Assurance Levels. Dutch version available at:
https://afsprakenstelsel.etoegang.nl/display/as/Normenkader+betrouwbaarheidsniveaus

Appendix 3: Dutch eIDAS architecture: Cross border use of the Dutch Trust Framework for Electronic Identification

Appendix 4: Glossary and abbreviations Dutch Trust Framework for Electronic Identification