Dutch Trust Framework for Electronic Identification "Afsprakenstelsel Elektronische toegangsdiensten"

Table of contents

Terms of use Dutch Trust Framework for Electronic Identification

Terms of use				
Version	G1.7		Valid from version of AS	1.13p

These Terms of Use apply to the services granted by Participants of the Service Providers and Service customers in the context of Trust Framework for Electronic Identification

This is an English translation of the Dutch Terms of Use and for convenience only. Only the Dutch version of these Terms of Use is legally binding. In the event of any discrepancy or inconsistency between this English translation and the Dutch version, the Dutch version shall prevail.

Article 1. Definitions

The terms used in these Terms of Use are written in capitals, have the following meanings:

Dutch Trust Framework Electronic Iderntification - Afsprakenstelsel Elektronische Toegangsdiensten (AS)

The Scheme of the Trust Framework Electronic Identification comprises governance, control, supervision, management, architecture, applications, technology, procedures and rules regarding the Trusted Network Electronic Identification in a certain determined version. The aim is reliable authentication and provision of identity information based on the eRecognition services of a well-regulated eRecognition Network.

Authentication service - Authenticatiedienst (AD)

A required Role within the Trusted Network Electronic Identification of the Trust Framework Electronic Identification filled by a Participant that has the responsibility for authenticating natural persons based on the Authentication Device used by the natural person.

Authentication mean

A set of attributes (e.g. a certificate) according to which authentication of a party can take place.

Management organisation (BO)

The Trust Framework Electronic Identification Management Organisation (AS) responsible for facilitating the management and further development of the Trust Framework Electronic Identification, as well as the control and monitoring of compliance with the Trust Framework Electronic Identification by the Service Providers (DA) and Participants on behalf of the Owner.

Level of Assurance

A relative level of the strength of evidence regarding an authentication/identity claim, authority, control of authority or expression of will that is formed by a coherent set of factors, where applicable consisting of: the strength of the prior registration, identification, authentication and issuance; the strength of the means itself and the use of the means (the authentication mechanism).

Security incident

An event that poses or may pose a threat to the reliability, confidentiality or availability of an electronic access service and/or a security breach that results in the significant likelihood of serious adverse effects on the protection of personal data.

Recognition by Electronic Identification (Herkenning)

In this context, (electronic) recognition means any of the functions of the Trusted Network Electronic Identification aimed enforce and controlling trust regarding identities, authorisations, wills and powers in relationships or transactions between service providers and businesses and the users involved.

Recognition Services

Recognition Services, namely: Authentication (authentication), verification of Authorisation, capture of an expression of will and the identifications and guarantees of non-repudiation required for this purpose as well as the registration processes required for this purpose.

Recognition broker (HM)

A required Role within the Trusted Network Electronic Identification filled by a Participant in the Trust Framework Electronic Identification that is the single point of contact through which service providers acquire Recognition Services, that has the responsibility to decouple messaging to and from service providers from internal messages within the Network, and that acts as a routeer to all participating authentication services, authorisation registries.

Permission manager

A User with the authority to register, suspend, revoke authorisations and otherwise perform related registration processes on behalf of a Service Customer.

Register of authorisations in Dutch: Machtigingenregister (MR)

A required Role within the Trusted Network Electronic Identification filled by a Participant in the Trust Framework Electronic Identitification – ''Afsprakenstelsel Elektronische Toegangsdienstenthat has the responsibility for registering, managing, controlling authorisations and other authorisations and making authorisation declarations (i.e. providing authorisation declarations upon User request).

Means Issuer

A required role within the Trusted Network Electronic Identification filled by an participant of the Trust Framework Electronic Identification. who has the responsibility for issuing Authentication means in accordance with the requirements of the specified Level of Assurances (LoA)

Participant

A party that fullfils one or more roles within the Trusted Network Electronic Identification in accordance with what is laid down in the Trust Framework Electronic Identification in this respect. Participants may perform roles for their own use and/or for use by third parties.

Service customer

A party using Electronic Access Services to purchase a service from a service provider. The service recipient is a party of the form

- natural person running a business (a sole proprietorship), or
- a non-natural person in accordance with the identification with which it is registered in the Netherlands Chamber of Commerce KvK Business Register (Handelsregister)r or in a comparable foreign public register in accordance with the regulations of the relevant country, or
- a natural person who purchases a service from a service provider as a private person; or
- a natural person who, as a citizen, purchases a service from a service provider authorised to use the Citizen service number (BSN)

A service customer is the User or is represented by a user.

Note: In propositions to companies, it is permissible to make the abstract term "service customer" concrete and replace it with "company".

Owner

The Ministery Interior and Kingdom Relations who is politically responsible for the secure and reliable operation of the Trust Framework Electronic Identification and, as trademark owner, responsible for protecting the word and figurative mark used the Trust Framework Electronic Identification.

User

A Natural person using Electronic Access Services to purchase a service from a service provider.
See also Service customer.

Terms of use

These terms of use

Note: This is an English translation of the Dutch Terms of Use and for convenience only. Only the Dutch version of these Terms of Use is legally binding. In the event of any discrepancy or inconsistency between this English translation and the Dutch version, the Dutch version shall prevail.

Trusted Network Electronic Identification

The collection of interconnected components that are regulated by the Trust Framework Electronic Identification and jointly provide Recognition Services and to this end consist of at least one fulfilment by a Participant of the roles Recognition Broker (HM), Resource Issuer (MU), Authentication Service (AD), Authorisation Register (MR) and BSN Link Register, their interconnections, the connections up to and including the interface with service providers and the processes for resource issuance, authorisation registration and notification for re-use from businesses, including the necessary facilities for management in accordance with the Trust Framework Electronic Identification.

Agreement

The agreement between the Service Customer and the Participant, or the agreement between the Service Provider (DV) and the Participant, under which the Participant provides Recognition Services and to which the Terms of Use apply.

Party

A person or partnership that occurs or could occur in the context of Recognition and can be uniquely identified and authenticated if necessary. Examples of parties include: Participants, service providers, companies, representatives, agents, ...

The term is used as a generalisation.

Single Sign On (SSO)

Single Sign On (SSO) comprises a feature which is facilitated in the Trust Framework Electronic Identification. SSO re-uses users authentication without logging in again

A feature that is facilitated as defined in the the Trust Framework Electronic Identification, which reuses a user's authentication, preventing that user from having to log in again.

Supervisor

The Minister of Digitalisation is owner of the Trust Framework Electronic Identification. Next to the role of owner is the Minister of Digitalisation supervisor. To separate the roles of Owner and Supervisor are a Committee of Experts is established by the Council of Ministers.

Authorised
The party authorised (by law or authorisation or power of attorney) to perform certain acts in the name of the represented party, the legal effects of which are imputed to the represented party. Insofar as authorised representative is a natural person, there is no restriction on the appearance of non- residents as authorised representatives. Thus, a foreign natural person can also be authorised representative.

Article 2. Scope of application

The Participant shall apply these Terms of Use to the Agreement that the Service Customer and the Service Provider enter into with a Participant under the Trusted Network Electronic Identification.

A Participant may perform one or more of the following roles.

- The Means Issuer issues authenticators and identifies natural persons.
- The Authentication Service, authenticates individuals.
- The Authorisations Register facilitates the registration, maintenance and monitoring of authorisations.
- The Recognition Broker performs a routing and navigation function and is the interface point between the Trusted Network Electronic Identification and the Service Providers.

Article 3. Interim termination of the Agreement by termination of participation

The Agreement terminates by operation of law if and as soon as the Participant's participation in the Trust Framework Electronic Identification ends. The Participant shall immediately notify the Service Customer and/or the Service Provider with whom the Participant has entered into an Agreement of such termination by means of a registered letter.

If the interim termination referred to in this Article occurs, the Participant shall be obliged to provide all cooperation to ensure the continuity of the provision of Electronic Access Services by other Participants.

Article 4. Limitation of liability

A Party's liability to the other Party is limited to its own acts and/or omissions in the context of (its role within) the Trust Framework Electronic Identification.

In the context of liability, the general rules of Dutch law regarding the content and scope of legal obligations to pay damages apply.

Article 5. Confidentiality

5.1 The Parties understand and respect that each Party may be subject to varying obligations under applicable legislation and/or internal rules and procedures concerning confidentiality

5.2 Information, which is subject to confidentiality, shall not be disclosed to other persons than those to whom it is necessary to share such information and who are bound by confidentiality either by national legislation or by agreement

Article 6. Network failure

6.1 A network failure comprises the failure of a transaction between the Service Customer and the Service Provider or between a Service Provider and a Service Intermediary to proceed properly, for example as a result of a Security Incident or as a result of the incorrect processing and/or transmission of:

- the authentication of a user and/or the Service Customer;
- the registration of an authorisation;
- an expression of will.

6.2 In the event of suspected network failure, the Parties shall take steps to determine the cause of the network failure. The Service Customer and Service Provider should cooperate in this and understand that the Management Organisation and/or engaging the Supervisor any time.

Article 7. Transfer of rights and obligations

7.1 The Parties are not authorised to transfer their rights and obligations under this Agreement to a third party except with the written consent of the other party. In case a Participant wishes to transfer its rights and obligations under the Agreement, the acquiring party must also be admitted to the Trusted Network Electronic Identification as a Participant in the same role.

Article 8. Applicable Law

8.1 Dutch Law is applicable on this Terms of Use

Obligations for the Service Customer

Article 10. Service customer

10.1 The Service Customer shall fulfil all its obligations under the Trust Framework Electronic Identification.

10.2 The Service Customer shall provide accurate and complete information to the Participant in a timely manner, if requested by the Participant.

10.3 If the Service Customer fails to provide timely, or incorrect and/or incomplete information, this cannot be attributed to the Participant, unless the Participant knew or should have known that incorrect and/or incomplete information existed and the Participant nevertheless processed this information.

10.4 The Service Customer shall immediately communicate all relevant mutations to the Participant, and immediately revoke or block related Authentication Agents and Authorisations.

10.5 If unauthorised or otherwise incorrect use is made of an Authentication Device and/or authorisation, or if this is suspected, the Service Customer shall immediately upon becoming aware of this report to the relevant Asset Issuer, or shall revoke the registration of the authorisation concerned.

10.6 If a Service Provider allows SSO functionality for the use of a service, it is the Service Customer's choice whether or not to use this functionality.

Article 11. Security obligation of the Service Customer

11.1 The Service Customer shall ensure the adequate security of the network connections and systems under its responsibility and used by the Service Customer in the context of the Trust Framework Electronic Identification Network.

11.2 The Service Customer shall report it to the Participant if a Security Incident is suspected. The Participant reports this suspicion of a Security Incident to the Management Organisation. The Management Organisation reports this suspicion to the Supervisor.

Article 12. Supervision by the Service Customer

12.1 The Service Customer is aware that an Authentication mean is personal and non-transferable. The information that the Service Customer can access, request and edit (change) using personal Authentication Means is often of a privacy-sensitive, confidential and personal nature. In this context, the Service Customer is urged to maintain strict confidentiality of its Authentication Means.

12.2 The Service Customer shall supervise and be responsible for the user acting on behalf of the Service Customer. The Service Customer shall not allow any practice that leads to careless actions of its representatives, such as the use of personal Authentication Means by multiple persons, the unauthorised use of personal Authentication Means, the use of Authentication Means for a purpose other than the purpose for which they were issued, etc.

12.3 The Service Customer is obliged to report abuse or suspected abuse of Authentication Means to the Participant. Simultaneously with this notification, a request for the withdrawal or suspension of the relevant Authentication Means shall be submitted by the Service Customer to the Participant.

12.4 The Service Customer shall ensure that the person it has designated as Authorisations Manager acts diligently in issuing and managing those authorisations as well as that those authorisations are used diligently

Article 13. Fulfilment of role(s) by the Service Customer

13.1 If the Service Customer itself performs one or more roles within the Trusted Network Electronic Identification, it shall be subject to all the obligations associated with the relevant role.

Obligations of the Service Provider

Article 14. Adoption of opening decision

14.1 The Service Provider fulfils all its obligations under the Trust Framework Electronic Identification.

14.2 The Service Provider shall announce that it has opened the electronic way, indicating which services can be obtained electronically.

14.3 In the opening decision, the Service Provider makes a choice for one or more Level of Assurances. When choosing one or more Reliability Levels, the Standardisation board "Forum Standaardisatie'' Reliability Level Guide can be used as a guide. The choice of a Reliability Level is the sole responsibility of the Service Provider. The Participant and the Service Provider are not liable for any damage arising as a result of a Reliability Level set by the Service Provider. This does not affect the Participant's liability for its own Service Provider.

Article 15. Reporting irregularities

15.1 In case the Service Provider observes or suspects irregularities with regard to recognition data provided to it, the Service Provider shall immediately notify the Recognition Broker with whom it has entered into an Agreement.

Article 16. Security service provider

16.1 The Service Provider is responsible for the security and control of its own systems and networks used, the website and the link with the Recognition Broker. The Service Provider shall comply with the requirements of the Trust Framework Electronic Identification regarding, inter alia, the security of the connection and its systems, the website and the link with the Recognition Broker.

16.2 To the extent that the Service Provider is a legal entity under public law, this government service provider - in addition to the (technical) requirements and pre-written security measures published b in the Trust Framework Electronic Identification - also complies with the requirements set by the National Cyber Security Centre (NCSC) regarding security for electronic services.

16.3 If, in the opinion of the Recognition Broker, the Service Provider does not meet the security requirements referred to in Articles 16.1 and 16.2, the Recognition Broker shall be entitled, in accordance with Article 23 of these Terms of Use, to shut down the Service Provider. The taking of such a measure shall be motivated by the Recognition Broker.

16.4 The Service Provider authorises an audit by an auditor to be appointed by the Recognition Broker upon reasonable suspicion or after causing a Security Incident.

Article 17. Single Sign On (SSO)

17.1 The Trusted Network Electronic Identification supports SSO. The Service Provider is responsible for choosing whether or not to allow SSO for its services.

17.2 When registering the service in the s catalogue of services, the Service Provider specifies whether it allows SSO.

17.3 The Service Provider shall provide accessible and adequate information on the use and operation of SSO to the Service Customer.

Article 18. Security

18.1 The Participant is responsible for the security and control of the network connections, native apps and systems it uses in the context of Trust Framework Electronic Identification. In doing so, the Participant complies with the requirements of the Trust Framework Electronic Identification.

Article 19. Level of Assurances (LoA)

1.1 The Participant supports the Reliability Levels set out in the Agreement.

Article 20. Information obligation

20.1 The Participant is obliged to provide all information, including information about the Agreement, to the Supervisor to the extent that this information is necessary for the Supervisor to assess (continued) participation in the Trust Framework Electronic Identification Network, to monitor compliance with the agreements of the Arrangement, or if this is necessary because of a complaint or an enforcement request.

Article 21. Privacy

21.1 The Participant will use the information provided for the purpose for which it has been provided. The Participant will not provide information to others than those to whom the Participant is entitled to provide information for the performance of the Agreement or is required to provide information by law.

21.2 The Participant shall only process personal data if and to the extent necessary for the performance of the Agreement.

21.3 Participant does not provide personal data relating to the user unless:

- the Service Provider or Service Customer requests these data in the context of legal proceedings; or
- there is a demand from authorized investigative body or regulator; and
- all this is done in accordance with the applicable legal rules on the provision of personal data.

21.4 The processing of personal data in the context of performance of the Agreement, shall be carried out by the Participant in accordance with the provisions of the General Data Protection Regulation (GDPR).

Article 22. Cookies

22.1 Certain settings chosen by the User use functional cookies, i.e. cookies that do not require explicit consent. These cookies are not used for purposes other than facilitating the setting chosen by the User.

Article 23. Supervision

23.1 The Supervisor supervises the Participants, the Management Organisation, the central facilities necessary to operate the Trusted Network Electronic Identification and handles enforcement requests, notifications and complaints regarding the secure and reliable operation of the Trust Framework Electronic Identification.

23.2 The Participant shall suspend access to its service in case of acute danger to the safe and reliable operation of Trust Framework Electronic Identification and consult with the Supervisor on further steps to be taken.

23.3 The Supervisor does not handle business disputes between Participants or Service Customers.