eIDAS-compliant Qualified Electronic Registered Delivery Services Practice Statement

Version 5.5*

24-05-2018

Contact: info@connect-solutions.be

Owner: **Connect Solutions bvba**
Zandstraat 187
3550 Heusden-Zolder
Belgium

www.connect-solutions.be

** Previous versions available upon request*

Version	Description	Date
5.4	eIDAS conformity	13-11-2017
5.5	Changes concerning GDPR	24-05-2018

Contents

.

1 Presentation

1.1 Introduction

Company name: Connect Solutions BVBA
Enterprise number: 0843.871.294
Registered place of business: Zandstraat 187, 3550 Heusden-Zolder, Belgium
Operational office: Grote Hemmenweg 81B, 3520 Zonhoven, Belgium
Activity: NACE CODE: 6201

CONNECT SOLUTIONS is the Provider of the Trust Service "Qualified Electronic Registered Delivery Services (eRDS)" in accordance with eIDAS Regulation (EU) No. 910/2014 of the European Parliament and Council, regulating the sending and receiving of messages between parties by electronic means and provision for the concerned parties of proof of the exchanged data and of the manner of its processing, as well as providing certainty regarding the integrity of the exchanged data and protecting against loss, theft, damage or unintentional change.

Name of Service: Aangetekende.email

Service type identifier: http://uri.etsi.org/TrstSvc/Svctype/EDS/Q

Service digital identity:

Issuer of TSP certificate: **CN = Qualified e-Szigno Organization CA 2016** **Certificate Serial Number: 00 90 27 49 84 CB F0 D2 D9 AF AF F3 0A**	
Name of TSP (as in certificate)	**Serial number of certificate**
CN = Connect Solutions	00 D3 03 BB 56 6C 66 7E AE 2A F4 68 8A 0A
CN = Connect Solutions	00 D3 04 A5 0F 65 13 0B E7 0A C2 49 CD 0A
CN = Connect Solutions	00 D3 05 97 EE 76 2B DB 53 C5 24 2D C9 0A

This Practice Statement includes a set of rules that CONNECT SOLUTIONS applies in connection with its role as Trust Service Provider in compliance with the eIDAS Regulation and, more specifically, as Provider of the Trust Service "Qualified Electronic Registered Delivery Services (eRDS)".

This Practice Statement is only one of a number of documents that must be read together as a single whole. Other important documents include the General Conditions, the functional description of the Aangetekende.email Service and the partner certificates and agreements.

In the pursuit of its activities CONNECT SOLUTIONS respects the administrative and management procedures laid down by Belgian and/or European law.

1.2 Access to the Service

The Aangetekende.email Service is offered as a web application and is accessible by means of the url: https://www.aangetekende.email

The Aangetekende.email Service is available only for and between Users with access to an active User Account on the Aangetekende.email Platform. To obtain access to the platform a User Account must first be created in accordance with the directions in the General Conditions and the functional description of the Aangetekende.email Service.

1.3 Organization and roles

The following roles are available in CONNECT SOLUTIONS.

Head of Service:	Responsible for the development of the application, the daily functioning, security and monitoring of the application and the IT/server environment and special point of contact for subcontractors.
Administrator/operator:	Responsible for a reliable and continuous operation of the application and the IT/server environment, i.e. set-up, protection, maintenance, monitoring and logging. This role is also in charge of the helpdesk.
Sales:	Responsible for the marketing, promotion and sale of the Service and special point of contact for end-users of the platform.
Internal audit:	Responsible for control of compliance with the instructions as laid down in eIDAS Regulation and for the application of the rules as set out in the present Practice Statement.

1.3.1 Segregation of duties

The internal audit role cannot be combined with other of the aforementioned roles. Combination of the roles of Head of Service, Administrator/operator and Sales is allowed but Connect Solutions strives to separate these roles.

1.3.2 Physical admission rights to facilities

Each internal role within Connect Solutions has physical access to the operational office and the server room.

The servers and QSCD devices are placed in a server rack with lockable door.

Only Connect Solutions staff, i.e. the Head of Service and the Administrator/operator roles have physical access to the server rack.

Internal procedures are in place to grant, change and revoke access rights to facilities.

1.3.3 Logical access rights

The Head of Service and Administrator/operator roles have full logical access to the server environment on which the Aangetekende.email platform resides. This encompasses access to the firewall, development tools, web server, database server, application server, application source code, signing function and loggings (see also 3.5.4)

No external parties have direct logical access to the server environment and other technical components of the Aangetekende.email environment.

The Head of Service, Administrator/operator and Sales roles have logical access to the administrative tool for verifying and approving/rejecting subscription requests for the Aangetekende.email service by end-customers. Access to the administrative tool is provided by means of authentication with the Belgian eID following the same mechanism as described in 3.5.1.

The internal audit role does not have direct logical access to the server environment and administrative tools to enforce its independency.

1.4 Subcontractors

CONNECT SOLUTIONS works alongside its Subcontractors for the following aspects:

- Timestamp service for the timestamps that CONNECT SOLUTIONS places as required under eIDAS Art. 44.1.
- Certificates (seals) for the electronic signatures attached by CONNECT SOLUTIONS as required under eIDAS Art. 44.1.

The abovementioned timestamp service and certificates (seals) are eIDAS-qualified. More info on the subject can be found in Chapters 3.3 and 3.4.

1.5 Personnel policy

When it comes to personnel policy CONNECT SOLUTIONS has always set a high bar for proficiency, reliability and confidentiality. Pursuing this policy enables us to accommodate our personnel requirements as regards the provision of Trust Services.

Reliability

Each prospective employee has to present a recent Model 2 extract from the municipal criminal records (formerly a certificate of good moral conduct) when applying for a position in the company. A *clean* extract from the criminal record cannot be taken as grounds for exclusion of the application. A "blotted" extract from the criminal record may, however, be taken as grounds for exclusion of the candidate, but only insofar as the recorded misdemeanours or offences might give cause for doubt as to that candidate's reliability, integrity or awareness of acceptable standards of behaviour.

If, during his/her employment with our company, an employee is sentenced under criminal law, this may be grounds for dismissal in accordance with the provisions of the Employment Regulation. The general criterion applied in the judgment of such matters is that the reliability, integrity and observance of acceptable standards may in no way be called into question. In this regard each employee is contractually bound by a duty of disclosure. Any additional entry in the municipal criminal records must be immediately reported to his or her employer. Failure to do so will, at the very least, raise serious questions as regards those criteria and may even lead to dismissal in accordance with het Employment Regulation.

Confidentiality

Our core activities consist of ICT solutions and services. That means that every colleague has (to a certain extent) access to the intellectual property of CONNECT SOLUTIONS and to our Clients' sensitive business information.

Each employee is therefore required to sign a confidentiality agreement in which he/she expressly undertakes to respect and protect the secrecy of the intellectual property and the business information of CONNECT SOLUTIONS and of its Clients.

Provision of Trust Services entails the possibility that employees will come into contact with personal data and/or information of a private nature of the Users of the Services. It is for that reason that the confidentiality agreement is made all the more stringent for the protection of the privacy of our Users. Each employee will further give his/her consent as regards possible future changes to the confidentiality agreement, for application simply in connection with legal requirements or criteria imposed by the Supervisor, and will sign the same on presentation. The employment contract may otherwise then be suspended or even terminated in accordance with the Employment Regulation.

Furthermore all provisions of the Employment Regulation and our corporate policy regarding the correct use of email, internet and social media remain fully effective.

Expertise, experience and qualifications

Each prospective employee is assessed for the necessary proofs of qualification of professional training necessary to carry out the function concerned in a proficient and qualitative manner.

If sufficient experience has been acquired in the actual work environment and can represent the equivalent of a professional training course (or courses), the relevant requirements are clearly mapped out in the vacancy and will be checked by reference to the proofs of experience submitted by the prospective employee.

If we consider necessary we may call on a procedure organized by a selection bureau that, according to the offered position and profile description, will attend to the recruitment, screening and selection of candidates. The final decision will, however, be taken internally, external advice being assigned a supporting but non-committal character.

When choosing a selection bureau due account will be taken of (i) the nature of the vacancy and (ii) the references, quality guarantees and ethical standards of the selection bureau.

Suitable training

Permanent training and ad hoc courses will be offered to keep our employees up-to-date and abreast of the latest developments in technology, security and the processing and protection of data and the legal aspects related to their work. Self-development, internal advancement, specialization and expansion of their field of knowledge are always encouraged and, wherever possible, supported by training courses, both internally and externally.

It goes without saying that action will be taken in response to the offer of specific vocational training courses in the broader context of permanent training as required by the Supervisor.

1.6 Quality of Suppliers and Subcontractors

The expected quality and performance of our Suppliers/Subcontractors are set out in contractual arrangements between CONNECT SOLUTIONS and the Supplier/Subcontractor. An appropriate SLA (Service Level Agreement) is concluded where applicable. It is the responsibility of the supplier/subcontractor to hire qualified personnel in order to meet the quality as set out in the contract and SLA.

1.7 Financial basis (insurance)

In case of liability for any damage that may occur despite all precautions and procedures, CONNECT SOLUTIONS shall fully comply with eIDAS Regulation 910/2014, account being also taken of the General Conditions. To that end a liability insurance is purchased which, if such should prove to be necessary, will cover the financial basis of the incident.

2 Accessibility

No special provisions are incorporated in the software of the Aangetekende.email Trust Service to facilitate accessibility for persons with a disability. Here use is made of possible features in the end-users' system configuration (voice control, read-out function, etc.).

3 Security policy

3.1 Risk analysis

CONNECT SOLUTIONS regularly conducts a risk analysis on security aspects concerning the offered Aangetekende.email Service. For each identified risk, proportional preventive and detective measures are taken that are designed to manage those risks and minimize their possible impact. Risk analysis concerns risks at technical level (infrastructure & hardware) and application level.

Significant factors in risk analysis include:

- Protection against unauthorized access to infrastructure, hardware and data.
- Protection against unauthorized access and changes to the application.
- Protection against unauthorized access to the seal certificates and private keys of CONNECT SOLUTIONS.
- Protection against unauthorized or falsified login on the platform.
- Protection of personal data against theft and against unauthorized input, consultation, change and use, ditto falsification of personal data.
- Protection of the transactional data against theft and against unauthorized input, consultation, change and use, ditto falsification of transactional data.
- Availability of the system.

3.2 Operational office

Connect Solutions has it operational office site in 3520 Zonhoven, Grote Hemmenweg 81B.
The server room where the servers and other technical components on which the Aangetekende.email application runs is also located in this office.

The management of the Aangetekende.email environment as well as the helpdesk function by the administrator/operator role is mainly performed at this location. The management or helpdesk function can occasionally also be performed remote from other locations with an internet connection, so called "mobile office". Any usage of "mobile office" shall only be set up in a controlled environment and not in publicly accessible locations.

Remote access to the Aangetekende.email environment is protected by a secure VPN connection with AES-256 encryption and multi-factor authentication (see also 3.5.4).

Paper documents related to the Aangetekende.email service are stored in the operational office. No external archives are used. Connect Solutions however strives to keep paper documents to a minimum and strives to maximally digitize documents.

The following security measures are implemented at the operational office.

3.2.1 Physical security

- Burglar alarm system and camera protection.
- Events triggered by the burglar alarm system and cameras are monitored 24/7 by an external security company and a procedure is in place to take appropriate action in case of burglar alarm including intervention after alarm.
- Al burglar alarm events are logged.
- The server room is a room without windows and is protected with a security door.
- An electronic access control system is in place to access the server room. For access to the TSP office a physical door key is used.
- The servers and QSCD devices are placed in a server rack with lockable door.
- All visitors entering the office are registered and accompanied.

3.2.2 Fire safety

- Fire detection and alarm system.
- Events triggered by the fire detection system are monitored 24/7 by an external security company and a procedure is in place to take appropriate action in case of fire alarm including alerting the fire brigade when needed.
- All fire alarm alerts are logged.
- Fire extinguisher and fire blanket are present and clearly visible in the office.
- Automatic fire extinguishing system has been installed in the server room, which is not hazardous to human life, and does not damage the IT equipment.

3.2.3 Air conditioning and air circulation

- The server room is equipped with an air conditioning system.
- The whole office incl. the server room is equipped with an air circulation system.

3.2.4 Electrical infrastructure

- UPS to protects IT equipment from voltage fluctuations in the external network, (short) power outages, spikes and other.
- Power generation equipment with automatic start in case of power outage with a capacity of 20 hours and which – by allowing refueling – is able to provide the necessary energy for any period of time.

3.2.5 Internet connectivity

- Redundant high capacity Internet Connection via different providers.

3.2.6 Waste disposal

- A shredder is present in the operational office capable to destroy paper documents and optical disks.

3.2.7 Laptop security & backup

- Laptops are equipped with antivirus software with real-time scan and automatic updates.
- An automatic lock mechanism is active on laptops with password unlocking. Passwords need to meet complex criteria.
- Laptops are backed-up at frequent intervals and encrypted backups are stored off-site.

3.3 eIDAS-qualified Timestamp

CONNECT SOLUTIONS uses an eIDAS-qualified timestamp service for its timestamps, placed under eIDAS Art. 44.1 (see Chapter 10).

On the date of the present document CONNECT SOLUTIONS enlists to that end the aid of the qualified timestamp service of Microsec (Company number: 01-10-047218, Registry Court of the Budapest-Capital Regional Court Registered Office: 1031 Budapest, Záhony utca 7. D. épület, Hungary).

Microsec operates the qualified timestamp service under policies laid down in Microsec's most recent and in force being *eIDAS conform Qualified Time Stamping Practice Statement*.

This document can be consulted at the following URL: https://e-szigno.hu/en/pki-services/certificate-policies-general-terms-and-conditions

In this context, CONNECT SOLUTIONS plays the following roles from the Microsec's point of view: Clients (Subscriber) and Relying Party (qTS verifier).

CONNECT SOLUTIONS fulfils all obligations a set out by Microsec to Subscribers in Microsec's most recent and in force being *eIDAS conform Qualified Time Stamping Practice Statement.*

CONNECT SOLUTIONS fulfils all applicable recommendations as set out by Microsec to Relying Parties in Microsec's most recent and in force being *eIDAS conform Qualified Time Stamping Practice Statement.* In particular, the signature on the timestamp is verified, the serial number of the Certificate used for signing the Timestamp is compared with the certificate serial number as listed in Microsec's "e-Szignó Qualified Time-Stamp" eIDAS Conformity Certificate (see: https://e-szigno.hu/assets/docs/e_Szigno_qualified_time_stamp.pdf) and the Hungarian Trusted List (http://www.nmhh.hu/tl/pub/HU_TL.pdf); and the validity and revocation status of the Certificate used for signing the Timestamp and other certificates in the certificate chain is verified based on current CRL or OCSP responses.

CONNECT SOLUTIONS will monitor and ensure that the timestamp service used for its Trust Service is Qualified according to eIDAS at all times.

3.4 eIDAS-qualified Electronic Seal

CONNECT SOLUTIONS uses eIDAS-qualified Seals as service certificate for the electronic signatures that it attaches under eIDAS Art. 44.1 (see Chapter 10).

On the date of the present document CONNECT SOLUTIONS enlists to that end the aid of the qualified Seals issued by Microsec (Company number: 01-10-047218, Registry Court of the Budapest-Capital Regional Court Registered Office: 1031 Budapest, Záhony utca 7. D. épület, Hungary).

Microsec operates the qualified electronic seal issuance under policies laid down in Microsec's most recent and in force being *eIDAS conform Qualified Time Stamping Practice Statement*.

This document can be consulted at the following URL: https://e-szigno.hu/en/pki-services/certificate-policies-general-terms-and-conditions
In this context, CONNECT SOLUTIONS plays the following roles from the Microsec's point of view: Subscriber / Subject / Creator of the electronic seal (also as qSealCD user) and Relying Party (qES verifier).

CONNECT SOLUTIONS fulfils all obligations a set out by Microsec to Subscribers in Microsec's most recent and in force being *eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement.*

CONNECT SOLUTIONS fulfils all applicable recommendations as set out by Microsec to Relying Parties in Microsec's most recent and in force being *eIDAS conform Qualified Certificate for Electronic Seal Certification Practice Statement.* In particular, the certificate used for issuing CONNECT SOLUTIONS' service certificate is compared with the certificate as listed in Microsec's "e-Szignó Qualified Seal" eIDAS Conformity Certificate (see: https://e-szigno.hu/assets/docs/e_Szigno_qualified_seal.pdf) and the Hungarian Trusted List (http://www.nmhh.hu/tl/pub/HU_TL.pdf); validity of seals placed with CONNECT SOLUTIONS service certificates are verified and the validity and revocation status of CONNECT SOLUTIONS' service certificate and other certificates in the certificate chain is verified based on current CRL or OCSP responses, before submitting sealed documents to Subscribers.

The Seals are produced on a QSCD (Qualified Electronic Seal Creation Device) USB stick. Each seal certificate is on a dedicated smartcard. Cryptographic keys on the service smartcards are generated already by Microsec and CONNECT SOLUTIONS gets smartcards in operational state fully prepared for use. This USB stick is kept safe in the operational office server room (see 3.2).

CONNECT SOLUTIONS operates service smartcards in accordance with related card issuer's (Microsec) user guidance.

CONNECT SOLUTIONS has internal procedures in place for the management of smartcards with CONNECT SOLUTIONS' keys for qualified electronic seals (delivery acceptance ensuring the genuineness of the delivered smartcards and the service certificates, activation, deactivation, usage, access to smartcard functions). These procedures will, among other things, ensure that the Seals are renewed in due time and will follow the revocation procedure whenever the certificate holder's key data may change in connection with the certificate (company name,

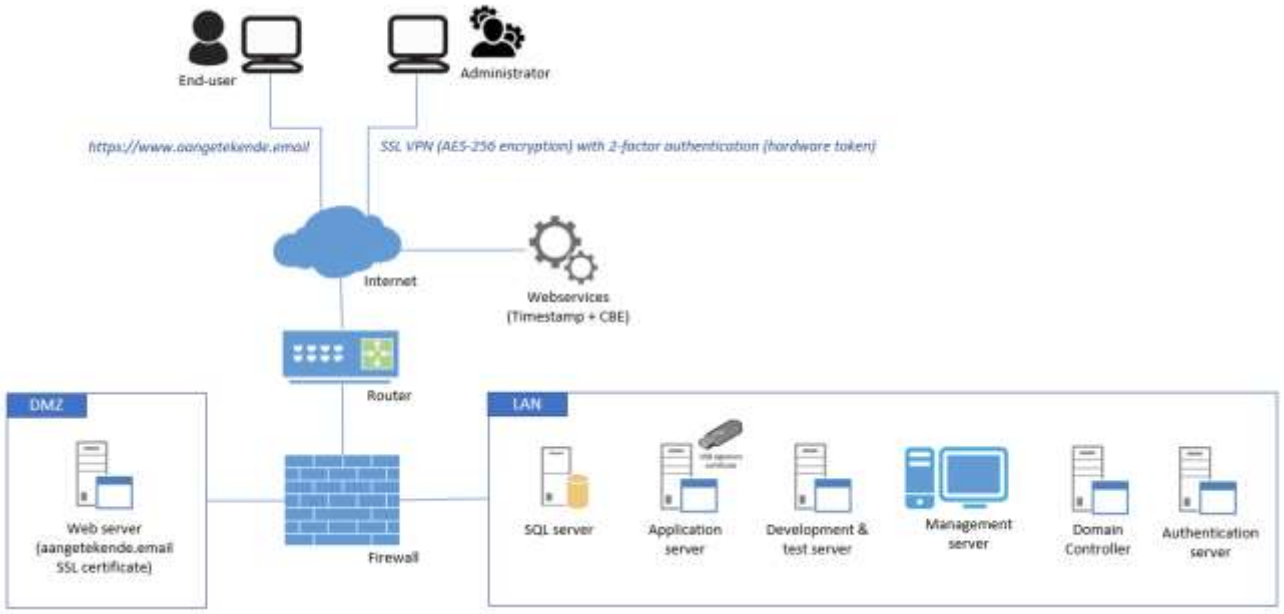
address, VAT number, etc.); if it should discover or suspect that the signature key has somehow become known or that the certificate is abused; if it replaces the certificate with another certificate (e.g., if the smartcard or the password for access to data is lost).

CONNECT SOLUTIONS will monitor and ensure that the issuer of the seal certificates as well as the QSCD used for its Trust Service are Qualified according to eIDAS at all times.

3.5 Logical network infrastructure

CONNECT SOLUTIONS makes use of reliable systems and products for storage of and access to data and for support of the processes, account being taken of the latest technological developments, such as firewalls, HTTPS traffic by means of internet, security modules for the storage of private keys (smartcard), two-factor authentication for remote admin login and database encryption. The technical environment is managed by Connect Solutions staff.

The following scheme depicts with the current Aangetekende.email environment.



SQL databases are encrypted. AES-256 encryption is used. The keys are managed by Connect Solutions staff.

A backup and recovery strategy is in place. All backups are encrypted (AES-256). The keys are managed by Connect Solutions staff.

Antivirus/malicious software protection is installed on each server.

3.5.1 End-user access to the platform

TLS is used for communication between the Aangetekende.email service and the end-users.

TLS version and channel encryption: TLS 1.2 AES-256

TLS channel end point:
- Web application on web server

HTTPS certificate www.aangetekende.email:
- Algorithm: sha256WithRSAEncryption
- Public key length: RSA (2048 Bits)

Authentication:

- Authentication of Aangetekende.email service to end-users: Certificate based (Extended Validation Certificate shown in the end-user's browser)
- Authentication of end-users to the Aangetekende.email service: eID authentication based.

Data exchange:

1. *End-user → Aangetekende.email service*

   The end-user enters the e-mail address (User account) he/she wants to access in the logon screen.

2. *Aangetekende.email service → End-user*

   The Aangetekende.email service verifies if the entered User account exists. If yes, the Aangetekende.email service generates a PDF file with a random unique number as content and calculates a hash code (sha256) of this PDF file. This hash code is sent to the End-user to sign electronically with the eID authentication certificate.

3. *End-User → Aangetekende.email service*

   The end-user signs the hash code electronically with the eID authentication certificate resulting in a signature block. This signature block is posted to the Aangetekende.email service.

4. *Aangetekende.email server → End-user*

   The Aangetekende.email service appends the signature block to the generated PDF file resulting in an electronically signed PDF file. Next the signature is validated against the content, the validity of the certificate with which the signature was placed is verified (CSP and OCSP responses) and the signature is verified with the certificate linked to the user account during the registration procedure. If all checks are positive, access to the platform is granted.

3.5.2 Interface to the timestamp service

TLS is used for communication between the application server and the timestamp service

TLS version and channel encryption: TLS 1.2 AES-256

TLS channel start and end points:
- Signature application on application server <-> timestamp service

HTTPS certificate *e-szigno.hu:
- Algorithm: sha256WithRSAEncryption
- Public key length: RSA (2048 Bits)

Authentication:

- Authentication of timestamp service to the signature application on the application server: Certificate based (Certificate of the Time-Stamping Unit.)
- Authentication to the timestamp service: username-password based.

Data exchange:

1. *Signature application → timestamp service*

   Time-stamp request incl. authentication data cf. RFC 3161.

2. *Timestamp service → signature application*

   Time-stamp issuance cf. RFC 3161.

Details about the time-stamp request and time-stamp response can be found in chapter 3 of the *eIDAS conform Qualified Time Stamping Practice Statement*. This document can be consulted at the following URL: https://e-szigno.hu/en/pki-services/certificate-policies-general-terms-and-conditions

3.5.3 Interface to the CBE webservice

TLS is used for communication between the application server and the CBE webservice.

TLS version and channel encryption: TLS 1.2 AES-128

TLS channel start and end points:
- CBE application on application server <-> CBE webservice

HTTPS certificate *economie.fgov.be:
- Algorithm: sha256WithRSAEncryption
- Public key length: RSA (2048 Bits)

Authentication:

- Authentication of CBE webservice to the CBE application on the application server: Certificate based (Certificate of the CBE webservice)
- Authentication to the CBE webservice: username - password based.

Data exchange:

1. *CBE application → CBE webservice*

   The CBE application sends a request to the CBE webservice containing the authentication data (username-password) and enterprise number of which data is requested.

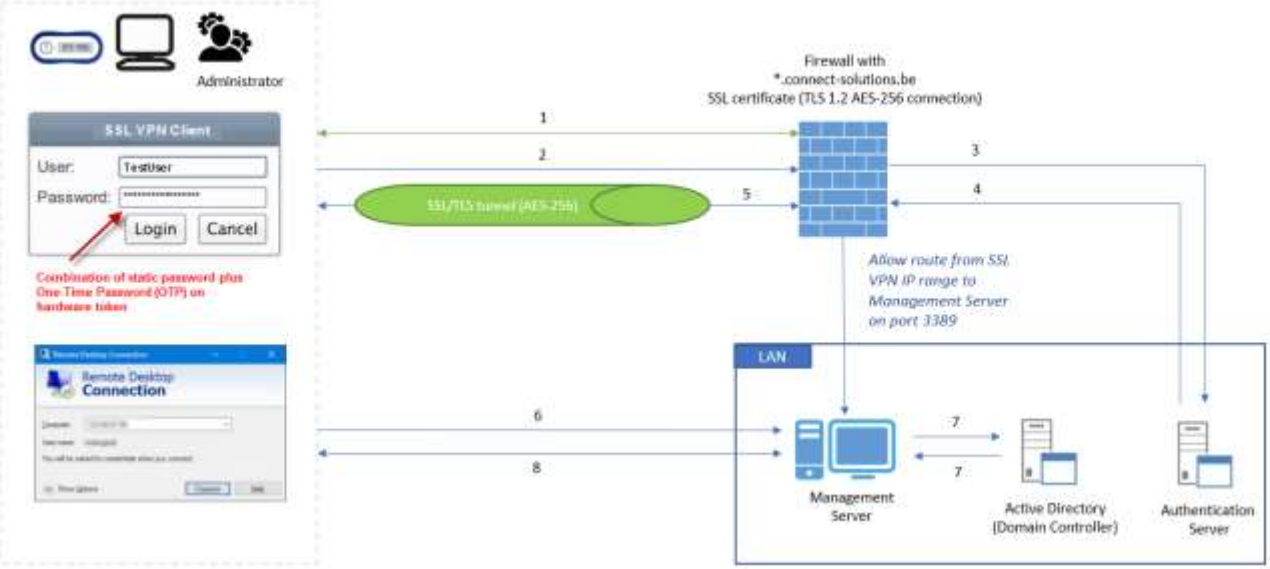
2. *CBE webservice → CBE application*

   The CBE webservice replies with an enterprise object containing the enterprise data like e.g. address, postal code, location, legal representatives of the company.

Details about the KBO webservice request and response can be found in the KBO webservice manual. This document can be consulted at the following URL: http://economie.fgov.be/nl/modules/publications/kbo/cookbook_service_web_public_search.jsp

3.5.4 Remote administrative access by TSP admin users

Remote access to the environment is provided conform the scheme below:



1. First a HTTPS connection is set up (TLS handshake). See parameters in the table below.
2. Once the HTTPS connection is set up, the administrator initiates a VPN authentication request to the firewall where username and password are submitted. The password is a concatenation of a static password (minimum length of 6 characters containing an uppercase character, a lowercase character, a digit and a special character) plus a One-Time Password (OTP) consisting of 6 digits shown on the hardware token.
3. The firewall sends the authentication request to the Authentication Server.
4. The Authentication Server checks the password combination. If it is correct, it sends a response to the firewall.
5. A SSL VPN connection is established. See parameters in the table below.

When the VPN is set up, the client is granted an IP address in the SSL VPN range. In the firewall, a rule is set up to allow this range to connect to 1 specific IP address i.e. the Management Server on port 3389.

Subsequently a RDP connection is made to the Management Server:

6. The management server IP address is entered together with Active Directory domain credentials (user and password).
7. The user and password are checked for validity.
8. If valid, a RDP connection is set up.

From the Management Server, the other servers can be accessed.

TLS channel start and end points	Server authentication HTTPS certificate *.connect-solutions.be installed on the firewall	TLS version and channel encryption
• SSL VPN client <-> Firewall	• Algorithm: sha256WithRSAEncryption • Public key length: RSA (2048 Bits)	TLS 1.2, AES-256

3.6 Logging

3.6.1 Environmental event logging

All environmental events (burglar alarm, fire alarm) are logged by the alarm system software.

Events triggered by the alarm system are monitored 24/7 by an external security company and a procedure is in place to take appropriate action.

3.6.2 Technical infrastructure logging

Firewall loggings and server monitoring loggings and are maintained and monitored on a permanent basis by the Administrator/operator role. Accesses to the server room are logged.

3.6.3 Application loggings

The Aangetekende.email application makes provision for various application loggings whereby any possible irregularities on the platform will be detected and the appropriate action will be taken. These application loggings are monitored on a permanent basis by the Administrator/operator role.

This may concern any of the items on the following non-exhaustive list:

- Loggings re. (un)successful logons on the platform
- Loggings re. incomplete sent messages
- Loggings re. (un)successful signature of sent messages
- Loggings re. (un)successful signature for receipt of messages
- Loggings re. (un)successful mass uploads
- Loggings re. (un)successful outbox downloads
- Loggings re. use of the Address Book
- Loggings re. changes to the general Account data
- Loggings re. changes to added/removed eID cards
- Loggings re. processed/incomplete subscriptions

Application loggings contain checksums to monitor on and alert any discrepancies between transmitted data and data saved in the database to ensure authenticity of transmitted data.

Application loggings are stored in an encrypted database on the SQL server.

3.6.4 Retention of loggings

All loggings are kept for a period of minimum one year. In case of intention to terminate activities and no successor is found, CONNECT SOLUTIONS will agree with the Supervisory Body what should happen with the loggings after cessation (see 9.4).

4 Security & personal data breach notification

CONNECT SOLUTIONS will report security & personal data breach incidents following the scheme in attachment 1.

Here an important distinction is made between a "security breach" and a "data leak".

A "security breach" is a security incident that has a significant impact on the trust service provided and possibly adversely affecting the natural or legal persons who are putting their trust in the trust service provided, but does not necessarily mean that personal data is leaked.

A "data leak" is a security breach where sensitive personal data of subscribers threatens to be made public unauthorized.

Depending on the nature of the security breach and their effect, the necessary stakeholders will be informed.

4.1 Informing the Supervisor and the Privacy Commission

For each security breach having a significant impact on the trust service provided and/or leak of personal data, the Supervisory Body (FSP Economy) is notified and not later than 24 hours after having become aware of the security breach.

The notification will include mention of the time/period of time on or during which the incident occurred, giving a (technical) description of the security incident, the way in which the incident was detected, the measures taken to contain the incident and any preventive measures to counter any similar incident that may occur in the future.

If not all of the data for the abovementioned notification happens to be immediately to hand, the Supervisory body will in any case be notified within the set time limit that the information provided is a true and accurate reflection of the situation to the best of their knowledge and belief, supplemented whenever possible by the latest incoming additional details and incident commentaries.

If it concerns a data leak where sensitive personal data threatens to be made public unauthorized, the Belgian Privacy Commission is also notified following the directives as set out by the Privacy Commission.

The most recently updated directives may be consulted on the Privacy Commission website: https://www.privacycommission.be/nl/melding-gegevenslekken-algemeen

4.2 Informing adversely affected Users

In case:

- the security breach likely has an adverse effect on the concerned natural or legal person putting their trust on the trust service provided,

and/or

- the personal data leaked was not encrypted or the data leak likely have an adverse effect on the privacy of the concerned natural or legal person,

the concerned natural or legal persons will be notified within undue delay.

Communication to the affected (legal) persons will be done in consultation with and following instructions of the Supervisory Body and Privacy Commission (if applicable).

The notification will minimum include mention of the time/period of time on or during which the incident occurred, giving a (technical) description of the security incident, the way in which the incident was detected, the measures taken to contain the incident and any preventive measures to counter any similar incident that may occur in the future.

4.3 Informing the Public

The public will be informed whenever a data leak occurs the impact of which exceeds the scope of the Aangetekende.email Trust Service, but always in consultation with and following the instructions of the Supervisors.

5 Regulatory supervision

5.1 Recurrent audit by the recognized Compliance Assessment Body

CONNECT SOLUTIONS will assign a recognized conformity assessment body to run an audit on the compliance of CONNECT SOLUTIONS and its Electronic Registered Delivery Services with the eIDAS Regulation at intervals of not more than 24 months. These recurrent audits are conducted at the costs of the TSP, namely CONNECT SOLUTIONS.

CONNECT SOLUTIONS will submit the resulting conformity assessment report within three working days of receipt to the Belgian Federal Public Service Economy (supervisory body).

Any failure to satisfy the requirements of the eIDAS Regulation as indicated by the Belgian FPS Economy (supervisory body) will be rectified within the period of time stipulated by the Belgian FPS Economy.

5.2 Audit requested by the Supervisory Body

At the request of the Belgian FPS Economy (supervisory body) CONNECT SOLUTIONS will assign a recognized conformity assessment body to run an audit on the compliance of CONNECT SOLUTIONS and its Electronic Registered Delivery Services with the eIDAS Regulation. These ad-hoc audits are conducted at the costs of the TSP, namely CONNECT SOLUTIONS.

CONNECT SOLUTIONS will submit the resulting compliance report within three working days of receipt to the Belgian FPS Economy (supervisory body).

Any failure to satisfy the requirements of the eIDAS Regulation as indicated by the Belgian FPS Economy (supervisory body) will be rectified within the period of time stipulated by the Belgian FPS Economy.

5.3 Constant respect of eIDAS requirements

Any failure to satisfy the requirements of the eIDAS Regulation as indicated by the Belgian FPS Economy (supervisory body) will be rectified within the period of time stipulated by the Belgian FPS Economy.

6 Commencement of Qualified Trust Service

CONNECT SOLUTIONS will not begin to offer the Qualified Trust Service until the status of qualified is included in the trust list published by FPS Economy (supervisory body).

When using the EU trust mark CONNECT SOLUTIONS will ensure that there is a link for the Qualified Trust Service to the relevant Trusted List on the website.

7 Protection of privacy

Art.5 of Regulation 910/2014 (eIDAS) includes "Data processing and protection". Art.5.1 refers to the integral Directive 95/46/EC with which Trust Services must be in compliance.

As of 25/05/2018 collection, storage and processing of personal data within Aangetekende.email is also done in accordance with EU Directive 2016/679 (GDPR).

7.1 Identification and pseudonyms

According to Article 5.2 pseudonyms are not explicitly forbidden in electronic transactions, but their admissibility depends on the national legislation.

Regarding eIDAS Article 5.2 the Trust Service Aangetekende.email does not give instructions or impose any restrictions on the used e-mail address other than requiring it to be a valid e-mail that is accessible and usable in the normal way for the user of the Trust Service Aangetekende.email. For reasons of reliability and integrity the User is advised to give an e-mail address to which the User has exclusive access. However, it is the User's responsibility to regard his e-mail notifications as an element of user-friendliness. It is the User's responsibility to consult the Aangetekende.email Platform on a regular basis.

When creating a User Account each User must identify himself by means of his own eID. The entered e-mail address is here linked to a particular eID with which the User may be identified with a high degree of certainty. For legal persons an additional control is carried out, namely by verification of an extract from the Crossroads Bank for Enterprises, which should show that the person wishing to use the User Account for the legal person is authorized to act on behalf of the legal person.

Sending and receiving with Aangetekende.email is possible only between active User Accounts on the Aangetekende.email Platform. Sending, signing for receipt and opening the registered e-mail is possible only by positive identification with a valid eID linked to the relevant User Account.

Transactions on the Aangetekende.email Platform are consequently made exclusively between registered and clearly identified parties, regardless of whether or not a used e-mail address may be classified as a pseudonym.

7.2 Directive 95/46/EU

Article 5.1 of eIDAS provides for the application of **Directive 95/46/EC** of the European Parliament and the Council of 24 October 1995. This Directive regulates the protection of natural persons concerning the processing of personal data and the free circulation of data.

The collection, storage and processing of personal data within Aangetekende.email is done completely in accordance with Directive 95/46/EC. In particular, we look further on Articles 6, 7, 8, 10 to 12 inclusive, 14 to 21 inclusive and 25.

Art.6 - Quality of personal data

Trust Service Aangetekende.email collects, processes and stores a set of personal data for each User. This data must be explicitly given by the User himself by (i) completion of the input fields and (ii) reading of the User's eID card data. This is done by inserting the User's eID in a card reader designed for the purpose connected to the data entry device and after the User gives confirmation by entering the PIN code.

When registering on the Aangetekende.email Service the User must state his express consent to the "*General Conditions*". The General Conditions give a very clear description as to what personal data will be kept, which processing will take place when, and why the keeping of particular personal data and its described processing are necessary in connection with the Trust Service Aangetekende.email.

Updated and correct data is crucial for reliable identification and signature. For this the User can always use the Aangetekende.email Platform to consult his stored personal data and, if necessary, correct, supplement or delete it. If, however, after completing the registration procedure, the User decides to remove personal data that belongs to the minimum set of required personal data, this can only be done by removing the entire User Account. Removal of the concerned data then becomes effective only after completion of the closure phase and the final removal of the User Account.

A control mechanism is built in that controls the validity of the eID. After expiry of the validity period of the eID the User must update his personal data with a new valid eID before he can have access to the functions of the platform.

Art.7 - Legitimate data processing

During the (initial) registration on the Aangetekende.email Platform express declaration of agreement with the *General Conditions* is an essential condition for the completion of the registration procedure. This is done by digital signature using the eID. The *General Conditions* describe, among other things, all the relevant personal data and the way in which that data will be processed.

Art.8 - Special categories of data

Personal data described under Art. 8.1 has no relevance in connection with Aangetekende.email and is therefore not called up, registered or stored in any other way.

Art.10 to 12 inclusive - Information to be given to the data subject

The identity and contact details of the company responsible for processing - CONNECT SOLUTIONS - and its representatives are clearly posted on the website of the Aangetekende.email Platform and are included in the General Conditions.

Personal data is exclusively entered by the concerned person himself by (i) completing the data input fields and (ii) reading of the User's eID card data. This is done by inserting the User's eID in a card reader designed for the purpose connected to the data entry device and after the User gives confirmation by entering the PIN code.

The User may consult his stored personal data and, if necessary, correct, supplement or remove it at any time. If, however, after completing the registration procedure, the User decides to remove personal data that belongs to the minimum set of required personal data, this can only be done by removing the entire User Account. Removal of the concerned data then becomes effective only after completion of the closure phase and the final removal of the User Account.

Art.14 - Right to object

At any time during or after the registration procedure the User of the Aangetekende.email Platform may decide to withdraw approval for storage and processing of his personal data. To do this the User must either terminate the started but not yet completed registration procedure or remove the created User Account. However, for the latter operation it is required that the User himself logs on in his User Account on the Aangetekende.email Platform and then follows the procedure for removal of the account.

Art.15 - Automated individual decisions

Each collection, processing and storage of (personal) data is exclusively used in connection with the Trust Service Aangetekende.email.

Further processing of personal data that may result in individual decisions as mentioned in Art. 15, para. 1, has no relevance for Trust Service Aangetekende.email and is therefore not executed.

Art.16 - Confidentiality of processing

The company responsible for processing and its employees and representatives are contractually bound to secrecy with regard to any personal data and content of sent messages with which they may come into contact. All persons involved in processing are also strictly forbidden to engage in any operations (search, adaptation or processing of personal data) other than those that are strictly necessary for the administration and maintenance of the Aangetekende.email Platform.

Personal data, the content of messages and their processed results are exclusively sent by protected channels (https internet connection) and stored in encrypted form on protected servers. The subject is explained in more detail in the following Article and in Chapter 3, “Security Policy”.

Art.17 - Security of processing

For the transfer, processing and storage of all data involved in the Trust Service Aangetekende.email exclusive use is made of protected and encrypted technologies. The subject is explained in more detail in the technical manual and in Chapter 3, ‘Security Policy'.

Art.18 to 21 inclusive – Notification to the supervisory body

The company will register with the supervisory authority for Trust Services (FPS Economy). Before the operational offer of the Trust Service to the public any possible additional questions and/or comments regarding the concerned services must be addressed with a positive result.

Art.25 – Transfer of personal data to third parties

Each collection, processing and storage of (personal) data is done through protected channels and on protected infrastructure and is used exclusively in connection with the Trust Service Aangetekende.email.

Trust Service Aangetekende.email is available exclusively for Users - natural persons - in possession of a valid Belgian eID, acting either on their own behalf or on behalf of a legal person of which they are a legal representative.

Before being admitted as User to the Aangetekende.email Platform the User must sign the General Conditions and in doing so commits him- or herself to treat any form of personal data with which he may come into contact with all due care and confidentiality and use it exclusively for purposes in connection with the Aangetekende.email Platform.

Any suspicion or report of suspected violation of confidential treatment of personal data strictly in connection with the Aangetekende.email Platform will be thoroughly investigated and, if necessary, will result in measures reflecting the established seriousness of the violation and its possible recurrent nature.

8 Liability

8.1 Liability for wilful damage or loss/damage due to negligence

The Aangetekende.email Platform and the associated services for the sending and receiving of registered e-mail messages form a Trust Service in application of Regulation 910/2014 Art.44. All procedures, software and hardware used are securely developed and selected. Permanent monitoring and maintenance must ensure that the platform and the offered services function optimally at all times and that the security of data is and remains guaranteed.

Users may therefore place their confidence in a stable, protected and reliable provision of service. In conformity with Regulation 910/2014 Art. 13, CONNECT SOLUTIONS is responsible for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.

8.2 Restrictions on use, liability and information of the User

The restrictions on the use of Trust Service Aangetekende.email and the restrictions in case of damage are described and explained extensively in the ***General Conditions***.

On registration with the Aangetekende.email Platform these General Conditions are offered in integral form to the User and must be accepted expressly and without reservation by the User as being '*read and approved*' by digital signature with the eID. Without approval and acceptance of the General Conditions the User cannot complete the registration process and therefore will not be allowed access to the Aangetekende.email Platform and the associated services.

In case of later changes to the General Conditions the User will be informed accordingly in the next logon on the Platform.

8.3 Harmonization with national law

The provisions in the General Conditions are checked by a lawyer for compliance with Belgian legislation. Changes of current law will be followed and respected proactively. Any statements or requests from the Supervisor will be acted on within the allotted time.

9 Continuity of the Service and Termination Plans

9.1 Notification of changes and intention to suspend activities

CONNECT SOLUTIONS will inform FPS Economy (supervisory body) regarding any changes in the provisions of qualified Trust Services and the intention to discontinue those activities.

9.2 Submittal to the Supervisory Body

Regarding supervision as described in Chapter 5, the Termination plan, meaning the complete content of chapter 9 of this document, is also submitted to FPS Economy (supervisory body). The Termination Plan is a shutting down operation and includes the continuity measures that guarantee Users a correct and reliable completion of all outstanding transactions from the time that the decision is taken to end the provision of Trust Service Aangetekende.email.

Changes to the Termination Plan will be submitted to the Supervisor.

9.3 Termination Plan

In case of cessation, the Supervisory Body as well as each User of the Aangetekende.email Platform will receive a message at the e-mail address attached to the User Account no later than 30 days before the Termination Plan becomes effective. In the notification, the User is informed that the service will be ended, including the date of entry into effect of the Termination Plan and the practical consequences.

The practical consequences are then as described below:

- Starting from the date the Termination Plan becomes effective, certain functions of the normal operational situation will no longer be possible. This concerns sending new registered e-mails, creation of a new User Account and adding new users to the existing User Account.

- All outstanding registered e-mails, i.e. sent before the date the Termination Plan became active, can still be signed for receipt and downloaded from the User Account within the timeframes as set out in chapter 10 of the General Conditions.

- After 45 days, when all users have had the opportunity to sign for receipt / download the outstanding registered e-mails within the timeframes as set out chapter 10 of the General Conditions, all User Accounts will be closed.

When a User Account is closed:

- All personal data, is permanently deleted to respect privacy rules.

- No registered e-mail content will be present anymore on the User Account, as CONNECT SOLUTIONS never stores e-mail content data longer then the availability period as described in chapter 10.1 of the General Conditions.

- Both Addressee and Sender have had the ability to download the signed message in PDF format from the inbox respectively outbox, containing the original e-mail message & attachments, qualified electronic signatures of Sender and Addressee and qualified electronic seals of Connect Solutions with proof of and date/time of sending and signing for receipt. The signatures and seals in the PDF file are of type PAdES LTV (long term validation), meaning that the validity of the certificates at the time of signing (CSP/OCSP responses) is included in the signatures and seals. This ensures that the validity of the signatures and seals can be verified for a long time and even after expiration of the certificates using signature validation software, without intervention of and even after cessation of the Trust Service by Connect Solutions.

9.4 Takeover by another qualified Service Provider

Before proceeding to termination of the Trust Service Aangetekende.email the company will try to find a successor that is prepared to continue the service uninterrupted. That successor must also have the status of qualified Trust Service Provider of Electronic Registered Delivery Services.

CONNECT SOLUTIONS will in that case inform FPS Economy (Supervisory Body) and keep it informed regarding the negotiations.

In case no successor is found, CONNECT SOLUTIONS will agree with the Supervisory Body what should happen with the loggings described in 3.6 after cessation.

10 Compliance of the Aangetekende.email Service with Art. 44.1 of the eIDAS Directive

In order to form a correct and complete idea of the working of the Aangetekende.email Service we advise you to read the document "Aangetekende.email - functional description". Here all the functions that the platform offers are described in detail, accompanied by screen prints. The General Conditions should also be read to obtain a complete picture.

In this Chapter the Aangetekende.email Service is tested against the requirements of eIDAS Regulation Art. 44.1. This Article reads as follows:

Qualified electronic registered delivery services shall meet the following requirements:

a) they are provided by one or more qualified Trust Service Provider(s);

b) they ensure with a high level of confidence the identification of the Sender;

c) they ensure the identification of the Addressee before the delivery of the data;

d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified Trust Service Provider in such a manner as to preclude the possibility of the data being changed undetectably;

e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the Sender and Addressee of the data; and

f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified Trust Service Providers, the requirements in points (a) to (f) shall apply to all the qualified Trust Service Providers.

10.1 Compliance with Article 44.1 (b)

The Aangetekende.email Service is available only for and between Users with access to an active User Account on the Aangetekende.email Platform. To obtain access to the platform a User Account must be created in accordance with the description in the General Conditions and the functional description of the Aangetekende.email Service.

During the registration procedure, the identity of the person(s) behind the account is checked by means of an authentication with the Belgian eID card. This is done by inserting the User's eID in a card reader designed for the purpose connected to the data input device, and the confirmation of identity by entering the personal PIN code. For corporate accounts, there is a further check to see whether the person is authorized to act on behalf of the company by means of a check in the CBE register. The User must sign the General Conditions for approval, expressly and without reservation, by means of a qualified electronic signature with the eID.

The account is not activated until after positive validation of the authentication, the validity of the eID certificates (expiry date, CRL and OCSP responses), valid signature on the General Conditions, and the validity of the mandate within the legal person (if applicable). The eID data, such as surname, first name and the public certificates of the eID is then attached to the User Account.

The User must log on in his User Account by entering the e-mail address attached to the User Account during the registration procedure. The User must then authenticate himself with his eID. Logging on in the User Account is possible only by entry of a valid e-mail address attached to the User Account, *and* of a eID card attached to that User Account *with* valid authentication *and* valid authentication certificate for the eID (expiry date, CRL and OCSP responses). In case of logging on a corporate account by a legal company representative, the application will run a check on the CBE webservice to see whether that person is still a legal representative in that company as stated above in the CBE. If not, access is denied. In case of logging on to a corporate account by a Mandated User, the application will run a check on the CBE webservice to see whether minimum one of the legal company representatives of the User Account still has the status of legal representative in that company as stated in the CBE. If not, access is denied.

As set out in Article 4 of the General Conditions, the status of Authorized Agent (or proxy) may be obtained for another User Account whereby incoming and outgoing messages in that User Account are included in the User Account of the Authorized User. As explained in that Article any such power of attorney will be conditional upon positive verification by CONNECT SOLUTIONS of the supporting legal evidence. Identification of the Authorized User is effected on the basis of the above principles.

During the sending of a new registered e-mail, the Sender must sign the message by means of a qualified electronic signature (LTV type) with the signature certificate of the Belgian eID card with which he logged on to the Platform and that was linked to the User Account during the registration process. The Addressee of the message will be able to verify the identity of the Sender by means of that qualified electronic signature on the message.

The application will check the validity of the Sender's qualified electronic signature and the validity of the signature certificate (expiry date, CRL and OCSP responses). Only after positive validation, CONNECT SOLUTIONS then adds a qualified electronic seal (LTV type) to the message with one of the certificates referred to in Chapter 1.1 and 3.4 as proof of verification and delivery and puts the message in the inbox of the Addressee and in the outbox of the Sender.

From that moment, the Sender has the ability to download (within the timeframes set out in the general conditions) the message from the outbox in PDF format containing the original e-mail message & attachments, qualified electronic signature of sender and qualified electronic seal of Connect Solutions with proof of and date/time of sending. The signatures and seals in the PDF file are of type PAdES LTV (long term validation), meaning that the validity of the certificates used at the time of signing/sealing (CSP/OCSP responses) is included in the signature/seal. This ensures that the validity of the signature/seal can be verified for a long time and even after expiration of the certificates using signature validation software, without intervention of Connect Solutions.

10.2 Compliance with Article 44.1 (c)

The Aangetekende.email Service is available only for and between Users with access to an active User Account on the Aangetekende.email Platform. To obtain access to the Platform a User Account must be created in accordance with the description in the General Conditions and in the functional description of the Aangetekende.email Service.

During the registration procedure, the identity of the person(s) behind the account is checked by means of an authentication with the Belgian eID card. This is done by inserting the User's eID in a card reader designed for the purpose connected to the data input device, and the confirmation of identity by entering the personal PIN code. For corporate accounts, there is a further check to see whether the person is authorized to act on behalf of the company by means of a check in the CBE register. The User must sign the General Conditions for approval, expressly and without reservation, by means of a qualified electronic signature with the eID.

The account is not activated until after positive validation of the authentication, the validity of the eID certificates (expiry date, CRL and OCSP responses), valid signature on the General Conditions, and the validity of the mandate within the legal person (if applicable). The eID data, such as surname, first name and the public certificates of the eID is then attached to the User Account.

The User must log on in his User Account by entering the e-mail address attached to the User Account during the registration procedure. The User must then authenticate himself with his eID. Logging on in the User Account is possible only by entry of a valid e-mail address attached to the User Account, *and* of a eID card attached to that User Account *with* valid authentication *and* valid authentication certificate for the eID (expiry date, CRL and OCSP responses). In case of logging on a corporate account by a legal company representative, the application will run a check on the CBE webservice to see whether that person is still a legal representative in that company as stated above in the CBE. If not, access is denied. In case of logging on to a corporate account by a Mandated User, the application will run a check on the CBE webservice to see whether minimum one of the legal company representatives of the User Account still has the status of legal representative in that company as stated in the CBE. If not, access is denied.

As set out in Article 4 of the General Conditions, the status of Authorized Agent (or proxy) may be obtained for another User Account whereby incoming and outgoing messages in that User Account are included in the User Account of the Authorized User. As explained in that Article any such power of attorney will be conditional upon positive verification by CONNECT SOLUTIONS of the supporting legal evidence. Identification of the Authorized User is effected on the basis of the above principles.

Before the e-mail message can be opened from the inbox by the Addressee, the Addressee must sign the message for receipt by means of a qualified electronic signature (LTV type) with the signature certificate of the Belgian eID card with which he logged on to the Platform and that was attached to the User Account during the registration process. The Sender of the message will be able to verify the identity of the Addressee having signed the message for receipt by means of the qualified electronic signature on that message.

The application will check the validity of the electronic signature of the Addressee and the validity of the signature certificate (expiry date, CRL and OCSP responses). The validity of the earlier attached electronic signature/seal, i.e., those by the Sender and by CONNECT SOLUTIONS as proof of delivery, will also be checked so as to guarantee that no changes have been made to the message meanwhile. Only after positive validation, CONNECT SOLUTIONS adds a qualified electronic seal (LTV type) with one of the certificates referred to in Chapter 1.1 and 3.4 as proof of verification and of signature for receipt.

From that moment, both Addressee and Sender have the ability to download (within the timeframes set out in the general conditions) the signed message in PDF format from the inbox respectively outbox, containing the original e-mail message & attachments, qualified electronic signatures of Sender and Addressee and qualified electronic seals of Connect Solutions with proof of and date/time of sending and signing for receipt. The signatures and seals in the PDF file are of type PAdES LTV (long term validation), meaning that the validity of the certificates at the time of signing (CSP/OCSP responses) is included in the signatures and seals. This ensures that the validity of the signatures and seals can be verified for a long time and even after expiration of the certificates using signature validation software, without intervention of Connect Solutions.

10.3 Compliance with Article 44.1 (d) + (e)

During the sending of a new registered e-mail, the Sender must sign the message by means of a qualified electronic signature (LTV type) with the signature certificate of the Belgian eID card with which he logged on to the Platform and that was linked to the User Account during the registration process.

The application will check the validity of the Sender's qualified electronic signature and the validity of the signature certificate (expiry date, CRL and OCSP responses). Only after positive validation, CONNECT SOLUTIONS then adds a qualified electronic seal (LTV type) to the message with one of the certificates referred to in Chapter 1.1 and 3.4 as proof of verification and delivery and puts the message in the inbox of the Addressee and in the outbox of the Sender.

From that moment, the Sender has the ability to download (within the timeframes set out in the general conditions) the message from the outbox in PDF format containing the original e-mail message & attachments, qualified electronic signature of sender and qualified electronic seal of Connect Solutions with proof of and date/time of sending. The signatures and seals in the PDF file are of type PAdES LTV (long term validation), meaning that the validity of the certificates used at the time of signing/sealing (CSP/OCSP responses) is included in the signature/ seal. This ensures that the validity of the signature/seal can be verified for a long time and even after expiration of the certificates using signature validation software, without intervention of Connect Solutions.

Before the e-mail message can be opened from the inbox by the Addressee, the Addressee must sign the message for receipt by means of a qualified electronic signature (LTV type) with the signature certificate of the Belgian eID card with which he logged on to the Platform and that was attached to the User Account during the registration process. The Sender of the

message will be able to verify the identity of the Addressee having signed the message for receipt by means of the qualified electronic signature on that message.

The application will check the validity of the electronic signature of the Addressee and the validity of the signature certificate (expiry date, CRL and OCSP responses). The validity of the earlier attached electronic signature/seal, i.e., those by the Sender and by CONNECT SOLUTIONS as proof of delivery, will also be checked so as to guarantee that no changes have been made to the message meanwhile. Only after positive validation, CONNECT SOLUTIONS adds a qualified electronic seal (LTV type) with one of the certificates referred to in Chapter 1.1 and 3.4 as proof of verification and of signature for receipt.

From that moment, both Addressee and Sender have the ability to download (within the timeframes set out in the general conditions) the signed message in PDF format from the inbox respectively outbox, containing the original e-mail message & attachments, qualified electronic signatures of Sender and Addressee and qualified electronic seals of Connect Solutions with proof of and date/time of sending and signing for receipt. The signatures and seals in the PDF file are of type PAdES LTV (long term validation), meaning that the validity of the certificates at the time of signing (CSP/OCSP responses) is included in the signatures and seals. This ensures that the validity of the signatures and seals can be verified for a long time and even after expiration of the certificates using signature validation software, without intervention of Connect Solutions.

As stated in the General conditions, it is the responsibility of the Addressee and the Sender to check ALL electronic signatures and seals in the downloaded PDF file for validity in order to be sure that no unauthorized changes have been made to the document. This can be done by opening the PDF file in signature validation software and checking the validity of the signatures and seals. In this way undetectable change of data may therefore be excluded. Because all signatures and seals added to the downloaded PDF file are of type LTV (long term validation), the validation of the signatures/seals can be done at any time in future using signature validation software without further intervention of Connect Solutions.

10.4 Compliance with Article 44.1 (f)

Qualified electronic seals added by CONNECT SOLUTIONS to the message with one of the certificates mentioned in Chapter 1.1 and 3.4 as proof of execution of the required controls and of delivery and receipt are given an eIDAS-qualified timestamp. See Chapter 3.3 for more info.

10.5 Belgian eID card

The Belgian eID card is issued by the Belgian Government to its citizens and contains two separate certificates, one for authentication and one signature certificate. There is only one PIN for both.

Electronic Signatures placed with the eID card are Qualified. The Qualified certificate for electronic signature on the eID card is issued by Certipost. Qualified status of Certipost can be found on the Belgian Trusted List (https://tsl.belgium.be).

The certificate is issued on a SSCD. Details can be found at the following URL:

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

11 Data protection and authenticity

All security mechanisms (preventative as well as detective) described in this document, in particular those described in chapter 3 and 10, contribute to the protection of transmitted data against the risk of loss, theft, damage or unauthorized alterations and the ability to check data authenticity.

If despite all security mechanisms a security breach should take place, the procedure as set out in chapter 4 will be followed.

Attachment 1