



Secure Email

Product Description

6.8.2021

Copyright © 2021 SSH Communications Security Corporation

This software and documentation are protected by international copyright laws and treaties. All rights reserved. SSH NQX® is a registered trademark of SSH Communications Security Corporation in certain jurisdictions.

SSH logos and names of products and services are trademarks of SSH Communications Security Corporation. Logos and names of products may be registered in certain jurisdictions.

All other names and marks are property of their respective owners.

No part of this publication may be reproduced, published, stored in an electronic database, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, for any purpose, without the prior written permission of SSH Communications Security Corporation.

THERE IS NO WARRANTY OF ANY KIND FOR THE ACCURACY, RELIABILITY OR USEFULNESS OF THIS INFORMATION EXCEPT AS REQUIRED BY APPLICABLE LAW OR EXPRESSLY AGREED IN WRITING.

Distributing, publishing and/or copying of this document is restricted, and requires a written statement from SSH Communications Security Corp.

SSH Communications Security Corporation
Karvaamokuja 2 B, FI-00380 Helsinki, Finland

Copyright © SSH Communications Security Corporation 2021 – All rights reserved

The information contained in this documentation is provided for informational purposes only. Specifications are subject to change without notice. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided “as is” without warranty of any kind, express or implied. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from SSH Communications Security Corporation (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of SSH Communications Security Corporation software.

	Contents
---	----------

Contents

1. Introduction	1
2. Technical execution	2
2.1 Virtual environment.....	2
2.2 Policy management	2
3. E-mail encryption solution	3
3.1 D-Control.....	3
3.2 D-Envelope	5

3.2.1 Handling messages with D-Envelope.....	7
3.2.2 Notification message.....	7
3.2.3 Reading messages.....	10
3.2.4 Replying to messages securely.....	14
3.2.5 Re-opening of message.....	16
3.2.6 Forwarding messages securely.....	16
3.2.7 Secure EmailDesktop Outlook plugin.....	16
3.2.8 Secure EmailOffice 365 webmail plugin (OWA).....	18
3.3 D-Compose.....	18
3.3.1 Multiweb-compose.....	23
3.4 D-Network.....	23
3.5 Other delivery methods.....	24
3.5.1 TLS Enforcing.....	24
3.6 Other supported standards to receiving messages.....	24
3.6.1 To receive messages using S/MIME or Open PGP.....	24
3.7 Tools for protecting internal e-mail traffic.....	25
3.8 Rest API for sending secure email.....	25
4. Administration and maintenance.....	26
4.1 D-Center.....	26
4.2 Console management.....	27
4.3 Certificate manager.....	27
4.4 Administration API.....	27
5. Requirements in operational environment.....	28
5.1 Hardware and operating system requirements.....	28
5.2 Installation.....	28
5.2.1 Secure Emailinstallation profile options.....	28
5.2.2 Configuration.....	30
5.2.3 Network connections and IP addresses.....	31
5.2.4 Cluster net (duplicated system).....	31
5.2.5 SMS interface.....	31
5.2.6 Firewall settings.....	31
5.3 Monitoring and Updates.....	32
6. Terminology.....	33

1. Introduction

Secure Email(Secure Email Gateway) secures your communication straightforwardly. The e-mail encryption solution makes it possible to protect messages that require confidential processing regardless of the address they are sent to.

In addition, you can prevent information leaks due to human errors and follow the compliance of information security guidelines in e-mail communications. Confidential material in e-mail traffic can be defined and identified in accordance with the company's data security policy. Furthermore Secure Emailcreates an overview of the organization's data security policy in terms of e-mail traffic.

The versatile software consists of independent applications for the organization to compile a suitable entity for responding to the challenges of e-mail communications. D-Control facilitates automatic protection and analysis of confidential e-mail messaging and monitoring of the realization of data security at the organizational level. D-Envelope particularly protects outbound confidential e-mail messaging. DCompose solves inbound confidential e-mail messaging. D-Network facilitates transparent but confidential e-mail messaging within the network of trust. D-Center is used for controlling the big picture, and it presents a variety of statis-tics on e-mail traffic.

The system supports and utilizes commonly-used standards and can thus also be utilized in other applications/services that send e-mail, such as CRM or ERP systems. Often, this also makes it possible to develop and streamline business processes.

2. Technical execution

2.1 Virtual environment

Secure Email supports an environment with multiple virtual instances. Each instance has its own domains. Instances have individual directories that include configurations, logs and secure message data. Also database tables and spool directories are instance specific. Each instance must have an IP-address (unique or shared with other instances), a fully qualified domain name and a certificate for that name.

2.2 Policy management

Secure Email can be integrated into any e-mail system in use, making its use completely transparent to the sender. The Secure Email server acts as a SMTP gateway either only for messages that are to be encrypted, or for all outgoing email traffic. In the first case, the existing e-mail system routes messages marked with the designated secure extension (default: '.s') to the Secure Email server, and in the latter, Secure Email recognizes messages that need to be encrypted according to policy management. (See chapter 5.2:

Installation)

It is possible to define the extension that denotes encrypted e-mail messages per instance.

3. E-mail encryption solution

3.1 D-Control

D-Control analyzes outbound e-mail and identifies messages requiring confidential processing based on definitions derived from the data security policy.

All outgoing messages are scanned. Normally in e-mail traffic the SMTP port 25 is used, however when scanning messages with D-Control mail is forwarded to port 24. This is done automatically with firewall or directly from client mail server.

- **Outgoing mail queue:** Outgoing mail will be separated from incoming mail by creating another mail queue to the server. The outgoing queue includes all messages that come from the internal network to D-Control.

Message subjects or contents (e.g., word, sentence, image or other content) and the name, type or content of the attached file can be used as the identifiers. Encryption rules can be configured by component.

- **Rules for messages:** Different instances can have their own rules that can be based on attachment name, message content (word, sentence, picture, other content) and message header.
- **Rules for attachments:** Attachments can have specified rules (a specific type, a specific name or all attachments). Rules are based on words/sentences inside attachments. Scanned attachment types are PDF, DOCX, pictures (JPEG, TIFF, and JPG), ODT, ODS, ODP, TXT, RTF, XLSX, CSV, GNR and HTML.
- **Regexp tag identifiers:** Custom Regexp tag identifiers (for example contract number, social security number or bank account number) can be created in addition to basic rules. These identifiers can be added to basic rules simply with its name.
- **Override rule:** These rules override all other D-Control rules. For example, if all PDF files are marked as encrypted, specified e-mail addresses can still send messages with PDF attachments unencrypted. Override rules can be based on attachment name, message content (word, sentence, picture, other content) and message header.

As a result of the analysis, e-mail messages considered confidential can alternatively be automatically encrypted or the sending of these messages without protection can be prevented, thereby preventing a potential data leak.

- **Encryption level:** The encryption level that is used to send confidential messages can be determined (options are Letter-level, Registered letter-level, forced TLS, over D-Network connection or over VPN connection). Message can also be rejected in which case if the rules match the message will not be delivered and the sender will be notified of it.
- **Sender notification (default: off):** Sender of a message can be notified if the message contained material that requires the use of protection. Notification informs that the message cannot be send unencrypted and gives instructions on how to operate. Alternatively sender can be reminded of forgetting to use protection with a notification that informs that the message was protected automatically and send forward.

D-Control also creates a clear insight into the state of the implementation of the organization's data security policy, taking into account the requirements for data security in terms of e-mail traffic. In practice, the data can be presented as various graphs or tables that can easily be utilized in other reporting.

- **Rules entered into groups:** Different rules can be grouped in order to make the statistics easier to manage. For example all rules relating to sales (tenders, contracts, IDs) can be named “Sales”. Different groups can be seen in statistics.

3.2 D-Envelope

D-Envelope is used by users within the organization. D-Envelope makes it possible to safely send and receive messages confidentially to or from any e-mail address whatsoever. Its use does not require any software to be installed on the sender's or recipient's workstations. Receiver reads the message with a browser using an encrypted TLS connection.

The e-mail encryption solution offers different levels of protection from easy to use security level up to the Finnish national protection level ST IV. For end-users the use of the solution is so straightforward, that email encryption works even without installations to an email client, without registrations and additional passwords.

The application's different levels of protection can be compared to the corresponding regular mail methods in terms of protection. The "letter" protection level corresponds to a normal letter, securing the message traffic. The "registered letter" protection level corresponds to sending a registered letter, meaning that the message traffic is secured and it is possible to confirm the correct recipient with a PIN code sent to his/her mobile phone. The "handed over personally" protection level corresponds to handing over to the addressee in person so that the receiver is authenticated electronically based to recipients Social Security Number (SSN). The sender must define the recipient's SSN. When the recipient tries to open the secure message SSN based authentication is required. Secure Email compares the SSN provided by the authentication provider to SSN defined by the sender. If the SSN defined by the sender matches to authentication provider's provided SSN, the recipient can read the message.

Social Security Number based authentication requires additional authentication service provider. Secure Email works with the following protocols/providers:

- BankID (Sweden and Norway)
- Finnish Mobile ID
- Finnish Trust Network (banking recognition with Signicat or Telia)
- Generic OpenID Connect based SSN authentication
- NemID
- Suomi.fi

In addition D-Envelope can be used for sending security classified material (e.g. Finnish national protection level ST IV) when the receivers are previously identified.

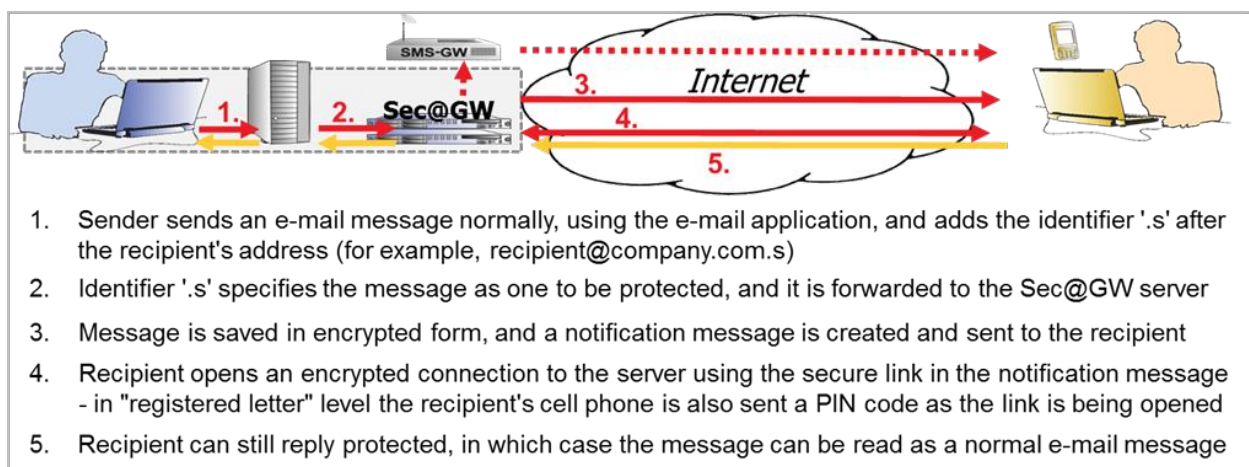


Figure 1. Illustrating the example of D-Envelope usage

When a sender uses their normal e-mail system to send a message. Adding a '.s' at the end of the recipient's address (for example recipient@example.com.s) will activate the "Letter" level. Using the

“registered letter” level is achieved by adding the recipients mobile phone number and ‘.s’ at the end of the recipients e-mail address (for example recipient@example.com.040123456.s). The “handed over personally” level is used by adding the personal identification number and ‘.s’ at the end of the recipients e-mail address (for example recipient@example.com.ddmmyzxxx.s). To use the “ST IV” level the sender adds identifier ‘.s4’ at the end of the recipient’s e-mail address (for example recipient@example.com.s4).

Instead of the actual message, the recipient receives a notification message that contains a link protected with the patented MessageLock™ technology. The actual message can be opened from the link with TLS protected browser connection. In addition, at the “registered letter” level the recipient is automatically provided a message-specific PIN code as an SMS for opening the message. SMS messages are generated and sent from Secure Emailserver to the recipient’s mobile phone through a SMS-gateway.

- **SMS pre-notification (default: off):** SMS pre-notification can be used to inform the recipient of a new secure message by text message in Registered letter level.
- **Notification message as SMS message:** Notification message of a new secure message can also be received by text message in “registered letter” level. Options are:
 - Email (default)
 - SMS
 - Email and SMS

When using the “handed over personally” level the receiver will be authenticated with bank credentials based on Social Security Number (BankID (Sweden and Norway), Finnish Mobile ID, Finnish Trust Network (banking recognition with Signicat or Telia), Generic OIDC based SSN authentication, NemID, Suomi.fi). Using the “ST IV” level the receiver will need to know the correct URL and pre-set password to open the message (for more details see the National Cyber Security Center Finland’s guideline “Usage policy and limitations for protective level 4).

The message is stored on the server for a limited time. The message can be reopened using cookies or a message-specific password or with the same authentication method as previously. It is also possible to reply using the secure channel directly to the sender’s normal mailbox. In addition, the message may be forwarded to a third party in a secure format.

- **Authorized senders within organization (default: all):** Allowed sender addresses can be listed, so that organization can define who has the access to the service. Unauthorized senders receive a notification informing them that they cannot send messages with D-Envelope. List of allowed senders can be updated from D-Center or synchronized from the organizations server (in real-time or scheduled for example once a day) using the LDAP/S protocol.
- **Limit number of recipients (default: off):** The amount of recipients in a secure message can be limited.
- **Encryption rule based on address (default: off):** Encryption rules can be controlled based on addresses. For example all e-mails coming from a specific sender address can be defined to be automatically encrypted. In this case, at least those emails must be routed to the Secure Emailserver
- **Instantly create an instance for protective level IV (default: off):** Secure Email encryption solution is approved by NCSA-FI as a solution for handling security classified material (protective level IV). It is possible to instantly create an instance that has the requirements of protective level IV configured. NOTE! This only applies to the instance settings. More definitions can be found in usage policy defined by NCSA-FI.

Besides that, it is possible to force “registered letter” level for specific recipients. In this case both e-mail address and GSM-number should be paired up in the D-Envelope so that sender would not need to include the number to the e-mail message. So if the message is marked to be encrypted (.s) and the number for recipient’s email is defined and domain is allowed to send encrypted mail, message is sent encrypted with SMS authentication.

- **Sensitivity header (default: off):** All incoming e-mails sent through D-Envelope (reply and forward messages) can have a customized "Sensitivity" header (options are personal, private, companyconfidential or none).
- **E-mail bounce handling (default: delete attachment):** If a sent message is bounced back by the mailer-daemon, the original message can be sent back encrypted and/or with attachment of the original message deleted.
- **Internal max size in reply (default: off):** If the size of the incoming message is larger than the internal mail server allows, D-Envelope sends a notification message instead of the actual message so that it can be read using D-Envelope application.
- **Allowed MIME/attachment types in D-Envelope (default: off):** Types of allowed (whitelist) or forbidden (blacklist) attachments in outgoing messages can be defined using MIME types and file extensions.
- **Allowed MIME/attachment types in reply (default: off):** Types of allowed (whitelist) or forbidden (blacklist) attachments in reply messages can be defined using MIME types and file extensions.
- **Allowed message size for individual user in reply (default: off):** The maximum message size that an individual address or domain is allowed to send can be defined.

3.2.1 Handling messages with D-Envelope

D-Envelope collects the needed information, encrypts the message, temporarily stores it on the server and creates a notification message. E-mails will always be stored on the server in encrypted form. Every e-mail message has a unique encryption key and identifier number that is stored to a database.

- **File encryption:** The encryption uses the AES algorithm with a 256-bit encryption key. For key generation, a cryptographically strong random number generator is used.
- **Database information:** The identifier is stored in a database along with other relevant information, such as message size, recipient(s) and session control information.
- **Storing encryption key (default: enabled):** Storage of the unique encryption key can be disabled. In this case if the notification message disappears, the message cannot be opened anymore. If the encryption key is stored in the database, maintenance has the possibility to generate a new notification message with the link.
- **Storing time of messages:** The storing time of messages is adjustable. Messages that haven't been opened are stored on server for a limited time (default: 60 days). Messages that have been opened, but not deleted are stored on the server for a limited time (default: 30 days).
- **Clean deleted messages from database (default: off):** When a message is deleted also the message's reference information is deleted from database.
- **Clean old messages from database (default: off):** When a message's reference information is older than configuration time (default: 1 year) it is deleted from database.

3.2.2 Notification message

Instead of sending the e-mail message traditionally, D-Envelope sends a notification message to the recipient that informs about the confidential message. The actual message will be held on the Secure Emailserver and can be read using the link in the notification message. The link opens a TLS encrypted connection and includes the message identifier and the encryption key in an encrypted format. The link is protected with the MessageLock™ technology, so access for reading encrypted e-mail messages is limited. Cookies or password will be required to reopen the message later (see chapter: Re-opening of message).



Figure 2. Example of D-Envelope's notification message

- **Content of notification message:** The content of notification message is fully customizable. The message can be sent in Text or HTML format, or both (default). There can be a different notification message for messages sent in "Letter", "Registered letter" and "Handed over personally" level.
- **Special templates:** Each sender and receiver e-mail address or domain can have their own personal notification message.
- **Message informs of included attachments (default: disabled):** Notification message informs of included attachments if there is any.

In "Registered letter" level SMS authentication is used. SMS authentication offers an additional way of authenticating the receiver. In SMS authentication D-Envelope sends a PIN code as SMS message to the receiver while the link is opened for the first time. D-Envelope sends the SMS message to mobile phone through SMS gateway. In "Letter" level it is also possible to define an own password needed to open the message. "Letter" level messages (normal and password protected) can be automatically converted to require "Mail OTP". In case of Mail OTP one-time-pin (OTP) code is required when opening the message. The OTP will be sent into recipient's email after the link has been opened.

- **MessageLock™ technology:** The notification message's link contains a message identifier number and encryption key in encrypted format. When the receiver opens the message, the following verifications are done:
 - a) the validity of the link is verified
 - b) the message identifier is matched against information in the database
 - c) the IP address of the computer is not found on blacklists (i.e. exploited computers)
 - d) if the domain has been configured to restrict usage based on IP address, the recipient's IP address is verified to have access
 - e) the status of the message (deleted/locked/open) is verified
 - f) optionally, additional checks are performed (no / password / SMS authentication)SMS authentication supports having more than one phone number assigned to the message. This means that several phone numbers can be added to the end of the receiver's e-mail

address and all listed mobile numbers are sent a unique PIN code. This functionality can be used in two mutually exclusive scenarios:

- a) the opening of a confidential message must be witnessed by at least two people or
 - b) a message sent in "Registered Letter" level must be accessible to more than one person.
- **Require all PIN codes associated to a message (default: off):** It can be required that all PINs must be entered to open the message. In this case the message does not open unless the receiver has all the PIN codes associated with the message.
 - **Additional pre-shared password for "letter" level message (default: off):** Sender can define a password needed for the receiver to open a message. Password is placed in the Subject field between chosen identifiers (for example {} marks). If system sends automatic messages, password can be added to message header (for example X-Password).
 - **Transform mail to use OTP-like security level (default: off):** It can be required that all "letter" or "password level" messages can be transformed to require one-time-pin code that will be provided to the same mail address as the original notification message has been sent.
 - **Strength of PIN number (default: 4 numbers):** It is possible to configure how secure a PIN number of a SMS authenticated message must be (e.g. length and special characters).
 - **PIN code entry / order new PIN code:** PIN code be entered (default: 5) and PIN code reordered (default: 10) limited amount of times. After too many tries the message is locked and cannot be opened again.
 - **Notify sender address (default: off):** In notification message it is possible to mark a certain address as sender instead of actual sender. For example all e-mails sent from first.name@example.com will be seen as sales@example.com.
 - **Define sender and reply-to addresses:** Sender address and reply-to address of a notification message can be defined to prevent the sending of possible replies to notification message.
 - **Notify sender S/MIME (default: off):** Notification messages can be protected with digital signature using S/MIME with sender address.
 - **Notify sender, Sender Policy Framework (SPF) support (default: on):** SPF specifies which servers are authorized to transmit e-mails. Normally D-Envelope uses recipient's e-mail address as sender when replying/forwarding secure e-mails. Because of SPF, e-mails going to external addresses might not be delivered to recipients. To avoid this, D-Envelope can change sender's address in notification message to the address defined in configuration and the original sender is marked to the Reply-to field if both sender and recipient are not local addresses. Original sender can be added to the text in notification message.
 - **Allow read receipt (default: on):** With read receipt sender gets a notification message when recipient reads the message. The read receipt also includes the identifiers and checksums of sent message's attachments. Sender can this way verify that message and attachments has gone through. This is forced to work automatically and the recipient will not be notified of it. Text can be customized.
 - **Automatic read receipt (default: off):** Read receipt can be forced to specific sender addresses. A read receipt is automatically sent to the original sender when a secured message is opened.
 - **Notification of unread message (default: off):** If a message has not been read within specified time the sender and/or receiver can be notified of it. Notification will be sent in plain text. Notification time of unread message is configurable per user address.

3.2.3 Reading messages

The actual message opens with a browser using a secure connection.

- **Traffic encryption:** The receiver opens the e-mail with a browser by clicking the link in the notification message. The connection is established by using standard TLS protocol (https). At server side no weak cipher is allowed so minimum strength of encryption is 128 bits (maximum 256-bit (AES)).

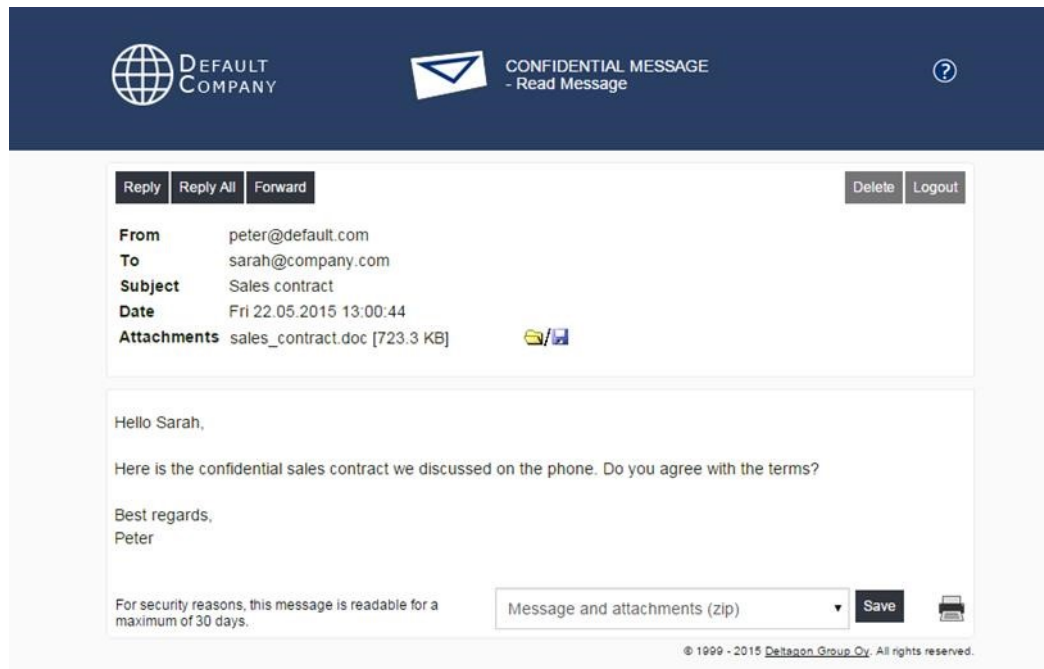


Figure 3. Example of a message that has been sent to an external user via D-Envelope (the user is reading the message in the web interface)

Functions:

- Reply using the same secure connection
- Reply all (setting, default: on)
- Forward (setting, default: off)
- Saving message (in text, html, zip, only the attachments as a ZIP, encrypted zip or S/MIME encrypted eml)
- Printing message
- Deleting message
- Storing message on the server (limited time only)
- Logout (Terminate session and possibility to set a password which will be required on the next time link opens)
- **Save as S/MIME encrypted eml (default: on):** A receiver of a message sent through D-Envelope can save it in S/MIME encrypted form if he/she has an S/MIME certificate in use.
- **Preview of attachments (default: off):** A receiver of a message can see a preview of the sent attachments (supported file types are pdf, jpeg, png, gif, tiff, txt, rtf and office documents). NOTE! For txt, rtf and office document support, required libreoffice packages must be installed.

- **Blocking the download of files (default: off):** Storing of attachments to a computer can be prevented by blocking attachment downloads. For example, allowing the attachment preview makes it possible to view the files but not download them.

The user interface language is set according to browser's language settings. Supported languages are Danish, Deutsch, English, Estonian, Finnish, Latvian, Lithuanian Norwegian, Russian and Swedish.

- **Disclaimer page (default: off):** Before a secure message is opened, the user can be shown a disclaimer about the confidentiality of the message whereby the reader knows that the message is opened unjustly if he/she is not the intended recipient. The disclaimer text can be customized and localized for each supported language.
- **Layout of user interface:** Layout will be custom-made to fit into organization's image.

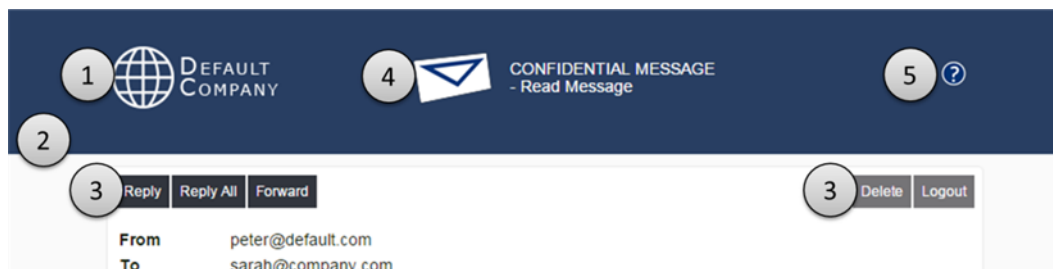


Figure 4. Example of a message that has been sent to an external user via D-Envelope (the user is reading the message in the web interface)

1. Logo
2. Colors (CSS)
3. Buttons (CSS)
4. Multiple options for envelope logo to choose from (including no logo), default can be seen below
5. Help can be shown either as a link or an image and it can be customized with CSS via D-Center

The user interface supports responsive layouts. By designing one, the UI will scale depending on the device monitor size.

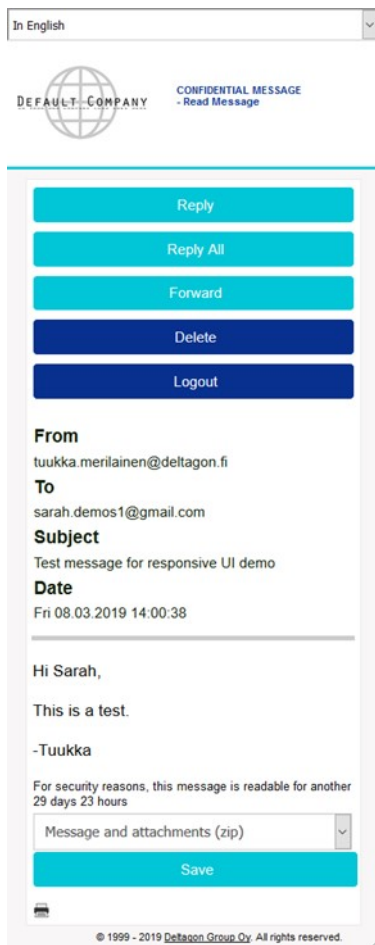


Figure 5. Illustration of the responsive designed user interface. Example of a message that has been sent to an external user via D-Envelope (the user is reading the message in the web interface)

- **Force user interface language (default: off):** Language in user interface can be forced so that only one language is in use. Normally language is set automatically according to browser settings.
- **Recipient can choose interface language (default: off):** Secure message recipients can choose to change the interface's language from a dropdown box if this option has been enabled.
- **Domain based IP-restriction (default: none):** Domain can be configured to only have restricted usage based on IP address (either single e-mail addresses or full domains). For example employee can be allowed to read secure messages only from organization's internal network.
- **Read only once (default: off):** Message can be read only once and will be automatically deleted from the server after it is read.
- **Session expiration (default: one hour):** As a message is opened a session is created for the user with which the message is accessible. Session expiration for reply and forwarded messages can also be configured. If session expires, message must be reopened and a new session starts. Users are shown a notification 5 minutes before expiration.
-

- **Session details:** Users IP address and browser's user agent can be checked and attached to the session when message is read. If one or both (default: user agent only) changes, session is invalidated and message can no longer be read with that session.
Customized help document: Texts in help document in user interface can be customized (default: off). Documents can be in PDF or HTML form.
- **Custom HTML content:** Custom HTML enables adding own HTML content to user interface (DEnvelope and D-Compose).
- **Check IP address from RBL lists:** It can be defined of how many RBL lists the message receiver's IP address is checked from and administrator can define which lists are used (default: dnsbl.ahbl.org and xbl.spamhaus.org). It can also be defined which IP addresses can bypass RBL lists.
- **Using client certificate to open secure messages (default: off):** User may be asked to provide client certificate or a password that will be linked to their e-mail address. The client certificate or user given password must be provided each time a secure message is opened. User can register when opening a secure message for the first time (may require approval by the administrator) or the user must register before a secure message can be sent to them (registration link is sent to the user by administrator).

A sender of the secured email can decide that strong authentication is required for the Recipient ("Handed over personally" security level). If strong authentication for the recipient is required he/she has to attempt authentication by using one of the following SSN based authentication methods (methods are configured and enabled by administrator):

- BankID (Sweden and Norway)
- Finnish Mobile ID
- Finnish Trust Network (banking recognition with Signicat or Telia)
- Generic OpenID Connect based SSN authentication
- NemID
- Suomi.fi

Strong authentication offers receiver's name and social security number. The connection between Secure Emailand service provider is established by using standard TLS protocol (https).

- **Electronic authentication determined by sender (default: off):** The receiver can be identified with a social security number added to the message. Sender adds receiver's social security number at the end of the e-mail address and then adds the '.s' identifier (for example receiver@company.com.ddmmyzxxx.s). The receiver is authenticated electronically by using one of the supported SSN authentication services. Only the receiver with correct social security number can open the message.

Please note: If this configuration is enabled at least one of the following configurations has to be enabled:

- **BankID authentication (default: off):** When message is opened user is authenticated with BankID authentication and message is locked to user. If read receipt is enabled the user's social security number or just four last digits is sent to sender as read receipt message. Customer must have an agreement with Svensk e-identitet (Sweden), ZignSec (Sweden and Norway) or Signicat (Sweden and Norway).

-

- **Finnish Mobile ID authentication (default: off):** When message is opened user is authenticated with Mobile ID and message is locked to user. If read receipt is enabled the user's social security number or just four last digits is sent to sender as read receipt message. Customer must have an agreement with Elisa.
- **Finnish Trust Network authentication (default off):** When message is opened user is authenticated with trust network banking recognition (Signicat or Telia OIDC authentication). Customer must have an agreement with Signicat or Telia.

Generic OpenID Connect based SSN authentication (default off): Secure Email supports any authentication services which are following OpenID Connect standard and provide user's SSN.

Configuration of the Generic OpenID Connect Authentication requires API specification from the authentication service provider.

- **NemID authentication (default: off):** When message is opened user is authenticated with NemID authentication and message is locked to user. If read receipt is enabled the user's social security number or just four last digits is sent to sender as read receipt message. Customer must have an agreement with ZignSec or Signicat.
- **Suomi.fi authentication (default: off):** When message is opened user is authenticated with Suomi.fi e-identification and message is locked to user. If read receipt is enabled the user's social security number or just four last digits is sent to the original sender as read receipt message. Customer must have a contract with eSuomi. Suomi.fi e-identification enables the citizens of Finland and the European Union to be recognized in a safe way by using various identification media such as bank-id and mobile certificates. The identification service environment is meant for the use of governmental authorities, agencies and institutions, courts of law and other judicial bodies.

3.2.4 Replying to messages securely

The recipient can reply to the original message by using the same secure TLS connection between browser and D-Envelope that was used to read the message. Attachments can also be added to the message and it is possible to configure automatic virus scan for the attachments. The reply message is sent from D-Envelope back to the original sender through the organization's internal network. (See picture: Example of D-Envelope usage).

- **Originator text (default: on):** The originator text will be seen in the beginning of the e-mail message.

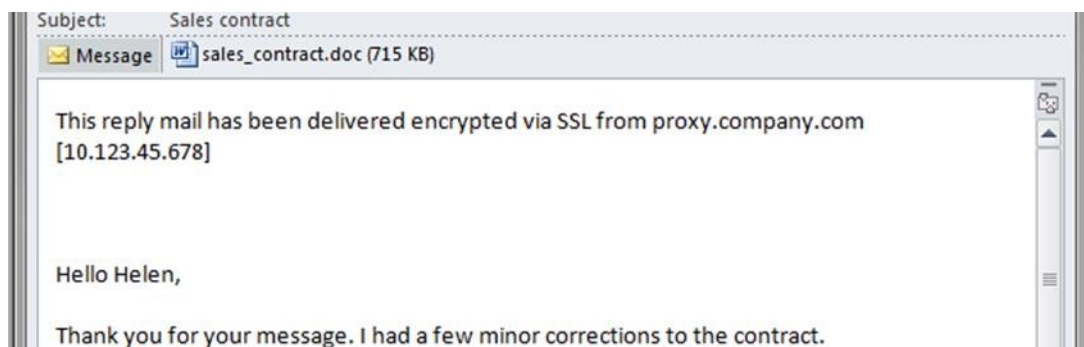


Figure 6. Example of a reply message to D-Envelope message

- **Allow reply to expired message (default: on):** It is possible to reply to an expired message if a receiver wants to start a secure messaging with the original sender of the message. Although an
-

expired message cannot be read, the recipient can reply to the original sender with a new secure message.

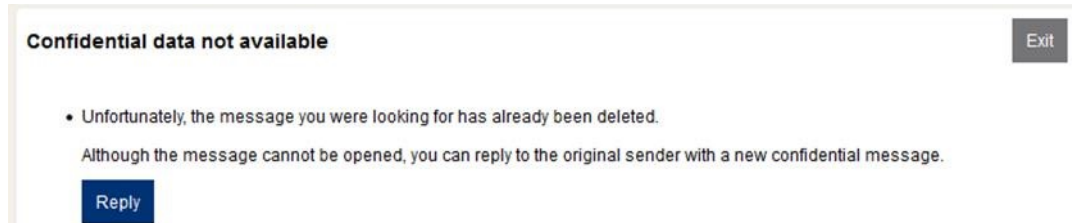


Figure 7. Example of a reply possibility to expired D-Envelope message

Prevent reply to specific address (default: off): Determine a list of e-mail addresses to which it is not possible to reply. The message is missing a reply button altogether if the sender is on this list.

This can be used to prevent reply messages to automatically generated messages whenever sent from a particular address, for example.

- **Allow adding recipients in reply (default: off):** If enabled, users can add additional recipients when replying to messages. The recipients can be restricted to ones with a domain local to the Secure Emailserver, or permitted globally to anyone. Messages destined outside of the organization's internal network are delivered securely as D-Envelope messages.

3.2.5 Re-opening of message

Message can be opened again if the user will logout from the system and store the message to server for a limited time. Reopening requires authentication that can be based on cookies, password, PIN code or strong SSN based authentication.

If the authentication is based on cookies, a cookie is saved to the browser and while opening the message user will be automatically identified with it. Message can only be reopened from the same computer/browser. If the authentication is based only on password or PIN code, the message can also be reopened from different computer/browser. It is also possible that both cookies and password or PIN are required when reopening the message. In this case the message can only be reopened from the same computer/browser with password or PIN.

- **Password logout in "letter" level (default: on):** Authentication in re-opening can be based on password or both password and cookies. User must enter own password in logout.
- **PIN code logout in "letter" level (default: off):** The user can enter their mobile number and receive a SMS message with PIN code next time the message is opened.
- **Strength of password:** It is possible to configure how secure the password must be (e.g. length, special characters, numbers and dictionary check for commonly used passwords).
- **Amount of password tries:** Password needed to re-open a message can be entered limited amount of times (default: 5) before the message is locked and cannot be opened again.
- **Logout confirmation for closing a tab (default: on):** JavaScript confirmation box pops up if user tries to close a page without using log out button.

3.2.6 Forwarding messages securely

The recipient can forward a message using the same secure TLS connection between browser and DEnvelope. The forwarded message is first sent to D-Envelope which creates a new unique secure message and sends a notification message.

- **Forward exact copy only (default: off):** Only an exact copy of the message can be forwarded. In other words, the original secure message cannot be modified when it is forwarded in the user interface.

3.2.7 Secure EmailDesktop Outlook plugin

Secure EmailOutlook plugin for Windows Outlook clients provides a graphical interface for selecting the appropriate security level for confidential information leaving the organization, and facilitates for a more streamlined implementation of data security policies in regards of e-mail channel.

Secure EmailOutlook plugin also provides additional granularity for applying security controls to the e-mail channel, while improving the end user experience and at the same time minimizing end user training requirements via more intuitive user interface.

Plugin installs as a button in the ribbon and can also be configured to prompt automatically upon pressing Send button. The plugin allows users to set recipient-specific security levels for each message.

All settings can be forced to specific values and users can customize any non-forced settings. Administrator can lock settings so that the end user cannot change the value or even decide if the setting is visible in the end user interface. Also names of security levels are customizable to match company's instructions and policies.

- **Secure Emailserver address:** Secure Emailserver address is required if centralized configuration management is in use or there is a need for D-Internal.
- **Extension (default: "s"):** Domain extension used to tag e-mails for encryption service.
- **STIV extension (default: "s4"):** Domain extension used to tag e-mails for "ST IV" level email security. Note that this requires the creation of a separate instance into the Secure Email with a dedicated domain to process these emails.
- **Available security levels in plugin:** Security level can be selected for each recipient separately. Depending on configuration, the security levels are: Letter, Registered letter, Handed over personally and ST IV,
- **Default security levels in plugin:** User can choose the default security level that is automatically suggested when a message is sent. Depending on configuration, the options are: none, no encryption, Letter, Registered letter, Handed over personally, ST IV and strongest available,

Necessary additional identifiers can be retrieved automatically from address book (and added information stored to contacts)

- **Utilization of address book:** It is possible to save the contact's mobile number (default: on) and social security identifiers (default: off) to the Outlook address book. Also possible to create a new contact and save the information when there is no existing contact (default: on).

Plugin also features message-specific settings such as making the messages readable only once and setting how long the message can be read.

- **Show Message options button (default: on):** If this option is selected the message-specific options chosen become available.
- **Read receipt in plugin (default: on):** User can choose to request a read receipt when the message has been opened for the first time without going to Outlook settings.
- **Readable only once in plugin (default: on):** If this option is chosen the message can only be read once and will be automatically deleted from the server after it is read.
- **Time message is readable in plugin (default: on):** User can choose how long an unread or read message is stored on the server. Possible to define a maximum limit the user can set for storing unread or read messages. If user tries to enter a longer time than allowed it is reset to the maximum and the field is highlighted.
- **Disable reply and forward (default: off):** Reply and/or Forward functions can be disabled in specific messages.
- **Use message-specific password in plugin (default: off):** Message-specific password can be set that is needed to open the message sent in "Letter" level.
- **Attachment preview in plugin (default: off):** Attachment preview can be set for specific messages that prevents the receiver from downloading attachment.
- **Prompt plugin popup:** Possible to choose that popup always opens from Send button (default: off) or that popup will not be displayed when all receivers share sending e-mail addresses' domain (default: on). In addition the domains that always prompt the plugin popup can be defined.

- **Increase security level for all in plugin (default: off):** Possible to increase the security level to all receivers of the message simultaneously. This function upgrades the lowest security level by one level until at the same level as the highest. Then all receivers are upgraded by one step at the time. It is also possible to simultaneously downgrade all receivers to have no encryption.
- **Enable digital signature (default: off):** It is possible to integrate the Outlook plugin with secSigned solution for digital signatures. The signing process can be started directly from the user's e-mail client with Secure EmailOutlook plugin.

Plugin supports using internal e-mail traffic protection (D-Internal).

- **Enable D-Internal Support (default: off):** If this option is enabled the user can choose when to use internal e-mail protection (options: never, only with secure levels or always).

3.2.8 Secure EmailOffice 365 webmail plugin (OWA)

Secure Emailplugin for Office 365 webmail (OWA) provides a graphical interface for selecting the appropriate security level for confidential information leaving the organization, and facilitates for a more streamlined implementation of data security policies in regards of e-mail channel.

The OWA plugin installs as a button in the message composing view. The OWA plugin allows users to set recipient-specific security levels for each message. If the plugin has been enabled through D-Center it can be installed organization wide in Outlook Web App administrator control panel, or per user in the users own options. The OWA plugin supports centralized configuration management just like desktop Outlook plugin does, but the configurations are separated from each other.

Following settings are available and configurable via D-Center:

- **Secure Emailserver address:** Secure Emailserver address is required if centralized configuration management is in use or there is a need for D-Internal.
- **Extension (default: "s"):** Domain extension used to tag e-mails for encryption service.
- **STIV extension (default: "s4"):** Domain extension used to tag e-mails for "ST IV" level email security. Note that this requires the creation of a separate instance into the Secure Emailwith a dedicated domain to process these emails.
- **Available security levels in plugin:** Security level can be selected for each recipient separately. Depending on configuration, the security levels are: Letter, Registered letter, Handed over personally and ST IV,
- **Default security levels in plugin:** User can choose the default security level that is automatically suggested when a message is sent. Depending on configuration, the options are: none, Letter, Registered letter, Handed over personally and ST IV.

3.3 D-Compose

With D-Compose an external party can proactively start confidential messaging.

In practice, the service can be linked to the company's Web site or alternatively the message sender must know an address defined for sending (e.g., <https://secure.example.com>). For example, sender can send secure message to a person or whole department (<https://secure.example.com/sales@example.com>) in a company without knowing the actual address. The link in the page offers all the information needed. The service is used over protected TLS connection with browser.

- **Support address (default: on):** Support address for the users to contact can be shown in DCompose either as a link or an image.

The addresses accepted as message senders and recipients can be specified, and user authentication can also be required (strong authentication, self-service registration, SMS-based identification).

- **Allowed addresses:** Addresses or domains allowed in From: and To: –fields can be modified.
- **Sender authentication (default: off):** The use of D-Compose can require sender authentication. Different options are:
- Email registration

- Single Sign-On (OpenID connect based) [Please note: this can be used only as a stand-alone authentication method]
- SMS authentication
- Strong SSN based authentication

In email registration sender receives a unique link to e-mail after registration. In Single Sign-On sender authentication is handled “on the fly”. In SMS authentication the sender receives a PIN code to a predefined mobile phone number. In Strong SSN based authentication sender has to authenticate him/herself in external SSN based authentication service (same methods are available in D-Compose that are available in D-Envelope).

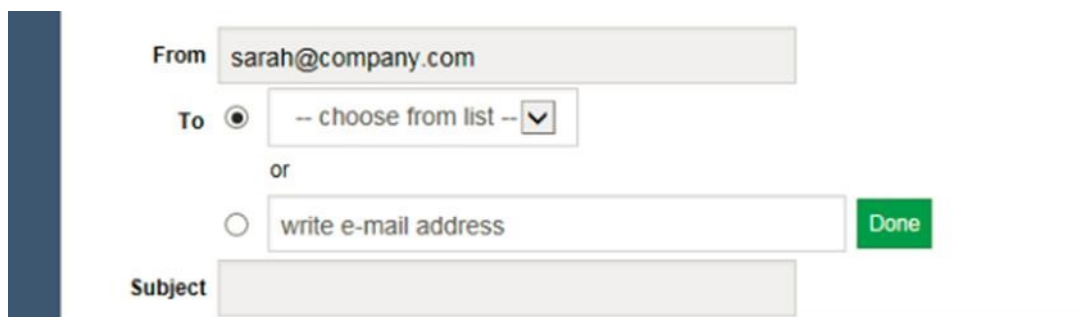
- **Life time for registered link (default: 30 days):** Life time for registered link can be changed. After that the registered link will expire and will be deleted from the server.
- **Amount of registration e-mails:** Maximum amount (default: 5) of registration e-mails sent to same address within a specified time limit (default: 14 hours) can be defined.
- **Registration e-mail:** The registration e-mail address can be modified.

The user interface language is set according to browser's language settings. Supported languages are English, Finnish, Swedish, Norwegian, Danish, Estonian, Latvian, Lithuanian, Russian and German.

- **Force user interface language (default: off):** Language in user interface can be disabled entirely or forced so that only one language is in use. Normally language is set automatically according to browser settings.
- **Sender can choose interface language (default: off):** Secure message senders can choose to change the interface's language from a dropdown box if this option has been enabled.

In addition, it is possible to offer the sender the desired recipient addresses to select from, thereby forwarding requests for feedback or tenders to the correct e-mail address.

- **Recipient drop-down list (default: off):** Allowed recipients in D-Compose can be placed to a dropdown list in To-field. Recipient addresses can be defined to show as aliases in a drop-down list, for example sales@domain can be shown as Sales. These aliases can be defined to be named according to language (for example “Sales” in English, “Myynti” in Finnish and “Försäljning” in Swedish). Options are both normal text field and drop-down list or only drop-down list. If both are in use, the alternatives can have radio buttons in front of them so that only one can be chosen.



The screenshot shows the 'To' field in the D-Compose interface. The 'From' field is filled with 'sarah@company.com'. The 'To' field has a radio button selected next to a dropdown menu containing '-- choose from list --'. Below this, the word 'or' is centered. There is another radio button next to a text input field containing 'write e-mail address'. A green 'Done' button is visible to the right of the text input field. The 'Subject' field is empty and located below the 'To' field.

Figure 8. Example of a recipient drop-down in D-Compose

The message sender can use the service to write a message and add attached files, if necessary. The sent message is transmitted as a normal e-mail message to the recipient's mailbox.

- **Cc and Bcc-fields in D-Compose (default: off):** Message can also be sent as carbon copy or blind carbon copy.

- **Dynamic receiver fields (default: off):** Receiver field address will be checked in real-time (options are invalid address form, correct address that is not allowed to receive messages and correct address that is allowed to receive messages). The sender can immediately see if the receiver address is invalid (for example includes Scandinavian alphabets) or if the domain is not allowed to receive messages. Receiver addresses can be edited in their own fields. If the message can be sent in "Registered letter" level, the receiver's GSM number can be placed in its own field.
- **Address book for registered users (default: off):** Registered users can add addresses faster and more efficiently with an address book. System remembers the addresses previously used and suggests them automatically when sender is writing down receiver address (minimum of 3 letters is required). Sender can also select the receivers from an address book in the user interface. In order to use the address book also the dynamic receiver fields must be allowed.
- **List of receiver addresses in address book (default: none):** It is possible to add a list of receiver addresses to the address book of all registered users of D-Compose in addition to the personal address list for each user. These global addresses are managed from D-Center. Receivers in a dropdown list can also be automatically sorted to alphabetical order. This makes it easier to add new receivers to the list.
- **Signature for registered users (default: off):** Registered users can use signature in messages sent from D-Compose. Secure Email remembers the previously used signature and provides it automatically.
- **Allowed MIME/attachment types in D-Compose:** Types of allowed (whitelist) or forbidden (blacklist) attachments can be defined using MIME types and file extensions.
- **Show SMS originator text (default: on):** This shows to the receiver that the message is SMS authenticated. Text is placed in the beginning of the actual message.
- **Require GSM authentication (default: off):** Sender must use GSM authentication when sending messages with D-Compose. Recipient's GSM number can be placed to its own field or optionally sender adds the number and '.s' at the end of the e-mail address (for example recipient@domain.tld.040123456.s). The GSM number can be required to be in international format (+xxx/00xxx).
- **Sensitivity header in D-Compose (default: off):** All incoming e-mails sent through D-Compose can have a customized "Sensitivity" header (options are personal, private, company-confidential or none).
- **Internal max size in D-Compose (default: off):** If the size of the incoming message is larger than the internal mail server allows, D-Compose sends a notification message instead of the actual message so that it can be read using D-Envelope application.
- **Allowed message size for individual user in D-Compose (default: off):** The maximum message size that an individual address or domain is allowed to send can be defined.
- **Request a read receipt in D-Compose:** Sender can request a read receipt. The read receipt is delivered as plaintext.
- **CAPTCHA check (default: off):** Captcha can be added to prevent spam messages generated by computers. Even though this has not been a problem so far, there is now a way to prevent attacks in the events where a message can be sent without registration. To ensure that the sent message is not generated by a computer, sender must enter the automatically generated challenge (options are numbers, characters, numbers and characters or simple mathematical equation) to be able to write a message. Style of the image shown can be modified to fit the company image (noise style, size of image, font size, length, text color, noise effect color, background color, curve of the image).

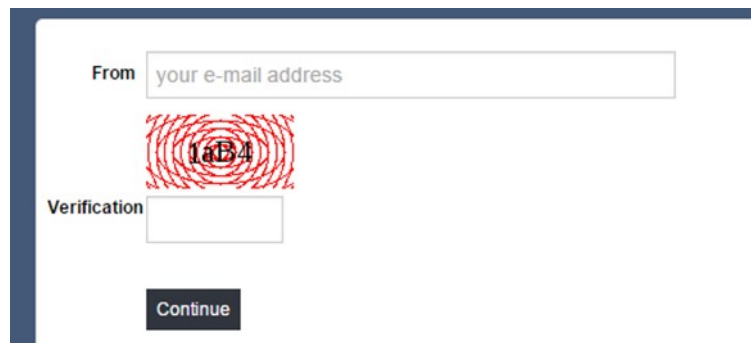


Figure 9. Example of a CAPTCHA check in D-Compose

- **Save sent message in S/MIME encrypted form (default: off):** The sender of a secure message can save the message he/she has sent through D-Compose in S/MIME encrypted form, if the sender can provide an S/MIME certificate. In this way only the owner of this certificate can open the saved message, even if it is saved to a shared folder for example.

An outside sender of a confidential message can be strongly authenticated. If the strong authentication is required for the sender in D-Compose he/she has to attempt authentication by using one of the following SSN based authentication methods (methods are configured and enabled by administrator):

- BankID (Sweden and Norway)
- Finnish Mobile ID
- Finnish Trust Network (banking recognition with Signicat or Telia)
- Generic OpenID Connect based SSN authentication
- NemID
- Suomi.fi

- **BankID authentication in D-Compose (default: off):** Sender must use the BankID authentication when sending messages with D-Compose. The authentication text with identity number (options are encrypted identity number, plaintext personal identity number or plaintext truncated number) will be seen in the beginning of the e-mail message sent to the receiver. Customer must have a contract with Svensk e-identitet (Sweden), ZignSec (Sweden and Norway) or Signicat (Sweden and Norway).
- **Mobile authentication in D-Compose (default: off):** Sender is authenticated with Mobile ID. Customer must have an agreement with Elisa.
- **Finnish trust network authentication in D-Compose (default off):** Sender is authenticated with trust network banking recognition (Signicat or Telia OIDC authentication). Customer must have an agreement with Signicat or Telia.
- **Generic OpenID Connect based SSN authentication in D-Compose (default off):** Secure Emails supports any authentication services which are following OpenID Connect standard and provide user's SSN. Configuration of the Generic OpenID Connect Authentication requires API specification from the authentication service provider.
- **NemID authentication in D-Compose (default: off):** Sender must use the NemID authentication when sending messages with D-Compose. The authentication text with identity number (options are encrypted identity number, plaintext personal identity number or plaintext truncated number) will be seen in the beginning of the e-mail message sent to the receiver. Customer must have an agreement with ZignSec or Signicat.

- **Suomi.fi authentication in D-Compose (default: off):** Sender must use Suomi.fi authentication when sending messages with D-Compose. The authentication text with identity number (options are encrypted identity number, plaintext personal identity number or plaintext truncated number) will be seen in the beginning of the e-mail message sent to the receiver. Customer must have a contract with Finnish Population Register Centre.

These strong authentication methods work alongside with email registration and SMS authentication methods and provide the name and social security number of the sender. The connection between Secure E-mail service provider is established by using standard TLS protocol (https).

3.3.1 Multiweb-compose

Each instance can have multiple D-Compose pages that have different configuration values (for example is the cc-field shown or does using require registration). It is also possible to define allowed sender and receiver addresses to different pages.

3.4 D-Network

D-Network facilitates protected and completely transparent e-mail messaging between organizations that have joined the D-Network service network. Data protection takes place at the "Company-Confidential" level without user action. Also the address information of both parties stay protected.

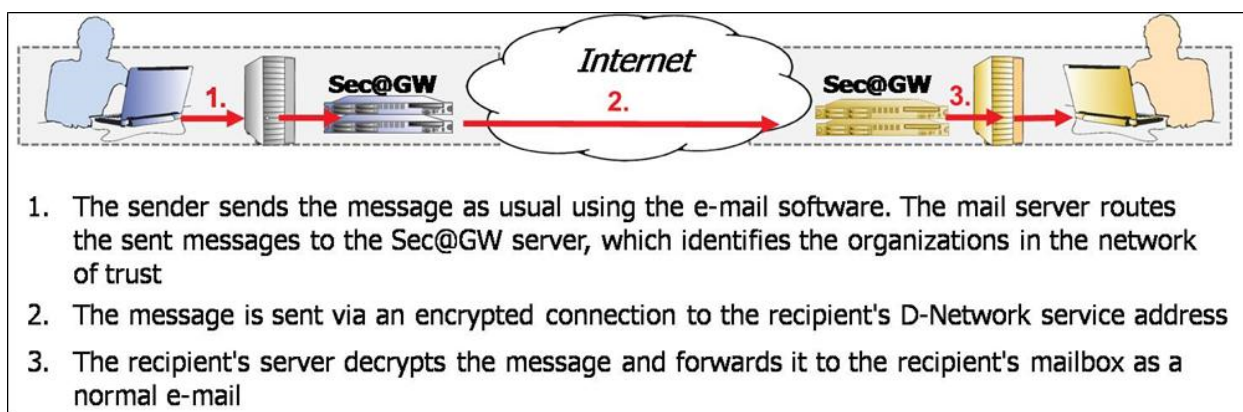


Figure 10. Example of D-Network operation in practice

Data transfer takes place directly between the parties' D-Network applications without proxies using a secure TLS-based transfer method.

The received message can be treated as a normal e-mail in the receiver's e-mail server.

- **Data transfer in D-Network:** When a message is marked to be sent using D-Network, first the receiver's domain is matched against information in the access rights database. If sending is allowed, the message is protected and a secured connection to receiver network is created. Information regarding session and identifier is sent over the protected connection so that receiving server can confirm that sending server has a right to send messages. If the sender has a right to send messages, the receiving server sends its own corresponding data as a reply, after which message is sent over the protected connection. In case the sending of message fails or is interrupted, an attempt to resend the message will be made for predefined amount of times after a pause. If resending fails after configured resend time message is sent using the next authentication level in line from encryption control rules.

- **D-Network Destination Manager:** It is possible to add custom D-Network destination servers. The destination servers must be Secure Email servers with D-Network capabilities. Servers belonging to the official D-Network distribution do not need to add other servers in the official distribution.

The System administrator can request that the organization be registered and added to D-Network from D-Center.

3.5 Other delivery methods

3.5.1 TLS Enforcing

TLS enabling makes e-mail delivery safe and trusted. An enforced TLS connection is set up between specific predefined servers and connection is confirmed with certificates which guarantee that mail is only processed by trusted servers and there are no other servers inside mail delivery route where message could be read.

The message is routed using the next hop principle (from point A to point B) where it is always routed to a pre-defined IP address. Message can never be routed according to MX records because if MX records changes the mail can go to different server than originally and there is no way of knowing what servers are in the middle.

By using enforced TLS encryption it can be defined either per-domain or per receiver to whom the mail is sent to. If the message for some reason cannot be delivered using TLS, message awaits in the server queue to be redelivered. If the message cannot be delivered to the receiver with TLS within predefined time limit, the sender is notified with a bounce message.

- **Firewall settings in TLS Enforcing:** In the sending Secure Email port 465 in firewall must be open to the mail server of the counterparty (incoming traffic) and port 25 in firewall must be open to the mail server of the counterparty (outgoing traffic). On the receiving end server must be able to receive TLS encrypted mail (port 25 or separately agreed). Server sends TLS encrypted mail to Secure Email cluster address port 465.

3.6 Other supported standards to receiving messages

Other supported standards enable the message receiver to read the secure message directly with his/her own e-mail program. If an outside receiver has an S/MIME certificate or an Open PGP keys in use, it is possible to register to receive messages using these standards.

- S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data.
- Open PGP (Pretty Good Privacy) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication.

The registration of an outsider has no effect on the operation of the sender: messaging remains transparent and sender doesn't need to have a corresponding method in use.

3.6.1 To receive messages using S/MIME or Open PGP

A receiver can register to receive messages using S/MIME or Open PGP standards. Organization can add specific receivers to use these protection methods or the receiver of secure message can register to the service. During registration the available encryption certificates or keys will be searched for from the ones installed on receiver browser or the receiver can upload the S/MIME certificate or PGP key. Lifetime of the virtual D-Internal S/MIME certificate can be defined as well as the allowed domains of who can request a virtual certificate.

Certificate/key management can be handled virtually and centralized.

- **Using S/MIME or Open PGP to receive messages:** User sends a secure message and Secure Email identifies the message to be encrypted with S/MIME or PGP based on a rule made for the receiver address. Secure Email creates a virtual address (original sender will be shown at name field), encrypts the email with S/MIME or PGP encryption and sends it from the virtual address to the receiver. Reply messages sent to the virtual address will be routed to Secure Email where they are decrypted and delivered to the user's inbox. Reply mail traffic must be routed to Sec@GW. This can be obtained by routing all incoming mail traffic through Secure Email or by using a specified domain.

In order to use this, the receiver certificate or public key must be known. Certificate or key can be obtained from a public directory, administrator can add the receiver address and certificate or key to a list of external S/MIME or PGP addresses or the receiver can register to receive all future messages sent in "letter" level as S/MIME or PGP encrypted messages. All certificate and key management is done by Sec@GW, so the user does not need an S/MIME certificate or PGP keys.

- **External S/MIME registration (default: off):** The receiver can register to receive all future secure messages as S/MIME encrypted message while reading a message sent in "letter" level.
- **External PGP registration (default: off):** The receiver can register to receive all future secure messages as PGP encrypted messages while reading a message sent in "letter" level.
- **Storing of virtual D-Internal S/MIME certificate key (default: on):** It can be defined that the virtual D-Internal S/MIME certificate key is not stored to database after it is created. In this case the certificate cannot be restored if lost.

3.7 Tools for protecting internal e-mail traffic

Company's internal e-mail traffic protection utilizes S/MIME or Open PGP encryption. The message is sent to the receiver with D-Envelope and therefore there is no need for complicated key/password exchange even though the messaging remains confidential throughout the whole message chain.

Secure Email can generate its own virtual certificates or keys (intended to be used between user and Sec@GW) or the organisations own certificates or keys can be used. The administrator can send users' certificates or keys to internal users or users can order them from Sec@GW. User can order the receiver's certificate or public key from Secure Email and then save the receiver address with certificate or key as contact to the e-mail client's address book or simply reply to the message sent by the system and select the message to be encrypted and signed.

- **Using internal S/MIME or PGP encryption:** Message will be sent S/MIME or PGP encrypted to the Secure Email server, which sends the messages to the receiver either in plain text or as encrypted message according to the rules configured to the server. Reply messages will be routed to Secure Email where they are S/MIME or PGP encrypted and delivered to the user's inbox.
- **Internal S/MIME registration (default: off):** The internal user can protect the internal e-mail traffic with S/MIME encryption.
- **Internal PGP registration (default: off):** The internal user can protect the internal e-mail traffic with PGP encryption.

3.8 Rest API for sending secure email

In some cases there may be a need to send secure email from automated systems or applications where opening up firewalls to allow email traffic may not be desirable or even possible. For such cases Secure Email exposes a HTTP Rest API secured with email/password pairs as well as IP restrictions that allows these systems to send emails secured by all the same security levels as using the normal email gateway. In addition to sending, the API includes functionality to list sent messages and to query their read status.

4. Administration and maintenance

4.1 D-Center

D-Center manages the operation of the Secure Emailsoftware applications. D-Center is a Web-based management tool for system administrators, used for editing all the key settings of Secure Emailand reviewing of collected statistics.

D-Center is divided into two main categories: system pages and instance pages.

System page includes:

- Logs
- Statistics
- Server Configuration
- Spam Filter
- Tools
- User Management
- System Update





Figure 11. Screenshot of D-Center's index page

Instance page includes:

- Logs
- Statistics
- Settings
- Tools

System can have multiple administrators with different permissions.

- **Admin user permissions:** There are three different access levels for each page in D-Center: no access, view only (page can be read but not edited) and full (right to edit page). Administration user permissions can be created and edited individually for each page. Menu bar changes according to the rights each administrator has been given (for example helpdesk employee only has access to logs). All the changes that are made to D-Center are logged into Audit trail. This makes it possible to see who has made changes and when.
- **Security settings for admin login:** Security requirements for administrator password, such as length, capital or small letters, special characters, numbers can be defined. Passwords can be set to expire. Expired passwords must be renewed after the first successful login after the password has expired. Admin user accounts can also be locked after too many failed password attempts.
- **E-mail statistics (default: off):** Statistics on the usage of confidential messaging can be sent as email to a predefined address monthly or weekly and statistics of junk mail filter monthly.
- **Third party program configuration:** Third party programs, such as rsyslog, postmantis, amavis and rsync, can be configured.

 SSH.COM	5. Requirements in operational environment
 SSH.COM	4. Administration and maintenance

4.2 Console management

When required, an expert from SSH Communications Security Corporation or a trusted partner can perform maintenance tasks (for example software updates) through a secure remote connection.

4.3 Certificate manager

All certificates affecting the function of Secure Email can be managed centralized from D-Center. Certificate requests (CSR) generated by Certificate Manager are sent to SSH Communications Security Corporation manually or from D-Center when making a request. After the requested certificate has been signed, it can be installed to the system from Certificate Manager.

4.4 Administration API

Secure Email includes a HTTP Rest API through which several aspects of the software can be managed, including:

- The creation and destruction of instances
- adding/removing instance mail domains
- activation/deactivation of instance software modules
- adding/removing instance UI templates
- restarting server services
- adding firewall rules

5. Requirements in operational environment

5.1 Hardware and operating system requirements

Currently supported operating systems are:

- RedHat Enterprise Linux, versions 7 or 8
- CentOS, versions 7 or 8

The mail delivery software is postfix and the web server is Apache.

Required hardware varies greatly depending on enabled software, usage and use cases. For the most basic variants the recommended virtual hardware is 4 CPU cores (2GHz), 8 GB RAM, 146 GB HDD and two network adapters (if clustered).

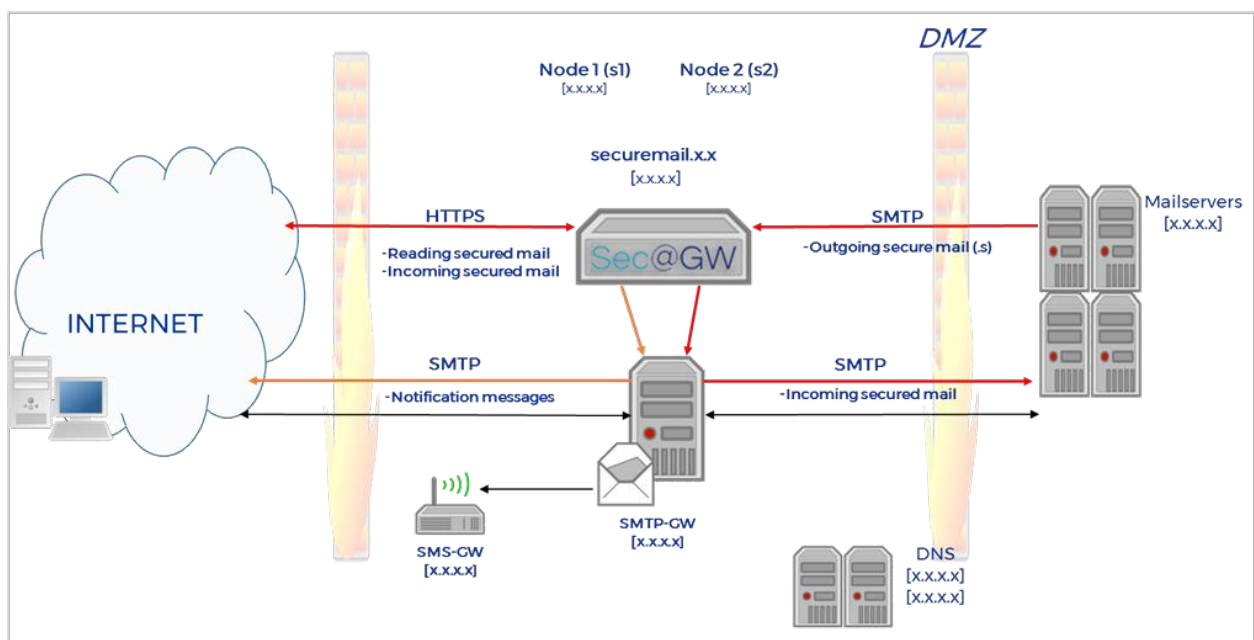
5.2 Installation

5.2.1 Secure Email installation profile options

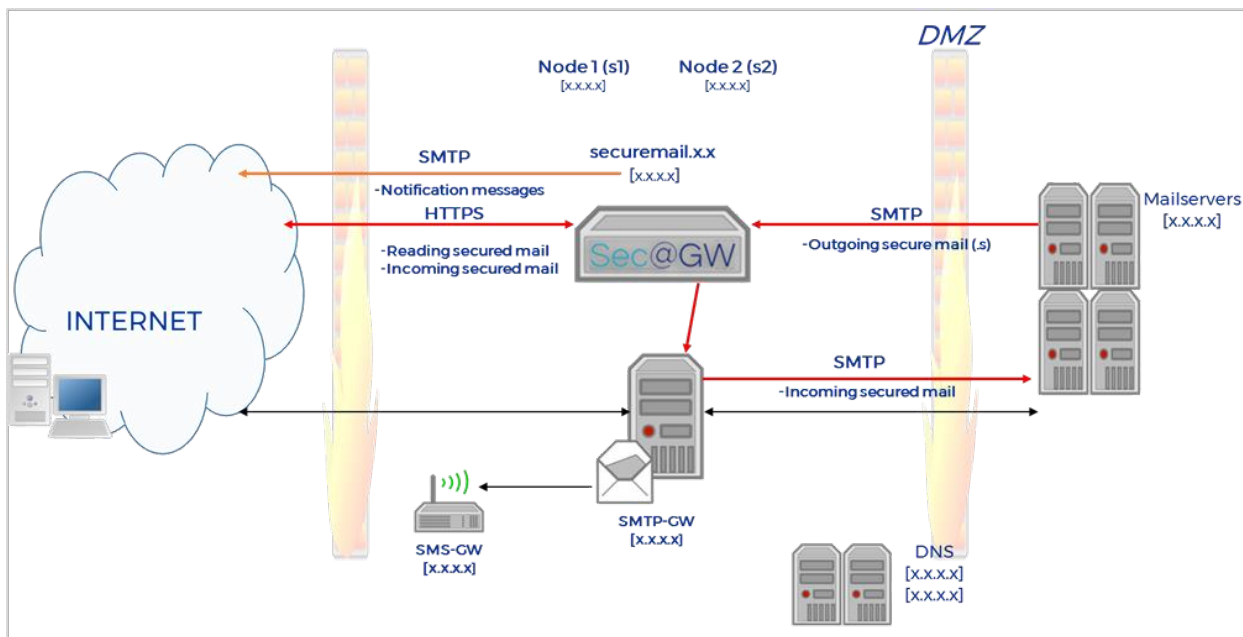
All outgoing e-mails can be sent through Secure Emailserver (smart host) or only e-mails marked with '.s' can be routed.

There are three ways that Secure Emailserver can be located in a network:

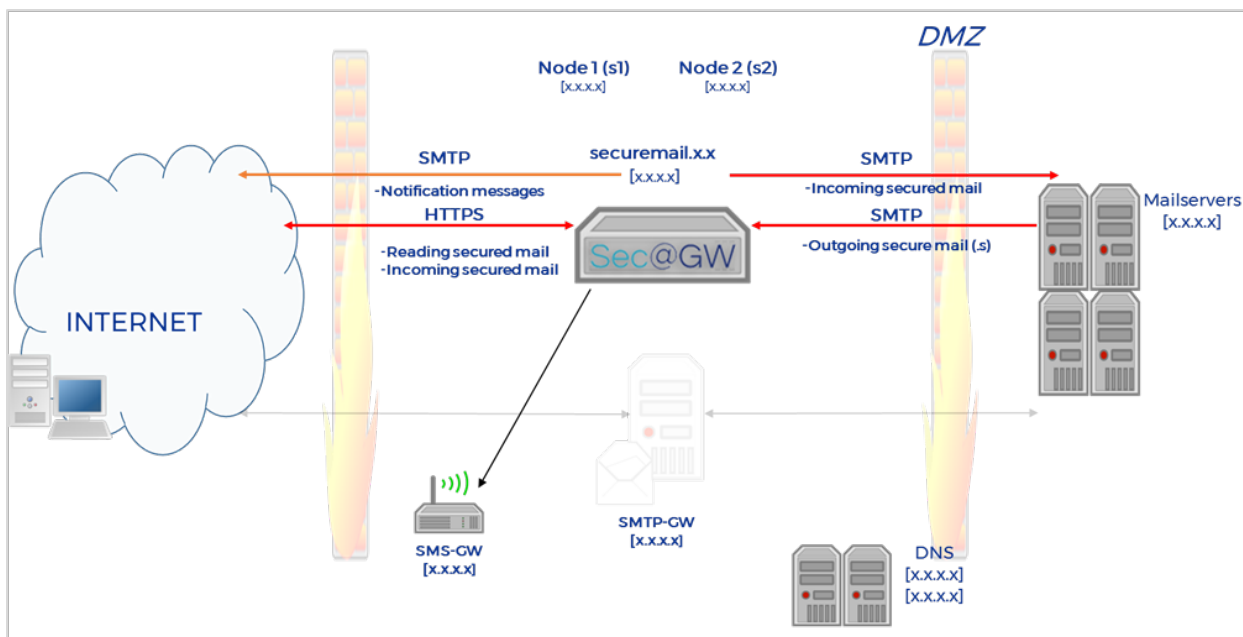
- Secure Email can use standard SMTP-gateway (relay host) to transport all messages (outgoing notification messages and incoming reply and D-Compose messages) (See Example 1)
- Secure Email can use standard SMTP-gateway to transport incoming messages (reply and D-compose messages). Notification messages are sent directly to Internet from Sec@GW. (See Example 2)
- Secure Email can act as a SMTP-gateway and send notification messages directly to Internet and incoming messages (reply and D-Compose messages) directly back to mail server. For example when there is no SMTP-gateway at use. (See Example 3)



Example 1. Network layout (using SMTP-gateway)



Example 2. Network layout (using SMTP-gateway incoming only)



Example 3. Network layout (without SMTP-gateway)

- **SMS-Gateway:** Secure Email can use modem or existing SMS-gateway. A PIN code is sent to receiver's SMS-gateway by using SMTP or HTTPS protocol.

5.2.2 Configuration

Accepted networks or IP addresses of mail servers that are allowed to send outgoing mail and outgoing mail routing (default route for outgoing mail; IP address) must be defined for configuration. Also default route for incoming mail; IP address (all incoming mail is routed to the following IP address, unless a

different route is specified) and incoming mail domains (domains that are allowed to receive mail from Internet).

5.2.3 Network connections and IP addresses

Servers are placed in to the network so that a secure or reliable connection to mail servers (typically to DMZ) can be made. Secure Emailserver requires one to three public IP addresses. One IP address (eth0:0 adapter) will be used as a cluster address through which e-mail traffic is relayed. This IP address is used by the active machine. If NAT is used in address translation, information of both public and network address translated addresses is needed.

Options:

- It is recommended that web-based management tool is separated from public network by defining DCenter with its own IP address and own port (default 443).
- For customized customer environments (eth0:x –adapters), additional IP addresses are needed. For these IP addresses port 443 should be opened from Internet. Customized customer's all traffic (SMTP, HTTPS) is routed through the virtual IP address (eth0:x).

For example:

- Customer X: eth0:1
- Customer Y: eth0:2

5.2.4 Cluster net (duplicated system)

Servers are in constant contact with each other concerning data and setting replication as well as automated monitoring. In order for the two servers to monitor each other, a dedicated connection is required (minimum of 100mbit full-duplex). Connection can be made with direct cable connection or connection through clutches. Usually, network uses addresses 10.0.0.20 (node 1) and 10.0.0.50 (node 2).

5.2.5 SMS interface

In Secure Emailsolution's "registered letter" level the receiver can be authenticated. SMS authentication works in a following way. Secure Email identifies the receiver's GSM number from the message, creates an SMS message and sends it to the customer's chosen SMS gateway in the net using e-mail or http(s) interface. Next, customer's SMS gateway sends the message forward to the receiver's mobile phone when the link in the notification message is opened.

5.2.6 Firewall settings

Firewall must allow the required connections. The following table shows requirements for basic installation; rules must be specified.

Table 1. Firewall settings

Connections to Secure Emailsystem (firewall settings)				
Port	Type	Source	Destination	Protocol / usage
443	TCP	*	Sec/c	HTTPS
25	TCP	Mailserver	Sec/c	SMTP, .s messages

25	TCP	Sec/c	Mailserver	SMTP, reply messages
25	TCP	Sec/c	*	SMTP, notification emails
53	TCP/UDP	n1, n2	Nameservers	DNS
123	NTP	n1, n2	NTP servers	NTP
22	TCP	193.184.14.150	n1, n2	SSH, Reporting & updates, Deltagon's maintenance
443	TCP	Sec/c	*	Deltagon updateserver, D-Network
443	TCP	n1, n2	193.184.14.150	Deltagon monitoring
443	TCP	n1, n2	193.184.14.151	Deltagon updateserver
80	TCP	n1, n2	Centos updateservers	CentOS updates
443	TCP	n1, n2	Redhat updateservers	Redhat updates

n1 = server 1

n2 = server 2 c

= cluster

5.3 Monitoring and Updates

The Secure Emailsoftware has a build-in monitoring agent. This can be used as a part of the support services. The agent will collect information on software's performance and critical processes and reports it to SSH Communications Security Corporation. SSH Communications Security Corporation maintains the monitoring environment which receives and analyses the information sent in by the software agent. The connection between the software agent and the monitoring environment is a secure https connection (port 443).

SSH Communications Security Corporation will also use the chosen connection for the software updates. In addition to the software level monitoring, the operational system level can be monitored with SNMP if wanted.

6. Terminology

Table 2. Terminology

Term	Definition
Sender	User who has permission to send secured emails to recipients via Secure Email
SSN	Social Security Number aka. Personal Identity Code/Number
Recipient	User who receives secured email from Sender has permission to https interface.
D-Center	Administrator Web GUI. Provides system and instance specific configuration possibilities.
D-Envelope	A Senderuser within the organization can use D-Envelope to send secured email to an external user. D-Envelope offers HTTPS Interface where Erecipient (external user) can read messages.
D-Compose	HTTPS Interface where personSender outside of the organization can start the secure email conversation.
Secure Email	Name for the gateway based email encryption security-solution.
Secure extension	Mark for the Secure Emailto process the message confidentially. Typically the extension is appended into the recipient's email address.
Security level	The encryption level that is used to send a confidential message to the recipient. Defines the overall level of security and required authentication methods for opening the secure message.The encryption level that is used to send confidential message to recipient.
ST -IV	Refers to Finnish national protection level which is comparable to the EU level: RESTREINT UE/EU RESTRICTED