Myndigheten för samhällsskydd och beredskap

Datum	Diarienr	Utgåva
2018-11-26		1.1

Avd. för cybersäkerhet och skydd av samhällsviktig verksamhet
Ronny Harpe
010-2404426
ronny.harpe@msb.se

Secure Messages Protection Profile

Table of content

1. Introduction

1.1 PP Reference

Title: Secure Messages Protection Profile

Version: 1.1

Status: Released

Date: 2018-11-26

PP Author: Yi Cheng, atsec information security AB

Keywords: identification, authentication, IDP, HTTPS, TLS

1.2 TOE Type

The Target of Evaluation (TOE) is a secure messaging service that allows users within an organization to send/receive sensitive messages to/from authorized external users. The external users can be private persons or persons within other organizations.

1.3 TOE Overview

The TOE described in this PP is software only and consists of a secure messaging server.

A user within an organization uses the TOE to send a sensitive message to an external user. The TOE stores this message in a local database and sends to the recipient a notification of incoming message via e.g. SMS. The recipient can then, after successful identification and authentication, read and reply to the message securely by using a web browser.

The TOE provides the following security functionalities:

- HTTPS connection for secure communications
- Time-limited storage of messages
- Identification and authentication of users
- Access control
- Logging
- Administration
    - Configuration of system settings
    - Configuration of trusted Identity Providers (IDPs)
    - User and account management
    - Other management functions

1.4 TOE Description

1.4.1 Introduction and intended use

This Protection Profile provides a high-level set of security requirements for secure messaging services, providing minimal functionalities that are necessary for such a product.

The key feature of the TOE is to provide organizations with secure means to exchange messages with authorized external users. To deploy the secure messaging service, an organization needs to install the TOE on a physically protected server that is under the organization's control. A user within the organization can use the TOE to compose a message for an external recipient. The TOE stores the message in a local database and sends a notification to the recipient which contains an HTTPS (HTTP over TLS) link to the organization's secure messaging service. This notification does not contain any secret information and can be sent via SMS, email or similar means of communication. By opening the link in a web browser, the recipient can log in to the secure messaging service, read the message and reply to the sender.

The external user logs in to the secure messaging service through an identity service provided by an external IDP who is trusted by the organization. If the user is a private person, she may use a digital ID associated to her Swedish personal number (e.g. e-legitimation) that is recognized by the external identity service (e.g. BankID). If the user is a person within another organization, she may either use a digital ID issued by that specific organization or utilize one of the national initiatives of digital ID for professionals (e.g. SITHS, myndighets CA, or E-identitet för offentlig sektor).

Internal users also log in to the TOE through a trusted identity service. This identity service is provided by an internal IDP. The internal IDP has information about the users within the organization, including identity, email address, role (administrator or not), group membership, etc.

An internal user also receives a notification when there is a new message for her in the TOE.

Please note that this PP does not mandate any specific types of user identities and associated credentials for user login. These are dependent on the internal/external identity services used by the organization.

Internal user sending a message

A user within the organization visits the web portal of the secure messaging service for internal users. After successful login, the internal user composes a message and sends it to an external recipient.

Attempt to send a message to an unknown email address leads to a warning message displayed to the sender. The sender is then required to enter an identifier specific to the external identity service (e.g. personal number) for the recipient.

After sending a message the user can see whether the recipient has opened the message. The sender can also revoke the message.

External user receiving a message

Instead of the actual message, the external recipient receives a notification message containing an HTTPS link. This user opens the link in a web browser, which establishes a secure connection between the browser and the organization's secure messaging server.

A login page is then presented to the external user. She is required to authenticate herself via an external identity service. If the organization allows more than one external identity service, the user is asked to choose one.

After successful login, the user sees all message boxes (inbox, sent, etc.) in her account. She can open the new message, read it and reply to the sender. Depending on the permission level set by the organization, the external user may be able to delete, forward or download the message. She may also take initiative and send a message to a user within the organization if that is allowed by the permission level.

1.4.2 The TOE architecture and functions

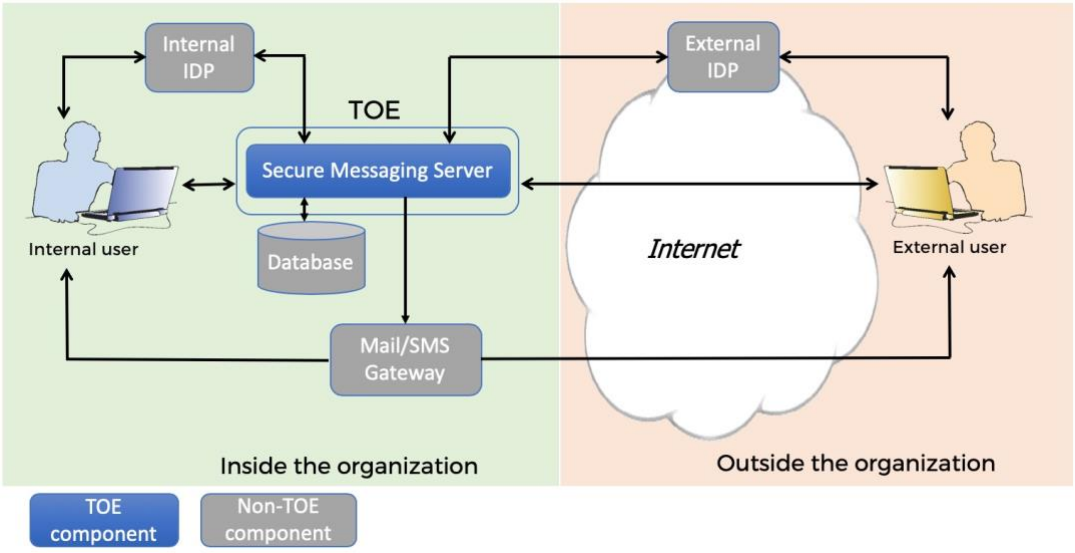


Figure 1 The Secure Messaging Service Overview

As shown in the figure above the TOE is the secure messaging server. Messages are stored in a local database. Please note that the database system (e.g. MySQL) is outside the TOE.

The TOE maintains accounts for users to send, receive and handle messages. There are two types of accounts: user accounts and function accounts.

A user account is owned by an individual user (administrator, internal user, or external user). When a user account is created, the TOE assigns a user id to the owner of the account. This user id is used by the TOE to uniquely identify a user within the system, so it is an internal user id. In addition to this internal user id, each user has one or more identifiers that are used for login via IDP(s). These user identifiers are also unique, i.e., one identifier maps to at most one user account.

Unlike user account, a function account is a group account devoted for a specific function. The email address associated to a function account usually indicates the function, e.g. “Socialtjänsten@kommunnamn.se”. A function account is not owned by any user, but a group of internal users has access to the messages in the account. The organization specifies which internal users are members of the group. Please note that an internal user can only log in to her user account. After successful login she may access the messages in a function account if she is a member of that group. The TOE checks user’s function account membership using security attributes obtained from the internal IDP. Please also note that the secure messaging service may support function accounts for external users, i.e. allow external users to access external function accounts based on group membership information provided by their respective organizations, but this PP does not mandate such functionality.

When an internal user sends a message to an external user who has not used the organization’s secure messaging service before, i.e. no account for the recipient email address exists, this internal user acts as an inviter inviting the external user to the secure messaging service. In this case the TOE requests the internal user to provide a user identifier (e.g. personal number) for the external user. This creates a binding between the recipient email address and the provided user identifier in the TOE. Later when the external user attempts to open the message via the HTTPS link in the received notification, she is required to sign up by authenticating herself via a trusted IDP. The TOE checks whether the identity asserted by the external IDP matches the user identifier that is bound to the user’s email address. If not the TOE rejects the sign-up attempt. Otherwise the TOE creates an account for this external user and binds the user identifier to the account. The user is automatically logged in and can view the message.

In case the organization allows an external user to sign up to the secure messaging service without invitation, she identifies herself to the TOE via an external IDP and registers her email address. The TOE sends a message with an HTTPS link to this email address. The user opens the link in the web browser, which proves to the TOE that she is the owner of the email address. The TOE then creates an account for this user and binds the email address and the user identifier provided by the external IDP to this account.

The HTTPS link is sent via SMS, email or similar means. There is a risk that the link becomes corrupt or modified during the transmission. If the modified link contains incorrect parameters (e.g. the one that identifies the received message) the link will fail. The link may also be modified to point to a site controlled by the attacker. To detect such attacks the user should verify that the server certificate is owned by the intended secure messaging server.

For an internal user, after she has successfully authenticated herself to the internal IDP, the TOE creates a user account and binds to it the user identifier and email address received from the IDP if no account for this user already exists.

The internal/external IDP(s) and the mail gateway (e.g. SMTP gateway) or SMS gateway are part of the TOE environment.

The web browsers used by users are also part of the TOE environment.

In the following paragraphs the TOE's security functionalities are described in more details.

1.4.3 The TOE security functionality (TSF) summary

HTTPS connection for secure communications

When a user connects to the secure messaging server using a web browser, an HTTPS (HTTP over TLS) connection is established between the user's browser and the TOE. The user's browser acts as the TLS client and the TOE as the TLS server. This requires that the TOE has a valid public key certificate for the TLS server and the issuer (root CA) is trusted by the browser.

All communications between the user and the TOE are protected by the established TLS connection.

Time-limited storage of messages

The TOE stores messages for a limited time in a local database. A message is permanently deleted after a pre-defined storage period (e.g. 30 days). This storage period can be configured by the administrator.

Identification and authentication (I&A) of users

Users of the TOE are divided into three categories: administrators, internal users and external users. Both administrators and internal users are employees of the organization which deploys the secure messaging service (the TOE). External users are either private persons or employees of other organizations who use the secure messaging service deployed by the organization.

The organization may use the same or different mechanisms to identify and authenticate internal and external users. There are three general factors for user authentication: something a user knows (e.g. password, PIN code), something a user has (e.g. smart card), and something a user is (e.g. fingerprint). ISO/IEC 29115, which is based on NIST SP 800-63, has defined four levels of assurance (LoA) for entity authentication and provided criteria and guidelines for achieving each of the four LoAs. The LoAs specify technical requirements in several areas, among which the authentication strength:

- LoA1 provides no identity proofing
- LoA2 provides single factor remote network authentication
- LoA3 provides multi-factor remote network authentication, and at least two authentication factors are required
- LoA4 is similar to LoA3 but only hard cryptographic tokens are allowed

The organization should, based on the sensitivity of the messages that will be exchanged between internal and external users, determine the appropriate authentication strength/LoA (level 2-4) and employ only I&A mechanisms that meet the strength/LoA requirement.

I&A of external users

An external user accesses the secure messaging service using the HTTPS link received in the notification message. A GUID (Globally Unique Identifier) is embedded in the HTTPS link to identify the user's email address. After successful HTTPS connection establishment, the TOE presents a login page to the external user. The user chooses the external IDP for which she has valid identity credential. The user authenticates herself to the external IDP which then provides the identity of the user and other user attributes to the TOE in the form of SAML (Security Assertion Markup Language) assertion, ID token, or similar.

The TOE extracts the user identifier from the identity information provided by the external IDP and compares it with the user identifier(s) that is bound to the user's email address. If there is a match, the external user is successfully authenticated to the TOE. Otherwise the login fails and the TOE displays an error message.

I&A of internal users and administrators

An internal user or administrator accesses the secure messaging service by visiting the web portal for internal users. The user authenticates herself to an internal IDP which provides the user identity, role, group membership and other security attributes to the TOE. The TOE extracts the user identifier from the identity information and uses it to locate the user account.

Administrators can also manage the TOE, e.g. editing configuration files, locally from the platform on which the TOE is running or remotely via a secure connection such as Secure Shell (SSH). In these cases it is the operational environment that authenticates the administrators and provides secure connection for remote management.

Access control

This PP defines three user roles: Administrator, Internal User, and External User. These correspond to the three user categories: administrators, internal users and external users, respectively.

TOE users in the Internal User role can send/receive messages to/from both internal users and external users. They can reply, forward, revoke, download and delete messages just like in a normal email application. Besides, if an internal user has membership in a function account, she can access all messages in that account and perform message operations as she does in her own account.

TOE users in the Administrator role can configure system settings for the secure messaging service, search and remove users, and perform other management operations. They cannot perform operations on individual messages as users in the Internal User role do.

TOE users in the External User role have limited rights. The administrator in the organization sets a permission level which determines the message operations external users are allowed to perform.

This PP defines two permission levels for external users:

Level 1. External users can only read and reply to received messages. They are not allowed to perform other message operations.

Level 2. External users can read, reply, download and delete messages. They can also send and forward messages, but only to internal users. They are not allowed to revoke messages.

Please note that an external user can never use the TOE to send or forward messages to another external user. She may download a message (if allowed) and use a non-TOE means (e.g. email) to send the message to another person. This kind of operation is out of the scope of this PP and the user herself is responsible for any consequences of sharing the information with others.

A product claiming conformance to this PP may support other permission levels as well. The ST author should specify the additional permission levels in the ST if that is the case.

Logging

The TOE generates a log of message operations (send, reply, delete, forward, etc.) performed by TOE users in the Internal User and External User roles. It records the time when the operation was performed, by whom, and on which message. But the message subjects and contents are not logged.

Management operations performed by administrators are also logged (configuration of system settings, account management, import of TLS keys, etc.).

Administration

Administrator of the TOE can configure the following in the TOE configuration files:

- The permission level for external users. It is a system wide setting and therefore applies to all external users.
- The private key and certificate for the TLS server. The TLS server key pair and corresponding public key certificate are generated outside the TOE. The administrator imports the private key and certificate into the TOE (using a PKCS#12 file for example) before the configuration.
- A list of IDPs that are trusted for authenticating users and providing user information to the TOE. This configuration can be done manually (e.g. manual import of the certificate of a trusted IDP into the TOE) or through some automatic discovery service.

The organization decides which IDPs are trusted. For instance, the organization may trust IDPs established by the government, police, banks, or by collaborating organizations. The list of trusted IDPs shall be specified in the organization's security policy.

The administrators of the TOE platform have access to the TOE configuration files. It is assumed that the administrators of the TOE platform are also administrators of the TOE. The administrators can manage the configuration files locally or remotely

through a secure connection (e.g. SSH). The secure connection is provided by the operational environment.

Administrators can perform the following management functions via the web interface after logging into the TOE:

- Set the time period for message storage.
- Search and remove users from the system. When a user is removed the user's account and all messages within it are permanently deleted.
- Create and delete function accounts.

1.4.4 Available non-TOE hardware/software/firmware

The TOE is the secure messaging server. The following items are outside the TOE physical boundaries and therefore considered part of the TOE operational environment:

- The operating system on which the TOE is installed.
- The hardware platform on which the TOE is running.
- The database system used by the TOE which is running on the same platform as the TOE.
- The internal/external IDP(s) that identify and authenticate users and provide users' security attributes to the TOE.
- The mail/SMS gateway or other facility through which notifications are sent.
- A reliable time source (which may be provided by the operating system).
- Web browsers used by users to access the TOE.
- A high-quality entropy source (which may be provided by the operating system).

2. Conformance Claims

2.1 CC Conformance Claim

This PP is CC Part 2 extended and CC Part 3 conformant. This PP claims conformance to CC version 3.1 Revision 5.

This PP does not claim conformance to any Protection Profile. This PP claims conformance to the EAL3 package of security assurance requirements, augmented with ALC_FLR.2.

2.2 Conformance Statement

This PP requires demonstrable conformance by any ST or PP claiming conformance to this PP.

3. Security Problem Definition

The security problem definition describes the security problem that is to be addressed by the TOE and its operational environment.

3.1 Threat Environment

This section describes the threat model for the TOE in term of threat agents, assets to be protected, and the actual threats addressed by the TOE.

3.1.1 Assets

The assets to be protected by the TOE are:

- Messages that are exchanged between users.
- Management data (user account information, system configuration files, TLS server keys).

3.1.2 Threat agents

Threat agents are:

- Attackers who have access to the communication paths over which the authorized users perform operations (e.g. reading, composing) on their messages and administrators perform management functions.
- Attackers or non-administrative users who attempt to access messages they are not authorized to via the TOE. This includes the cases where one user attempts to access messages in another user's account or to access messages in a function account for which she does not have membership.
- Attackers or non-administrative users who attempt to gain administrator access to the TOE.
- Non-administrative users who attempt to perform message operations that are not allowed (e.g. forwarding to a third party).

The motivation of a threat agent is assumed to be commensurate with the assurance level claimed by this PP. Therefore, threat agents are assumed to have basic attack potential.

3.1.3 Threats

The TOE addresses the following threats.

T.EAVESDROP

An attacker tries to eavesdrop on messages or management data when they are transmitted between the TOE and user's web browser.

T.TAMPER

An attacker tries to tamper with messages or management data (i.e. replacing or modifying the content) when they are transmitted between the TOE and user's browser, without being detected.

T.MASQUERADE

An attacker pretends to be an authorized user or a non-administrative user pretends to be another user at login time. An attacker or a non-administrative user may also pretend to be an administrator. This includes the case where the user/attacker tries to fake or modify the user identity provided by an IDP.

T.UNAUTHORIZED

A logged in non-administrative user tries to access messages they are not authorized to or perform message operations that are not allowed. A non-administrative user may also attempt to perform management functions. This includes the case where the user tries to fake or modify the user attributes provided by an IDP.

3.2 Organizational Security Policies

The TOE and/or its operational environment shall comply with the following organizational security policies (OSPs) as security rules, procedures, practices or guidelines imposed by an organization upon its operation.

P.MANAGEMENT

The TOE and the operational environment shall provide administrators with secure means to manage the TSFs.

P.TRUSTED_IDP

The TOE shall ensure that only trusted IDPs are used for user identification and authentication.

P.ERASURE

Messages shall be permanently deleted after a pre-configured time period. Messages in an account (user account or function account) shall also be permanently deleted upon request from an authorized user and when the account is removed.

P.LOGGING

Message operations performed by users and management operations performed by administrators shall be logged. Message subjects and contents shall not be logged.

3.3 Assumptions

This section specifies the assumptions that must be satisfied by the TOE operational environment.

A.PLATFORM

It is assumed that the underlying operating system and the hardware platform on which the TOE is installed work correctly and have no undocumented security critical side effects on the security functions of the TOE. It is also assumed that the operating system and device firmware are updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.PHYSICAL

It is assumed that the TOE is located in a physically secure environment under the organization's control, i.e. no unauthorized persons have physical access to the TOE and its underlying system.

A.BROWSER

It is assumed that the web browsers used by users to access the secure messaging service are trustworthy and function correctly. It is further assumed that the issuer of the TOE's TLS server certificate (root CA) is in the browser trust store.

A.USER

It is assumed that the users verify that the server certificate presented by the browser, which is used to establish the HTTPS connection, is owned by the intended secure messaging server before login.

A.IDP

It is assumed that one or more trusted IDPs are available and they meet the authentication strength/LoA requirement set by the organization. It is further assumed that these IDPs provide user identity and other user attributes to the TOE.

A.ADMIN

It is assumed that the administrators are competent, trustworthy and follow the organization's security policies. It is further assumed that the administrators of the TOE platform are also administrators of the TOE.

A.TIME

It is assumed that the TOE is provided with a reliable time source.

A.DATABASE

It is assumed that the database system is trusted and works correctly. It is further assumed that data transfer between the TOE and the database is secure.

4. Security Objectives

The security objectives provide a concise statement of the intended response to the security problem.

4.1 Security Objectives for the TOE

O.CHANNEL

The TOE shall enforce a secure communication channel to user's browser which protects information transmitted to and received from the browser against unauthorized disclosure and provides means for the TOE to detect any modification of incoming information from the browser. The secure channel also provides means for the browser to verify the integrity of information transmitted from the TOE to the browser.

O.AUTHENTICATE

The TOE shall ensure that users are uniquely identified and authenticated before allowing them to access the secure messaging service.

O.MANAGE

The TOE shall provide administrators with secure means to manage the TSFs.

O.TRUSTED_IDP

The TOE shall ensure that only trusted IDPs are used for user identification and authentication.

O.AUTHORIZE

The TOE shall ensure that users can only access messages and perform operations on them as they are authorized to. The TOE shall also ensure that only administrators can perform management functions.

O.ERASURE

The TOE shall permanently delete messages after a pre-configured time period. The TOE shall also permanently delete messages upon request from an authorized user and permanently delete all messages in an account (user account or function account) when the account is removed.

O.LOGGING

The TOE shall log message operations performed by users and management operations performed by administrators. The TOE shall not log message subjects or contents.

4.2 Security Objectives for the TOE Operational Environment

OE.PLATFORM

The operational environment must ensure that the underlying operating system and the hardware platform on which the TOE is installed work correctly and that they have no undocumented security critical side effects on the security functions of the TOE. The operational environment must also ensure that the operating system and device firmware are updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

OE.PHYSICAL

The operational environment must ensure that the TOE is located in a physically secure environment under the organization's control, i.e. no unauthorized persons have physical access to the TOE and its underlying system.

OE.AUTHENTICATE

The operational environment must ensure that administrators are authenticated before allowing them to manage the TOE.

OE.MANAGE

The operational environment must provide secure means for administrators to manage the TOE, including secure connection for remote management.

OE.BROWSER

The operational environment must ensure that the web browsers used by users to access the secure messaging service are trustworthy and function correctly. The operational environment must also ensure that the issuer of the TOE's TLS server certificate (root CA) is in the browser trust store.

OE.USER

The operational environment must ensure that the users verify that the server certificate presented by the browser, which is used to establish the HTTPS connection, is owned by the intended secure messaging server before login.

OE.IDP

The operational environment must ensure that one or more trusted IDPs are available and they meet the authentication strength/LoA requirement set by the organization. The operational environment must also ensure that these IDPs provide user identity and other user attributes to the TOE.

OE.ADMIN

The operational environment must ensure that the administrators are competent, trustworthy and follow the organization's security policies. The operational

environment must also ensure that the administrators of the TOE platform are also administrators of the TOE.

OE.TIME

The operational environment must provide a reliable time source to the TOE.

OE.DATABASE

The operational environment must ensure that the database system is trusted and works correctly. The operational environment must also ensure that data transfer between the TOE and the database is secure.

4.3 Security Objectives Rationale

4.3.1 Security objectives coverage

The following table provides a mapping of the security objectives for the TOE to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective for the TOE	Threats / OSPs
O.CHANNEL	T.EAVESDROP, T.TAMPER
O.AUTHENTICATE	T.MASQUERADE
O.MANAGE	P.MANAGEMENT, P.ERASURE
O.TRUSTED_IDP	P.TRUSTED_IDP, T.MASQUERADE, T.UNAUTHORIZED
O.AUTHORIZE	T.UNAUTHORIZED
O.ERASURE	P.ERASURE
O.LOGGING	P.LOGGING

The following table provides a mapping of the security objectives for the operational environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats /OSPs
OE.PLATFORM	A.PLATFORM
OE.PHYSICAL	A.PHYSICAL
OE.AUTHENTICATE	T.MASQUERADE
OE.MANAGE	P.MANAGEMENT
OE.BROWSER	A.BROWSER, T.EAVESDROP, T.TAMPER
OE.USER	A.USER
OE.IDP	A.IDP, T.MASQUERADE, T.UNAUTHORIZED
OE.ADMIN	A.ADMIN, T.UNAUTHORIZED
OE.TIME	A.TIME, P.LOGGING
OE.DATABASE	A.DATABASE, P.ERASURE

4.3.2 Security objectives sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

Threat	Rationale for the security objectives
T.EAVESDROP	This threat is addressed by O.CHANNEL which ensures that there is a secure channel between the TOE and user's browser. This secure channel provides confidentiality for any TSF or user data transmitted between the TOE and the browser, such as messages sent to and from the external user. O.CHANNEL is supported by OE.BROWSER which ensures that user's browser is trustworthy and functions correctly and that the issuer of the server certificate is trusted by the browser.
T.TAMPER	This threat is addressed by O.CHANNEL which ensures that there is a secure channel between the TOE and user's browser. This secure channel provides message origin authenticity and integrity for any TSF or user data transmitted between the TOE and the browser, such as messages sent to and from the external user. O.CHANNEL is supported OE.BROWSER which ensures that user's browser is trustworthy and functions correctly and that the issuer of the server certificate is trusted by the browser.
T.MASQUERADE	This threat is addressed by O.AUTHENTICATE which ensures that the TOE uniquely identifies and authenticates users before allowing them to access the TOE, and by O.TRUSTED_IDP which ensures that user identity assertions/claims are provided by trusted IDPs. O.AUTHENTICATE is supported by OE.IDP which ensures that the IDP(s) meet the authentication

	strength/LoA requirement set by the organization and provide user identity and other user attributes to the TOE. This threat is also addressed by OE.AUTHENTICATE which ensures that the operational environment authenticates administrators before allowing them to manage the TOE.
T.UNAUTHORIZED	This threat is addressed by O.AUTHORIZE which ensures that users can only access messages and perform operations on them as they are authorized to and that only administrators can perform management functions, and by O.TRUSTED_IDP which ensures that user attributes (e.g. role, group membership) are provided by trusted IDPs. O.AUTHORIZE is supported by OE.IDP which ensures that user attributes are provided to the TOE. The TOE makes authorization decision based on relevant attributes. O.AUTHORIZE is also supported by OE.ADMIN which ensures that administrators of the TOE platform (who have access to TOE configuration files) are also administrators of the TOE.

The following rationale provides justification that the security objective of the TOE is suitable to address each individual OSP and that each security objective tracing back to an OSP actually contributes in addressing the OSP.

OSP	Rationale for the OSP
P.MANAGEMENT	This OSP is addressed by O.MANAGE which ensures that the TOE provides administrators with secure means to manage the TSFs and by OE.MANAGE which ensures that the operational environment provides administrators with secure means to manage the TOE, including secure connection for remote management.
P.TRUSTED_IDP	This OSP is addressed by O.TRUSTED_IDP which ensures that only trusted IDPs are used for identifying and authenticating users.
P.ERASURE	This OSP is addressed by O.ERASURE which ensures that messages are permanently deleted after a pre-configured time period and that messages in an account are permanently deleted when the account is removed. O.ERASURE is supported by OE.DATABASE which ensures that messages are permanently deleted from the storage media. This OSP is also addressed by O.MANAGE which ensures that administrators are provided with secure means to configure the time period for scheduled message deletion.
P.LOGGING	This OSP is addressed by O.LOGGING which ensures that message operations performed by users and management operations performed by administrators are logged. O.LOGGING is supported by OE.TIME which provides a secure time stamp for logged events.

The following rationale provides justification that the security objectives of the TOE environment are suitable to address each individual assumption and that each security objective tracing back to an assumption actually contributes in addressing the assumption.

Assumption	Rationale for the assumption
A.PLATFORM	Addressed by OE.PLATFORM, which is identical to the assumption.
A.PHYSICAL	Addressed by OE.PHYSICAL, which is identical to the assumption.
A.BROWSER	Addressed by OE.BROWSER, which is identical to the assumption.
A.USER	Addressed by OE.USER, which is identical to the assumption.
A.IDP	Addressed by OE.IDP, which is identical to the assumption.
A.ADMIN	Addressed by OE.ADMIN, which is identical to the assumption.
A.TIME	Addressed by OE.TIME, which is identical to the assumption.

A.DATABASE	Addressed by OE.DATABASE, which is identical to the assumption.

5. Extended Components Definition

This PP defines five extended components: FDP_DEL_EXT.1, FDP_DEL_EXT.2, FIA_IDP_EXT.1, FIA_IDP_EXT.2 and FIA_IDP_EXT.3. The first two are specified in section 5.1 and the others in section 5.2.

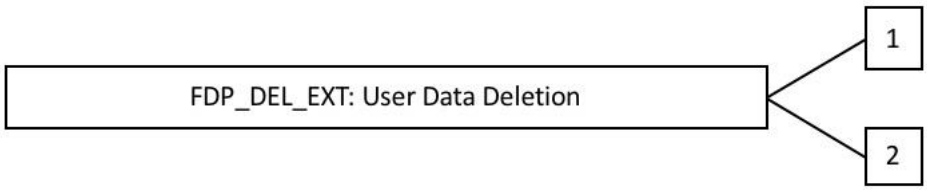
FCS_TLSS_EXT.1 and FCS_RBG_EXT.1 are taken directly from the extended components defined in [cPPND] section C.2.2.8 and C.2.1.1 for specification of the TLS protocol and random number generation, respectively.

5.1 User data deletion (FDP_DEL_EXT)

Family behaviour

This family defines the requirements for the TSF to delete user data when the data is no longer needed. This is a new family defined for the FDP class.

Component levelling



FDP_DEL_EXT.1 Scheduled data deletion, requires the TSF to delete user data after a specified time period.

FDP_DEL_EXT.2 Event-triggered deletion, requires the TSF to delete user data when specified events occur.

Management: FDP_DEL_EXT.1

The following actions could be considered for the management functions of FMT:

a) Specification of the time period after which specific user data should be deleted.

Management: FDP_DEL_EXT.2

The following actions could be considered for the management functions of FMT:

a) Management of the events that should occur prior to deleting the user data.

Audit: FDP_DEL_EXT.1, FDP_DEL_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: Unsuccessful message deletions.

5.1.1 FDP_DEL_EXT.1 – Scheduled data deletion

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DEL_EXT.1.1 The TSF shall delete [assignment: *list of objects or information type*] after [assignment: *time period*].

5.1.2 FDP_DEL_EXT.2 – Event-triggered deletion

Hierarchical to: No other components.

Dependencies: No dependencies.

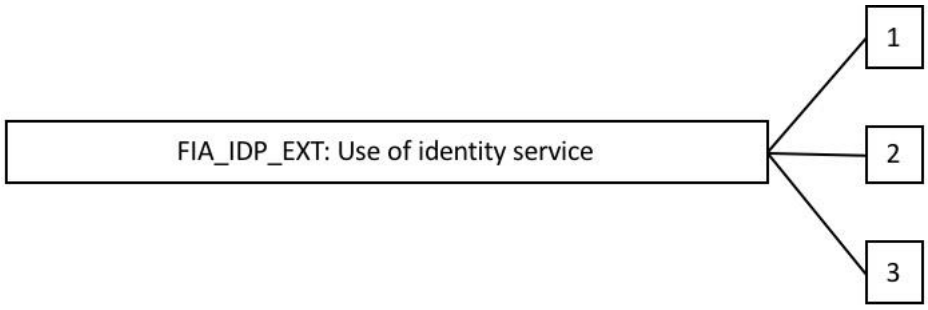
FDP_DEL_EXT.2.1 The TSF shall delete [assignment: *list of objects or information type*] when any of the following events occur: [assignment: *list of events*].

5.2 Use of identity service (FIA_IDP_EXT)

Family behaviour

This family defines the requirements for the TSF to use identity service provided by a trusted Identity Provider (IDP). This is a new family defined for the FIA class.

Component levelling



FIA_IDP_EXT.1 Redirection to IDP, requires the TSF to redirect users to a trusted IDP for identification and authentication.

FIA_IDP_EXT.2 Acceptance of user information from IDP, requires the TSF to make origin authenticity and integrity verifications before accepting user identity and specified user attributes from an IDP.

FIA_IDP_EXT.3 Authentication to the TOE, requires the TSF to authenticate the user identity provided by the IDP in accordance with the rules specified in the component.

Management: FIA_IDP_EXT.1, FIA_IDP_EXT.2

The following actions could be considered for the management functions of FMT:

a) Configuration of trusted IDP(s).

Management: FIA_IDP_EXT.3

There are no management activities foreseen.

Audit: FIA_IDP_EXT.1, FIA_IDP_EXT.2

There are no auditable events foreseen.

Audit: FIA_IDP_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

Minimal: The final decision on authentication.

5.2.1 FIA_IDP_EXT.1 – Redirection to IDP

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_IDP_EXT.1.1 The TSF shall redirect users to a trusted IDP for identification and authentication.

5.2.2 FIA_IDP_EXT.2 – Acceptance of user information from IDP

Hierarchical to: No other components.

Dependencies: FIA_IDP_EXT.1 Redirection to IDP

FIA_IDP_EXT.2.1 The TSF shall make the following verifications

- The origin of the user information must be verified to be a trusted IDP using [assignment: *origin authentication mechanism*];
- The integrity of the user information must be correctly verified using [assignment: *integrity verification mechanism*];
- [assignment: *additional verifications*]

before accepting user identity and [assignment: *list of user attributes*] from a trusted IDP.

5.2.3 FIA_IDP_EXT.3 – Authentication to the TOE

Hierarchical to: No other components.

Dependencies: FIA_IDP_EXT.2 Acceptance of user information from IDP

FIA_IDP_EXT.3.1 The TSF shall authenticate the user identity provided by the IDP in accordance with the following rules: [selection: *the user is accepted without further authentication*, *[assignment: rules for authenticating the user to the TOE]*].

6. Security Requirements

6.1 Security Functional Requirements

The following table lists all the functional components that are relevant for this PP.

Component	Component name
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FCS_RBG_EXT.1	Random bit generation
FCS_TLSS_EXT.1	TLS server protocol
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_DEL_EXT.1	Scheduled data deletion
FDP_DEL_EXT.2	Event-triggered deletion
FIA_ATD.1	User attribute definition
FIA_IDP_EXT.1	Redirection to IDP
FIA_IDP_EXT.2	Acceptance of user information from IDP
FIA_IDP_EXT.3	Authentication to the TOE
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FTP_ITC.1	Inter-TSF trusted channel

The following convention is used for operations applied to the Security Functional Requirements: assignments and selections are indicated in **bold**, iterations indicated by appending a letter to the requirement (e.g. FCS_COP.1a), and refinements indicated by **bold underscore** for additions and by ~~**bold strike through**~~ for deletions.

6.1.1 Security functional policies implemented by the TOE

The TOE implements the following access control policy.

Message access control SFP

This SFP regulates the access to messages stored in the TOE. It demands that subjects (users) can only access objects (messages) according to the rules as specified in Table 1 below.

	Administrator	Internal User	External User
Messages in user account	No access	All operations (i.e. send a new message, read, reply, forward, download, delete, and revoke) are allowed if the user is the owner of the account the message belongs to	If the user is the owner of the account the message belongs to, the user can perform • read and reply only when the permission level is set to 1 • read, reply, delete, download, forward and send to internal users when the permission level is set to 2. Forward/send to external users and revoke not allowed. • [assignment: *rules based on additional permission levels*]
Messages in function account	No access	All operations are allowed if the user is a member of the function account	No access

Table 1 Message access rules

While internal users can perform all possible operations on messages in their own accounts or in function accounts they have access to, this SFP restricts the message operations allowed for external users according to the permission level set in the system for external users.

6.1.2 FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the **not specified** level of audit; and
c) The following:
- **User sign-up, login and logout**
- **Message operations (send, read, reply, delete, forward, revoke and download)**
- **Management operations**
  - **Creation and removal of accounts (both user accounts and function accounts)**
  - **Modification of system settings**
  - **Modification of the list of trusted IDPs**
  - **Import, change and removal of TLS server key and certificate**
- **[assignment: *other specifically defined auditable events*]**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit*

relevant information].

Application note: All message operations, internal/external user and administrator sign-up, login and logout, and management operations performed by administrators shall be logged.

6.1.3 FAU_GEN.2 – User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application note: For each auditable action performed by a user, the TOE shall associate it with the unique internal user id.

6.1.4 FCS_CKM.2 – Cryptographic key ~~distribution~~establishment

FCS_CKM.2.1 The TSF shall ~~**distribute**~~**perform** cryptographic key~~s~~ **establishment** in accordance with a specified cryptographic key ~~**distribution**~~**establishment** method **[selection:**

- ***RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";***
- ***Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";***
- ***Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";***
- ***Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3.***

] ~~**that meets the following: [assignment:** ***list of standards*****]**~~.

Application note: This SFR addresses the establishment of session keys (encryption/decryption keys and HMAC keys) to be used by the TLS record layer. The ST author shall choose one or more of the cryptographic key establishment methods listed in the SFR.

6.1.5 FCS_CKM.4 – Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Application note: This SFR addresses destruction of the session keys (encryption/decryption keys and HMAC keys) used by the TLS record layer.

6.1.6 FCS_COP.1a – Cryptographic operation (symmetric encryption and decryption)

FCS_COP.1.1a The TSF shall perform **symmetric encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [selection: *CBC, CTR, GCM*] mode** and cryptographic key sizes **[selection: *128 bits, 192 bits, 256 bits*]** that meet the following: **AES as specified in ISO 18033-3, [selection: *CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772*]**.

Application note: This SFR addresses symmetric encryption and decryption functions used by the TLS record layer to protect message confidentiality. The ST author shall choose encryption algorithms and key sizes corresponding to the ciphersuites selected in FCS_TLSS_EXT.1.

6.1.7 FCS_COP.1b – Cryptographic operation (signature generation)

FCS_COP.1.1b The TSF shall perform **digital signature generation** in accordance with a specified cryptographic algorithm **[selection:**

- ***RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [assignment: 2048 bits or greater],***
- ***Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment: 256 bits or greater]***

] ~~**and cryptographic key sizes [assignment: *cryptographic key sizes*]**~~ that meet the following: **[selection:**

- ***For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***
- ***For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4.***

].

Application note: This SFR addresses the generation of digital signature for TLS server authentication. The ST author shall choose digital signature algorithms corresponding to the ciphersuites selected in FCS_TLSS_EXT.1.

6.1.8 FCS_COP.1c – Cryptographic operation (hash)

FCS_COP.1.1c The TSF shall perform **secure hash** in accordance with a specified cryptographic algorithm **[selection: *SHA-1, SHA-256, SHA-384*]** ~~**and cryptographic key sizes [assignment: *cryptographic key sizes*]**~~ **and message digest sizes [selection: *160, 256, 384*] bits** that meet the following: **ISO/IEC 10118-3:2004**.

Application note: This SFR addresses the hash functions used in TLS. The ST author shall choose hash algorithms and message digest sizes corresponding to the ciphersuites selected in FCS_TLSS_EXT.1. Please note that SHA-1 can only be selected

for usage in HMAC (FCS_COP.1d) to calculate message authentication code, and should not be selected for anything else (such as generating hash for digital signature).

6.1.9 FCS_COP.1d – Cryptographic operation (keyed hash)

FCS_COP.1.1d The TSF shall perform **keyed hash** in accordance with a specified cryptographic algorithm [**selection: *HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384*]** and cryptographic key sizes [assignment: *cryptographic key sizes*] **and message digest sizes [selection: *160, 256, 384*] bits** that meet the following: **ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**.

Application note: This SFR addresses the HMAC function used by TLS record layer to protect message integrity. The ST author shall choose hash algorithms and message digest sizes corresponding to the ciphersuites selected in FCS_TLSS_EXT.1.

6.1.10 FCS_RBG_EXT.1 – Random bit generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: *Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [*assignment: number of software-based sources] software-based noise source, [assignment: number of hardware-based sources] hardware- based noise source*] with a minimum of [selection: *128 bits, 192 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

Application note: This SFR addresses the generation of random numbers for TLS.

6.1.11 FCS_TLSS_EXT.1 – TLS server protocol

FCS_TLSS_EXT.1.1 The TSF shall implement **TLS 1.2 (RFC 5246)** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- ***TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268***
- ***TLS_RSA_WITH_AES_192_CBC_SHA as defined in RFC 3268***
- ***TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268***
- ***TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268***
- ***TLS_DHE_RSA_WITH_AES_192_CBC_SHA as defined in RFC 3268***
- ***TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268***
- ***TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492***
- ***TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA as defined in RFC 4492***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC***

4492

- ***TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492***
- ***TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA as defined in RFC 4492***
- ***TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492***
- ***TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246***
- ***TLS_RSA_WITH_AES_192_CBC_SHA256 as defined in RFC 5246***
- ***TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246***
- ***TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288***
- ***TLS_RSA_WITH_AES_192_GCM_SHA256 as defined in RFC 5288***
- ***TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288***
- ***TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289***

].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and **TLS 1.1**.

FCS_TLSS_EXT.1.3 The TSF shall [selection: *perform RSA key establishment with key size [selection: 2048 bits, 3072 bits, 4096 bits]; generate EC Diffie-Hellman parameters over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves; generate Diffie-Hellman parameters of size [selection: 2048 bits, 3072 bits]*].

Application note: This SFR specifies the TLS connection between the TOE and user's web browser. Only the server side is authenticated.

6.1.12 FDP_ACC.1 – Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Message access control SFP** on

- **Subjects: users**
- **Objects: messages**
- **Operations: send (new message), read, reply, forward, download, delete, revoke.**

6.1.13 FDP_ACF.1 – Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Message access control SFP** to objects based on the following:

- **Subjects: users**
- **Objects: messages**
- **Subject security attributes:**
  - **Internal user id**
  - **Email address**
  - **Role: Administrator, Internal User and External User**
  - **Function account membership**
  - **[assignment: *additional attributes*]**
- **Object security attributes:**
  - **Message id**
  - **Email address**
  - **[assignment: *additional attributes*]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- **The rules specified in Table 1;**
- **[assignment: *additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Application note: This SFR addresses access control of messages stored in the TOE. Each message has a message id and belongs to an account identified by email address. TOE users in the Administrator role does not have access to any individual messages. TOE users in the Internal User role have full access to messages in their own accounts and in those function accounts they are member of. TOE users in the External User role only have access to messages in their own accounts and can only perform message operations allowed according to the permission level. The permission level is a system wide setting and configured during TOE installation. The ST author that claims

compliance to this PP may want to add additional rules based on some additional security attributes. In this case the ST author has to specify these rules and the additional security attributes used by these rules through an appropriate instantiation of the assignment operations. The ST author may also define additional permission levels for external users in Table 1.

6.1.14 FDP_DEL_EXT.1 – Scheduled data deletion

FDP_DEL_EXT.1.1 The TSF shall delete **messages** after [assignment: *time period*].

Application note: This SFR addresses scheduled deletions of messages after the pre-configured message storage period. The TOE issues commands to the database to delete messages. It is the database system that ensures the messages be permanently deleted from the storage media (OE.DATABASE). The ST author shall specify the moment the time period starts when performing the assignment.

6.1.15 FDP_DEL_EXT.2 – Event-triggered deletion

FDP_DEL_EXT.2.1 The TSF shall delete **messages** when any of the following events occur:

- **An authorized user requests to delete the messages**
- **The account to which the messages belong is removed**
- **[assignment: *other events*]**

Application note: The TOE deletes messages upon user request, under the condition that the user is authorized to perform the delete operation (FDP_ACF.1). When the administrator removes a user account or function account from the system, the TOE deletes all messages in that account. The TOE issues commands to the database to delete the relevant messages. It is the database system that ensures the messages be permanently deleted from the storage media (OE.DATABASE).

6.1.16 FIA_ATD.1 – User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **Internal user id**
- **One or more user identifiers**
- **Email address**
- **Role**
- **Function account membership**
- **[assignment: *additional attributes*]**

Application note: The ST author may specify additional attributes that are associated to users.

6.1.17 FIA_IDP_EXT.1 – Redirection to IDP

FIA_IDP_EXT.1.1 The TSF shall redirect users to a trusted IDP for identification and authentication.

Application note: The TSF relies on IDP for user identification and authentication. Internal users and administrators are redirected to an internal IDP and external users

to an external IDP. The IDPs the users are redirected to must be on the list of trusted IDPs.

6.1.18 FIA_IDP_EXT.2 – Acceptance of user information from IDP

FIA_IDP_EXT.2.1 The TSF shall make the following verifications

- The origin of the user information must be verified to be a trusted IDP using [assignment: *origin authentication mechanism*];
- The integrity of the user information must be correctly verified using [assignment: *integrity verification mechanism*];
- [assignment: *additional verifications*]

before accepting user identity and **the following user attributes (if provided)**

- **Role**
- **Function account membership**
- **[assignment: *additional user attributes*]**

from a trusted IDP.

Application note: This SFR applies to the acceptance of user identity and associated user attributes (function account membership, etc.) from a trusted IDP. These user information may be provided to the TOE in the form of SAML assertions, OpenID Connect ID tokens, etc. The ST author shall specify the mechanism(s) that are used for origin authentication and integrity verification. The ST author may specify additional verifications to be made before accepting user information from an IDP, e.g. the validity time period has not passed.

6.1.19 FIA_IDP_EXT.3 – Authentication to the TOE

FIA_IDP_EXT.3.1 The TSF shall authenticate the user identity provided by the IDP in accordance with the following rules:

- **At initial sign-up,**
  - **for internal users and administrators, the user identity is accepted without further authentication;**
  - **for external users with invitation, the user identity must match the user identifier that is provided by the inviter;**
  - **for external users without invitation, the email address provided by the user must be verified to belong to the user;**
- **At login time,**
  - **for internal users and administrators, the user identity is accepted without further authentication;**
  - **for external users, the user identity must match one of the user identifiers that are bound to the user's email address;**
- **[assignment: *additional rules for authenticating the user to the TOE*].**

Application note: This SFR applies to the authentication of administrators, internal and external users to the TOE. After the user has successfully authenticated herself to the IDP, the TOE receives the user identity from the IDP and makes no or additional checks/verifications before accepting the user into the secure messaging service, depending on whether the user is internal/external, whether it is an initial sign-up or normal login, and whether the external user signs up with or without invitation.

6.1.20 FIA_UAU.1 – Timing of authentication

FIA_UAU.1.1 The TSF shall allow **access to the web portal of the secure messaging service and selection of identity service** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note: This SFR applies to the authentication of administrators, internal and external users. A user is only allowed to go to the portal and select the identity service before she is authenticated.

6.1.21 FIA_UID.1 – Timing of identification

FIA_UID.1.1 The TSF shall allow **access to the web portal of the secure messaging service and selection of identity service** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note: This SFR applies to the identification of administrators, internal and external users. A user is only allowed to go to the portal and select the identity service before she is identified. The identity service identifies and authenticates the user and then provides the authenticated user identity to the TOE in the form of SAML assertion, ID token, or similar.

6.1.22 FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf on that user:

- **Internal user id**
- **User identifier**
- **Email address**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- **For internal users and administrators, the TOE shall assign a unique internal user id and associate the user identifier and email address provided by the internal IDP to the internal user id;**
- **For external users who sign up with invitation, the TOE shall assign a unique internal user id and associate the user identifier and email address provided by the inviter to the internal user id;**
- **For external users who sign up without invitation, the TOE shall assign a unique internal user id and associate the user identifier provided by the external IDP and the email address provided by the external user herself after successful email address verification to the internal user id.**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users:

- **Internal user id cannot be changed;**
- **[assignment: *additional rules for the changing of attributes*].**

Application note: The TOE assigns a unique internal user id when a user account is created. For an invited external user the inviter provides the user identifier and email address which the TOE associates to the external user's account. For an external user who signs up without invitation, she provides her email address after authenticating herself to the external IDP. To verify that the provided email address does belong to the user, the TOE sends a message with an HTTPS link to this email address. If the user visits this HTTPS link, the verification succeeds and the TOE creates an account for this user. The verified email address and the user identifier provided by the external IDP are then associated to the account. For internal users and administrators, when they log in to the TOE for the first time, the TOE associates the user identifier and email address provided by the internal IDP to their accounts.

6.1.23 FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **manage** the **TSF data** to **Administrator**.

Application note: Only administrators can configure message storage period, permission level for external users and list of trusted IDPs. Only administrators can manage the keys and certificate for the TLS server.

6.1.24 FMT_SMF.1 – Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions*:*

- **Configure system settings (message storage period, permission level for external users)**
- **Configure the list of trusted IDPs**
- **Search and remove users**
- **Create and delete function accounts**
- **Import key and certificate for TLS server**
- **[assignment: *list of any additional management functions to be provided by the TSF*].**

Application note: In case a specific TOE is also providing additional management functionalities, the ST author has to instantiate the assignment operation to cover those functionalities.

6.1.25 FMT_SMR.1 – Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **Administrator, Internal User and External User**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note: The TOE maintains these three roles. The TOE enforces user authentication and assigns role to them.

6.1.26 FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **another Trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **no functions**.

Application note: The TSF applies to the trusted TLS channel between the TOE and user's web browser. Any communications through this channel is always initiated by the user's web browser and never by the TOE.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

SFR	Security objectives
FAU_GEN.1	O.LOGGING
FAU_GEN.2	O.LOGGING
FCS_CKM.2	O.CHANNEL
FCS_CKM.4	O.CHANNEL
FCS_COP.1a (symmetric encryption and decryption)	O.CHANNEL
FCS_COP.1b (signature generation)	O.CHANNEL
FCS_COP.1c (hash)	O.CHANNEL
FCS_COP.1d (keyed hash)	O.CHANNEL
FCS_RBG_EXT.1	O.CHANNEL
FCS_TLSS_EXT.1	O.CHANNEL
FDP_ACC.1	O.AUTHORIZE
FDP_ACF.1	O.AUTHORIZE
FDP_DEL_EXT.1	O.ERASURE
FDP_DEL_EXT.2	O.ERASURE
FIA_ATD.1	O.AUTHENTICATE, O.AUTHORIZE
FIA_IDP_EXT.1	O.AUTHENTICATE, O.TRUSTED_IDP
FIA_IDP_EXT.2	O.AUTHENTICATE, O.AUTHORIZE, O.TRUSTED_IDP
FIA_IDP_EXT.3	O.AUTHENTICATE
FIA_UAU.1	O.AUTHENTICATE

FIA_UID.1	O.AUTHENTICATE
FIA_USB.1	O.AUTHENTICATE
FMT_MTD.1	O.ERASURE, O.AUTHORIZE, O.TRUSTED_IDP
FMT_SMF.1	O.MANAGE, O.TRUSTED_IDP, O.CHANNEL
FMT_SMR.1	O.AUTHORIZE, O.MANAGE
FTP_ITC.1	O.CHANNEL

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security Objective	**Rationale**
O.CHANNEL	The objective: • The TOE shall enforce a secure communication channel to user's browser which protects information transmitted to and received from the browser against unauthorized disclosure and provides means for the TOE to detect any modification of incoming information from the browser. The secure channel also provides means for the browser to verify the integrity of information transmitted from the TOE to the browser. Is met by: • FCS_CKM.2 which specifies the establishment of session keys for the TLS record layer. • FCS_CKM.4 which specifies the destruction of session keys used by the TLS record layer. • FCS_COP.1a which specifies the encryption and decryption of TLS traffic. • FCS_COP.1b which specifies the generation of signature for TLS server authentication. • FCS_COP.1c which specifies the hash algorithms used with HMAC for TLS traffic integrity protection. • FCS_COP.1d which specifies the HMAC operations for TLS traffic integrity protection • FCS_RBG_EXT.1 which specifies the generation of random numbers to be used by TLS. • FCS_TLSS_EXT.1 which specifies the TLS protocol. • FMT_SMF.1 which provides the specific management function for import of TLS server key and certificate. • FTP_ITC.1 which ensures that there is a trusted channel between the TOE and user's browser.
O.AUTHENTICATE	The objective: • The TOE shall ensure that users are uniquely identified and authenticated before allowing them to access the secure messaging service.

	Is met by: • FIA_ATD.1 which specifies the security attributes that are used for user authentication. • FIA_IDP_EXT.1 which ensures that the TOE redirects the user to a trusted IDP. • FIA_IDP_EXT.2 which requires the TOE to verify that the user information (id and other attributes) is originated from a trusted IDP and has not been tampered with. • FIA_IDP_EXT.3 which specifies the rules for the TOE to authenticate the user identity provided by the IDP at initial sign-up and normal login. • FIA_UAU.1 which requires users to successfully authenticate themselves before being allowed to access their messages. But the users can access the web portal of the secure messaging service and select the identity service before being authenticated. • FIA_UID.1 requires users to successfully identify themselves before being allowed to access their messages. But the users can access the web portal of the secure messaging service and select the identity service before being identified. • FIA_USB.1 which specifies the initial association of security attributes with subjects and the rules for changing attributes.
O.AUTHORIZE	The objective: • The TOE shall ensure that users can only access messages and perform operations on them as they are authorized to. The TOE shall also ensure that only administrators can perform management functions. is met by: • FDP_ACC.1 and FDP_ACF.1 which ensure that users can only access messages that belong to them, and for external users they can only perform message operations that are allowed according to the permission level. • FIA_ATD.1 which specifies the security attributes that are used for access control. • FIA_IDP_EXT.2 which ensures that the TOE verifies the origin and integrity of user information (id and other attributes) before using the information to make access control. • FMT_MTD.1 which ensures that only administrators can manage the TSF data. • FMT_SMR.1 which associates users with roles.
O.MANAGE	The objective: • The TOE shall provide administrators with secure means to manage the TSFs. is met by: • FMT_SMF.1 which specifies the management functions of the TOE.

	• FMT_SMR.1 which defines the administrator role.
O.TRUSTED_IDP	The objective: • The TOE shall ensure that only trusted IDPs are used for user identification and authentication. is met by: • FIA_IDP_EXT.1 which ensures that users are redirected to trusted IDP. • FIA_IDP_EXT.2 which ensures that information received from the IDP is origin authenticated and integrity verified. • FMT_MTD.1 which ensures that only administrators can modify the list of trusted IDPs. • FMT_SMF.1 which provides the specific management function for configuring trusted IDPs.
O.ERASURE	The objective: • The TOE shall permanently delete messages after a pre-configured time period. The TOE shall also permanently delete messages upon request from an authorized user and permanently delete all messages in an account (user account or function account) when the account is removed. is met by: • FDP_DEL_EXT.1 which ensures that messages are deleted after the pre-configured storage period. Note it is the database system (part of the TOE environment) that ensures messages are permanently deleted from the storage media. • FDP_DEL_EXT.2 which ensures that, when a user is removed from the system, all messages belonging to this user are deleted. It also ensures that a message is deleted when an authorized user requests that. • FMT_MTD.1 which ensures that only administrators can configure the storage period before messages are permanently deleted.
O.LOGGING	The objective: • The TOE shall log message operations performed by users and management operations performed by administrators. The TOE shall not log message subjects or contents. is met by: • FAU_GEN.1 which specifies the logging function. • FAU_GEN.2 which ensures that each logged event is associated to the identity of the user that caused the event.

6.2.3 Dependency analysis between security functional components

The following table demonstrates the dependencies of SFRs and how the SFRs for the TOE resolve those dependencies. For FDP_DEL_EXT.1, FDP_DEL_EXT.2, FIA_IDP_EXT.1, FIA_IDP_EXT.2 and FIA_IDP_EXT.3, the dependencies are specified in Chapter 5. For FCS_TLSS_EXT.1 and FCS_RBG_EXT.1 the dependencies are specified in [cPPND]. The dependencies of the other SFRs are specified in CC Part 2.

SFR	Dependencies	Resolved?
FAU_GEN.1	FPT_STM.1	No, satisfied by OE.TIME instead
FAU_GEN.2	FAU_GEN.1 FAU_UID.1	Yes, by FAU_GEN.1 Yes, by FAU_UID.1
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, satisfied by FMT_SMF.1 instead. The TLS server key pair is generated outside the TOE and imported into the TOE by the administrator. The importation is not governed by any access control SFP. Yes, by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	No, satisfied by FCS_CKM.2 instead as the keys are established using FCS_CKM.2.
FCS_COP.1a (symmetric encryption and decryption)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, satisfied by FCS_CKM.2 instead as the keys are established using FCS_CKM.2. Yes, by FCS_CKM.4
FCS_COP.1b (signature generation)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, satisfied by FMT_SMF.1 instead. The TLS server key pair is generated outside the TOE and imported into the TOE by the administrator. No, no key destruction is needed because the TLS server private key is kept in the TOE for use as long as the corresponding certificate is valid. When the certificate expires, the private key may be archived.
FCS_COP.1c (hash)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, since no key is needed for hash operation No, no key destruction is needed since there is no key associated with hash operation

FCS_COP.1d (keyed hash)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	No, satisfied by FCS_CKM.2 instead as the keys are established using FCS_CKM.2. Yes, by FCS_CKM.4
FCS_RBG_EXT.1	-	-
FCS_TLSS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	No, satisfied by FMT_SMF.1 instead. The TLS server key pair is generated outside the TOE and imported into the TOE by the administrator. Yes, by FCS_CKM.2 Yes, by FCS_COP.1a Yes, by FCS_COP.1b Yes, by FCS_COP.1c Yes, by FCS_COP.1d Yes, by FCS_RBG_EXT.1
FDP_ACC.1	FDP_ACF.1	Yes, by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	Yes, by FDP_ACC.1 No, there are no default values for those attributes that are used to enforce the Message access control SFP
FDP_DEL_EXT.1	-	-
FDP_DEL_EXT.2	-	-
FIA_ATD.1	-	-
FIA_IDP_EXT.1	-	-
FIA_IDP_EXT.2	FIA_IDP_EXT.1	Yes, by FIA_IDP_EXT.1
FIA_IDP_EXT.3	FIA_IDP_EXT.2	Yes, by FIA_IDP_EXT.2
FIA_UAU.1	FIA_UID.1	Yes, by FIA_UID.1
FIA_UID.1	-	-
FIA_USB.1	FIA_ATD.1	Yes, by FIA_ATD.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Yes, by FMT_SMR.1 Yes, by FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Yes, by FIA_UID.1
FTP_ITC.1	-	-

6.3 Security Assurance Requirements

The security assurance requirements of this Protection Profile are those defined in CC part 3 for the assurance level EAL3 augmented with ALC_FLR.2.

Assurance class	**Assurance components**

ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorization controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_FLR.2 Flaw reporting procedures
	ALC_LCD.1 Developer defined life-cycle model
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.4 Security Assurance Requirements Rationale

The assurance level EAL3 has been chosen as appropriate for a messaging service that is deployed in a secure and well managed environment. The security assurance requirements for EAL3 are designed to provide evidence that the TOE has been methodically tested and checked, and that it provides protection suitable for an environment requiring moderate confidence in security at a reasonable development and evaluation cost.

EAL 3 is augmented with ALC_FLR.2 to ensure that instructions and procedures for the reporting and remediation of identified security flaws are in place.

7. Abbreviations

CA	Certification Authority
CC	Common Criteria
CSEC	Swedish Certification Body for IT Security
GUID	Globally Unique Identifier
EAL	Evaluation Assurance Level
HTTPS	HTTP over TLS
IDP	IDentity Provider
LoA	Level of Assurance
OSP	Organizational Security Policy
PP	Protection Profile
RFC	Request for Comment
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

8. References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; Part 2: Security functional components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002; Part 3: Security assurance components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004.

[cPPND] Collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14-March-2018.

[ISO15446] Technical Report ISO/IEC TR 15446, Information technology – Security techniques – Guide for the production of protection profiles and security targets, Edition 3, 2017-10.

[ISO29115] International Standard ISO/IEC 29115, Information technology – Security techniques – Entity authentication assurance framework, Edition 1, 2013-04.

[NIST80063] NIST SP 800-63-2, Electronic Authentication Guideline, August 2013.

[RFC 5246] The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August 2008.