ULAK.IM Secure Instant Messenger v2.0

SECURITY TARGET LITE v1.4

Document History

Version	Date	Description
1.0	28 November 2023	First Publication
1.1	06 Dec 2023	ST-document update
1.2	11 Dec 2023	ST-document update
1.3	20 Dec 2023	ST-document update
1.4	27 Dec 2023	ST-document update

Mustafa Kemal Mah. Dumlupınar Blv. No:280-G 1110 Çankaya / ANKARA
Ayrıntılı Bilgi: Furkan ÇETİN Telefon: (0312) 443 02 00 Faks: (0312) 443 06 10
E-Posta: furkan.cetin@ordulu.com Website: www.ordulu.com

ORDULU

CONTENTS

1 INTRODUCTION 5

1.1 ST REFERENCE AND TOE REFERENCE 5

1.2 TOE OVERVIEW 5

1.2.1 TOE Usage and Security Feature 5

1.2.2 TOE Type 6

1.2.3 Non-TOE Hardware/Software/Firmware 6

1.3 TOE DESCRIPTION 7

1.3.1 Physical Scope of TOE 7

1.3.2 Logical Scope of TOE 8

2 CONFORMANCE CLAIM 9

2.1 CC CONFORMANCE CLAIM 9

2.2 PP CLAIM 10

2.3 PACKAGE CLAIM 10

3 SECURITY PROBLEM DEFINITION 10

3.1 ASSETS 10

3.2 THREAT AGENTS 10

3.3 THREATS 11

3.4 ORGANIZATIONAL SECURITY POLICY 11

3.5 ASSUMPTIONS 12

4 SECURITY OBJECTIVES 13

4.1 SECURITY OBJECTIVES FOR TOE 13

4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT 14

4.3 SECURITY PROBLEM DEFINITION - SECURITY OBJECTIVES RATIONALE 15

5 EXTENDED COMPONENT DEFINITION 18

5.1 USER DATA DELETION (FDP_DEL_EXT) 18

5.1.1 FDP_DEL_EXT.1 Scheduled data deletion 19

5.1.2 FDP_DEL_EXT.2 Event-triggered deletion 19

5.2 USE OF IDENTITY SERVICE (FIA_IDP_EXT) 19

5.2.1 FIA_IDP_EXT.1 Redirection to IDP 20

5.2.2 FIA_IDP_EXT.2 Acceptance of user information from IDP 20

5.2.3 FIA_IDP_EXT.3 Authentication to the TOE 21

6 SECURITY REQUIREMENTS 21

6.1 OVERVIEW 21

6.2 SECURITY FUNCTIONAL REQUIREMENTS (SFR) 22

6.2.1 Security functional policies implemented by the TOE 22

6.2.2 Security Audit 24

6.2.3 Identification and Authentication 25

6.2.4 User Data Protection 29

6.2.5 Cryptographic Support 31

6.2.6 Security Management 35

6.2.7 Trusted Path/Channels 37

6.2.8 SFR – Security Objective Rationale 38

6.2.9 SFR Dependency Rationale 43

6.3 SECURITY ASSURANCE REQUIREMENTS (SAR) 46

6.3.1 Security Assurance Requirements Rationale 47

7 TOE SUMMARY SPECIFICATION 47

7.1 SECURITY AUDIT 47

7.2 IDENTIFICATION AND AUTHENTICATION 48

7.3 SECURE COMMUNICATION 48

7.4 USER DATA PROTECTION 49

7.5 SECURITY MANAGEMENT 49

REFERENCES 50

1 INTRODUCTION

1.1 ST REFERENCE AND TOE REFERENCE

ST Lite Title	Security Target Lite ULAK.IM Secure Instant Messenger v2.0
ST Lite Version	v1.4
TOE Title	ULAK.IM Secure Instant Messenger v.2.0
TOE Version	v2.0
Assurance Level	EAL4+ (ALC_FLR.3)
Author	Ordulu Technology INC.
Date	27 December 2023

1.2 TOE OVERVIEW

1.2.1 TOE Usage and Security Feature

The Target of Evaluation (TOE) is a secure module which belongs a communication service that consists of two main components, namely the ULAK.IM Server and the ULAK.IM Client App. While ULAK.IM Server is an integration management server designed to manage both desktop and mobile communication process, ULAK.IM Client App is an application that provide secure messaging platform.

Server provides confidentiality, integrity, authenticity, forward secrecy for all instant messenger, voice, and video in centralized management interface. Once a user is verified/authenticated by the organization, s/he can send a sensitive message to a user or a group via client app and the recipient can read and reply to the message securely. The system supports one-to-one (one sender and one recipient) messaging and group messaging (more than one sender and recipient).

TOE uses a user's mobile internet or wi-fi (when available) to send and receive messages. Adding to that, the desktop client can be connected via a QR code, as a second client after the initial registration. TOE uses standard cellular telephone numbers as identifiers and uses end-to-end encryption to secure all communications.

Additionally, with the end-to-end encryption feature of TOE, a message can only be viewed by the sending and receiving parties. It is not possible for the components in between to decrypt messages, including the server. Messages can only be encrypted and decrypted on the devices of the sending and receiving parties.

Secure communication for video and voice calls is provided with the WebRTC protocol through TOE. Voice and video calls are also encrypted end-to-end. With the common encryption key generated at the start of each conversation, audio and video packets are encrypted, and this encryption key changes with each call.

The TOE provides the following security functionalities:

- Security audit
- Identification and authentication
- Secure communications
- User data protection
- Security management

1.2.2 TOE Type

TOE is a secure messaging service that allows users within an organization to send/receive sensitive messages to/from authorized users. The TOE can be categorized as “Network and Network-Related Devices and Systems” in accordance with the categories identified on the Common Criteria Portal that lists all certified products.

1.2.3 Non-TOE Hardware/Software/Firmware

The server and client operation system, proxy-pass and load balancer, databases are the minimum system requirements that TOE needs to operate. Those are outside the TOE physical boundaries and yet considered part of the TOE operational environment.

1.3 TOE DESCRIPTION

1.3.1 Physical Scope of TOE

TOE includes both client and server's components. The Client component is referred to here for both mobile and desktop client application. The TOE components can be seen in Figure 1 and were inserted into red dotted boxes.

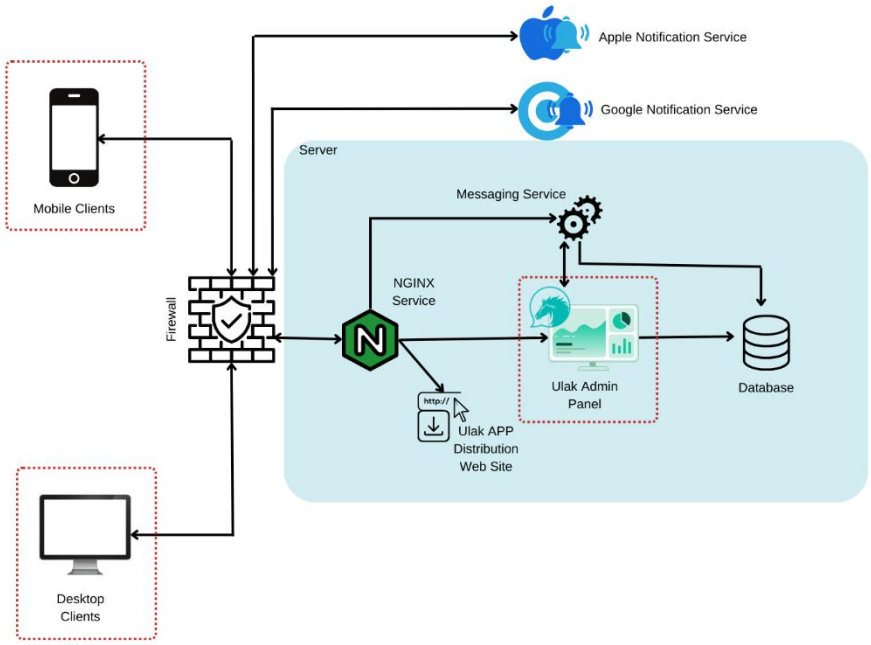


Figure 1. Physical Boundaries of TOE

- **ULAK.IM Client**

ULAK.IM client is on mobile (Android, iOS) and desktop platform. The client is able to establish encrypted calls and live chats with clients on other devices using message server. Any mobile device is initialized with phone number and signature via Admin Panel or mobile phone. ULAK.IM Client Application is the TOE.

- **ULAK.IM Server**
  - **Admin Panel**

    The management functionalities are performed using the Admin Panel. The functionalities mean verifying users, configuring settings as well as account

management. The admin panel offers a web interface that is accessible using a web browser from the administrator's local machine.

1.3.2 Logical Scope of TOE

The logical boundary consists of the security functionality of TOE is summarized as below:

- **Security Audit**
  The TOE generates audit records with a reliable time stamp for security events like logins and user management activity. The administrators have the ability to view the audit trail.

- **Identification and Authentication:**
  All users are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. In order to login to Admin Panel, administrators authenticate themselves by username and password. When using the mobile application, the user performs initial authentication via passcode.

- **Secure Communication:**
  Users communicate over the encryption key. (AES-256-bit encryption is created for each mutual message exchange of users, using asymmetric cryptography with the key referred to as the encryption key). Users who create public keys using Diffie-Hellman transfer data in an encrypted manner. Communication with the server uses TLS 1.3 protocol. The server certificate is signed using the SHA2 hash algorithm and uses the RSA 2048-bit asymmetric key. Key exchange X25519 and asymmetric keys formed from double elliptic curve are used in end-to-end encryption. Messages are encrypted using AES-256 with 256-bit keys. Each user has temporary and permanent asymmetric keys. When two users start talking for the first time, a common symmetric encryption key is created using key exchange permanent and temporary keys. This common encryption key changes in mutual messages as long as the two users continue to talk to each other.

- **User Data Protection:**
  TOE users in user role can send/receive messages. They can reply, forward, revoke, download and delete messages.

  TOE users in administrator role can configure system settings for the secure messaging service, search and remove users, and perform other management operations from

Admin Panel. The administrator in the organization sets a permission level which determines the message operations users are allowed to perform. However, they cannot perform operations on individual messages as users.

TOE has also a functionality called disappearing message. Once enabled, new messages sent in the individual or group chat will disappear after a period of time.

- **Security Management:**
  The administrators of the TOE platform have access to the TOE configuration files. The administrators can manage the configuration files locally or remotely. The followings are the actions that administrators can consider;
    - Configuration of system settings
    - Configuration of trusted Identity Providers (IDPs)
    - User and account management (add/remove/update)
    - Bot management
    - Application update

2 CONFORMANCE CLAIM

2.1 CC CONFORMANCE CLAIM

This ST claims conformance to

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017, [1]
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, [2]- Extended
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, [3]- Conformant

And the

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017, [4]

has to be taken into account.

2.2 PP CLAIM

This ST does not claim any conformance to any protection profile. However, it uses the following source as reference;

- Secure Messages Protection Profile v.1.1, 2018-11-26 [5]

2.3 PACKAGE CLAIM

Evaluation Assurance Level is EAL4 augmented with ALC_FLR.3.

3 SECURITY PROBLEM DEFINITION

3.1 ASSETS

The assets to be protected by the TOE are:

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

3.2 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.
- 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).

3.3 THREATS

Identifier	Threat Statement
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.MODIFY	An attacker tries to modify 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.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data by sending impermissible information through the TOE resulting the exploitation of protected resources such as IDP.
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

3.4 ORGANIZATIONAL SECURITY POLICY

Identifier	Security Statement
P.NETWORK	There should be an appropriate network layer protection, that there is a firewall in place that only permits access through required ports for users to access the web- server.
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.LOGGING	Message operations performed by users and management operations performed by administrators shall be logged. Message subjects and contents shall not be logged.

P.ERASURE	Messages in an account shall be permanently deleted upon request from an authorized user and when the account is removed. Additionally, The TOE shall permanently delete messages after a time period, if configured.

3.5 ASSUMPTIONS

Identifier	Assumption Statement
A.ADMIN	The Administrator is not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
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.
A.TIMESTAMP	The underlying operating system will have a reliable time source that the TOE can utilize for generating audit log timestamps.
A.IDP	It is assumed that one or more trusted IDPs are available and they meet the necessary authentication requirements.
A.UPDATE	The underlying platform on which the TOE operates will be regularly updated with the latest security patches and fixes to ensure data stored on the platform remains protected and secure.
A.PHYSICAL	It is assumed that the TOE (server) is located in a physically secure environment, no unauthorized persons have physical access to the TOE and its underlying system.

4 SECURITY OBJECTIVES

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.1 SECURITY OBJECTIVES FOR TOE

Identifier	Objective Statement
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.
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.ERASURE	The TOE shall also permanently delete messages upon request from an authorized user and permanently delete all messages in an account when the account is removed.
O.LOGGING	The TOE shall log message operations performed by users and management operations performed by administrators. Authorized users can view the logs.
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.

4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

Identifier	Objective Statement
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.
OE.ADMIN	The operational environment must ensure that the administrators are competent, trustworthy and follow the organization's security policies
OE. TIMESTAMP	The operational environment must provide a reliable time source to the TOE
OE.IDP	The operational environment must ensure that one or more trusted IDPs are available and they meet the authentication requirement. The operational environment must also ensure that these IDPs provide user identity and other user attributes to the TOE
OE.UPDATE	The developer shall provide updates of the TOE on a regular basis.
OE.PHYSICAL	The operational environment must ensure that the TOE is located in a physically secure environment under the organization's control.
OE.MANAGE	The operational environment must provide secure means for administrators to manage the TOE, including secure connection for remote management
OE.NETWORK	The operational environment must provide a firewall that only permits access through required ports for users to access the web- server.

4.3 SECURITY PROBLEM DEFINITION - SECURITY OBJECTIVES RATIONALE

The following table demonstrates that all security objectives for the TOE trace back to the threats, operational security policy in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.EAVESDROP	O.CHANNEL	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.
T.MODIFY	O.CHANNEL	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.
T.UNAUTHORISED_ACCESS	O.TRUSTED_IDP O.AUTHORIZE OE.IDP	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.
T.MASQUERADE	O.AUTHENTICATE O.TRUSTED_IDP OE.IDP	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 requirement and provide user identity and other user attributes to the TOE.
P.NETWORK	OE.NETWORK	This policy is addressed by OE.NETWORK which ensures that operational environment must provide a firewall.
P.MANAGEMENT	O.MANAGE OE.MANAGE	This policy 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	O.TRUSTED_IDP	This policy is addressed by O.TRUSTED_IDP which ensures that only

		trusted IDPs are used for identifying and authenticating users.
P.LOGGING	O.LOGGING OE. TIMESTAMP	This policy 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.TIMESTAMP which provides a secure time stamp for logged events.
P.ERASURE	O.ERASURE O.MANAGE	This policy is addressed by O.ERASURE which ensures that messages are permanently deleted after a time period and that messages in an account are permanently deleted when the account is removed. It is also addressed by O.MANAGE which ensures that administrators are provided with secure means to configure the time period for scheduled message deletion.
A.ADMIN	OE.ADMIN	This assumption has been established to directly address this objective.
A.PLATFORM	OE.PLATFORM	This assumption has been established to directly address this objective.
A.TIMESTAMP	OE. TIMESTAMP	This assumption has been established to directly address this objective.
A.IDP	OE.IDP	This assumption has been established to directly address this objective.
A.UPDATE	OE.UPDATE	This assumption has been established to directly address this objective.
A.PHYSICAL	OE.PHYSICAL	This assumption has been established to directly address this objective.

5 EXTENDED COMPONENT DEFINITION

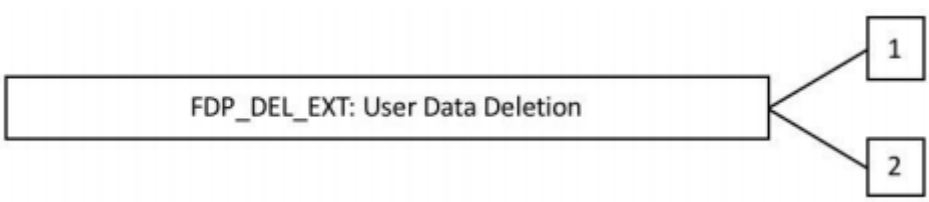
This PP defines five extended components: FDP_DEL_EXT.1, FDP_DEL_EXT.2, FIA_IDP_EXT.1, FIA_IDP_EXT.2 and FIA_IDP_EXT.3.

5.1 USER DATA DELETION (FDP_DEL_EXT)

Family behavior

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 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.

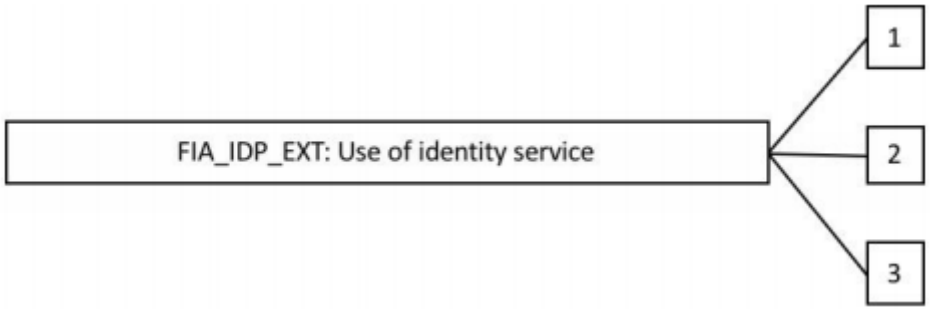
FDP_DEL_EXT.2.1 The TSF shall delete [assignment: *list of objects or information type*] when any of the following events occur: [assignment: *list of events*].

5.2 USE OF IDENTITY SERVICE (FIA_IDP_EXT)

Family behavior

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 ST:

a) 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 OVERVIEW

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1r5 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using **bolded text** and are surrounded by square brackets as follows [**assignment**].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using ***bold italics text*** and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using **bolded text**, for additions, and ~~strike-through~~, for deletions.
- **Iteration**. The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_ACC.1/a and FDP_ACC.1/b.

6.2 SECURITY FUNCTIONAL REQUIREMENTS (SFR)

6.2.1 Security functional policies implemented by the TOE

The TOE implements the following access control policy.

	Administrator	Mobile Client User	Desktop Client User
Message Access Control SFP	No Access	All operations (i.e. send a new message, read, reply, forward, download, delete) are allowed if the user is the owner of the account the message belongs to	All operations (i.e. send a new message, read, reply, forward, download, delete) are allowed if the user is the owner of the account the message belongs to
Admin Panel Access Control	All operations (i.e.: configuring, adding, removing, and updating the system and account settings like verifying user accounts. Additionally, the admin can view all the audit information from the audit records.	No Access	No Access

The security functional requirements are expressed using the notation stated in Section 5.1 above and itemized in the table below.

SFR	Identifier
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.2	Restricted audit review
FIA_ATD.1/Panel	User attribute definition
FIA_ATD.1/Client	User attribute definition
FIA_UID.1/App	Timing of identification
FIA_UID.2/Panel	User identification before any action
FIA_UAU.1	User timing of authentication
FIA_UAU.2	User authentication before any action
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
FDP_ACC.1/Message	Subset access control
FDP_ACC.1/Panel	Subset access control
FDP_ACF.1/Message	Security attribute-based access control
FDP_ACF.1/Panel	Security attribute-based access control
FDP_DEL_EXT.1	Scheduled data deletion
FDP_DEL_EXT.2	Event-triggered deletion
FCS_CKM.1/RSA	Cryptographic key generation
FCS_CKM.1/Enc-Dec	Cryptographic key generation
FCS_CKM.2/RSA	Cryptographic key establishment
FCS_CKM.2/Diff	Cryptographic key establishment
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/Enc-Dec	Cryptographic operation
FCS_COP.1/Hash	Cryptographic operation
FCS_COP.1/Sign	Cryptographic operation

FMT_MSA.1/Panel	Management of security attributes
FMT_MSA.3/Message	Static attribute initialization
FMT_MSA.3/Panel	Static attribute initialization
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
FTP_TRP.1	Trusted Path

6.2.2 Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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~~ **system**;

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, delete and download)**
- **Management operations**
  - **Creation and removal of accounts**
  - **Modification of system settings**
  - **Modification of the list of trusted IDPs**
  - **System logs]**

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, [**none**].

Application note: This SFR is used to the generation of audit data for all message operations, user and administrator sign-up, login and logout.

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**administrators**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Application note: This SFR is applied within the admin panel so that all audit information can be read.

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Application note: This SFR is applied within the admin panel to only authorized users so that all audit information can be reviewed.

6.2.3 Identification and Authentication

FIA_ATD.1/Panel User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**username, password, and role**].

Application note: This SFR is applied over the admin panel by administrators so that the security attributes such as the username, password and roles are maintained at the level of the user.

FIA_ATD.1/Client User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**phone number/IDP**].

Application note: This SFR is applied so that the client defines the user's initial authentication via phone number.

FIA_UID.1/App Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UID.1.1 The TSF shall allow [**access to the mobile/desktop application of the secure messaging 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 is applied so that the user is only allowed to go to the identity service before the user is authenticated.

FIA_UID.2/Panel User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 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 is applied so that the user is pre-identified on the admin panel before being authenticated.

FIA_UAU.1 User Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [**access to the Admin Panel login page**] on behalf of the user to be performed before the user is authenticated.

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

Application note: This SFR is applied so that the user can access the admin panel login page.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UID.2/Panel User identification before any action

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 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 is applied so that the user is authenticated on the admin panel.

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.

Application note: This SFR is applied so that users are redirected to a trusted IDP for identification and authorization.

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 [**signature**];
- The integrity of the user information must be correctly verified using [**digital signature verification**];
- [**none**]

before accepting user identity and [**none**] from a trusted IDP.

Application note: This SFR is applied for the acceptance of user identity and attributes from a trusted IDP. This user information is provided to the TOE in the Connect ID tokens.

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: [*[*

- ***At initial sign-up,***
  - ***for identified users, the user identity is accepted without further authentication;***
  - ***for unidentified users with invitation, the user identity must match the user identifier that is provided by the inviter;***
- ***At login time,***
  - ***for identified users, the user identity is accepted without further authentication]***]

Application note: This SFR is applied so that the user is successfully authenticated 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.

6.2.4 User Data Protection

FDP_ACC.1/Message Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based 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 and delete**].

FDP_ACF.1/Message Security attribute-based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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: user name, phone number; Object security attributes: Message bubble, contact**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**All operations (i.e. send a new message, read, reply, forward, download, delete) are allowed if the user is the owner of the account the message belongs to**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**no additional rule**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no additional rule**].

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 phone number. TOE users in the Administrator role does not have access to any individual messages. TOE users in the user role have full access to messages in their own accounts.

FDP_ACC.1/Panel Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute-based access control

FDP_ACC.1.1 The TSF shall enforce the [**Admin Panel access control SFP**] on [**Subjects: administrators; Objects: system settings, account settings; Operations: configure, add, remove, update**].

FDP_ACF.1/Panel Security attribute-based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [**Admin Panel access control SFP**] to objects based on the following: [**Subjects: administrators; Objects: system settings, account settings; Subject security attributes: user and groups; Object security attributes: IDP, signature, update package**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**All operations are allowed if the administrator has permission.**].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**admin can update user to VIP user**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**user is deleted from Admin Panel**].

Application note: This SFR addresses access control of system and account settings stored in the TOE. Each of these security attributes are managed from an authorized account identified by email address.

FDP_DEL_EXT.1 Scheduled data deletion

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DEL_EXT.1.1 The TSF shall delete [**messages**] after [**configured 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).

FDP_DEL_EXT.2 Event-triggered deletion

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_DEL_EXT.2.1 The TSF shall delete [**messages**] when any of the following events occur: [**A user requests to delete their own messages.**]

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). 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).

6.2.5 Cryptographic Support

FCS_CKM.1/RSA Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**2048 bit**] that meet the following: [**ISO/IEC 9796-2, NIST SP 800-56A, FIPS 186-4**].

Application Note: This SFR addresses the generation of session keys used by the RSA record layer to create a signature.

FCS_CKM.1/Enc-Dec Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES.CBC**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**NIST SP 800-21, FIPS 197**].

Application Note: This SFR addresses the creation of a 256-bit key accordingly to the standard of AES.CBC

FCS_CKM.2/RSA Cryptographic key ~~distribution~~ establishment

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall ~~distribute~~ **perform** cryptographic key~~s~~ **establishment** in accordance with a specified cryptographic key ~~distribution~~ **establishment** method [**RSA-based key establishment schemes with 2048-bit key size**] ~~that meets the following: [assignment: list of standards]~~.

FCS_CKM.2/Diff Cryptographic key ~~distribution~~ establishment

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1 The TSF shall ~~distribute~~ establish cryptographic keys in accordance with a specified cryptographic key ~~distribution~~ establishment method [**Diffie Hellman (X3DH)**] that meets the following: [**NIST SP 800-56A**, **RFC 3526, RFC 7748.]**

Application Note: This SFR is applied to a created curve25519 key used for key establishment via Extended Triple Diffie-Hellman method by the TLS record layer.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zerorization**] that meets the following: [**FIPS 140-2]**.

Application Note: This SFR is applied for the destruction of all symmetric keys at the end of each session used by the TLS record layer.

FCS_COP.1/Enc-Dec Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**message encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES-CBC mode**] and cryptographic key sizes [**256 bit**] that meet the following: [**FIPS 197, NIST SP 800-21**].

Application note: This SFR addresses symmetric encryption and decryption functions used by the TLS record layer to protect message confidentiality.

FCS_COP.1/Hash Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**secure hash**] in accordance with a specified cryptographic algorithm [**SHA256**] ~~and cryptographic key sizes [**assignment:** *cryptographic key sizes*]~~ that meet the following: [**FIPS180, ISO/IEC 10118-3:2004.**].

Application note: This SFR addresses the secure hash that is used to ensure the integrity of the TLS connection.

FCS_COP.1/Sign Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [**digital signature verification**] in accordance with a specified cryptographic algorithm [**Elliptic Curve Digital Signature Algorithm (ECDSA)**] and cryptographic key sizes [**512 bit**] that meet the following: [**ANSI X9.62, ISO/IEC 14888-3, RFC6090**].

Application Note: This SFR addresses the generation of digital signature for TLS server authentication.

6.2.6 Security Management

FMT_MSA.1/Panel Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**Admin Panel access control SFP**] to restrict the ability to [***change_default, modify, delete***] the security attributes [**credentials**] to [**Administrator**].

FMT_MSA.3/Message Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**Message access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3/Panel Static attribute initialization

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**Admin Panel access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [**manage**] the [**TSF data**] to [**Administrators**].

Application note: This SFR is applied so that only administrators can configure groups, permission level for users and list of trusted IDPs. Only administrators can delete the keys and certificate for the TLS server.

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)**
- **Configure the list of trusted IDPs**
- **Search and remove users**
- **Configure certificate for TLS server**
- **Bot management**
- **TOE update**]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [**Administrator, User**].

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

Application note: This SFR is applied to maintain these two roles. The TOE enforces user authentication and assigns roles to them.

6.2.7 Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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 [**secure voice and live chat**].

Application note: This SFR is applied to the trusted TLS channel between the users.

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification, disclosure***].

FTP_TRP.1.2 The TSF shall permit [***remote users***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial user authentication***].

6.2.8 SFR – Security Objective Rationale

SFR	Objectives
FAU_GEN.1	O.LOGGING
FAU_SAR.1	O.LOGGING
FAU_SAR.2	O.LOGGING
FIA_ATD.1/Panel	O.AUTHENTICATE, O.AUTHORIZE
FIA_ATD.1/Client	O.AUTHENTICATE, O.AUTHORIZE
FIA_UID.1/App	O.AUTHENTICATE
FIA_UID.2/Panel	O.AUTHENTICATE
FIA_UAU.1	O.AUTHENTICATE
FIA_UAU.2	O.AUTHENTICATE

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
FDP_ACC.1/Message	O.AUTHORIZE
FDP_ACC.1/Panel	O.AUTHORIZE
FDP_ACF.1/Message	O.AUTHORIZE
FDP_ACF.1/Panel	O.AUTHORIZE
FDP_DEL_EXT.1	O.ERASURE
FDP_DEL_EXT.2	O.ERASURE
FCS_CKM.1/RSA	O.CHANNEL
FCS_CKM.1/Enc-Dec	O.CHANNEL
FCS_CKM.2/RSA	O.CHANNEL
FCS_CKM.2/Diff	O.CHANNEL
FCS_CKM.4	O.CHANNEL
FCS_COP.1/Enc-Dec	O.CHANNEL
FCS_COP.1/Hash	O.CHANNEL
FCS_COP.1/Sign	O.CHANNEL
FMT_MSA.1/Panel	O.AUTHORIZE, O.MANAGE
FMT_MSA.3/Message	O.AUTHORIZE, O.MANAGE
FMT_MSA.3/Panel	O.AUTHORIZE, O.MANAGE
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
FTP_TRP.1	O.CHANNEL

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.

Objectives	Rationale
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. Is met by: • FCS_CKM.1/RSA, FCS_CKM.1/Enc-Dec which generates the necessary keys for secure communication • FCS_CKM.2/RSA, FCS_CKM.2/Diff which specify the establishment of session keys for the TLS record layer. • FCS_CKM.4 which specifies the destruction of session keys. • FCS_COP.1/Enc-Dec which specifies the encryption and decryption of messaging. • FCS_COP.1/Sign which specifies the verification of signature for TLS server authentication. • FCS_COP.1/Hash which specifies the hash algorithms used for traffic integrity protection. • 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 user and another IT product. • FTP_TRP.1 which ensures that data sent by users is protected from modification or disclosure.
O.AUTHENTICATE	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/Panel, FIA_ATD.1/Client which specify the security attributes that are used for 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. • 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_UID.1/App, FIA_UID.2/Panel requires users to successfully identify themselves before being allowed to access messaging service and select the identity service before being identified. • FIA_UAU.2 which requires users to successfully authenticate themselves before being allowed to any action.
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. Is met by: • FDP_ACC.1/Message, and FDP_ACF.1/Message which ensure that users can only access messages that belong to them, and they can only perform message operations that are allowed according to the permission level. • FDP_ACC.1/Panel, and FDP_ACF.1/Panel which ensure that only administrators have access to admin panel and allowed to manage the configurations. • FIA_ATD.1/Panel and FIA_ATD.1/Client which specify 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_MSA.1/Panel which encounters the objective by restricting user access to security attributes. • FMT_MSA.3/Message and FMT_MSA.3/Panel which encounter the objective by restricting access to provide default values for security attributes that are used to enforce the related SFP. • FMT_MTD.1 which ensures that only administrators can manage the TSF data. • FMT_SMR.1 which associates users with roles.
O.MANAGE	The TOE shall provide administrators with secure means to manage the TSFs. Is met by: • FMT_MSA.1/Panel which encounters the objective by restricting user access to manage. • FMT_MSA.3/Message and FMT_MSA.3/Panel which encounter the objective by restricting access to manage. • FMT_SMF.1 which specifies the management functions of the TOE. • FMT_SMR.1 which defines the administrator role.
O.TRUSTED_IDP	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 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 when the account is removed. Is met by: • FDP_DEL_EXT.1 which ensures that messages are deleted after the pre-configured storage period. • 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 sees that. • FMT_MTD.1 which ensures that only administrators can configure the storage period before messages are permanently deleted.
O.LOGGING	The TOE shall log message operations performed by users and management operations performed by administrators. Is met by: • FAU_GEN.1 which specifies the logging function. • FAU_SAR.1 and FAU_SAR.2 which maintains a profile of system usage and suspicion rating to each profile along with threshold condition to indicate possible security violation.

6.2.9 SFR Dependency Rationale

SFR	Dependency	Satisfied
FAU_GEN.1	FPT_STM.1	Time stamp provided by operational environment
FAU_SAR.1	FAU_GEN.1	Yes
FAU_SAR.2	FAU_SAR.1	Yes
FIA_ATD.1/Panel	-	-

FIA_ATD.1/Client	-	-
FIA_UID.1/App	-	-
FIA_UID.2/Panel	-	-
FIA_UAU.1	FIA_UID.1	Yes
FIA_UAU.2	FIA_UID.1	FIA_UID.1/App
FIA_IDP_EXT.1	-	-
FIA_IDP_EXT.2	FIA_IDP_EXT.1	Yes
FIA_IDP_EXT.3	FIA_IDP_EXT.2	Yes
FDP_ACC.1/Message	FDP_ACF.1	FDP_ACF.1/Message
FDP_ACC.1/Panel	FDP_ACF.1	FDP_ACF.1/Panel
FDP_ACF.1/Message	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Message FMT_MSA.3/Message
FDP_ACF.1/Panel	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Panel FMT_MSA.3/Panel
FDP_DEL_EXT.1	-	-
FDP_DEL_EXT.2	-	-
FCS_CKM.1/RSA	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_CKM.2/RSA TSF is for TLS establishment, thus there is no destruction
FCS_CKM.1/Enc-Dec	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1/Enc-Dec Yes
FCS_CKM.2/RSA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/RSA TSF is for TLS establishment, thus there is no destruction
FCS_CKM.2/Diff	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	TSF is for TLS establishment so neither key creation nor import operation is necessary within the SFR. Also the public key used in the operation does not have confidentiality

		requirements so FCS_CKM.4 is also not required here
FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1/Enc-Dec
FCS_COP.1/Enc-Dec	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1/Enc-Dec Yes
FCS_COP.1/Hash	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	No key is needed for hash No key destruction is needed for hash
FCS_COP.1/Sign	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	TSF is for TLS establishment so this SFR satisfied by refined FCS_CKM.2/Diff. FCS_CKM.4 is also not required here.
FMT_MSA.1/Panel	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Panel Yes Yes
FMT_MSA.3/Message	FMT_MSA.1 FMT_SMR.1	There no restriction to attributes in client part Yes
FMT_MSA.3/Panel	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Panel Yes
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Yes Yes
FMT_SMF.1	-	
FMT_SMR.1	FIA_UID.1	FIA_UID.1/App FIA_UID.2/Panel (as hierarchical)
FTP_ITC.1	-	-

FTP_TRP.1	-	-

6.3 SECURITY ASSURANCE REQUIREMENTS (SAR)

The security assurance requirements of this ST are those defined in CC part 3 for the assurance level EAL4 augmented with ALC_FLR.3.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_TDS.3 Basic modular design
	ADV_IMP.1 Implementation representation of the TSF
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.3 Systematic flaw remediation
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.3 Focused vulnerability analysis

6.3.1 Security Assurance Requirements Rationale

The assurance level EAL4 has been chosen as appropriate for a messaging service that is deployed in a secure and well-managed environment. The security assurance requirements for EAL4 are designed to provide evidence that the TOE has been focused 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 4 is augmented with ALC_FLR.3 to ensure that instructions and procedures for the reporting and remediation of identified security flaws are in place.

7 TOE SUMMARY SPECIFICATION

7.1 SECURITY AUDIT

TOE will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the event) when the following events occur:

- User sign-up, login and logout
- Message operations (send, read, reply, delete, forward, revoke and download)
- Management operations:
    - Creation and removal of accounts
    - Modification of system settings
    - Modification of the list of trusted IDPs
    - Change and removal of TLS server key and

Administrators have the capability to review these audit records via admin panel. Timestamps are generated for audit logs by utilizing the underlying operational environment. The TOE does not generate its own timestamps for use in audit records.

Related SFRs: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2

7.2 IDENTIFICATION AND AUTHENTICATION

Administrators and users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces. Users must enter their phone's passcode to access the functionality that application provides.

Administrator users may access admin panel via the web interface that the platform provides. These roles must provide a username and password for authentication with the TOE. Once the TOE verifies that the provided username and password are authentic, the user will be provided with the web interface that provides access to the functions assigned to their user ID/role.

The TOE also extracts the user identifier from the identity information provided by IDP and compares it with the user identifier(s) that is bound to the user's phone numbers. If there is a match, the user is successfully authenticated to the TOE.

In the first registration, user information is signed with an elliptical curve key structure for verification and the signature is saved to the server.

Related SFRs: FIA_ATD.1/Panel, FIA_ATD.1/Client, FIA_UID.1/App, FIA_UID.2/Panel, FIA_UAU.1, FIA_UAU.2, FIA_IDP_EXT.1, FIA_IDP_EXT.2, FIA_IDP_EXT.3, FCS_COP.1/Sign and FMT_SMR.1

7.3 SECURE COMMUNICATION

The TOE establishes a trusted path using the TLS v.1.3 for the communications between Server and Client. The SSL session is based on mutual authentication of the TOE, and the remote instance, using installed digital certificates. In addition, for the message service, TOE provides the end-to-end encrypted channel between the TOE and another instantiation of the TOE.

Secure communications as provided are also encrypted end-to-end. Data packets are encrypted with the common encryption key generated at the beginning of each conversation, and this encryption key changes with each call. TOE performs the communication with the server encrypted for network security. The packets sent to the server contain only encrypted message data and the information to whom the message will be sent. This data is sent to the server in encrypted form, the server opens the encrypted packet and sees to whom it should forward the message, but never accesses the message content. Communication with the server uses TLS 1.3

protocol. The server certificate is signed using the hash algorithm and uses RSA 2048 bit asymmetric key.

Related SFRs: FTP_ITC.1, FTP_TRP.1, FCS_CKM.1/Enc-Dec, FCS_COP.1/Enc-Dec, FCS_CKM.4, FCS_CKM.1/RSA, FCS_CKM.2/RSA, FCS_CKM.2/Diff, FCS_COP.1/Hash

7.4 USER DATA PROTECTION

TOE implements access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorized parties. TOE users can send/receive messages. They can reply, forward, revoke, download and delete messages. TOE users in the Administrator role can configure system settings for the secure messaging service, search and remove users, and perform other management operations. The administrator in the organization sets a permission level which determines the message operations users are allowed to perform. Moreover, message is permanently deleted after a pre-defined storage period. This period and disappearing message rules can be configured by the administrator.

Related SFRs: FDP_ACC.1/Message, FDP_ACC.1/Panel, FDP_ACF.1/Message, FDP_ACF.1/Panel, FDP_DEL_EXT.1 and FDP_DEL_EXT.2.

7.5 SECURITY MANAGEMENT

TOE provides a suite of management functions to authorized users and Administrators. These functions allow for the configuration to suit the environment in which it is deployed. Additionally, management roles may perform the following tasks by Administrators:

- Configure system settings (message storage period, permission)
- Configure the list of trusted IDPs
- Search and remove users
- Configure certificate for TLS server
- Bot management
- TOE update

Administrators and/or authorized user may assign and adjust the functions available to other authorized users. These roles may access the TOE via the web interface provided by admin panel.

Related SFRs: FMT_MSA.1/Panel, FMT_MSA.3/Message, FMT_MSA.3/Panel, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

REFERENCES

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003

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

[5] Secure Messages Protection Profile, Version 1.1, 2018-11-26.