# Security Target

## Soprano GAMMA

| | |
|---|---|
| Document Reference: | GAMMA_ST_1.1 |
| Document Status: | Released |
| Document Version: | 1.1 |
| Issue Date: | 29 April 2016 |


| | |
|---|---|
| Prepared by: | Dan Pitcher (BAE Systems) |
| Approved by: | Matthew Murphy (Soprano) |

# Table of contents

1 Document information ..... 4
1.1 Amendment history ..... 4
1.2 Copyright statement ..... 4
2 Security Target Introduction (ASE_INT) ..... 5
2.1 ST Identification ..... 5
2.2 TOE Identification ..... 5
2.3 Document organisation ..... 6
2.4 References ..... 6
2.5 TOE overview ..... 7
2.5.1 TOE type and usage ..... 7
2.6 TOE description ..... 7
2.6.1 Physical scope of the TOE ..... 7
2.6.2 Logical scope of the TOE ..... 8
3 Conformance Claims (ASE_CCL) ..... 11
3.1 CC conformance claim ..... 11
3.2 Protection Profile conformance claim ..... 11
4 Security Problem Definition (ASE_SPD) ..... 12
4.1 Threats ..... 12
4.2 Assumptions ..... 12
4.3 Organisational security policies ..... 13
5 Security Objectives (ASE_OBJ) ..... 14
5.1 Objectives ..... 14
5.2 Security objectives for the environment ..... 14
6 Extended Components Definition (ASE_ECD) ..... 16
6.1 Overview ..... 16
7 Security Functional Requirements (ASE_REQ) ..... 17
7.1 Overview ..... 17
7.2 Audit (FAU) ..... 19
7.2.1 FAU_GEN.1 Audit data generation ..... 19
7.2.2 FAU_GEN.2 User identity association ..... 19
7.2.3 FAU_STG.1 Protected audit trail storage ..... 20
7.2.4 FAU_STG.4 Prevention of audit data loss ..... 20
7.3 Communication (FCO) ..... 20
7.3.1 FCO_NRR.2 Enforced proof of receipt ..... 20
7.4 Cryptographic Support (FCS) ..... 21
7.4.1 FCS_CKM.1(1) Cryptographic key generation (RSA) ..... 21
7.4.2 FCS_CKM.1(2) Cryptographic key generation (AES) ..... 21
7.4.3 FCS_CKM.2 Cryptographic key distribution (AES) ..... 21
7.4.4 FCS_CKM.4 Cryptographic key destruction ..... 22
7.4.5 FCS_COP.1(1) Cryptographic operation (AES) ..... 22
7.4.6 FCS_COP.1(2) Cryptographic operation (RSA) ..... 22
7.4.7 FCS_COP.1(3) Cryptographic operation (Signatures) ..... 23
7.5 User Data Protection (FDP) ..... 23
7.5.1 FDP_ACC.1(1) Subset access control (MEMS) ..... 23
7.5.2 FDP_ACC.1(2) Subset access control (GAMMA) ..... 24
7.5.3 FDP_ACF.1 Security attribute based access control ..... 24
7.5.4 FDP_RIP.1 Subset residual information protection ..... 25

7.6 Identification and Authentication (FIA) ..... 25
7.6.1 FIA_AFL.1 Authentication failure handling ..... 25
7.6.2 FIA_UAU.2 User authentication before any action ..... 25
7.6.3 FIA_UAU.7 Protected authentication feedback ..... 25
7.6.4 FIA_UID.2 User identification before any action ..... 26
7.6.5 FIA_SOS.1 Verification of secrets ..... 26
7.7 Security management (FMT) ..... 26
7.7.1 FMT_MSA.1 Management of security attributes ..... 26
7.7.2 FMT_MSA.3 Static attribute initialisation ..... 27
7.7.3 FMT_REV.1 Revocation ..... 27
7.7.4 FMT_SMF.1(1) Specification of Management Functions (MEMS) ..... 27
7.7.5 FMT_SMF.1(2) Specification of Management Functions (GAMMA) ..... 28
7.7.6 FMT_SMR.1 Security roles ..... 28
7.8 Protection of the TSF (FPT) ..... 28
7.8.1 FPT_STM.1 Reliable time stamps ..... 28
7.9 TOE Access (FTA) ..... 28
7.9.1 FTA_SSL.3 TSF-initiated termination ..... 28
7.9.2 FTA_SSL.4 User-initiated termination ..... 29
7.10 Trusted path/channels (FTP) ..... 29
7.10.1 FTP_ITC.1 Inter-TSF trusted channel ..... 29
7.10.2 FTP_TRP.1 Trusted path ..... 29
7.11 Security assurance requirements ..... 30

**8 TOE summary specification (ASE_TSS) ..... 31**
8.1 Overview ..... 31
8.2 Audit ..... 31
8.3 Communication ..... 31
8.4 Cryptographic Support ..... 31
8.5 Data Protection ..... 32
8.6 Identification and Authentication ..... 33
8.7 Security management ..... 33
8.8 TOE Access ..... 34
8.9 Trusted path/channels ..... 34

**9 Rationale ..... 35**
9.1 Security objectives rationale ..... 35
9.1.1 Threat/OSP rationale ..... 35
9.1.2 Assumption/objectives rationale ..... 36
9.2 Security requirements rationale ..... 37
9.2.1 Tracing of SFRs to security objectives ..... 37
9.2.2 Dependency analysis ..... 39
9.3 Security assurance requirements justification ..... 42

# 1 Document information

## 1.1 Amendment history

| Version | Date | Author(s) | Revisions |
|---|---|---|---|
| OL.1 | 19-Dec-14 | DJP | Initial outline draft |
| OL.2 | 21-Jan-15 | DJP | Second outline draft |
| 0.1 | 28-Jan-15 | DJP | Initial draft release |
| 0.2 | 13-Feb-15 | DJP | Initial release to evaluators. |
| 0.3 | 24-Jul-15 | DJP | Updated to address issues raised in EOR_ASE 1.0 and design changes. |
| 0.4 | 13-Oct-15 | DJP | Updated to address change in TOE version. |
| 0.5 | 04-Mar-16 | DJP | Updated to address issues raised in EOR_ASE 2.0. |
| 0.6 | 04-Mar-16 | DJP | Updated to address issues raised in EOR_ASE 3.0 |
| 1.0 | 17-Mar-16 | DJP | Initial release. |
| 1.1 | 29-Apr-16 | DJP | Updated to address certifier comments. |

## 1.2 Copyright statement

# 2 Security Target Introduction (ASE_INT)

## 2.1 ST Identification

**Table 1 – ST identification**

| | |
|---|---|
| **ST Title** | Security Target - Soprano GAMMA |
| **ST Version** | 1.1 |
| **ST Release Date** | 29 April 2016 |

## 2.2 TOE Identification

**Table 2 – TOE identification**

| | |
|---|---|
| **TOE Name** | Soprano GAMMA |
| **TOE Version(s)** | Soprano GAMMA for iOS (Version 3.0.9 (CC))<br>Soprano GAMMA for Android (Version 3.0.9 (CC))<br>Soprano GAMMA Server (Version b473)<br>Soprano GAMMA Registration Server (Version b1)<br>Soprano Mobile Enterprise Messaging Suite (MEMS) (Version b649) |
| **Protection Profile** | N/A |
| **CC Identification** | Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1 (Revision 4), September 2012<br>Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 (Revision 4), September 2012 |

## 2.3 Document organisation

This document is divided into the following sections:

- Section 2 (Security Target Introduction (ASE_INT)) provides the introductory material for the ST;
- Section 3 (Conformance Claims (ASE_CCL)) provides the conformance claims for the evaluation;
- Section 4 (Security Problem Definition (ASE_SPD)) provides the security problem to be addressed by the TOE and the operational environment of the TOE;
- Section 5 (Security Objectives (ASE_OBJ)) defines the security objectives for the TOE and the environment;
- Section 6 (Extended Components Definition (ASE_ECD)) provides a definition and justification for any extended components from CC Parts 2 or 3 that have been developed for the evaluation;
- Section 7 (Security Functional Requirements (ASE_REQ)) contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE;
- Section 8 (TOE summary specification (ASE_TSS)) provides a summary of the TOE specification, identifying the IT security functions provided by the TOE; and
- Section 9 (Rationale) provides the rationales for the various sections of the Security Target.

## 2.4 References

[1] Common Criteria Part 1 (Introduction and general model), Version 3.1 Revision 4, September 2012

[2] Common Criteria Part 2 (Security functional components), Version 3.1 Revision 4, September 2012

[3] Common Criteria Part 3 (Security assurance components), Version 3.1 Revision 4, September 2012

[4] Common Criteria Evaluation Methodology (CEM), Version 3.1 Revision 4, September 2012

## 2.5 TOE overview

### 2.5.1 TOE type and usage

The Target of Evaluation (TOE) is Soprano GAMMA. GAMMA is a secure messaging platform for use in enterprise environments. The TOE is comprised of three primary components:

- The GAMMA application (for Android or iOS) – a mobile messaging app running on Android and iOS platforms that allows users to exchange rich media messages using IP based communications with fall-back SMS support for last-mile coverage;
- The GAMMA server – a central server that processes and relays all messages exchanged between mobile devices;
- The GAMMA registration server – which provides a centralised platform for all application installation activities;
- The Mobile Enterprise Messaging Suite (MEMS) – a central server that provides the administration functionality to the GAMMA product, as well as APIs that allow integration with customers' business IT systems.

## 2.6 TOE description

### 2.6.1 Physical scope of the TOE

Users' mobile devices run the GAMMA app to securely send and receive messages on both the Google Android and Apple iOS platforms. Users download the GAMMA app from the corresponding Google Play Store or Apple App Store.

The GAMMA application communicates with the GAMMA server during registration and for every message that is sent or received. The communication channel between the application and server is protected by the Transport Layer Security (TLS) protocol.

The Mobile Enterprise Messaging Suite (MEMS) provides the following main functions:

- Customer administration. The MEMS server provides a web interface that, among other functions, allows customer administrators to manage users, contacts, as well as configure enterprise-wide settings, such as enabling end-to-end encryption;
- GAMMA secure messaging. In addition, the MEMS server provides users with a web interface for sending messages and includes extended features not available in the GAMMA app, such as the option to define expiry times for sent messages and the ability to wipe (recall) already sent messages;
- Business integration APIs. The MEMS server exposes a set of APIs that can be used by enterprise business applications to integrate with the messaging system. MEMS supports HTTP, WSDL, SMPP and SMTP interfaces.

Both the GAMMA server and MEMS server can be deployed either in an open cloud or a private cloud setting.

The Soprano Registration Server is used during the initial setup of the GAMMA client and provides the functionality required to register a unique device with an enterprise instance or deployment of GAMMA.

#### 2.6.1.1 Non-TOE software/hardware requirements

The following table outlines any non-TOE software or hardware requirements for the successfully installation and operation of the TOE:

**Table 3 – Non-TOE software and hardware requirements**

| Component | Requirements |
|---|---|
| Soprano GAMMA (Android) | **Software:**<br>Android 5.0+ (Lollipop)<br>**Evaluated devices:**<br>Samsung Galaxy S6, HTC One |
| Soprano GAMMA (iOS) | **Software:**<br>iOS 8<br>**Evaluated devices:**<br>iPhone 6, iPhone 6 Plus |
| Soprano GAMMA Server | **Software:**<br>Linux RHEL6 (x64)<br>**Hardware:**<br>Sufficient to meet requirements for Red Hat Enterprise Linux 6 |
| Soprano MEMS | **Software:**<br>Linux RHEL6 (x64)<br>TLSv1.2-enabled browsers (Firefox v24 and later, Internet Explorer 8 and later, Chrome v30 and later)<br>**Hardware:**<br>Sufficient to meet requirements for Red Hat Enterprise Linux 6 |
| GAMMA Registration Server | **Software:**<br>CentOS 6.4<br>**Hardware:**<br>Sufficient to meet requirements for CentOS 6.4. |

### 2.6.2 Logical scope of the TOE

The TOE is a software-only TOE, comprised of the components listed in Table 2 – TOE identification. The connections between each of the distributed components is illustrated in the following figure:

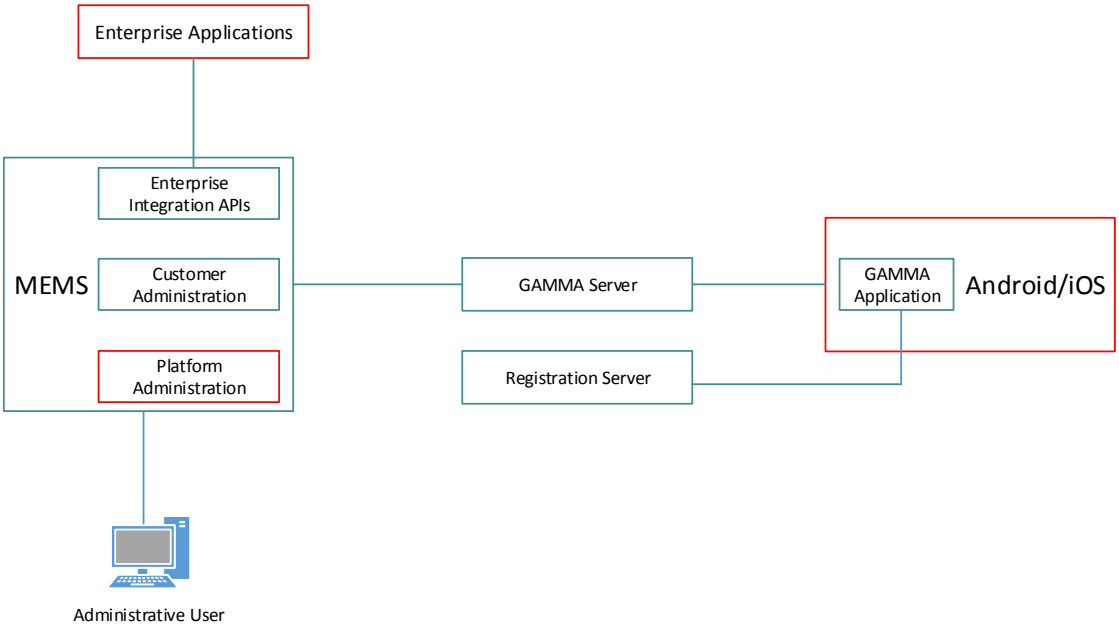


**Figure 1 - Soprano GAMMA architecture**

In the above image, components marked with a red line are not included in the scope of the evaluation (i.e. the enterprise applications, platform administrator functionality and the underlying mobile operating system).

The TOE provides the following security functionality:

**Table 4 – Security features**

| TSF | Description |
|---|---|
| Security audit | The TOE generates and stores audit files for a variety of auditable events. These events record the identity of the user that caused the event to occur, the date and time, the success/failure of the event and any other pertinent information.<br>The TOE also provides protected storage for audit logs to prevent unauthorised modification and will alert administrative users if storage space is no longer available. |
| Communication | The TOE provides proof-of-receipt for GAMMA messages sent between users. |
| Cryptographic support | The TOE implements a variety of key generation and cryptographic functions to protect user data both at rest and in transit between components of the TOE. |
| User data protection | The TOE implements access control mechanisms to ensure that authorised users only have access to the functionality they have been granted by a customer/platform administrator. |
| Identification and authentication | The TOE implements mechanisms to ensure that users are both identified and authenticated before any access to TOE functionality or TSF data is granted. |
| Security management | The TOE provides a suite of management functions for both GAMMA and MEMS, allowing enterprise to customise the solution to meet its needs. |

| TSF | Description |
|---|---|
| Protection of the TSF | The TOE generates reliable timestamps for use in other security functions (particularly during the generation of audit logs). |
| TOE access | The TOE provides session control mechanisms for both automated closing of sessions by the TOE and manual termination of sessions by users. |
| Trusted path/channels | The TOE provides a secure channel between its components using Transport Layer Security (TLS) to prevent TOE data modification or disclosure while in transit. |

#### 2.6.2.1 Summary of out of scope items

The following TOE features/components are not included in the scope of the evaluation:

- Soprano administration functionality of the GAMMA Server, GAMMA Registration Server and MEMS platforms;
- Any enterprise applications that use the Enterprise Integration APIs; and
- The underlying mobile operating system (iOS or Android).

# 3 Conformance Claims (ASE_CCL)

## 3.1 CC conformance claim

The ST and TOE are conformant to version 3.1 (Revision 4) of the Common Criteria for Information Technology Security Evaluation.

- **Part 2 conformant**. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 4.
- **Part 3 conformant**. Conformant with Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 4. The claimed assurance package is EAL2.

## 3.2 Protection Profile conformance claim

Neither the ST nor TOE claim conformance to any Protection Profiles.

# 4 Security Problem Definition (ASE_SPD)

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a set of **threats** that the TOE must mitigate,
b) specific **assumptions** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and
c) relevant **organisational security policies** that specify rules or guidelines that must be followed by the TOE and/or the operational environment.

## 4.1 Threats

**Table 5 – Identified threats**

| Threat | Threat statement |
|---|---|
| T.EAVESDROPPING | A malicious third party may attempt to intercept communications sent between users of the TOE. |
| T.REQUEST | An authenticated user may attempt to perform unauthorized actions on stored resources that may comprise the confidentiality and/or integrity of the stored identity information. |
| T.WEAK_CRYPTO | Inappropriate cryptographic functions are implemented by the TOE that may be exploited by a (potential) attacker, using cryptographic analysis techniques, in order to gain access to TOE data. |
| T.UNAUTHORISED_ACCESS | An unauthorised user or third party may gain unauthorised physical access to a device containing the TOE, allowing direct access to TOE data for export, modification or other purposes. |

## 4.2 Assumptions

**Table 6 – Assumptions**

| Assumption | Assumption statement |
|---|---|
| A.ACCEPTABLE_USE | It is assumed that there is an enterprise acceptable use policy in place governing the use of the GAMMA application. |
| A.INSTALL | It is assumed that the Soprano GAMMA application is delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.<br>It is assumed that the Soprano MEMS environment will be provisioned and configured in accordance with documented procedures. |
| A.LOGICAL_PROTECT | Any internet connection to a server role is assumed to be appropriately secured by a firewall or similar network security mechanism. |
| A.NO_EVIL | It is assumed that there will be one or more competent administrators assigned to manage the MEMS/GAMMA Server, its platform and the security of the information both of them contain.<br>It is also assumed that the administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation. |

| Assumption | Assumption statement |
|---|---|
| A.PHYSICAL_PROTECT | It is assumed that the MEMS server, GAMMA Server, registration server and their associated platforms will be located within facilities providing controlled access to the TOE. |
| A.UNTRUSTED | It is assumed that no untrusted software is installed on the servers/devices the TOE is installed/provisioned on. |

## 4.3 Organisational security policies

There are no organisational security policies for this Security Target.

# 5 Security Objectives (ASE_OBJ)

## 5.1 Objectives

**Table 7 – Objectives**

| Objective | Objective statement |
|---|---|
| O.AUDIT_REVIEW | The TOE shall generate audit data and provide the facility for administrators to review these logs. |
| O.AUTH | The TOE shall prevent unauthorised users from gaining access to TOE functionality or data. |
| O.AUTH_CONTROL | The TOE shall implement methods to prevent the brute forcing of authentication mechanisms. |
| O.CRYPTO | The TOE will implement cryptographic capabilities to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. |
| O.PROTECTED_COMMS | The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities. |
| O.SESSION_LOCK | The TOE shall provide mechanisms that mitigate the risk of an unattended session being hijacked. |
| O.WIPE | The TOE shall allow users to wipe messages that they no longer wish to be available to recipients. |

## 5.2 Security objectives for the environment

**Table 8 – Security objectives for the environment**

| Objective | Objective statement |
|---|---|
| OE.APPS | Soprano GAMMA users will not install any applications on their device that directly impact the security functionality provided by the TOE. |
| OE.INSTALL | The operational environment shall ensure that the TOE is delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.<br>The operational environment shall enable the administrator to ensure that the machines the TOE is installed on support the secure operation of the TOE. |
| OE.LOGICAL_SECURITY | The operational environment shall provide sufficient logical security (such as firewalls) to protect the TOE from external (and internal) malicious users. |
| OE.NO_EVIL | The operational environment shall provide one or more competent administrators assigned to manage the TOE, its platform and the security of the information both of them contain.<br>The operational environment will ensure that the administrator(s) are not careless, wilfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation. |

| Objective | Objective statement |
|---|---|
| OE.PHYSICAL_SECURITY | Physical security mechanisms, commensurate with the value of the TOE and the data it contains, are provided by the environment to prevent unauthorised access to the TOE and TSF data. |
| OE.TRUSTED_USERS | TOE users are trusted to use the application in line with the guidance documentation and any applicable enterprise policies. |

# 6 Extended Components Definition (ASE_ECD)

## 6.1 Overview

Neither the TOE nor ST are claiming conformance to any extended requirements from CC Part 2 or CC Part 3.

# 7 Security Functional Requirements (ASE_REQ)

## 7.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (Rev 4) of the CC, Part 2 providing functional requirements and Part 3 providing assurance requirements.

Part 2 of the CC 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 number at the end of the component identifier (e.g. FCS_COP.1(1) and FCS_COP.1(2)).

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

**Table 9 – Security functional requirements**

| Identifier | Title |
|---|---|
| **Audit (FAU)** | |
| FAU_GEN.1 | Audit data generation |
| FAU_GEN.2 | User identity association |
| FAU_STG.1 | Protected audit storage |
| FAU_STG.4 | Prevention of audit data loss |
| **Communication (FCO)** | |
| FCO_NRR.2 | Enforced proof of receipt. |
| **Cryptographic Support (FCS)** | |
| FCS_CKM.1(1) | Cryptographic key generation (RSA) |
| FCS_CKM.1(2) | Cryptographic key generation (AES) |
| FCS_CKM.2 | Cryptographic key distribution (AES) |
| FCS_CKM.4 | Cryptographic key destruction |
| FCS_COP.1(1) | Cryptographic operation (AES) |
| FCS_COP.1(2) | Cryptographic operation (RSA) |
| FCS_COP.1(3) | Cryptographic operation (Signatures) |

| Identifier | Title |
|---|---|
| **User Data Protection (FDP)** | |
| FDP_ACC.1(1) | Subset access control |
| FDP_ACC.1(2) | Subset access control |
| FDP_ACF.1 | Security attribute based access control |
| FDP_RIP.1 | Subset residual information protection |
| **Identification and authentication (FIA)** | |
| FIA_AFL.1 | Authentication failure handling |
| FIA_SOS.1 | Verification of secrets |
| FIA_UAU.2 | User authentication before any action |
| FIA_UAU.7 | Protected authentication feedback |
| FIA_UID.2 | User identification before any action |
| **Security Management (FMT)** | |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.3 | Static attribute initialisation |
| FMT_REV.1 | Revocation |
| FMT_SMF.1(1) | Specification of Management Functions (MEMS) |
| FMT_SMF.1(2) | Specification of Management Functions (GAMMA) |
| FMT_SMR.1 | Security roles |
| **Protection of the TSF (FPT)** | |
| FPT_STM.1 | Reliable time stamps |
| **TOE Access (FTA)** | |
| FTA_SSL.3 | TSF-initiated termination |
| FTA_SSL.4 | User-initiated termination |
| **Trusted path/channels (FTP)** | |
| FTP_ITC.1 | Inter-TSF trusted channel |
| FTP_TRP.1 | Trusted path |

## 7.2 Audit (FAU)

### 7.2.1 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:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the [***not specified***] level of audit; and<br>c)[**the list of auditable events in Table 10 – Auditable events**]. |
| **FAU_GEN.1.2** | The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity ~~(if applicable)~~, and the outcome (success or failure) of the event; and<br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**]. |
| **Notes** | None |

**Table 10 – Auditable events**

| Platform | Auditable events |
|---|---|
| MEMS | Login<br>Contacts: create, read, update and delete<br>Group: create, read, update and delete<br>Lists: create, read, update and delete<br>Message sent/received<br>Licences: grant/revoke/modify<br>Change preferences/settings |
| GAMMA Application | Login<br>Message sent/received |

### 7.2.2 FAU_GEN.2 User identity association

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FAU_GEN.1 Audit data generation<br>FIA_UID.1 Timing of identification |
| **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. |
| **Notes** | None |

### 7.2.3 FAU_STG.1 Protected audit trail storage

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FAU_GEN.1 Audit data generation |
| **FAU_STG.1.1** | The TSF shall protect the stored audit records in the audit trail from unauthorised deletion. |
| **FAU_STG.1.2** | The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail. |
| **Notes** | None |

### 7.2.4 FAU_STG.4 Prevention of audit data loss

| | |
|---|---|
| **Hierarchical to** | FAU_STG.3 Action in case of possible audit data loss |
| **Dependencies** | FAU_STG.1 Protected audit trail storage |
| **FAU_STG.4.1** | The TSF shall [***ignore audited events***] and [**provide the administrator with warnings**] if the audit trail is full. |
| **Notes** | None |

## 7.3 Communication (FCO)

### 7.3.1 FCO_NRR.2 Enforced proof of receipt

| | |
|---|---|
| **Hierarchical to** | FCO_NRR.1 Selective proof of receipt |
| **Dependencies** | FIA_UID.1 Timing of identification |
| **FCO_NRR.2.1** | The TSF shall **enforce the generation of** evidence of receipt for received [**messages sent using the GAMMA application**] at **all times**. |
| **FCO_NRR.2.2** | The TSF shall be able to relate the [**online status field**] of the recipient of the information, and the [**read status field**] of the information to which the evidence applies. |
| **FCO_NRR.2.3** | The TSF shall provide a capability to verify the evidence of receipt of information to [***originator***] given [***the recipient is not in "offline" or "do not disturb" mode***]. |
| **Notes** | None |

## 7.4 Cryptographic Support (FCS)

### 7.4.1 FCS_CKM.1(1) Cryptographic key generation (RSA)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_CKM.1(1).1** | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***RSA GenKey 9.31***] and specified cryptographic key sizes [***2048 bits***] that meet the following: [***FIPS PUB 186-4***]. |
| **Notes** | FIPS PUB 186-4: Digital Signature Standard (DSS) |

### 7.4.2 FCS_CKM.1(2) Cryptographic key generation (AES)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FCS_CKM.2 Cryptographic key distribution, or<br>FCS_COP.1 Cryptographic operation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_CKM.1(1).1** | The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [***PBKDF2***] and specified cryptographic key sizes [***256 bits***] that meet the following: [***NIST SP 800-132***]. |
| **Notes** | NIST SP 800-132: Recommendation for Password-Based Key Derivation |

### 7.4.3 FCS_CKM.2 Cryptographic key distribution (AES)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_CKM.2.1** | The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [***one-time key encrypted with recipient's public key and sent alongside encrypted message***] that meets the following: [***NIST SP 800-56B***]. |
| **Notes** | NIST SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes. Using Integer Factorization Cryptography. |

### 7.4.4 FCS_CKM.4 Cryptographic key destruction

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>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 [***zeroization***] that meets the following: [***none***]. |
| **Notes** | None |

### 7.4.5 FCS_COP.1(1) Cryptographic operation (AES)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_COP.1(1).1** | The TSF shall perform [***encryption and decryption***] in accordance with a specified cryptographic algorithm [***AES in CBC mode***] and cryptographic key sizes [***256 bits***] that meet the following: [***FIPS PUB 197***]. |
| **Notes** | FIPS PUB 197: Advanced Encryption Standard (AES) |

### 7.4.6 FCS_COP.1(2) Cryptographic operation (RSA)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_COP.1(2).1** | The TSF shall perform [***encryption and decryption***] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes [***2048 bits***] that meet the following: [***PKCS #1 v2 (OAEP)***]. |
| **Notes** | N/A |

### 7.4.7 FCS_COP.1(3) Cryptographic operation (Signatures)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FDP_ITC.1 Import of user data without security attributes, or<br>FDP_ITC.2 Import of user data with security attributes, or<br>FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| **FCS_COP.1(3).1** | The TSF shall perform [***digital signatures and signature verification***] in accordance with a specified cryptographic algorithm [***RSA***] and cryptographic key sizes [***2048 bits***] that meet the following: [***FIPS 186-3***]. |
| **Notes** | FIPS PUB 186-3: Digital Signature Standard (DSS) |

## 7.5 User Data Protection (FDP)

### 7.5.1 FDP_ACC.1(1) Subset access control (MEMS)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FDP_ACF.1 Security attribute based access control |
| **FDP_ACC.1(1).1** | The TSF shall enforce the [***access control SFP***] on [<br>• ***Subjects***<br>o ***Administrators***<br>o ***Customer Administrators***<br>• ***Objects***<br>o ***Users***<br>o ***Groups***<br>o ***Lists***<br>o ***Licenses***<br>• ***Operations***<br>o ***Create***<br>o ***Read***<br>o ***Update***<br>o ***Delete***] |
| **Notes** | The TOE uses Uninform Resource Identifiers in tandem with user licensing to determine access to functions. |

### 7.5.2 FDP_ACC.1(2) Subset access control (GAMMA)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FDP_ACF.1 Security attribute based access control |
| **FDP_ACC.1(2).1** | The TSF shall enforce the [***access control SFP***] on [<br>• ***Subjects***<br>o ***GAMMA users***<br>• ***Objects***<br>o ***Contacts***<br>o ***Groups***<br>o ***Messages***<br>• ***Operations***<br>o ***Create***<br>o ***View***<br>o ***Modify***<br>o ***Delete***] |
| **Notes** | The TOE uses Uniform Resource Identifiers in tandem with user licensing to determine access to functions. |

### 7.5.3 FDP_ACF.1 Security attribute based access control

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FDP_ACC.1 Subset access control<br>FMT_MSA.3 Static attribute initialisation |
| **FDP_ACF.1.1** | The TSF shall enforce the [***access control SFP***] to objects based on the following: [***granted license and requested URIs***]. |
| **FDP_ACF.1.2** | The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***a user or administrator is able to access a function if they have a) requested a valid URI and b) their license permits access to that URI***]. |
| **FDP_ACF.1.3** | The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***]. |
| **FDP_ACF.1.4** | The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***]. |
| **Notes** | N/A |

### 7.5.4 FDP_RIP.1 Subset residual information protection

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FDP_RIP.1.1** | The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**deallocation of the resource from**] the following objects: [***user message lists***]. |
| **Notes** | N/A |

## 7.6 Identification and Authentication (FIA)

### 7.6.1 FIA_AFL.1 Authentication failure handling

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FIA_AFL.1.1** | The TSF shall detect when [**3**] unsuccessful authentication attempts occur related to [***authenticating with the GAMMA application***]. |
| **FIA_AFL.1.2** | When the defined number of unsuccessful authentication attempts has been [**surpassed**], the TSF shall [***increase the period of time required between authentication attempts***]. |
| **Notes** | None |

### 7.6.2 FIA_UAU.2 User authentication before any action

| | |
|---|---|
| **Hierarchical to** | FIA_UAU.1 Timing of authentication |
| **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. |
| **Notes** | None |

### 7.6.3 FIA_UAU.7 Protected authentication feedback

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FIA_UAU.1 Timing of authentication |
| **FIA_UAU.7.1** | The TSF shall provide only [***obscured feedback***] to the user while the authentication is in progress. |
| **Notes** | None |

### 7.6.4 FIA_UID.2 User identification before any action

| | |
|---|---|
| **Hierarchical to** | FIA_UID.1 Timing of identification |
| **Dependencies** | None |
| **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. |
| **Notes** | None |

### 7.6.5 FIA_SOS.1 Verification of secrets

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | None |
| **FIA_SOS.1.1** | The TSF shall provide a mechanism to verify that secrets meet:<br>**[GAMMA application: PIN must be four (4) digits**<br>**MEMS/GAMMA portal: Passwords must be at least ten (10) characters long, maximum of sixteen (16). Must include numbers, uppercase and lowercase characters. Cannot have more than three (3) of the same character]** |
| **Notes** | None |

## 7.7 Security management (FMT)

### 7.7.1 FMT_MSA.1 Management of security attributes

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management Functions |
| **FMT_MSA.1.1** | The TSF shall enforce the [***access control SFP***] to restrict the ability to [**modify**] the security attributes [***enable message encryption setting***] to [***customer administrators***]. |
| **Notes** | None |

### 7.7.2 FMT_MSA.3 Static attribute initialisation

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |
| **FMT_MSA.3.1** | The TSF shall enforce the [***access control SFP***] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP. |
| **FMT_MSA.3.2** | The TSF shall allow the [***customer administrator***] to specify alternative initial values to override the default values when an object or information is created. |
| **Notes** | None |

### 7.7.3 FMT_REV.1 Revocation

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | FMT_SMR.1 Security roles |
| **FMT_REV.1.1** | The TSF shall restrict the ability to revoke [***licenses***] associated with the [**users**] under the control of the TSF to [***customer administrators***]. |
| **FMT_REV.1.2** | The TSF shall enforce the rules [***none***]. |
| **Notes** | None |

### 7.7.4 FMT_SMF.1(1) Specification of Management Functions (MEMS)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FMT_SMF.1(1).1** | The TSF shall be capable of performing the following management functions: [<br>• ***Manage users;***<br>• ***Manage lists;***<br>• ***Manage groups;***<br>• ***Wipe/revoke messages;***<br>• ***Generate message metadata reports;***<br>• ***Change personal information;***<br>• ***Grant/revoke licenses for the GAMMA application;***<br>• ***Modify preferences/general settings; and***<br>• ***Enable/disable secure messaging***]. |
| **Notes** | None |

### 7.7.5 FMT_SMF.1(2) Specification of Management Functions (GAMMA)

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FMT_SMF.1(2).1** | The TSF shall be capable of performing the following management functions: [<br>• ***Send/receive messages;***<br>• ***Manage groups; and***<br>• ***Configure application settings***]. |
| **Notes** | None |

### 7.7.6 FMT_SMR.1 Security roles

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FMT_SMR.1.1** | The TSF shall maintain the roles [***customer administrator, administrator, user***]. |
| **FMT_SMR.1.2** | The TSF shall be able to associate users with roles. |
| **Notes** | None |

## 7.8 Protection of the TSF (FPT)

### 7.8.1 FPT_STM.1 Reliable time stamps

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FPT_STM.1.1** | The TSF shall be able to provide reliable time stamps. |
| **Notes** | None |

## 7.9 TOE Access (FTA)

### 7.9.1 FTA_SSL.3 TSF-initiated termination

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FTA_SSL.3.1** | The TSF shall terminate an interactive session after a [***30 minute period of inactivity***]. |
| **Notes** | None |

### 7.9.2 FTA_SSL.4 User-initiated termination

| | |
|---|---|
| **Hierarchical to** | No other components |
| **Dependencies** | No dependencies |
| **FTA_SSL.4.1** | The TSF shall allow user-initiated termination of the user's own interactive session. |
| **Notes** | None |

## 7.10 Trusted path/channels (FTP)

### 7.10.1 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 [***the TSF***] to initiate communication via the trusted channel. |
| **FTP_ITC.1.2** | The TSF shall initiate communication via the trusted channel for [**all communication between the GAMMA application, GAMMA server, MEMS platform and GAMMA registration server**]. |
| **Notes** | None |

### 7.10.2 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 [**the TSF, 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,** [***transmission of messages, all administrative actions***]]. |
| **Notes** | None |

## 7.11 Security assurance requirements

**Table 11 – Security assurance requirements**

| Assurance class | Assurance component |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.2 Security-enforcing functional specification |
| | ADV_TDS.1 Basic design |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | AGD_PRE.1 Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.2 Use of a CM system |
| | ALC_CMS.2 Parts of the TOE CM coverage |
| | ALC_DEL.1 Delivery procedures |
| 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.1 Evidence of coverage |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing – sample |
| AVA: Vulnerability assessment | AVA_VAN.2 Vulnerability analysis |

# 8 TOE summary specification (ASE_TSS)

## 8.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

## 8.2 Audit

The TOE provides an audit capability that will generate an audit log entry when the following events occur:

- MEMS – Login
- MEMS – Contact CRUD
- MEMS – Group CRUD
- MEMS – List CRUD
- MEMS – Message sent/received
- MEMS – License granting/revoking/modification
- MEMS – Configuration and preference changes
- GAMMA – Login
- GAMMA – Message sent/received

When generating an audit log, the TOE will record the ID of the user/process that caused the log to be generated, the date/time, success/failure of the event and any other pertinent information (FAU_GEN.1, FAU_GEN.2)

Audit data is provided to administrators in a read-only format via the web browser – administrators may not modify or change any audit logs once they have been generated and stored by the TOE (FAU_STG.1). The TOE will store audit data and, if the storage capacity for stored audit logs is met, will ignore new auditable events to prevent the deletion of existing log data and provide the administrator with warnings until additional storage capacity is made available (FAU_STG.4).

The TOE generates its own timestamps which are used during the generation of audit logs. These timestamps are generated using the time source of the underlying operating system (FPT_STM.1).

## 8.3 Communication

The TOE provides proof-of-receipt for messages sent using the GAMMA application. Each sent message is assigned a status – sending, sent, delivered and read. The TOE will track the status of each message and, unless the recipient is set to “Do Not Disturb” or is appearing offline, will update the status to reflect when the message has been read. This is also done on a per-user basis when in group conversations (FCO_NRR.2).

## 8.4 Cryptographic Support

The TOE generates cryptographic keys for its own use. The following key generation functionalities are implemented and utilised (FCS_CKM.1(1), FCS_CKM.1(2)):

- Generation of 2048-bit RSA keys using the PKCS#1 v1.5 method, in accordance with FIPS PUB 186-4 (Digital Signature Standard); and
- Generation of 256-bit AES keys using PBKDF2 (Password-Based Key Derivation Function 2), in accordance with NIST SP 800-132: Recommendation for Password-Based Key Derivation

The keys generated by the TOE are used in the following cryptographic functions (FCS_COP.1(1), FCS_COP.1(2)):

- AES-CBC-256 (in accordance with FIPS PUB 197) is used for the encryption and decryption of messages sent between GAMMA users. The encrypted message, along with a generated shared secret, is delivered to the recipient to allow for the secure delivery and decryption of messages; and
- 2048-bit RSA (in accordance with PKCS #1 v2.0 with Optional Asymmetric Encryption Padding (OAEP)) is used for the encryption of the aforementioned shared secret. If a single message has more than a single recipient, the shared secret used is encrypted using a different RSA key for each recipient.

The TOE distributes keys via the following method (FCS_CKM.2):

- For each message to be encrypted and sent, the TOE generates a one-time cryptographic key (per recipient);
- The message is encrypted using the one-time key;
- The one-time key is then encrypted using the public key of the recipient; and
- Both the encrypted message and encrypted key are then bundled together and delivered to the recipient.

The TOE also generates and verifies digital signatures using RSA in accordance with FIPS 186-3 (FCS_COP.1(3)).

Both the encrypted message payload and encrypted shared secret are bundled together and sent, via a secure TLS channel, to the GAMMA server. Once received by the GAMMA server, the encrypted messages and keys are then passed on to their intended recipients (which may be between one and fifty (50) users, depending on size of the enterprise, group settings, etc.).

If a message is sent to be sent to more than one recipient, a unique shared secret is generated and used for each user.

The TOE will, when no longer requiring them, destroy cryptographic keys and other sensitive cryptographic material so they can no longer be used. As keys and CSPs are used persistently while the TOE is installed, zeroization is performed when the application is uninstalled or the user's phone is factory reset/wiped (FCS_CKM.4).

## 8.5 Data Protection

The MEMS platform implements a licensing system to prevent administrators/customer administrators from gaining access to functions or TSF data that they are not permitted to access.

Each license specifies a set of Uniform Resource Indicators (URIs) that the administrative user is permitted to access. Upon requesting a URI from the MEMS server, the TOE will compare the requested URI to the list of permitted functions in the administrator's license. If there is a match, access to the function/data is permitted. If the administrator does not have permission to access the functions/data, the TOE will return an error and deny access (FDP_ACC.1(1), FDP_ACF.1).

The GAMMA application uses the same mechanism for controlling access to functions – each user is allocated a license with a specific set of URIs. The user requests these URIs

by navigating through the application and, if access is permitted, the TOE will provide the user with access to the TOE functionality and TSF data (FDP_ACC.1(2)).

Users may revoke (remote wipe) messages if they no longer wish them to be available to recipients once they have been delivered. Users must log in to the GAMMA portal and navigate to the GAMMA -> Remote Wipe menu. Users may then choose to revoke a single message, a set of messages based on search criteria or all messages that they have sent to a destination device (FDP_RIP.1).

## 8.6 Identification and Authentication

Both GAMMA and MEMS users must successfully identify themselves and authenticate with the TOE prior to being given access to any TOE functionality or TSF data. On the GAMMA application, this is done via a four-digit PIN set during initial application configuration. The MEMS platform requires a username and password combination prior to any access being granted (FIA_UAU.2, FIA_UID.2).

The TOE provides only obscured feedback (i.e. asterisks or other blocking characters) to TOE users while authentication is in progress (FIA_UAU.7).

After 3 failed authentication attempts, the TOE will increase the period of time required before the user may re-attempt authentication. This period of time increases exponentially with each failed authentication attempt and this prevents brute-forcing of the TOE's authentication mechanisms (FIA_AFL.1).

The GAMMA application requires the users to set a 4 digit PIN for authentication. Passwords for the GAMMA server/MEMS must be 8-16 characters, comprised of upper/lowercase characters and numbers and cannot have more than three of the same character (FIA_SOS.1).

## 8.7 Security management

The TOE provides three (3) different roles for users of the TOE (FMT_SMR.1):

- **Users:** Standard users of the GAMMA application;
- **Administrators:** Have access to a subset of MEMS functionality to allow them to administer the instance of MEMS and GAMMA used by their enterprise; and
- **Customer Administrators:** Have full access to manage their provisioning of MEMS and GAMMA. Customer administrators are the only role with the ability to revoke user licenses and to enable/disable the message encryption function provided by the TOE.

Customer administrators and Administrators have access to the following management functionality via the MEMS platform (FMT_SMF.1(1)):

- Management (creation, modification and deletion) of individual users, groups and messaging lists;
- Send/receive messages to users/groups/lists;
- Change personal information;
- Remote wipe of delivered messages;
- Report on historical message metadata;
- Granting and revoking of user licenses for GAMMA (FMT_REV.1);

- Enabling/disabling of the message encryption function (FMT_MSA.1); and
- Modify preferences/general settings.

Objects may contain default values upon their creation (such as licenses). The TOE allows customer administrators to specify alternate values to meet their requirements (FMT_MSA.3).

Users have access to the following functionality on the GAMMA app and GAMMA portal (FMT_SMF.1(2)):

- Send/receive messages to users/groups/lists;
- Manage groups; and
- Configure application settings.

## 8.8 TOE Access

The TOE will automatically close MEMS sessions after a thirty (30) minute period of inactivity. (FTA_SSL.3). GAMMA sessions continue to run until the user closes the application.

TOE users may close their sessions manually by logging out of the platform (MEMS) or closing the application (GAMMA) (FTA_SSL.4).

## 8.9 Trusted path/channels

The TOE implements Transport Layer Security (TLS) to provide a secure channel between its distributed components. As indicated in Figure 1 - Soprano GAMMA architecture, TLS is used to provide a trusted channel between the MEMS platform and any connected enterprise applications or administrators, GAMMA server, registration server and instances of the GAMMA application on individual mobile devices (FTP_ITC.1, FTP_TRP.1).

# 9 Rationale

## 9.1 Security objectives rationale

The security objectives rationale is provided to demonstrate that the identified threats are countered and the assumptions are met.

### 9.1.1 Threat/OSP rationale

The following table provides a mapping of threats to objectives and adequate justification for the mapping.

**Table 12 – Threats to objectives mapping**

| Threat | Objective | Justification |
|---|---|---|
| T.EAVESDROPPING | O.PROTECTED_COMMS<br>O.CRYPTO | The threat of a malicious internal or external user intercepting traffic sent between components of the TOE is mitigated by:<br>**O.CRYPTO:** This objective ensures that the TOE uses cryptographic methods (i.e. encryption) of sufficient strength to prevent decryption in a feasible time period by a third party.<br>**O.PROTECTED_COMMS:** The TOE utilises its cryptographic library to secure data sent between components of the TOE both in transit and at rest. |
| T.REQUEST | O.AUTH_CONTROL<br>O.WIPE<br>O.SESSION_LOCK | The threat of a malicious user gaining unauthorized access to TOE data/resources is mitigated by:<br>**O.AUTH_CONTROL:** The TOE implements mechanisms to prevent the brute-forcing of identification and authentication methods.<br>**O.WIPE:** The TOE provides the capability for users to wipe sent/received messages, deleting them from the GAMMA application and preventing users from accessing the data.<br>**O.SESSION_LOCK:** The TOE will automatically lock sessions after a pre-determined period of time to prevent accidental or malicious use of an unattended session. |
| T.WEAK_CRYPTO | O.CRYPTO | The threat of weak cryptographic methods that provide insufficient security is mitigated by:<br>**O.CRYPTO:** The TOE implements a suite of FIPS 140-2 approved cryptographic methods, ensuring that sufficient strength is provided for the protection of data both in transit and at rest. |

| Threat | Objective | Justification |
|---|---|---|
| T.UNAUTHORISED_ACCESS | O.AUDIT_REVIEW<br>O.AUTH_CONTROL<br>O.AUTH<br>O.SESSION_LOCK | The risk of a malicious (or other) user gaining access to the TOE is mitigated by:<br>**O.AUDIT_REVIEW:** The TOE provides access to audit records for tracking of both user and administrator actions.<br>**O.AUTH_CONTROL:** The TOE implements mechanisms to prevent the brute-forcing of identification and authentication methods.<br>**O.AUTH:** The TOE implements mechanisms requiring users to successfully authenticate with the TOE before they are permitted access to TSF data and functionality.<br>**O.SESSION_LOCK:** The TOE implements session timeouts to prevent accidental or malicious use of another users session that has been left unattended. |

### 9.1.2 Assumption/objectives rationale

The following table provides a mapping of the security objectives for the environment and their relevant assumptions, as well as a justification for the mapping.

**Table 13 – Assumptions to objectives mapping**

| Assumption | Objective | Justification |
|---|---|---|
| A.ACCEPTABLE_USE | OE.TRUSTED_USERS | The objective is a direct instantiation of the assumption and is therefore met. |
| A.LOGICAL_PROTECT | OE.LOGICAL_SECURITY | The objective is a direct instantiation of the assumption and is therefore met. |
| A.INSTALL | OE.INSTALL | The objective is a direct instantiation of the assumption and is therefore met. |
| A.NO_EVIL | OE.NO_EVIL | The objective is a direct instantiation of the assumption and is therefore met. |
| A.PHYSICAL_PROTECT | OE.PHYSICAL_SECURITY | The objective is a direct instantiation of the assumption and is therefore met. |
| A.UNTRUSTED | OE.APPS | The objective is a direct instantiation of the assumption and is therefore met. |

## 9.2 Security requirements rationale

### 9.2.1 Tracing of SFRs to security objectives

**Table 14 – SFR to objectives mapping**

| Objective | SFR | Demonstration |
|---|---|---|
| O.AUDIT_REVIEW | FAU_GEN.1<br>FAU_GEN.2<br>FAU_STG.1<br>FAU_STG.4<br>FPT_STM.1 | FAU_GEN.1 generates audit records for a set of auditable events.<br>FAU_GEN.2 associates each audit log with a specific user.<br>FAU_STG.1 ensures that audit storage is protected against modification and/or deletion.<br>FAU_STG.4 ensures that the administrator is given warnings when storage space for audit logs has been filled.<br>FPT_STM.1 ensures that accurate timestamps are used when the TOE generates audit logs. |
| O.AUTH | FIA_UAU.7<br>FIA_UID.2<br>FIA_UAU.2 | FIA_UAU.7: The TOE provides obscured feedback to users while authentication is underway.<br>FIA_UID.2 and FIA_UAU.2: The TOE requires users to be successfully identified and authenticated prior to giving access to TSF data and TOE functions.<br>FMT_SMF.1(1) and FMT_SMF.1(2) defines the functionality available to authenticated users of the TOE.<br>FMT_SMR.1 defines the roles that can be assumed by TOE users.<br>FDP_ACC.1(1), FDP_ACC.1(2), FDP_ACF.1, FMT_MSA.1 and FMT_MSA.3 define the access control mechanisms used to determine the functions available to TOE users depending on their role |
| O.AUTH_CONTROL | FIA_AFL.1 | FIA_AFL.1: The TOE will restrict user access to authentication methods after a defined number of failed authentication attempts. |

| Objective | SFR | Demonstration |
|---|---|---|
| O.CRYPTO | FCS_CKM.1(1)<br>FCS_CKM.1(2)<br>FCS_CKM.2<br>FCS_CKM.4<br>FCS_COP.1(1)<br>FCS_COP.1(2)<br>FCS_COP.1(3) | FCS_CKM.1(1): The TOE generates cryptographic keys in accordance with an approved standard.<br>FCS_CKM.1(2): The TOE generates cryptographic keys in accordance with an approved standard.<br>FCS_CKM.2: The TOE distributes cryptographic keys in accordance with an approved key distribution method.<br>FCS_CKM.4: The TOE destroys cryptographic keys when they are no longer needed.<br>FCS_COP.1(1): The TOE performs cryptographic operations in accordance with an approved standard.<br>FCS_COP.1(2): The TOE performs cryptographic operations in accordance with an approved standard.<br>FCS_COP.1(3): The TOE performs cryptographic operations in accordance with an approved standard. |
| O.PROTECTED_COMMS | FTP_ITC.1<br>FTP_TRP.1 | FTP_ITC.1 and FTP_TRP.1 : The TOE establishes a secure channel between its distributed components and any connected users/applications to protect data against disclosure or modification. |
| O.SESSION_LOCK | FTA_SSL.3<br>FTA_SSL.4 | FTA_SSL.3: The TOE will automatically close a user session after a defined period of non-activity.<br>FTA_SSL.4: The TOE allows the user to manually close their active session. |
| O.WIPE | FMT_REV.1<br>FDP_RIP.1<br>FCO_NRR.2 | FMT_REV.1: TOE users can remotely wipe/revoke messages sent to other TOE users.<br>FDP_RIP.1: The TOE ensures that wiped messages are removed from user message lists.<br>FCO_NRR.2: The TOE provides users with information regarding the delivery status of their message (sent, delivered, read). |

### 9.2.2 Dependency analysis

The following table provides a dependency analysis for the SFRs chosen within this security target. For SFRs that have not been included a rationale is provided after the table.

**Table 15 – SFR dependency analysis**

| SFR | Dependencies | Dependency met? |
|---|---|---|
| FAU_GEN.1 Audit data generation | FPT_STM.1 Reliable time stamps | Yes |
| FAU_GEN.2 User identity association | FAU_GEN.1 Audit data generation | Yes |
| | FIA_UID.1 Timing of identification | Yes |
| FAU_STG.1 Protected audit storage | FAU_GEN.1 Audit data generation | Yes |
| FAU_STG.4 Prevention of audit data loss | FAU_STG.1 Protected audit trail storage | Yes |
| FCO_NRR.2 Enforced proof of receipt. | FIA_UID.1 Timing of identification | Yes |
| FCS_CKM.1(1) Cryptographic key generation (RSA) | FCS_CKM.2 Cryptographic key distribution, **or**<br>FCS_COP.1 Cryptographic operation | Yes, met by FCS_COP.1(2) |
| | FCS_CKM.4 Cryptographic key destruction | Yes |
| FCS_CKM.1(2) Cryptographic key generation (AES) | FCS_CKM.2 Cryptographic key distribution, **or**<br>FCS_COP.1 Cryptographic operation | Yes, met by FCS_CKM.2 and FCS_CKM.1(1) |
| | FCS_CKM.4 Cryptographic key destruction | Yes |
| FCS_CKM.2 Cryptographic key distribution (AES) | FDP_ITC.1 Import of user data without security attributes, **or**<br>FDP_ITC.2 Import of user data with security attributes, **or**<br>FCS_CKM.1 Cryptographic key generation | Yes, met by FCS_CKM.1(2) |
| | FCS_CKM.4 Cryptographic key destruction | Yes |
| FCS_CKM.4 Cryptographic key destruction | FDP_ITC.1 Import of user data without security attributes, **or**<br>FDP_ITC.2 Import of user data with security attributes, **or**<br>FCS_CKM.1 Cryptographic key generation | Met by FCS_CKM.1(1) and (2) |

| SFR | Dependencies | Dependency met? |
|---|---|---|
| FCS_COP.1(1) Cryptographic operation (AES) | FDP_ITC.1 Import of user data without security attributes, **or**<br>FDP_ITC.2 Import of user data with security attributes, **or**<br>FCS_CKM.1 Cryptographic key generation | Met by FCS_CKM.1(2) |
| | FCS_CKM.4 Cryptographic key destruction | Yes |
| FCS_COP.1(2) Cryptographic operation (RSA) | FDP_ITC.1 Import of user data without security attributes, **or**<br>FDP_ITC.2 Import of user data with security attributes, **or**<br>FCS_CKM.1 Cryptographic key generation | Met by FCS_CKM.1(1) |
| | FCS_CKM.4 Cryptographic key destruction | Yes |
| FCS_COP.1(2) Cryptographic operation (Signatures) | FDP_ITC.1 Import of user data without security attributes, **or**<br>FDP_ITC.2 Import of user data with security attributes, **or**<br>FCS_CKM.1 Cryptographic key generation | Met by FCS_CKM.1(1) |
| | FCS_CKM.4 Cryptographic key destruction | Yes |
| FDP_ACC.1(1) Subset access control | FDP_ACF.1 Security attribute based access control | Yes |
| FDP_ACC.1(2) Subset access control | FDP_ACF.1 Security attribute based access control | Yes |
| FDP_ACF.1 Security attribute based access control | FDP_ACC.1 Subset access control | Met by FDP_ACC.1(1) and (2) |
| | FMT_MSA.3 Static attribute initialisation | Yes |
| FDP_RIP.1 Subset residual information protection | None | N/A |
| FIA_AFL.1 Authentication failure handling | FIA_UAU.1 Timing of authentication | Met by FIA_UAU.2 |
| FIA_SOS.1 Verification of secrets | None | N/A |
| FIA_UAU.2 User authentication before any action | FIA_UID.1 Timing of identification | Met by FIA_UID.2 |
| FIA_UAU.7 Protected authentication feedback | FIA_UAU.1 Timing of authentication | Met by FIA_UAU.2 |
| FIA_UID.2 User identification before any action | None | N/A |

| SFR | Dependencies | Dependency met? |
|---|---|---|
| FMT_MSA.1 Management of security attributes | FDP_ACC.1 Subset access control, **or**<br>FDP_IFC.1 Subset information flow control | Met by FDP_ACC.1(1) and (2) |
| | FMT_SMR.1 Security roles | Yes |
| | FMT_SMF.1 Specification of Management Functions | Met by FMT_SMF.1(1) |
| FMT_MSA.3 Static attribute initialisation | FMT_MSA.1 Management of security attributes | Yes |
| | FMT_SMR.1 Security roles | Yes |
| FMT_REV.1 Revocation | FMT_SMR.1 Security roles | Yes |
| FMT_SMF.1(1) Specification of Management Functions (MEMS) | None | N/A |
| FMT_SMF.1(2) Specification of Management Functions (GAMMA) | None | N/A |
| FMT_SMR.1 Security roles | FIA_UID.1 Timing of identification | Met by FIA_UID.2 |
| FPT_STM.1 Reliable time stamps | None | N/A |
| FTA_SSL.3 TSF-initiated termination | None | N/A |
| FTA_SSL.4 User-initiated termination | None | N/A |
| FTP_ITC.1 Inter-TSF trusted channel | None | N/A |
| FTP_TRP.1 Trusted path | None | N/A |

## 9.3 Security assurance requirements justification

The assurance package for the evaluation is Evaluation Assurance Level 2 (EAL2).

EAL2 assurance requirements provide confidence in the security functionality of the TOE by analysis using a functional and interface specification, guidance documentation and the high-level design of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities.

EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.