Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Soprano GAMMA

Certification Report
2016/99

17 May 2016
Version 1.0

Amendment Record

Version	Date	Description
1.0	17 May 2016	Final

Executive Summary

This report describes the findings of the IT security evaluation of Soprano GAMMA v3.0.9 (CC) against Common Criteria.

The Target of Evaluation (TOE) is Soprano GAMMA. The TOE is a product that is designed to send and receive messages on both the Google Android and Apple iOS platforms. Both the GAMMA server and MEMS server can be deployed either in an open cloud or a private cloud setting.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **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. 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
- **Cryptological 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
- **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.

The report concludes that the product has complied with the Evaluation Assurance Level (EAL) 2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Systems Applied Intelligence and was completed on 22 March 2016.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) Do not click external links while actively logged in to the MEMS platform.
e) Ensure that the operating system that the MEMS platform is operating on, has all relevant security updates applied to it. Additionally a server hardening program for the chosen OS should be run in order to ensure no easily exploitable vulnerabilities are exposed
f) Configure the MEMS to ensure a minimum password length as per the requirements of the ISM
g) Ensure that when connecting to the MEMS web app, users use a browser capable of connecting with the latest versions of TLS
h) Disable any unused services like FTP and SMTP.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

This page is left intentionally blank

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Soprano GAMMA against the requirements of the Common Criteria (CC), Evaluation Assurance Level (EAL) 2

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 1) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is Soprano GAMMA

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Soprano GAMMA
Software Version	Soprano GAMMA for iOS (Version 3.0.9 (CC)) Soprano GAMMA for Android (Version 3.0.9 (CC)) Soprano GAMMA Server (Version b473) Soprano GAMMA Registration Server (Version b1) Soprano Mobile Enterprise Messaging Suite (MEMS) (Version b649)
Hardware Platforms	iPhone 6 Model: OS version: 8.4.1 iPhone 6 Plus Model: MGCM2LL/AOS version: 8.4.1 HTC One M9 Samsung Galaxy S6 Model: SM-G920I OS

	version: 5.1.1
Security Target	Soprano GAMMA Security Target Version 1.1, 04 May 2016
Evaluation Technical Report	Evaluation Technical Report Soprano GAMMA, v1.0 dated 10 May 2016 Document reference EFS –T040 ETR
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Conformant, September 2012, Version 3.1.Rev4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev4
Conformance	EAL 2
Sponsor	Parliament of Victoria (contact-Marshall Lee) 55 St Andrews Place East Melbourne Victoria 3002 Australia
Developer	Soprano Design Pty Ltd Level 11, 132 Arthur St North Sydney NSW 2060 Australia
Evaluation Facility	BAE Systems Applied Intelligence Level 1, 14 Childers Street, Canberra, ACT, 2601 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The TOE is Soprano GAMMA v3.0.9 (CC). The TOE is a product that is designed to send and receive messages on both the Google Android and Apple iOS platforms. Both the GAMMA server and MEMS server can be deployed either in an open cloud or a private cloud setting.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **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. 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
- **Cryptological 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
- **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

2.4 TOE Architecture

The TOE consists of the following major architectural 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.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies. The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Soprano CC Guidance document (Ref 2). The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

Functionalities evaluated are as follows:

- Security Audit
- Communication
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 4) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

The following components are considered outside of the scope of the TOE:

- 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).

2.6 Security

2.6.1 Security Policy

There was no organisational security policies defined in the Security Target.

2.7 Usage

2.7.1 Evaluated Configuration

- The TOE consists of the Soprano Gamma. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Soprano CC Guidance document (Ref 2).

2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- You (or your designated Customer Administrator) may request a GAMMA installation URL from Soprano. This URL, when opened on your target device, will connect to the Soprano servers and automatically download the package file for the GAMMA application. **Note:** Android users may be required to temporarily allow the installation of non-market applications to complete the TOE installation. To allow this, navigate to ‘Settings > Lock Screen and Security’ and check the “Unknown sources” box.
- Alternatively, a Mobile Device Management (MDM) platform may be used for deployment of the application if required by your enterprise security settings/device configuration. Once the application has been downloaded, your Android or iOS operating system will automatically run checks against the downloaded application to determine whether the download has been tampered with in any way. If for some reason this check fails, please notify

your system administrator (who may need to contact Soprano Design). If the downloaded package passes the Android/IOS integrity checks, the installation process will begin.

- Once the application has been installed and initialised for the first time, you will be prompted to either automatically enrol with the GAMMA servers or to enter a registration key. Please contact your GAMMA administrator for your key, or automatically enrol if instructed to do so. Once server registration is complete (via SMS or the entry of a pre-made key), you will be prompted to complete configuration of the application. This includes setting a four-digit PIN to be used for authentication. Ensure that your PIN is unique (not used elsewhere – bank cards, etc.) and do not share it with any other person.

2.7.3 Installation of the TOE

The guidance documentation (Ref 2) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

To verify the version of the GAMMA application, perform the following actions:

- Android: From the main screen, click the Menu button and go to Settings. In the resultant screen, click Settings. The version number is listed under "GAMMA Version"
- iOS: From the main screen, click Edit. The version number is listed under "Gamma Version".

To verify the build of the MEMS platform, perform the following:

- Access the MEMS platform via your web browser of choice
- View the source code for the page
- Look for references to /static_bxxx (where "xxx" is a three-digit number). These references may be in CSS link tags or in Javscript script tags in the head of the page. The three-digit number found above is the MEMS build number
- Additional automatic verification is run by the iOS or Android operation system which will notify the user in case of a failure.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased: Soprano CC Guidance document (Ref 2). All Common Criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

No assumptions were noted in the testing documentation or the resultant reports.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Ref 5 and 6).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 3).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 7) were also upheld. The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from Soprano CC Guidance document (Ref 2).

3.3 Testing

3.3.1 Testing Coverage

The evaluators have examined the provided developer test documentation and found that it shows the correspondence between the tests present in the test documentation and the TSFIs identified within the functional specification. Furthermore, the Evaluator repeated a subset of developer's tests as well as performing functional and vulnerability tests developed by the Evaluator.

3.3.2 Test phases

Testing is determined in the assurance activities in the CEM. The evaluation was conducted during the period between the 25th of February 2016 and the 10th of March 2016.

3.4 Penetration Testing

The evaluators performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

The CC provides assurance through active investigation. Active investigation is an evaluation of the IT product in order to determine its security properties.Whilst some potential vulnerabilities have been discovered by the evaluator whilst conducting penetration testing they were deemed to require greater than a basic attack potential or out of scope of the TOE itself.

Issues were identified in the underlying operational environment of the web app portion of the TOE. Whilst potentially allowing denial of service attacks against the underlying operating system they could be solved through proper configuration and maintenance and do not expose the TOE itself. These underlying problems have been brought to the attention of the developer. Additional information on the potential vulnerabilities is available upon request.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with EAL 2. Agencies can have confidence that the scope of an evaluation against an EAL 2 covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

4.3 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref 8) the Australasian Certification Authority **certifies** the evaluation of the Soprano GAMMA product performed by the Australasian Information Security Evaluation Facility, BAE Systems Applied Intelligence.

BAE Systems Applied Intelligence **has determined** that Soprano GAMMA upholds the claims made in the Security Target (Ref 1) and **has met** the requirements of the Common Criteria (CC) evaluation assurance level EAL2.

The analysis is supported by testing as outlined in the CEM assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.4 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 4) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) Do not click external links while actively logged in to the MEMS platform
e) Ensures that the operating system that the MEMS platform is operating on, has all relevant security updates applied to it. Additionally a server hardening program for the chosen OS should be run in order to ensure no easily exploitable vulnerabilities are exposed
f) Configure the MEMS to ensure a minimum password length as per the requirements of the ISM
g) Ensure that when connecting to the MEMS web app, users use a browser capable of connecting with the latest versions of TLS
h) Disable any unused services like FTP and SMTP.

Annex A – References and Abbreviations

A.1 References

1. Security Target – Soprano GAMMA ,04 May 2016 v 1.1

2. Guidance Documentation:

   - Soprano CC Guidance 1.1, 29 April 2016

   - Guidance – Soprano GAMMA Product Manual for A2P & P2P deployments v3.0, August 2015

3. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4

4. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

5. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012, Version 3.1 Revision 4

6. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4

7. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014

8. Evaluation Technical Report Soprano GAMMA v1.0, 10 May 2016

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CSRF	Cross Site Request Forgery
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
ISM	Information Security Manual
MEMS	Mobile Enterprise Messaging Suite
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interfaces
TSP	TOE Security Policy