COMMON CRITERIA GUIDANCE
SOPRANO GAMMA 4.1

Reference	GAMMA-4.1-AGD	Status	Released
Version	1.0	Release Date	1 March 2018
Owner	Soprano Design Pty Ltd	Pages	8 (Including Cover)

LIST OF CONTENTS

DOCUMENT INFORMATION

1.1 Amendment history

Version	Date	Revisions
0.1	1 March 2018	Initial draft
1.0	1 March 2018	Initial release

1.2 Copyright statement

2 INTRODUCTION

This document provides supplementary user and administrator guidance for Soprano Design customers using the Common Criteria evaluated version of the Soprano GAMMA product.

This document should be used in tandem with the GAMMA Product Manual (August 2015) to ensure that the GAMMA product is configured in accordance with the CC evaluated configuration and used in a secure manner.

This document is divided in to the following sections:

- **Section 3- Deployment Process** describes the procedure for downloading and installing the GAMMA application and gaining access to the web portal; and
- **Section 4**Error! Reference source not found. **- Using GAMMA** provides additional guidance on steps that can be taken to ensure that the product is being used securely.

2.1 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

[5] Security Target – Soprano GAMMA 4.1, Version 1.1, 1 March 2018

[6] GAMMA Product Manual for A2P & P2P Deployments, Version 3.0, August 2015

3 DEPLOYMENT PROCESS

3.1 Secure delivery

Soprano GAMMA is provided as two platforms for you to access:

- The Soprano GAMMA **application**, which is compatible with Android and iOS devices; and
- The Soprano GAMMA **MEMS platform**, which provides a variety of GAMA functionality, and allows you (or your designated administrator) to manage your instance of the GAMMA suite.

The following sections describe the steps you can take to ensure that you are accessing the correct (and evaluated) version of the GAMMA application and MEMS platform.

3.2 Downloading and installing the GAMMA application

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 PIN of between 4 and 8 alphanumeric characters 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.

3.3 Accessing the MEMS platform

See also: "Administrative Setup" chapter of the GAMMA Product Manual

Once initial provisioning by Soprano support staff is complete, your designated customer administrator will be sent an email from Soprano with a username and temporary password to log in to the MEMS platform. The authenticity of this email can be verified by examining the headers of the email address and by contacting Soprano directly (via phone) to confirm.

Access the web portal via the URL provided – the authenticity of the platform can be verified by examining the URL and the certificate used to provide a secure connection between your device and the remote platform.

Once authenticated, follow the steps in the GAMMA Product Manual to configure your instance of GAMMA. Ensure that:

- You enable the “Require Encryption” option to place the instance into Common Criteria evaluated mode; and
- The option to allow application users to skip setting a PIN is not enabled at any time.

Standard users can access the GAMMA web portal via a URL provided to them by their administrative users. A username and password must be set for these accounts that meets the following criteria:

- At least eight (8) characters long, maximum of sixteen (16);
- Must include numbers, uppercase and lowercase characters; and
- Cannot have more than three (3) of the same character

4 USING GAMMA

4.1 General usage advice

In order to ensure that you are using the GAMMA application securely, it is important to keep the following guidance in mind when using either the GAMMA application or the web portal:

- Comply with any enterprise policies for device management or acceptable use that may be in place.
- Ensure that the “Require Encryption” option is enabled within MEMS. This option must be enabled for the device to be operating in its Common Criteria evaluated configuration;
- Do not enable the option for application users to skip setting an application PIN at any time;
- Do not disclose your PIN or password to anyone, even your own enterprise administrators;
- Do not leave your devices unattended – ensure that your mobile device is set to automatically lock the screen and has a PIN/other authentication mechanism enabled; and
- If using Android, ensure that the “Block Untrusted Sources” option is enabled to prevent the installation of applications (this includes custom device ROMs) that may undermine the security of your device.
    - **Note:** Disabling this option may be required for initial installation of the TOE and should be re-activated immediately.

4.2 Audit records

Not all auditable events defined in the GAMMA Security Target (see FAU_GEN.1) are presented as explicit audit log records. Some records (such as the User, Group and List CRUD records) are presented on the page for each individual user/group/list instead of being included in the system audit trail.

4.3 Verify product version

Verification of TOE version

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”.

Verification of MEMS build

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.

--- END OF DOCUMENT ---