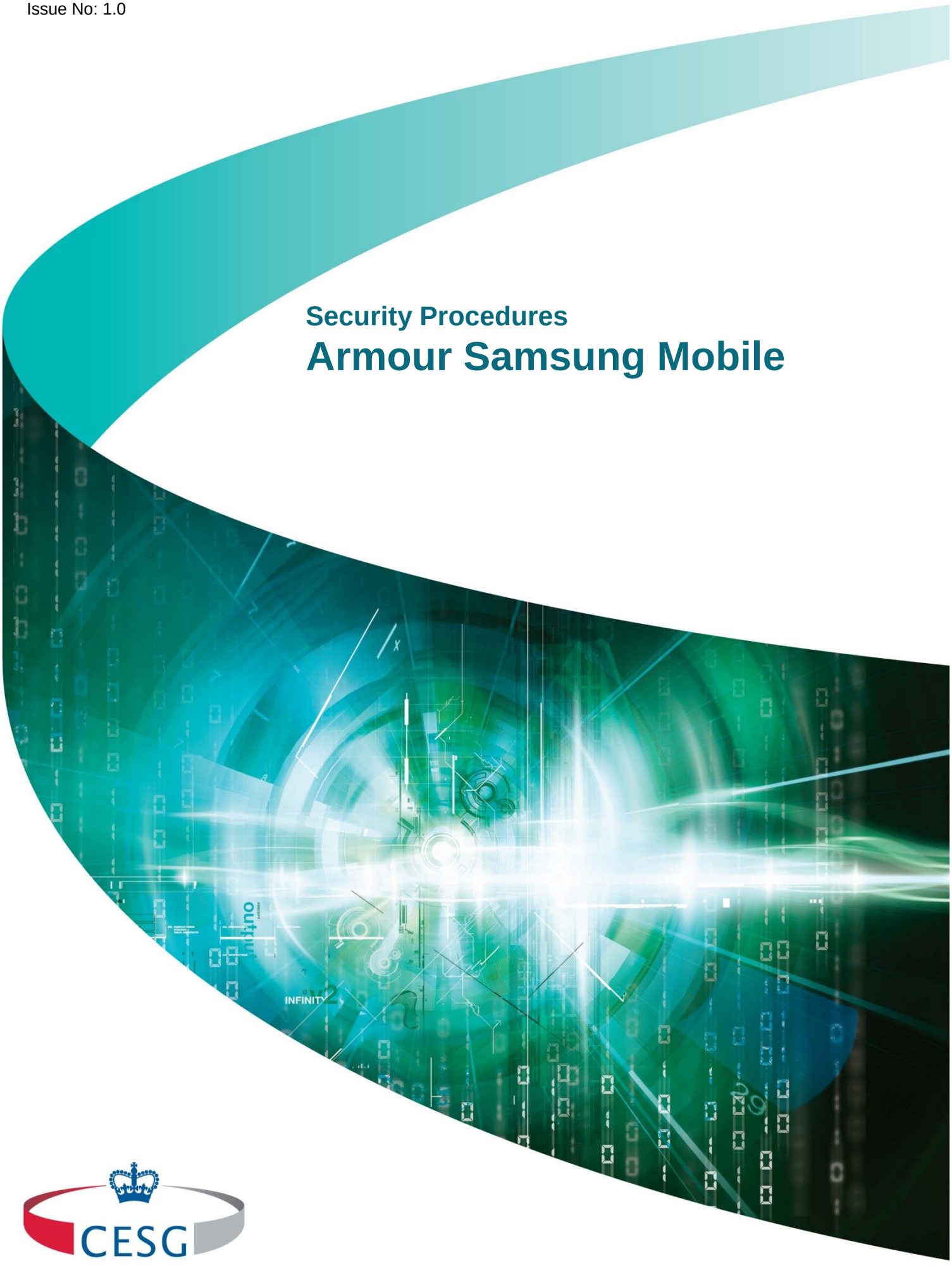
March 2016
Issue No: 1.0

## Security Procedures

# Armour Samsung Mobile



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

# Security Procedures

# Armour Samsung Mobile

Issue No: 1.0
March 2016



## Document history

| Version | Date | Comment |
|---|---|---|
| 1.0 | March 2016 | First public issue |

# About this document

These Security Procedures provide guidance in the secure operation of Armour Samsung Mobile, an encryption product for protecting voice, video, messaging and other data up to OFFICIAL SENSITIVE level, to and from Samsung mobile devices.

This document is intended for System Designers, Risk Managers and Accreditors. CESG recommends you establish whether any departmental or local standards, which may be more rigorous than national policy, should be followed in preference to those given in these Security Procedures.

The Security Procedures come from detailed technical assessment carried out by CESG. They do not replace tailored technical or legal advice on specific systems or issues. CESG and its advisors accept no liability whatsoever for any expense, liability, loss, claim or proceedings arising from reliance placed on this guidance.

# Related documents

The documents listed in the References section are also relevant to the secure deployment of this product. For detailed information about device operation, refer to the Armour Samsung Mobile product documentation.

# Points of contact

For additional hard copies of this document and general queries, please contact CESG using the following details.

**CESG Enquiries**
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

enquiries@cesg.gsi.gov.uk
Tel: 01242 709141

We welcome feedback, positive or negative, about this document. Please send your feedback to enquiries@cesg.gsi.gov.uk

# Contents:

# Chapter 1 - Outline Description

1. The **Armour Samsung Mobile** client forms part of the **Armour Mobile** product line, which includes infrastructure (i.e. server-based) elements which handle call signalling, key management and user provisioning.

2. The Armour Mobile system is intended to provide a standards-based secure communications solution for government and enterprise using MIKEY-SAKKE (M-S) key management in line with the CPA security characteristic (SC) (see reference [a]) while adhering to the associated RFCs (references [b], [c], [d]) and, for interoperability purposes, evolving in line with the "Secure Chorus" standards (see references [e] to [i]).

3. The Armour Samsung Mobile client uses standards-based signalling (Session Initiation Protocol; SIP) and media (Secure Real Time Protocol; SRTP) to transport audio, video and messaging, using CESG's MIKEY-SAKKE Public Key Infrastructure (PKI) mechanism for key distribution, with additional protection for each client's keys and cryptography provided through embedding the main cryptographic algorithm and key store within the Trusted Execution Environment (TEE) of the Samsung device.

4. This document does not cover Armour Mobile clients running on Samsung devices that do not provide full TEE support, nor non-Samsung devices or operating systems (OS's) other than Android.

## Certification

5. Armour Samsung Mobile v1.0 has undergone CPA assessment and has been certified as meeting the requirements as described in the Secure Real-Time Communications Client Security Characteristic (SC) v2.1 (reference [a]). Later versions are automatically covered by this certification until the certificate expires or is revoked, as stated on the product's certificate and on the CPA website.

6. This certification covers only the Armour Samsung Mobile client application. No server-side functionality is included.

## Components

7. Armour Samsung Mobile comprises the components listed in Table 1, which may be networked as shown in Figure 1. When installed together, the server components – excluding the Gateway – are referred to collectively as the **Armour Core**.

8. Armour server components are individually version-controlled. However, all server releases to customers are provided as a single, version-controlled Armour Core release.

| Component | Comments |
|---|---|
| Armour Samsung Mobile client application | 'Rich world' mobile application. |
| *The following elements are outside the scope of this certification. They are required for the client to function correctly, and are included to provide context.* | |
| Armour Samsung Mobile trusted application (TA) | 'Trusted' mobile application. |
| Armour SIP Server (SIP) | Provides standards-based call / message signalling. May comprise multiple servers to include STUN, ICE and/or TURN functions for NAT. |
| Armour Bootstrap Server (BSS) | Provides initial provisioning of the client application in a secure manner. |
| Armour Key Management Server (KMS) | Provides initial key material and subsequent updated key material to the trusted application, via the client application. |
| Armour Key Authority Server (KAS) | Generates all key material for use by the KMS. |
| User Management Server (UMS) | Allows an authorised administrator to define users and their communities (i.e. their keying and whether they can call each other). |
| Armour Media Proxy Server (MPS) | Optional router for encrypted media; may also act as an extraction point for recording encrypted media. |

**Table 1 – Components of Armour Samsung Mobile**

9. Notes accompanying Table 1:

- For most customers it is expected that all the server components would be owned and maintained by the deploying organisation or another organisation trusted by the customer

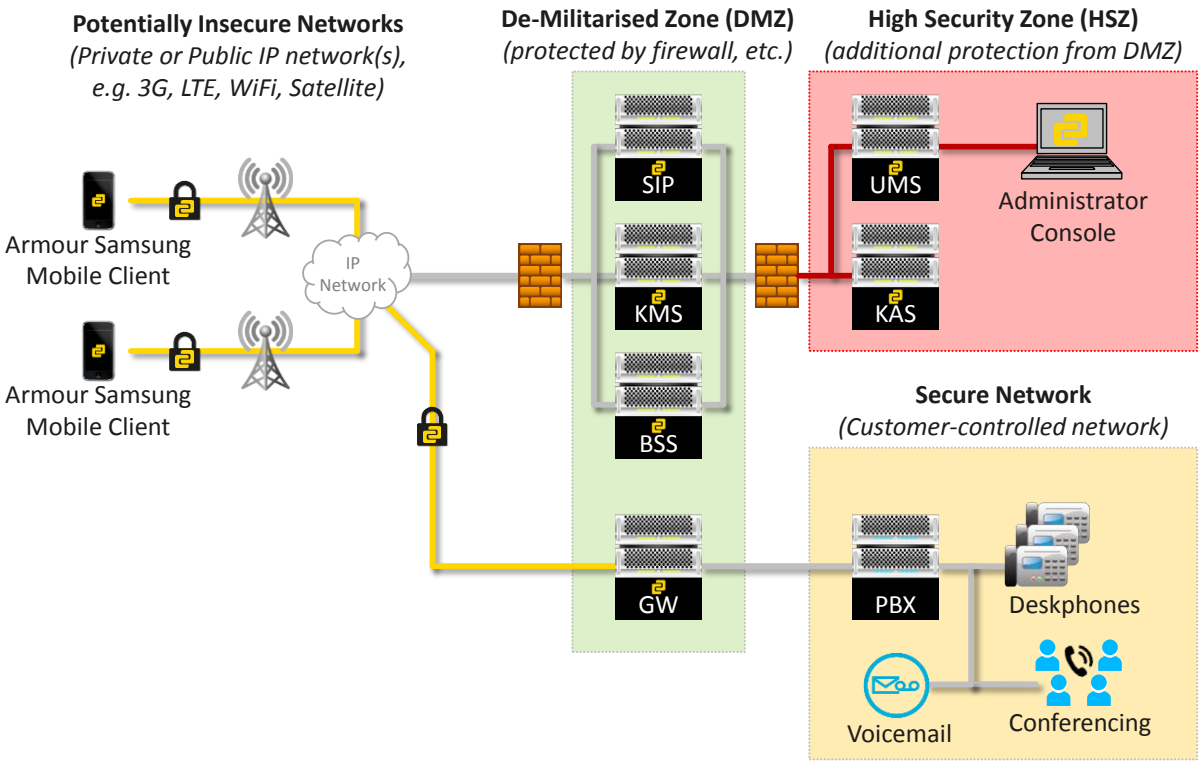



**Figure 1 – Example network configuration for Armour system components**

10. Given its optional nature, a Media Proxy Server is not shown in Figure 1 but could be located within the DMZ or in another security domain provided it has access to the IP Network over which the clients send their encrypted media.

## Security Zones

11. Figure 1 differentiates between four security zones; one or more of these may be merged if the organisation's security requirements allow or if operational needs dictate:

    - Insecure: areas of the network which are not protected, necessitating the need for encrypting media (using the Armour product)
    - DMZ: Armour Core servers that require connectivity to the insecure network because they must communicate directly with the client devices
    - HSZ: Armour Core servers that handle consolidated user information and key material and so must not be connected directly to the insecure network
    - Secure: areas of the network within an organisation's existing security perimeter

12. The different network security zones must be protected from each other using firewalls (as a minimum) as per Architectural Pattern No.2 – Walled Gardens for Remote Access (AP2) (reference [j]) Only the defined set of ports required by each Armour server [o] must be allowed through the respective firewalls.

## Terminology

13. The following terms are used in this document:

- ‘Must’ and ‘Mandatory’ are used to express a requirement that is essential to obtain assurance. Implementations that do not meet this requirement must not be used to protect classified data
- ‘Should’ and ‘Strongly Recommended’ indicate a requirement that is highly desirable but not binding. The consequences of any deviation from these requirements must be fully understood and the risks managed accordingly
- ‘Could’ and ‘Recommended’ are used to express a non-mandatory requirement that may enhance security or functionality

# Chapter 2 - Security Functionality

This chapter summarises the security functionality of the Armour Samsung Mobile product.

## Secure Services

14. Multiple Secure Services are supported, including voice and video calling (over IP) and instant messaging. Except where these need to be explicitly differentiated, they are referred to hereafter as simply “Secure Services”.

## Authentication of Mobile Clients

15. Authentication ensures only licensed mobile clients can use a Secure Service. Initial provisioning of the licence and server authentication information will only be provided once the client has correctly authenticated itself to the Armour Bootstrap Server (BSS).

16. Before the mobile client can use a Secure Service it must first have been provisioned with the relevant key(s) for that Secure Service. The Armour KMS will only provide these keys once the client has correctly authenticated itself to the server.

17. In addition, the mobile client must register with the Armour SIP Server to which it is affiliated, via TLS. The SIP Server checks that the client is authorised to use the Secure Service and (if configured to do so) defines the Armour Media Proxy Server through which the secure media must pass (otherwise the clients determine a media path using STUN or a similar technology).

18. Connections between mobile clients are authenticated using the M-S signing technologies (reference [b]).

## Session Key Establishment

19. A session is defined as a single instance / use of a Secure Service (i.e. one voice or video call, or one message). Per-session keys are established between clients based on the client-specific and community-specific keys defined by each client’s KMS as per the M-S key management mechanisms.

## Session Encryption

20. The session-specific media is encrypted using the Advanced Encryption Standard (AES) algorithm with 128 bit session keys (derived from a shared secret exchanged using the M-S identity-based encryption scheme) and initialisation vectors as defined in (reference [k]).

## Other Features

21. Armour Samsung Mobile may be used over standard wireless packet-based networks, including 2.5G, 3G, 4G / LTE and Wi-Fi.

22. The Media Proxy Server may be used to control routing of the Secure Service for routing efficiency or to provide a point where the media can be extracted and stored for monitoring purposes.

## CESG Approval

23. Armour Samsung Mobile has been approved by CESG to protect classified information as shown in Table 2.

| Classification of Unencrypted Media | Classification of Encrypted Media |
|---|---|
| OFFICIAL | None |
| OFFICIAL SENSITIVE | None |

**Table 2 – Protection provided by Armour Samsung Mobile**

## Restrictions on Use

24. Armour Samsung Mobile is only approved for use on Samsung devices as defined in reference [l], running Android operating system 5.0 “Lollipop” or later.

# Chapter 3 - Secure Operation

25. The following recommendations outline a configuration for Armour Samsung Mobile that is in line with the Security Characteristic for a Secure Real-Time Communications Client (see reference [a]). These requirements should be followed unless there is a strong business requirement not to do so. Such instances should be discussed with your Accreditor.

26. It is assumed that the organisation and users conform with the latest version of CESG's guidance for their platform, available at reference [m].

## Pre-installation

27. Before installation of the client software, it is assumed that all necessary Armour infrastructure components are in place and that the new user has been set up on the system by an authorised administrator via the UMS (the UMS configures the other servers to prepare them for the new user).

28. It is assumed that the mobile device is managed by a Mobile Device Management (MDM) system (as per reference [m] sections 6 and 7) which also controls deployment of applications to the device. This capability must be used to avoid potential vulnerabilities from, or clashes with, other voice/video products, i.e. it is recommended that no other voice or video calling applications are allowed on the device other than the built-in OS calling functionality.

29. If a VPN is used on the client (as per reference [m] sections 2, 4.1), it must be configured to provide access from the client to the Armour servers and to the other mobile clients with which it intends to communicate.

30. Users must establish if any departmental or other organisation standards (which are more rigorous than this policy) must be applied.

## Installation

31. The Armour Samsung Mobile client application should be downloaded from an app store controlled by the user's organisation (see reference [m], sections 2, 4.10). If the organisation does not have a controlled app store, the application may be installed manually on to a device by an authorised member of the organisation or downloaded from a public app store.

32. Installation of the Armour Samsung Mobile trusted application (TA) must be from an authorised Trusted Application Manager (TAM) and is automatically performed by the client application during its configuration phase (provided that the client is licensed to do so, i.e. it is provided with the authorisation key for the download during its configuration).

33. The installation process is described in the product User Manual (reference [n]).

## Configuration

34. The Armour Samsung Mobile client is configured for use with a given Armour infrastructure during its provisioning phase, using the following steps:

    - The user is provided (out of band) with their provisioning information, generated by the Armour UMS
    - Once installed, the client application prompts the user to enter their provisioning information (before downloading the 'trusted' component)
    - The information is used to authenticate the user and device to the Armour BSS which configures the client with all the information it requires to contact the other Armour servers, as well as its licence (controlling the Secure Services it may access) and a KMS authentication token
    - The client downloads the 'trusted' application component and requests its M-S key material from the Armour KMS using the KMS authentication token
    - The client is now ready to access its Secure Services
    - NOTE: Once the user has been provisioned (or if the provisioning process has irreparably failed), the provisioning information is invalidated automatically by the BSS (and/or manually by the UMS) and so is no longer protected material as it cannot be reused

35. The configuration process shall be described in the product User Manual (reference [n])

## Operation

36. The Armour Samsung Mobile client must be installed and configured as described earlier in this section before it can provide any Secure Services.

37. Organisations should produce their own procedures for the use of mobile devices and the Armour Samsung Mobile client – see reference [m] for guidance. These procedures should include guidance on overseas use given the cryptographic nature of this product.

38. The device on which the Armour Samsung Mobile client is deployed should be managed using a Mobile Device Management (MDM) system which meets the security and operational needs of the organisation.

## Maintenance and Updates

39. Updates to the Armour Samsung Mobile client ('Rich World' and 'Trusted' components) must only be provided by Armour through the specific delivery mechanism agreed with the organisation. Where the organisation does not have a definitive delivery mechanism, updates could be delivered through the public app store (for the 'Rich World' component) and the appropriate TAM (for the 'Trusted' component). Devices must always be upgraded to the latest available Client version to ensure they have the latest security functionality.

## Servers

40. The Armour Core servers must be installed as described in reference [o].

41. It is important that organisations have a patching regime to ensure that security patches are applied quickly to all aspects of the Armour Mobile system, including operating system updates and Armour Core software updates.

42. All server and hardware components should be hardened in line with good industry practice. Manufacturer's hardening guidelines should be followed where they exist.

43. The principle of least privilege should be applied to all accounts used within the system. Administrator accounts should have the minimal capability required to perform their function. Unnecessary privilege should be removed; this will reduce the impact of a compromise.

## System Logs

44. The production version of the Armour Samsung Mobile client does not provide any user-readable logs; errors which occur during use will be displayed to the user via a screen dialog.

45. Audit logs will be produced by the Armour Core servers, with all warnings and error conditions that may affect security being reported through the UMS interface to the authorised administrator(s).

46. In addition to any immediate security-related actions triggered by warnings or error conditions displayed to the administrator(s), said administrator(s) must review the full audit logs at least once per month to ensure all issues captured in the logs are assessed for security impacts (malicious activity, etc.) and the appropriate mitigating actions are taken.

## Personnel Security Requirements

47. The Armour Samsung Mobile client should only be handled by authorised users. (Note: the Armour servers must only be handled by personnel authorised and cleared as appropriate to the classifications designated for each server by the user's organisation.)

## User Education

48. End users should read the Armour Samsung Mobile User Manual (reference [n]) prior to use and/or the organisation may provide training based upon the User Manual content.

## Key Material

49. The primary key material for the Armour Mobile system resides in the Key Authority Server (KAS) configuration. Modification of the key material requires the KAS to be restarted with the command line option to trigger regeneration of all underlying keys within the system.

50. All Armour Mobile servers have X.509 certificates used for TLS to protect traffic between the servers. These certificates may be manually updated if required or modified as part of a re-install process.

51. The interval for renewal of client private key material is configurable on the UMS by an administrator, but shall be no greater than one month to ensure the requirements of reference [k] are met.

# Chapter 4 - Security Incidents

## Loss, Tampering and other Compromises

52. Loss, theft or compromise of a device using Armour Samsung Mobile must lead to its registration details and key material being revoked (by an administrator, through the Revoke function on the UMS) on all Armour Core servers (to prevent misuse of the device). If dealt with quickly, loss or theft of an individual mobile device is unlikely to have wider consequences for the security of the overall system.

53. Compromise or suspected compromise of any of the Armour servers must be treated as a potential compromise of the entire system. System use must be suspended while the incident is investigated.

- If an operating system or software-level compromise is indicated, the server must be rebuilt and reinstalled and key material regenerated (see Key Material on p.11).
- If a firmware or hardware-level compromise is indicated, the affected servers must be replaced and the software installed afresh.

## Incident Management

54. In the event of a security incident that results in the compromise of information protected by Armour Samsung Mobile, the organisation's IT security incident management policy should ensure that the organisation's security officer (e.g. Department Security Officer; DSO) is informed.

55. Inform CESG if a compromise occurs that is suspected to have resulted from a failure of Armour Samsung Mobile.

56. This product does not use CESG-supplied keys, therefore it is not necessary to inform the CESG Comsec Incident Notification Reporting and Alerting Scheme (CINRAS).

# Chapter 5 - Disposal and Destruction

## Routine Reuse or Recovery of Equipment

57. A Samsung Android device installed with Armour Samsung Mobile may be reused provided the device is factory reset before reuse to delete all applications and data (including key material) from the device. The Armour Samsung Mobile software must then be reinstalled, and the new user provisioned via the UMS, etc.

58. The recovery process for an Armour server is to rebuild it from backup or, if needed, to install it afresh. If required, new key material may be provided (see Key Material on p.11).

## Routine Disposal of Equipment

59. If the mobile device is not to be reused it must be destroyed in accordance with HMG IA Standard No.5 – Secure Sanitisation of Protectively Marked Information or Sensitive Information (IS5) (reference [p]).

60. If a server is not to be reused, its hard drive must be erased in accordance with IS5 (reference [p]). The server can then be reused or disposed of by normal means.

## Emergency Destruction of Equipment

61. As per Routine Disposal.

# References

Unless stated otherwise, these documents are available from the CESG website.


[a] CPA Security Characteristic – Secure Real-Time Communications Client (available from www.cesg.gov.uk/servicecatalogue/CPA)

[b] Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI), RFC6507, *IETF*, 2012.

[c] Sakai-Kasahara Key Encryption (SAKKE), RFC6508, *IETF*, 2012.

[d] MIKEY-SAKKE: Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY), RFC6509, *IETF*, 2012.

[e] One-to-One Communications, issue 0.3, *Secure Chorus Forum*, Mar 2015.

[f] KMS Communications, issue 0.2, *Secure Chorus Forum*, Jan 2015.

[g] KMS Protocol Specification, issue 0.01, *Secure Chorus Forum*, Nov 2014.

[h] Software Library Specification, issue 0.31, *Secure Chorus Forum*, Mar 2015.

[i] Group Communications, issue 0.10, *Secure Chorus Forum*, Nov 2014.

[j] Architectural Pattern No.2 -Walled Garden for Remote Access

[k] Technical Specification: A MIKEY-SAKKE / SRTP profile, issue 1.0, Jan 2013.

[l] S14.30 MIKEY-SAKKE Secure Voice Supported Devices, Samsung, Sep 2015.

[m] End User Devices Security Guidance: Android 4.4, 10 Jun 2014.

[n] MAN011 Armour Samsung Mobile User Manual, *Armour Communications*, Sep 2015.

[o] MAN015 Armour Core Installation Manual, *Armour Communications*, Sep 2015.

[p] HMG Information Assurance Standard No 5 – Secure Sanitisation of Protectively Marked Information or Sensitive Information

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141

Email: enquiries@cesg.gsi.gov.uk