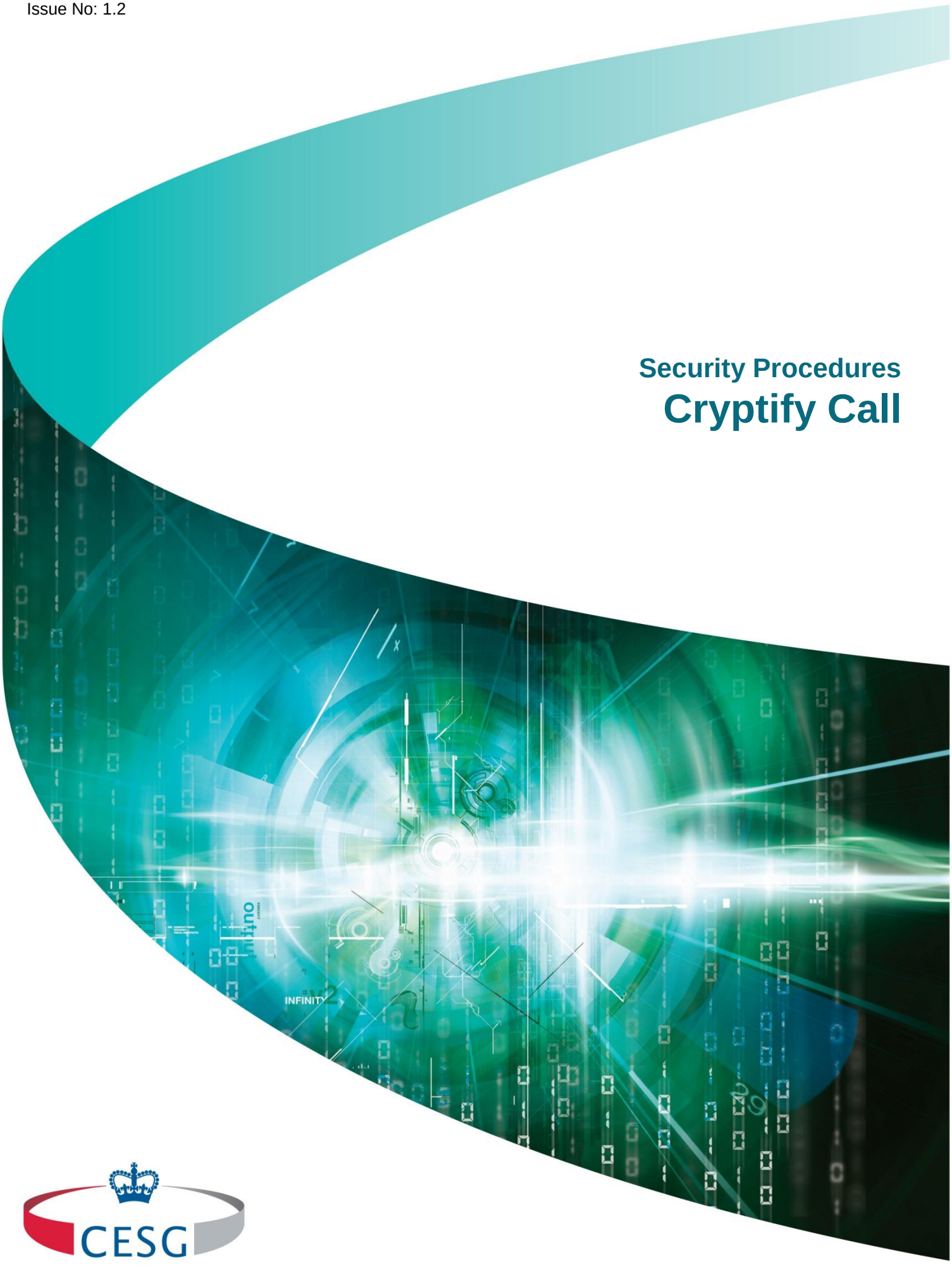
October 2015
Issue No: 1.2

Security Procedures

Cryptify Call



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

Security Procedures

Cryptify Call

Issue No: 1.2
October 2015

Document History

Version	Date	Comment
1.0	November 2013	First issue
1.2	October 2015	First public release

About this document

These Security Procedures provide guidance in the secure operation of Cryptify Call.

Cryptify Call is an application that provides encrypted and authenticated voice communication between two parties using a standard smartphone.

This document is intended for System Designers, Risk Managers and Risk Management Advisors.

The Security Procedures come from a detailed technical assessment carried out under the CPA scheme. 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 Cryptify Call 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

CESG welcomes feedback and encourage readers to inform CESG of their experience, good or bad in this document. Please email: enquiries@cesg.gsi.gov.uk

Contents:

Chapter 1 - Introduction

1. Cryptify Call is a voice encryption solution for Smartphones, the iOS and Android variants of which have been granted CPA approval when deployed in accordance with these Security Procedures.

2. The solution uses the CESG preferred MIKEY-SAKKE algorithms for key exchange and Advanced Encryption Standard (AES) for media encryption. The design of the system and the use of MIKEY-SAKKE ensure that the organisation provisioning the service remains in full control of all of the key material.

3. Cryptify Call provides a similar interface to the normal phone dialler application and uses phone numbers (which may be the same as the user's normal phone number if desired) as the identifier for a user.

4. Cryptify Call provides end to end encrypted voice communications between two parties and mutual trusted authentication of the parties.

Certification

5. Cryptify Call Version 3 has undergone CPA assessment and has been certified as meeting the Foundation Grade requirements as described in the CPA Secure VoIP Client Security Characteristic v2.0 (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. CPA certification indicates that Cryptify Call is suitable for use for communication at the OFFICIAL tier in line with the Government Classification Policy.

7. The Certification applies to the Cryptify Call application when deployed on:

   - an iOS platform that is running iOS version 6 and above (but see paragraph 13)
   - an Android platform that is running Android v4.0 and above

8. The certification is not dependent upon the selected communication provider.

Components

9. Cryptify Call comprises the following components, where the complete system referred to in this document is defined as the combination of the three components:

Component	Classification Level	Comments
Cryptify Call Application (CCA)	OFFICIAL	Loss or compromise of a single client does not compromise the complete system
Cryptify Management System (CMS)	The same as the highest classification of the data being protected	Loss or compromise of the CMS will compromise the complete system including all users
Cryptify Rendezvous Server (CRS)	OFFICIAL	Loss or compromise of the CRS will not compromise the security of the system, but can impact availability of the service

Table 1 – Components of Cryptify Call

Chapter 2 - Security Functionality

End-to-end encrypted and authenticated voice

10. End-to-end encrypted and authenticated voice allows two end-users to communicate securely using VoIP, compliant with Technical Specification No. 500, A MIKEY-SAKKE / SRTP profile (reference [b]).

11. Communication between the application and the CRS to establish a call is via TLS using the TLS_PSK_WITH_AES_128_CBC_SHA algorithm.

12. Voice data between two users uses SRTP protected with AES 128. The traffic is routed via the CRS but the CRS does not hold the key for that traffic.

Limitations on use

13. For iOS, the Cryptify Call application relies upon the cryptographic services provided by the iOS operating system's CoreCrypto Kernel Module. If the most recent version of iOS does not have FIPS approval, the accreditor must balance the risks of using Cryptify Call with services that are not fully certified against the benefits of using the latest version of an operating system that is likely to be inherently more secure.

14. For Android, as the Cryptify Call application includes the cryptographic services provided by the FIPS approved OpenSSL FIPS Object Module; the Android devices on which Cryptify Call runs can be upgraded to the latest version of Android.

Chapter 3 - Secure Operation

15. The following recommendations outline a configuration for Cryptify Call that complies with the Security Characteristic for Secure VoIP Client. These requirements should be followed unless there is a strong business requirement not to do so. Such instances should be discussed with your Risk Management Advisor.

16. Please note that the CMS contains the Key Management Server (KMS) Master Secret, KMS Secret Authentication Keys and the private keys for all the users.

- The CMS **must** never be connected to any network at any time
- The CMS **must** never be physically accessible by unauthorized users

17. While the CRS is not involved in any encryption operations, it is still vital for the availability of the service and could potentially be subject to attack where the ultimate target is the mobile devices.

- The CRS **must** only be managed by trusted administrators under the control of the deployment organisation, and those administrators must audit the CRS to ensure no malicious activity is taking place
- Only specific devices **shall** be able to connect to the CRS (and then only over specific ports) protected by a hardware firewall that only allows TLS and other required protocols
- Devices, when provisioned, **shall** be configured to only connect to a specific CRS

Pre-installation

18. Before installing Cryptify Call, CESG recommends that you take the following actions:

- Configure the CCA device in accordance with:
  - the End User Device Security Guidance for Apple iOS (reference [c]); or
  - the End User Device Security Guidance for Android (reference [d])
- Ensure the pre-requisites, as described in the Cryptify Call product documentation, are fulfilled. Refer to the manuals for the CMS (reference [e]), CRS (reference [f]), and
  - CCA for iPhone (reference [g]); or
  - CCA for Android phone (reference [h])
- Ensure that no other VoIP applications are installed on the CCA Phone (DEP.1.M824 in Secure VoIP Client Security Characteristic (reference [a]))
- The CCA phone should run the most recent version of an operating system as possible (but see paragraphs 13 and 14). If there is no End User Device Guidance for a recently released operating system, contact CESG Enquiries

System installation and configuration

19. Please follow the *Installation and Configuration* procedure in the CMS manual (reference [e]).

20. Please follow the *Initial Installation and Configuration* procedure in the CRS manual (reference [f]).

User device installation and configuration

21. CESG recommends that CCA is installed as part of the platform provisioning process using the platform Configurator or an alternative Mobile Device Management (MDM) solution.

22. Follow the *add a user* procedure in the CMS manual (reference [e]) to create necessary keys and configuration data for the user.

Initial key distribution

23. CESG recommends scanning the QR code directly from the screen from the CMS computer in order to avoid printing the private keys. This is done by selecting *view QR code* in the *user details* menu.

24. If printed versions of the QR codes must be used (for example because the device configuration is being performed at a different location to the CMS), they must be marked with the classification of the system, transported and, as soon as they have been used, destroyed in accordance with the highest classification of the data to be carried by the system.

Monthly key update

25. Following Technical Specification No. 500, A MIKEY-SAKKE / SRTP profile (reference [b]) the private key material shall be rekeyed every month. Please follow the *Monthly key updates* procedure in the CMS manual (reference [e]), and the CRS manual (reference [f]).

26. A new blank CD-R should be used for each transfer to avoid the possibility of introducing malicious code onto the CMS.

27. CESG recommends that the CRS only holds keys for the current month and the following month.

Routine tasks

28. The logs available on the CRS should be checked at least monthly before the keys for the following month are loaded to check for unexpected entries. The available logs are described in the CRS manual (reference [f]).

Compromise recovery - Client

29. Follow this operation if a device is, or is suspected to be, compromised.

30. Perform a wipe using the MDM as described in the *End User Devices Security Guidance* to remotely wipe the device.

31. Select *Destroy keys* in the user details view in the CMS. This will prevent the comprised device from rekeying, as the update key used to protect the monthly key updates will be changed. **Note that MIKEY-SAKKE keys for the identity, i.e. the phone number, will remain compromised for the current month and any future months that are already distributed to the phone.**

32. Follow the *Block User* procedure in the CRS manual (reference [f]) to prevent the compromised user from accessing the CRS using the already distributed keys. This will block the compromised device from further communication.

Re-configuration

33. This operation is provided in case a device needs to be re-configured, and there is no possibility that the device has been compromised.

34. Select *view QR* in the user details view in the CMS.

35. Follow the *Manual Key Updates* procedure in the manual for the CCA Phone.

Compromise recovery - KMS

36. Follow this operation if the CMS is, or is suspected to be, compromised.

37. Follow the *Delete an Account* procedure to remove the compromised CMS from the CRS. This will prevent all users belonging to the compromised CMS from further secure communication.

38. Follow the Secure Operations for *Pre-Installation, Install and Configure* as well *Initial key distribution* to create a new CMS and to provision users with new key material.

39. Follow the *Manual Key Updates* procedure in the CCA phone manual to install the new keys onto each of the phones that used the compromised CMS.

Compromise recovery – QR code

40. Follow the procedure for a compromised client to block the lost key.

41. Follow the '*add a user'* procedure in the CMS manual (reference [e]) to create a new key and configuration data for the user.

42. Follow the *Manual Key Updates* procedure in the manual for the CCA phone to install the new key.

Compromise recovery – monthly update disk

43. Follow the procedure for a compromised KMS.

Overseas use

44. Should a deployment approve the use of Cryptify Call for use overseas then the guidance provided in HMG IA Standard No. 4 – Protective Security Controls for a the Handling and Management of Cryptographic Items (IS4) (reference [i]) may prove helpful although, as the product itself is not classified, the requirements for incident reporting in the document do not apply. CESG Threat Briefing No. 1 Assessment of Technical Threat (reference [j]) gives additional information on threat sources to be considered. Care must also be taken to ensure the product does not infringe controls regarding the import, export or use of cryptographic devices in the countries visited.

Chapter 4 - Security Incidents

Tampering and other compromises

45. The following table provides instructions to be followed if you suspect or identify a compromise to Cryptify Call. The actual procedures and policies should be complied with in conjunction with system accreditation requirements.

Component	Classification Level	Action if lost or compromised
CCA	OFFICIAL	Follow the *Compromise Recovery - Client* Secure Operations above.
CMS	The same as the highest classification of the data being protected	Follow the *Compromise Recovery - KMS* Secure Operations above.
CRS	OFFICIAL	Please re-install CRS as described in the manual (reference [f]).

Table 2 - Actions to be taken after actual or suspected Comsec incidents

Incident management

46. If a security incident results in the compromise of information protected by Cryptify Call, the local IT security incident management policy should ensure that the Department Security Officer (DSO) is informed.

47. Depending on the severity of the incident the DSO should, at their discretion, ensure that GovCertUK is informed.

48. If the incident is believed to be due to a failure of the product then the vendor and CESG Enquiries should be informed.

Chapter 5 - Disposal and Destruction

Routine destruction of equipment

49. Follow the steps outlined in the HMG IA Standard No.5 (IS5) Secure Sanitisation (reference [k]) when disposing of client devices, the CMS, monthly update disks or QR codes.

50. For client devices the procedures appropriate for flash memory should be followed (as these exceed those required for DRAM).

51. For the CMS, the procedures selected will depend upon the type of disk fitted to the PC (SSD or magnetic hard disk).

52. For the monthly update disk the procedures appropriate for a CD should be followed.

53. For printed QR codes the procedures appropriate for paper should be followed.

References

Unless stated otherwise, these documents are available from the CESG website. Users who do not have access should contact CESG Enquiries to enquire about obtaining documents.

[a] CPA Security Characteristic – *Secure VoIP Client, Version 2.0* (available from www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA)

[b] Technical Specification No. 500, A MIKEY-SAKKE / SRTP profile Issue 1.0, January 2013, CESG

[c] End User Devices Security Guidance: Apple iOS, (available from https://www.gov.uk/government/collections/end-user-devices-security-guidance)

[d] End User Devices Security Guidance: Android, (available from https://www.gov.uk/government/collections/end-user-devices-security-guidance)

[e] CAB-12:048, Cryptify Management System, Rev B (supplied with the Cryptify Call product)

[f] CAB-12:047, Cryptify Rendezvous Server, Rev B (supplied with the Cryptify Call product)

[g] CAB-12:049, Cryptify Caller Application for iPhone, Rev C (supplied with the Cryptify Call product)

[h] CAB-13_013-CCA_Android_Manual-RevA (supplied with the Cryptify Call product)

[i] HMG Information Assurance Standard No. 4, Protective Security Controls for the Handling and Management of Cryptographic Items – latest issue available from the CESG website.

[j] Technical Threat Briefing No. 1, Assessment of Technical Threat

[k] HMG Information Assurance Standard No. 5, Secure Sanitisation – latest issue available from the CESG website.

Glossary

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCA	Cryptify Call Application
CMS	Cryptify Management System
CRS	Cryptify Rendezvous Server
DSO	Department Security Officer
FIPS	Federal Information Processing Standards
KMS	Key Management server
MDM	Mobile Device Manager
PSK	Pre-Shared Key
QR Code	Quick Response Code (a 2D barcode)
SHA	Secure Hash Algorithm
SRTP	Secure Real Time Protocol
SSD	Solid State Drive
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol

CESG provides advice and assistance on information security in support of UK Government. Unless otherwise stated, all material published on this website has been produced by CESG and is considered general guidance only. It is not intended to cover all scenarios or to be tailored to particular organisations or individuals. It is not a substitute for seeking appropriate tailored advice.

CESG Enquiries
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 (0)1242 709141
Email: enquiries@cesg.gsi.gov.uk