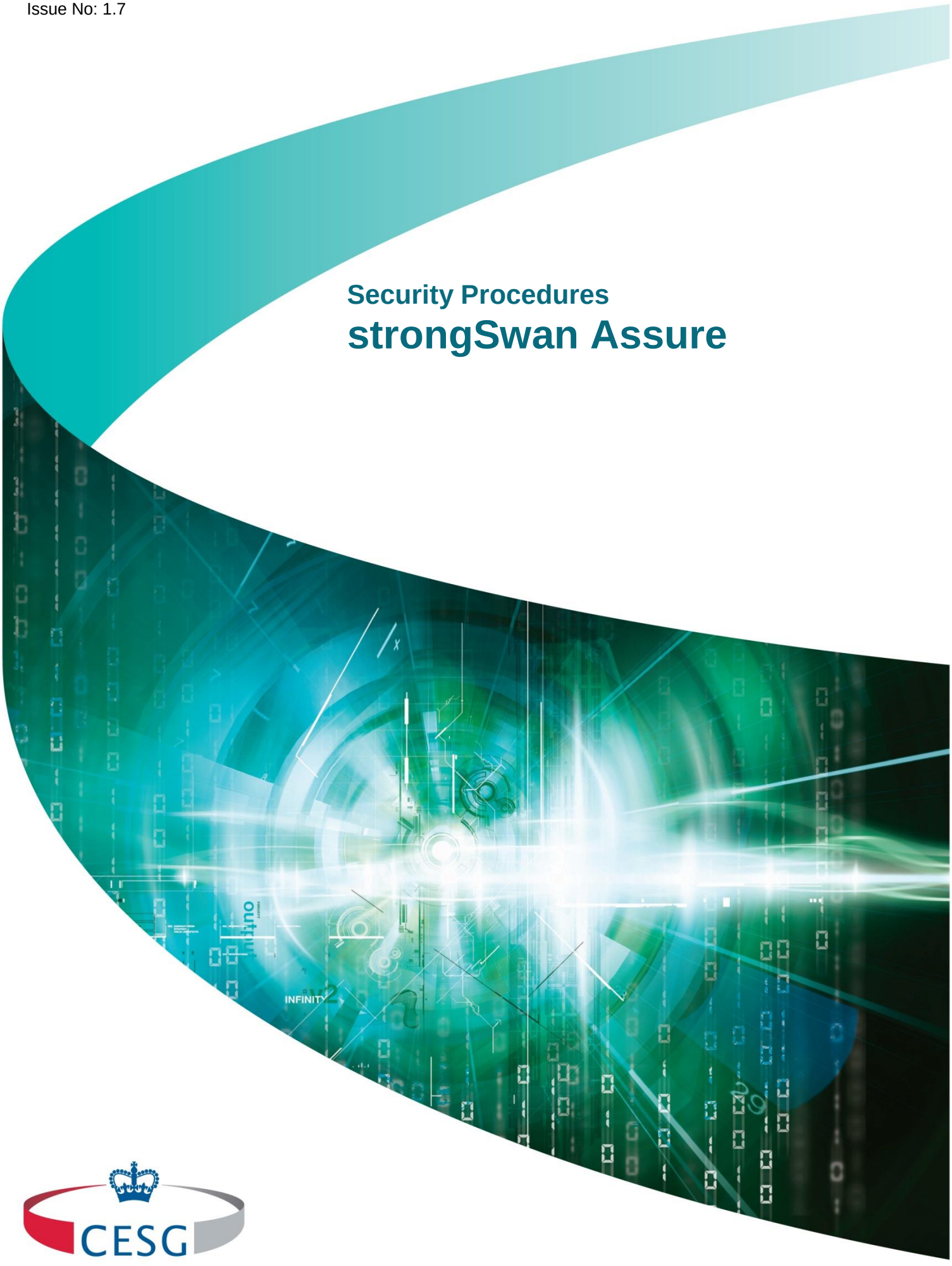
October 2016
Issue No: 1.7

# Security Procedures
# strongSwan Assure



CESG

NATIONAL TECHNICAL AUTHORITY
FOR INFORMATION ASSURANCE

# Security Procedures

# strongSwan Assure

Issue No: 1.0
October 2016

The copyright of this document is reserved and vested in the Crown.

## Document history

| Version | Date | Comment |
|---|---|---|
| 1.0 | October 2016 | First issue |

# About this document

These Security Procedures provide guidance in the secure operation of strongSwan Assure.

This document is intended for System Designers, Risk Managers and Accreditors. CESG recommend 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 under the CPA scheme. They do not replace the need for 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 strongSwan Assure product documentation.

# Points of contact

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

**NCSC**
Hubble Road
Cheltenham
GL51 0EX
United Kingdom

Email: enquiries@ncsc.gov.uk
Tel: 0300 0200 964

# Feedback

We welcome feedback, positive or negative, about this document. Please email your comments to enquiries@ncsc.gov.uk

# Contents:

# Chapter 1 - Outline Description

## Certification

1. strongSwan Assure for Ubuntu and OS X has undergone CPA (Commercial Product Assurance) assessment and has been certified as meeting the Foundation Grade requirements. These Security Procedures apply to product version 1.0.1 and later for both OS X and Ubuntu.

## Security Functionality

2. strongSwan Assure is a complete IPsec solution providing encryption and authentication to servers and clients. It can be used to secure communications with remote networks, so that connecting remotely is the same as connecting locally.

3. strongSwan Assure uses IKEv2 (Internet Key Exchange) protocol to establish security associations between peers. IKE provides strong authentication of both peers and derives unique cryptographic session keys. Authentication is based on X.509 certificates or pre-shared keys.

4. strongSwan Assure uses public key authentication, using ECDSA X.509 certificates to verify the authenticity of the peer. Certificates can be self-signed, in which case they have to be installed on all peers, or signed by a common Certificate Authority. Certificate Revocation Lists (CRLs) may be used to verify the validity of certificates. CPA compliant deployments must use a certificate authority and CRLs.

5. strongSwan Assure implements the PSN end-state IPsec profile in the configuration that was assessed.

6. strongSwan Assure provides both gateway and client functionality for Ubuntu and client functionality for OS X. By default the product acts as a client, however a gateway package is installed which changes configuration to meet CPA requirements for a gateway. Gateway functionality is activated by a single line configuration file change to accept incoming connections and a set of scripts which are installed to secure the host operating system on the Gateway Machine. The changes that will convert to operation as a gateway are documented in Chapter 2 of the User Documentation (Ubuntu Gateway Installation) (reference [c]).

7. The IPv6 functionality of the product has not been assessed. IPv6 functionality in the product is implicitly linked with the host platform's IPv6 stack and support for IPv6 must be disabled in the host operating system.

# Chapter 2 - Secure Operation

8. The following recommendations outline a configuration for strongSwan Assure that is in line with the Security Characteristics for IPsec Security Gateway (reference [a]) and IPsec VPN for remote working software client (reference [b]). These requirements should be followed unless there is a strong business requirement not to do so. Such instances should be discussed with your Accreditor.

9. The product should only be used to connect to other assured VPN gateways or clients.

## Pre-installation

10. For VPN Gateways, initial setup and certificate provisioning (reference [c]) should be performed in an appropriately accredited environment for the classification of the data that the device is handling. The device should be deployed in an appropriately accredited data centre for the classification of the data that the device is handling. Only authorised administrators should have access to the room.

11. For VPN Clients, initial setup and certificate provisioning (reference [c]) should be performed in an appropriately accredited environment for the classification of the data that the device is handling. Only authorised administrators should perform the setup.

12. The equipment should use tamper evidence (e.g. stickers) to make entry to system internals detectable by physical inspection. Tamper stickers should be uniquely identifiable to prevent an attacker successfully replacing it with a new, undamaged sticker.

13. The OS installation process for the hosts must not be performed by cloning the disk image of a master installation as this will result in the seed file that is used to re-initialise the random number generator after a reboot being duplicated. Any other non-standard OS installation procedures that may compromise the machine's ability to gather data on random events during installation to provide initial entropy to the system should also be avoided.

14. Before installing strongSwan Assure you should take the following actions:

    - End points should be hardened to meet CESG end user device guidance (references [d] & [d]). The guidance on Software Whitelisting / Software Restriction is also applicable to the Gateway
    - Packages to be installed have their signatures verified following procedures outlined in Chapter 1 (Pre installation) of the User Documentation (reference [c])
    - On Ubuntu, for simple installation using the apt package management utility, the packages should be added as an apt source, also documented in Chapter 1 of the User Documentation (reference [c]). This allows

package dependencies and conflicts to be automatically resolved during installation

- Only Administrative users should have logon rights to the Gateway

## Installation

15. Ubuntu client end points should be installed as outlined in Chapter 3 of the User Documentation (strongSwan Assure Ubuntu Client Installation) (reference [c]).

16. Ubuntu gateway end points should be installed as outlined in Chapter 2 of the User Documentation (strongSwan Assure Ubuntu Gateway Installation) (reference [c]).

17. OS X clients should be installed as outlined in Chapter 4 of the User Documentation (strongSwan Assure OS X Client Installation) (reference [c]).

## Configuration

18. The majority of configuration is automatic. Chapters 2, 3 and 4 of the User Documentation (reference [c]), as appropriate for the type of installation, describe the remaining steps to configure the product to ensure that it meets the CPA requirements. Configuration of the VPN and installation of the machine certificates must be done by trusted personnel in an appropriately accredited, secure environment. This includes VPN software clients.

19. When a replacement certificate is provisioned for a gateway, the old certificate must be revoked on the certificate authority and the updated revocation list published. If using the product as a certificate authority then please refer to Chapter 7 of the User Documentation for revoking certificates (reference [c]).

20. Chapter 11 of the User Documentation (reference [c]) describes the required installation specific configuration and specifies configuration items that must not be changed in order to retain compliance with the PSN end state profile. In particular, CRL handling (in the config setup section of the configuration file) must be included in the installation and it must not be modified from the example provided in the manual. The only permitted change to the IKE parameters (in the conn %default section of the configuration file) is to modify the *auto=add* line to either *auto=start* to start the connection automatically when strongSwan loads or *auto=route* to start the connection automatically if something attempts to use it.

21. Split tunnelling must be disabled as described in Chapter 3 of the User Documentation (reference [c]).

## Operation

22. A separate X.509 certificate must be installed on every client and Gateway. The certificates may be generated either with the supplied PKI tool or using an existing capability within the organisation. Installing certificates is addressed in Chapters 8 and 11 of the strongSwan Assure User Documentation (reference [c]).

23. Certificates must be chained to a trusted, non-public certificate authority and must have a maximum lifetime of 2 years.

24. Due to the way revocation lists are processed by the product, CRLs must be generated with a 24 hour lifetime to ensure that they are refreshed regularly. This requirement is met if the product is used as a CA as described in Chapter 5 of the User Documentation (reference [c]). If a different CA is used then that CA must be configured to generate CRLs with a 24 hour lifetime.

25. It is important to follow Chapter 11 of the strongSwan Assure User Documentation (reference [c]), which details how to use client and gateway machines. Chapters 5, 6 and 7 detail how to use the supplied PKI tool to manage certificates and, if the product is being used as a CA, these must also be followed.

## Maintenance and updates

26. Prior to installation, the user should ensure that they are registered to receive product update notifications from Sirius.

27. The source of software updates must be verified before applying updates.

    **Ubuntu**
    The developer gpg key is installed as part of the initial installation; verification is performed automatically as part of the installation process.

    **OS X**
    The source of the updates should be verified as described in Chapter 1 – Pre Installation in the User Documentation (reference [c]).

    **On both platforms**
    If the platform has been configured in accordance with the end user guidance (reference [d]), updates can only be installed by an authorised administrator.

28. The latest available software version should always be used unless there is a reason why this is not possible (e.g. latest version requiring an upgrade to other system components that cannot yet be performed). An analysis must be performed on the associated risks. Risks that cannot be mitigated should be referred to the relevant risk owner.

## System logs

29. The default log level for strongSwan Assure is level 1 (generic control flow with errors). Log level 2 is acceptable. Log level 3 or above should not be used as they can include sensitive information.

30. The default log location is /var/log/ipsec.log and by default is only accessible to the root user.

31. The Audit logs must be reviewed regularly to detect unexpected entries. A review period should be defined in internal policy documentation.

32. Organisational procedures must be in place for incident resolution.

### User education

33. Chapter 11 of strongSwan Assure documentation (reference [c]) contains instructions on how to start up and shut down connections on client machines. The many connection parameters depend on local setup and an accompanying user guide should be provided with each installation.

### Disposal and destruction

34. It is important to follow Chapter 9 of strongSwan Assure documentation, which covers disposal and uninstallation procedures (reference [c]).

# Chapter 3 - Security Incidents

| Component | Classification | Action if lost or compromised |
|---|---|---|
| Any installation package | NONE | Do not install product if any component fails signature check. See strongSwan Assure documentation Chapter 1. |
| CA Key compromised | The highest classification of any data held on the network being protected | Revoke and remove all root CA certificates from all gateways. See Chapter 10 of strongSwan Assure documentation |
| Client certificate compromised | The highest classification of any data held on the network being protected | Revoke. See Chapter 10 of strongSwan Assure documentation. |
| Gateway or Client Hardware | The highest classification of any data held on the network being protected | If there is a reason to suspect hardware tampering, the system must be removed from service immediately. Any product that shows evidence of tampering must not be returned to service and any certificates for that device should be revoked. |

**Table 1 – Actions to be taken after actual or suspected COMSEC incidents**

## Incident management

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

## StrongSwan Assure quality issues

36. Contact CESG if a compromise occurred that is suspected to have resulted from a failure of strongSwan Assure

# Chapter 4 - Disposal and Destruction

## Routine destruction of equipment

37. When equipment is destroyed, Certificates which have been issued for the equipment should be revoked, following the procedures documented in Chapter 7 (Revoking Certificates) of the strongSwan Assure User Documentation (reference [c]).

38. In order to ensure that all copies of key material on the device have been removed the hard disk / solid state disk within the equipment should be wiped in accordance with IA Standard No. 5 – Secure Sanitisation (reference [f]).

# References

Unless stated otherwise, these documents are available from the NCSC.

[a] CPA Security Characteristic IPsec VPN Gateway, Version 2.5 (Available from CPA section of NCSC website)

[b] CPA Security Characteristic IPsec VPN for Remote Working - Software Client, Version 2.3 (Available from CPA section of NCSC website)

[c] strongSwan Assure User Documentation (Chapters 1-11) (Supplied with product)

[d] End User Devices Security Guidance: Apple OS X 10.11

[e] End User Devices Security Guidance: Ubuntu 14.04 LTS.

[f] HMG IA Standard No. 5 – Secure Sanitisation – Latest Issue

NCSC
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX

Tel: +44 0300 0200 964
Email: enquiries@cesg.gsi.gov.uk

© Crown Copyright 2016. Communications on CESG telecommunications systems may be monitored or recorded to secure the effective operation of the system and for other lawful purposes.