CESG ASSURED SERVICE
CAS SERVICE REQUIREMENT
TELECOMMUNICATIONS

Issue 1.1

Document History

Version	Date	Description
0.1	November 2012	Initial Draft Version
1.0	September 2013	Issued version
1.1	December 2015	Minor corrections; alignment with revised GPG 32 and Security Procedures

Soft copy location

DiscoverID 44993858

This document is authorised by:

Technical Director External Capability Development, CESG

This document is issued by CESG

For queries about this document please contact:

Service Assurance Administration Team
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Tel: +44 (0)1242 221 491
Email: cas@cesg.gsi.gov.uk

The CAS Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time.

CONTENTS

REFERENCES

[a] The Process for Performing CAS Assessments, v1.2, October 2013, CESG

[b] Good Practice Guide No. 32- Audit Handbook for CESG Assured Service (Telecoms) – latest issue available from the CESG website.

[c] Security Procedures – Telecommunications Systems and Services – latest issue available from the CESG website.

[d] Security Policy Framework (SPF), Cabinet Office

I. OVERVIEW

1. This document is a CAS Service Requirement – it describes requirements for a particular type of assured Service for assessment and certification under CESG's CESG Assured Service (CAS) scheme.

A. Service Aims

2. This service requirement aims to provide appropriately audited secure Telecommunications for HMG in line with relevant HMG IA policy [d] and guidance (as detailed in section III.A of this document).

B. Variants

3. There are no variants for the CESG Assured Service for telecommunications services.

4. **Scope of Service offering** – Telecommunications Services shall be assessed and certified against all clauses in CESG Security Procedures – Telecommunications Systems and Services (see [c]).

C. Typical Use Case(s)

5. Telecommunications across HMG networks using industry developed and supported systems with a high availability requirement.

D. Likely threats this Service will provide mitigations against

6. The threats on this service come under four categories:

- *Loss of service availability:*
  A telecommunications network loses the high level of availability required by HMG customers either by systemic failure, accident or as a result of a denial of service attack.
- *Insider attack:*
  A member of the service provider team (or a third party used as part of the Telecommunications process) attempts to subvert the Telecommunications process and removes, replaces, or transfers data.
- *Unauthorised access to Telecommunications:*
  Attacker gains access to network (either the voice / data or management layers) which has been either incorrectly or incompletely security configured and is able to retrieve data from the network.
- *Physical Attack:*
  Intruder gains physical access and then attacks the network equipment.

E. Out of scope

7. CAS does not cover security and availability of telecommunications that are outside the physical bounds of the declared service or service slice.

8. Certain interconnect and peering configurations between Communications Providers may be unsuitable for carrying assured services, because they cannot meet the minimum availability target for these Security Procedures. These interconnect options **must** be excluded from the scope of assured service.

9. Where a service is offered without managed Customer Premises Equipment (CPE), the CPE will normally be excluded from the scope of the assured service.

F. Future Enhancements

10. CESG welcomes feedback and suggestions on possible enhancements to this Service Requirement.

II. SERVICE REQUIREMENT FORMAT

12. All CAS Security Requirements contain a list of mitigations which the Service must meet.

13. Each mitigation includes informational text in italics, describing the threat that it is expected to mitigate. It also lists at least one specific mitigation, which describes what must actually be done to achieve that requirement. In some cases there is additional explanatory text which expands upon these requirements.

14. In the requirements listed below, the following terminology can be used:

- 'Must', 'Mandatory' and "Required" are used to express a mitigation that is essential. All mitigations and detailed mitigations are mandatory unless there is an explicit caveat, such as 'not applicable to this Service offering'.

- 'Should' and 'Strongly Recommended' are used whenever a requirement is highly desirable, but is not essential. These are likely to become mandatory in future iterations of the Security Requirement.

- 'Could' and 'Recommended' are used to express a non-mandatory requirement that may enhance security or functionality.

15. For example:

MITXXX - [A mitigation]
This mitigation is required to counter [a threat]
For a CAS Service [requirement].
For example [further explanatory comment].

III. REQUIREMENTS

A. Mitigations

MIT001 – Requirements for the Information Security Management System (ISMS)

This mitigation is required to ensure the scope of the ISMS is relevant and complete.

The Telecommunications Service Provider must adhere to the requirements and scope described in chapter 2 of HMG Security Procedures – Telecommunications Systems and Services.

MIT002 - HMG IA Standard Security Procedures – Telecommunications Systems and Services [c] is followed

This mitigation is required to ensure that confidence can be gained that the ISMS meets the security and availability required for a service or service slice.

The Telecommunications Service Provider must adhere to the requirements and scope described in chapter 5 and the Appendix of HMG Security Procedures – Telecommunications Systems and Services.

MIT003 – Continuous Audit and Improvement

This mitigation is required to ensure that the service is consistently working as expected and that any security flaws are identified and fixed.

Processes described in the CESG Good Practice Guide No. 32- Audit Handbook for CESG Assured Service (Telecoms) [b] must be in place for providing regular internal audits of the service being delivered, in order to ensure that all processes are being correctly followed and that the service conforms to industry good practice aligned to HMG standards and requirements.

Audits should be conducted by a separate member of staff from the team providing the instance of the service being audited. Processes must be in place to identify and fix any issues identified where the service is not being delivered as expected.

IV. GLOSSARY

16. The following definitions are used in this document:

Term	Meaning
CAS	CESG Assured Service
CPE	Customer Premises Equipment
CPNI	Centre for the Protection of National Infrastructure
ISMS	Information Security Management System