CESG ASSURED SERVICE
CAS SERVICE REQUIREMENT
DESTRUCTION

Version 1.0

Document History

Version	Date	Description
0.1	June 2012	Initial Draft Version
1.0	July 2012	Initial Release Version

Soft copy location

DiscoverID 19799020

This document is authorised by:

Deputy Technical Director (Assurance), 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, CESG

[b] HMG IA Standard No. 5 - Secure Sanitisation, CESG

[c] HMG IA Standard No. 4 – Supplement No.9 - Destruction and Disposal of Cryptographic Items, CESG

[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. Destruction Services aim to provide appropriately audited secure destruction of HMG Media and Assets (as listed in Appendix A of HMG IA Standard No. 5) in line with relevant HMG IA policy and guidance (as detailed in section III.A of this document).

B. Variants

3. There are a number of different types of destruction/sanitisation services which can be assessed via this assurance service – these are the scope of the service provided, the type of the service provided and the location of the service. A service can be assessed against any or all of the options described below, and will be described accordingly in any CESG literature regarding the service.

4. **Scope of Service offering** – Destruction Services can be assessed and certified against the destruction of any Media Type and Impact level covered within Appendix A of HMG IA Standard No. 5, up to and including the full range of Media Types at all Impact Levels, or simply a subset of this list. For the purposes of CAS, services covered can be those offering either full Destruction or simply Sanitisation processes, as defined in point 4 below.

5. **Type of Destruction Service offering** –

   i. ***Sanitisation*** – An offering of the Service where the media is intended for re-use but which requires the secure erasure of existing data. The end state of the media will be that it is suitable for re-use at either the same Impact Level, or at a lower Impact Level, depending on the requirements of the customer and as defined within HMG IA Standard No.5.

   ii. ***Destruction*** – An offering of the Service where the media is intended for full destruction and final disposal. The end state of the media will be that it is destroyed in such a way that it is unusable, and is releasable to any environment, as defined within HMG IA Standard No.5.

6. **Location of destruction activities** –

   i. ***Mobile Service*** – Destruction Services where the Service Provider has secure vehicles fitted with destruction equipment that can destroy items at the customers own site or where items are transported using secure vehicles by the Service Provider for destruction at a CPNI approved facility.

ii. ***Fixed Site Service*** – Destruction Services where destruction is carried out on the Service Provider's appropriately approved site.

C. Typical Use Case(s)

7. Destruction or sanitisation of any Media Type listed within Appendix A of HMG IA Standard No. 5, in line with the requirements specified within section III.A of this document.

D. Likely threats this Service will provide mitigations against

8. The attacks on this service come under four categories:

- *Retrieval of data from destroyed media:*
  Attacker gains access to media which has been either incorrectly or incompletely destroyed and is able to retrieve some or all of the data from the media.
- *Insider attack:*
  A member of the Service Provider team (or a third party used as part of the destruction process) attempts to subvert the destruction process and removes, replaces, or transfers data from a piece of media in their care, which is intended for destruction.
- *Unauthorised access to the media prior to destruction:*
  An attacker gains access to an item of media while in the care of the Service Provider and is able to remove it, replace it, or transfer data from it.
- *Improper treatment of data:*
  The Service Provider destroys the wrong media item.

E. Out of scope

9. CAS does not cover the destruction and disposal of cryptographic items, as defined within IS4 Supplement No.9 - Destruction and Disposal of Cryptographic Items.

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 - Staff are appropriately cleared

This mitigation is required to prevent unescorted uncleared personnel from gaining access to sensitive information.

The Destruction Service Provider staff must be suitably cleared as appropriate to the level of media being handled (as detailed in the explanatory comment below). This includes any staff who have potential access to Media prior to destruction, or records regarding customer data.

This must be as per the requirements of the Secure Policy Framework document. At present DV clearance is required for providers offering destruction of IL6 media, SC for destruction of media up to and including IL5, and BPSS for destruction of media up to and including IL4.

MIT002 - HMG IA Standard No. 5 Destruction Methodology is followed

This mitigation is required to ensure that confidence can be gained that media has been appropriately sanitised.

This mitigation is required to counter exploitation of a failed or partial destruction.

All destruction must follow the appropriate processes relevant to the media type and Impact Level of the data being destroyed/sanitised, as defined in the requirements listed in Appendix A of HMG IA Standard No. 5.

MIT003 – Items for Destruction are subject to Auditing and Asset management

This mitigation is required to ensure that media is fully accounted for throughout the destruction process and that any discrepancies can be investigated at an early stage.

All Destruction Service Providers must produce a full audit trail covering the entire service, from taking receipt of any media through to its final disposal. Appropriate audit documentation must be provided to the end customer to show that data has been processed and sanitised/destroyed appropriately. The Service Provider must have a documented process for raising and investigating any discrepancies, and informing the relevant data owner of such occurrences.

MIT004 - Assured equipment and facilities are used

This mitigation is required to ensure that destruction equipment or facilities used as part of the Service meet the requirements of HMG IA Standard No. 5 and so confidence can be gained that media is being successfully sanitised/destroyed.

This mitigation is required to counter exploitation of a failed or partial destruction.

The destruction process must use approved products/devices appropriate to the media type and Impact Level of the data being destroyed/sanitised, as defined in Appendix A of IS5. In addition, if part of the destruction methodology relies on the use of external facilities (e.g 3rd party incineration facilities) then these facilities must also be approved, as per the requirements of Appendix A of HMG IA Standard No. 5.

For example, destruction equipment used by the Service Provider should be approved to CESG, CPNI or BS EN 15713:2009 standards, depending on media type and Impact Levels and corresponding requirements of HMG IA Standard No. 5. Where final physical destruction is required, for items marked CONFIDENTIAL (IL4) and above, this should be undertaken using equipment or a service provider approved by the Centre for the Protection of National Infrastructure (CPNI).

MIT005 - Destruction equipment is used correctly

This mitigation is required to ensure that Service Providers are using destruction Products as they were intended to be used.
This mitigation is required to counter exploitation of a failed or partial destruction.

All destruction products/devices must be used in line with Manufacturer's operating procedures, user guides and any published Security Procedures. Destruction Service Provider staff must be appropriately trained in the correct usage of such equipment and processes must be in place to verify that equipment is being used correctly.

MIT006 – Equipment is maintained

This mitigation is required to ensure that Service Providers undertake regular maintenance of Products and secure transportation used as part of the Service, so that confidence can be gained that Products are working in accordance with their certifications and reducing the risk of unexpected disruption to the Service.
This mitigation is required to counter exploitation of a failed or partial destruction.

All equipment used as part of the Destruction Service (Including but not limited to destruction equipment and secure transportation where the service is being offered as a mobile service) must be subject to regular maintenance, and maintenance records must be kept.

MIT007 - Data handling processes are being followed

This mitigation is required to ensure that the correct data handling processes are in place and being followed by Service Provider staff.

The data handling processes supporting the destruction of must meet the relevant requirements, as defined in the Personnel Security and Physical Security sections of the Secure Policy Framework document. As well as covering the handling of the media itself, this should also cover the handling and storage of destruction equipment, and audit records collected during the destruction process.

MIT008 – Keep items secure during transportation

This mitigation is required to ensure that processes are in place and understood by Servicer Provider staff in order to reduce the risk of compromise of data and media during transit.

Where the service is being offered as a mobile service (which involves the transportation of any items of media, regardless of whether these have been rendered unusable prior to transportation) then Security Procedures must be in place surrounding the use of the transportation while transferring media. These Security Procedures must meet the relevant data handling requirements, as defined in the Personnel Security and Physical Security sections of the Secure Policy Framework document.

MIT009 – 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 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 media is being destroyed as expected. 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
BS EN 15713:2009.	A physical destruction standard for products
CAS	CESG Assured Service
CPNI	Centre for the Protection of National Infrastructure
Media	In this context Media refers to any item of Media described within Appendix A of HMG IA Standard No. 5

PAGE IS INTENTIONALLY LEFT BLANK