CESG ASSURED SERVICE
CAS SERVICE REQUIREMENT
PSN CA (IPSEC)
Version 1.0

© Crown Copyright 2013 – All Rights Reserved
Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>October 2013</td>
<td>Initial issue</td>
</tr>
</tbody>
</table>

Soft copy location

DiscoverID 32963695

This document is authorised by:
Technical Director for COTS Assurance

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 221491
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

I. OVERVIEW ............................................................................................................................................ 5
   A. Introduction ....................................................................................................................................... 5
   B. Service aims ....................................................................................................................................... 5
   C. Future enhancements ....................................................................................................................... 5
   D. PSN on boarding and initial steps ..................................................................................................... 5
   E. Conduct of the assessment ............................................................................................................... 6
   F. Assumptions ....................................................................................................................................... 6

II. REQUIREMENTS ................................................................................................................................. 7
   A. Requirements for a PSN CA service ................................................................................................. 7
       Cryptographic Assurance .................................................................................................................... 7
       Entropy Generation ............................................................................................................................ 8
       Entropy Design Description .............................................................................................................. 8
       Entropy Justification ........................................................................................................................... 9
       Operating Conditions ...................................................................................................................... 9
       Health Testing ................................................................................................................................. 9
       Certificate validation ......................................................................................................................... 10
       Security architecture ....................................................................................................................... 10
   B. Format and delivery of evidence for a potential PSN CA service .................................................. 10

III. GLOSSARY ........................................................................................................................................ 12
REFERENCES

[a] The Process for Performing CAS Assessments, CESG
[d] HMG IA Standard No.4 - Supplement 10 Compliance, Issue 1.0, April 2011
[e] HMG IA Standard No.4 - Supplement 11 Incident reporting for cryptographic items, Issue 3.0, April 2013
[g] CAS PSN CA Service Requirement, version 1.8, July 2012 – CESG 21035544
[i] PSN certificate and CRL profiles for IPsec IL3, version 1.0, February 2013 - PSNA
[j] PSN Certificate Practice Template – PSNA
[k] PSN compliance public services network programme, version 3.7, July 2012
I. OVERVIEW

A. Introduction

1. This document provides the CESG Assured Service (CAS) requirements for provision of a Certificate Authority (CA) that is part of the Public Services Network (PSN) Public Key Infrastructure (PKI).

2. This CAS service requirement supersedes the CAS PSN CA service requirement (ref[g]). Exceptionally, much of the structure of that document is retained in preference to the standard format for a CAS service requirement.

B. Service aims

3. Operation of a PKI allows mutual recognition and trust between entities that use certificates issued by a CA. The process defined in this document sets out requirements that potential providers of a PSN IL3 service must satisfy.

C. Future enhancements

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

D. PSN on boarding and initial steps

5. A potential industry service Provider of a PSN CA must follow the standard PSN service compliance process (ref[k]). The service provider offers evidence of compliance against the PSN Code to the PSNA; the Code of Practice (CoP) which describes an agreement of service provider obligations and the Code of Interconnection (ColCo) which contains requirements of how the PSN network will connect to the PSN backbone known as the Government Conveyance Network (GCN). The PSNA describes these codes in the PSN Code Template (ref[l]). PSNA can be contacted via email (currently psn@cabinet-office.gsi.gov.uk).

6. If PSNA approves the PSN Code, PSNA will give authority to proceed with a CAS assessment and pass details of the potential PSN CA service to CESG.

7. Upon an approved application, CESG will provide information about relevant CESG cryptographic policy and standards (as detailed later in this document), access to the PSN Certificate Policy (CP) (ref[h]) plus PSN certificate and CRL profiles (ref[i]), and access to the PSN Certificate Practice Statement (CPS) template (ref[j]).

8. The Provider must contract with CESG to perform the evaluation, compile an 'evidence pack', and return it to CESG.
E. Conduct of the assessment

9. The basic assurance requirement is for the service provider to present evidence that their service satisfies PSN CA service requirements and related CESG cryptographic policy. The format of the evidence is at the discretion of the service provider. The purpose of the evidence is to demonstrate that the proposed service is well designed, well implemented and well operated in line with industry good practice and relevant CESG Good Practice Guides and cryptographic policy.

10. The CAS assessment team may require clarification or additional evidence before giving a CAS assurance recommendation. Possible forms of additional evidence include new/updated documentation, design review(s) and an ITHC with improved scope.

11. The CAS assessment team will take a pragmatic approach when determining which elements of CESG policy and guidance are relevant to a PSN CA, and the degree of risk associated with limited or non-compliance to a control.

F. Assumptions

12. Work is in hand to achieve HMG accreditation of the PSN CA by the PGA, and the outcome will be accreditation granted by the PGA.

13. The PSN on boarding process and accreditation by the PGA will confirm that service procedures implemented by the Provider to support the PSN CA service are mapped (where applicable) to the mandatory requirements of the Security Policy Framework (SPF) (ref[b]).

14. Accreditation by the PGA will confirm that risks are identified, understood and mitigated to an acceptable degree.

15. The assertion about physical security of premises and equipment made in the PSN Code and validated by PSNA will be confirmed by the PGA as part of the process of accreditation.

16. The assertion about security clearances of staff made in the PSN Code and validated by PSNA will be confirmed by the PGA as part of the process of accreditation.

17. This assurance methodology assumes that a significant proportion of the service being assessed is complete, and that the provider has clear designs and processes in place for any incomplete elements. This assurance methodology should not be used against unfinished systems or those still in the design stage, and is separate from accreditation of the service.
II. REQUIREMENTS

A. Requirements for a PSN CA service

18. Each PSN CA service must comply with the PSN CP (ref[h]). Evidence of compliance must include a CPS defined against the PSN CP (ref[h]).

19. Each PSN CA must generate certificates and Certificate Revocation Lists (CRLs) in the format defined in the PSN certificate and CRL profiles (ref[i]).

20. Evidence will be required that the PSN CA will be subject to the compliance regime outlined in IS4 Supplement 10, Compliance (ref[d]), and will report any cryptographic incidents in accordance with the guidance provided in IS4 supplement 11, Incident reporting for Cryptographic Items (ref[e]).

Cryptographic Assurance

21. Each PSN CA must comply with relevant CESG cryptographic policy, specifically Cryptographic Mechanisms, Algorithms and Protocols (ref[j]), and apply relevant cryptographic assurance requirements (including operational and physical requirements) for the implementation of cryptographic mechanisms (signing certificates and CRLs), the protection of signing keys, the protection of interactions between service elements and the protection of interactions between the PSN CA service and external elements.

22. Evidence will be required that any key material or cryptographic systems are handled in accordance with the policy for the classification and handling of such materials throughout their life cycle, as outlined in IA Standard 4, Management of Cryptographic Systems (IS4) (ref[c]).

23. Assurance of a PSN CA service for use in protecting the 334 tier of PSN requires confidence that a number of security relevant cryptographic controls have been implemented correctly. This confidence is reached via independent assessment of the cryptographic primitives. A service entering assurance must have had its cryptographic primitives tested via either the CAVP or CMVP FIPS process, CPA, or a previous CESG cryptographic assessment⁴. The cryptographic primitives which must be assessed are those which are used in the production, signing, and revocation of PSN end-entity certificates for IPsec devices, in accordance with the PSN CP.

24. The certificate profile is specified in PSN certificate and CRL profiles (ref[i]). The supported algorithms are

- ‘interim’ profile: 2048 bit RSA and SHA-1; and
- ‘end state’ profile: ECDSA-256 and SHA-256

⁴ A vendor who believes that an alternative certification may cover the correct implementation of cryptographic primitives should contact CESG.
25. The PSN CA service provider must supply evidence of independent validation of all these primitives, and a statement regarding the applicability of such validation i.e. their assessment of why all security critical uses of cryptography within the operation of the PSN CA are covered by the validation.

26. Evidence must also be provided that the various cryptographic primitives have been tested end to end in a variety of common PSN CA service use cases (e.g. generation of a certificate, revocation of a certificate, renewal of a certificate); this testing may have been performed by the service provider, or via a third party. The intent is to show how the various products and components implementing cryptographic functionality within the provision of the service are working correctly together to provide the correct cryptographic protection of information.

27. As part of the CESG design review of the PSN CA service, any cryptographic areas which need particular attention will be highlighted.

Entropy Generation

28. The generation of entropy for use in key generation and other cryptographic purposes is a critical security control, and must be independently validated by CESG to ensure sufficient provision of random bits for the intended purpose within a PSN CA.

29. Sufficient entropy for the generation of PSN CA signing keys can be ensured by:
   - (RECOMMENDED) CESG evaluation of the design and implementation of the entropy generation within the service, including provision of additional entropy via a hardware-based noise source; or
   - CESG evaluation of the design and implementation of the entropy generation within the service, and provision of additional external entropy i.e. from UK KPA; or
   - provision of the PSN CA signing keys from UK KPA.

30. Sufficient entropy for generation of signatures (which require per-signature secrets) can be ensured by CESG evaluation of the design and implementation of the random number generation within the service, and provision of additional entropy via a hardware based noise source.

31. A PSN CA must generate non-sequential certificate serial numbers which include at least 20 bits of entropy.

32. To enable CESG evaluation of the design and implementation of the entropy source, the service provider must provide the following information.

Entropy Design Description

33. Documentation shall cover the design of the entropy source as a whole, including the interaction of all entropy source components. It must describe the
operation of the entropy source; how it works, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation must describe the entropy source design indicating where the random comes from, where it is passed next, any post-processing of the raw outputs (hash, XOR, etc), if / where it is stored and, finally, how it is output from the entropy source. Any conditions placed on the process (e.g. blocking) must be described in the entropy source design. Diagrams and examples are encouraged.

34. The design must include a description of the content of the security boundary of the entropy source, and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

Entropy Justification

35. There must be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source exhibiting probabilistic behaviour (an explanation of the probability distribution and justification for that distribution, given the particular source, is one way to describe this). This argument must include a description of the expected entropy rate and explain how it is ensured that sufficient entropy is going into the Deterministic Random Number Generation’s seeding process. This discussion will justify why the entropy source can be relied upon to produce bits with sufficient entropy.

Operating Conditions

36. Documentation must include the range of operating conditions under which the entropy source is expected to generate random data. It must clearly describe the measures that have been taken in the system design to ensure the entropy source continues to operate under those conditions. Similarly, documentation shall describe the conditions under which the entropy source is known to malfunction or become inconsistent. Methods used to detect failure or degradation of the source shall be included.

Health Testing

37. All entropy source health tests and their rationale must be documented. This will include a description of the health tests, the rate and conditions under which each health test is performed (e.g. at start-up, continuously, or on demand), the expected results for each health test, and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.

38. CESG will validate that the documentation and analysis provided by the service provider is logically consistent and sound, and that the evidence provided is consistent with the design of the entropy source. CESG may also request samples from the raw (unwashed) entropy provider for testing.
Certificate validation

39. Any aspects of the service which validate certificates must do so in accordance with the requirements in RFC5280, and the service provider must provide evidence of this validation behaviour. The validation must ensure that all certificate elements identified in the PSN certificate and CRL profiles (ref[i]) are processed correctly, and in particular that the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates. If the basicConstraints extension is not present or the cA flag is set to FALSE in a certificate then the service must not treat the certificate as a CA certificate.

Security architecture

40. The logical and physical design of the security architecture of the PSN CA, including separation of roles/functions, will be required. The results of a CESG design review of that security architecture will also be required.

41. General CA design and operation documentation will be required, including secure configuration that complies with PSN requirements and the configuration control process.

42. The scope and results of an IT Health Check will be required.

B. Format and delivery of evidence for a potential PSN CA service

43. The evidence provided for the CAS assessment must be linked to the requirements of this service requirement and to relevant HMG IA Standards and cryptographic policy.

44. Although the format of the evidence is at the discretion of the Provider, the evidence should be presented (where possible) in a common portable format, such as PDF.

45. Evidence provided in relation to the PSN CP (ref[h]) should be reused if relevant.

46. At CESG discretion, the results from a CESG design review held before the PSN CA was submitted for CAS assessment may be sufficient and an additional design review will not be needed during the CAS assessment. If a new design review is needed, CESG will provide information about the process for preparing for and participating in a design review.

47. All valid and relevant evidence of existing assurance should be presented, e.g. CAS(T) approval for an underlying network (if connected and reliant upon networked services), ISO/IEC27001 for server hosting, and security enforcing product certifications such as CAPS/CPA/CC where applicable.

48. The Provider must list the full range of PSN CA service functions that the PSN CA service provides (in the first instance, PSN only asks for support to end-entity
cryptographic devices using IPsec and the scope of this service requirement is limited to that service function – but existing CAs may also be supporting identity (personnel/device), web services, email, smartcards etc). All PSN certificates must be issued under the PSN CP (ref[h]) with a PSN CP OID.

49. CESG encourages Providers to obtain an industry recognised certification for all or part of their PSN CA service. While certification is not mandatory, details of certification should be submitted as part of the evidence pack when it is available and applicable. Valid industry recognised certification such as the following list will be accepted as supporting evidence. Please note - this list is not exhaustive. Other evidence of independent assessment will be accepted if the scope of the review is relevant to the PSN CA service being evaluated. (Associated documentation that details the differences between the current live CA service and PSN specific elements of the proposed PSN CA service will usually be required).

- ETSI TS 101 456/047
- ISO 2188:2006 PKI Implementation Audit
- tScheme
### III. GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Certificate Authority. An entity that issues digital certificates</td>
</tr>
<tr>
<td>CAPS</td>
<td>CESG Assisted Products Service. A CESG assurance service</td>
</tr>
<tr>
<td>CAS</td>
<td>CESG Assured Service</td>
</tr>
<tr>
<td>CAVP</td>
<td>Cryptographic Algorithm Validation Program. Validation of cryptographic algorithms under the security management and assurance group of NIST</td>
</tr>
<tr>
<td>CC</td>
<td>Common Criteria. An international assurance service</td>
</tr>
<tr>
<td>CMVP</td>
<td>Cryptographic Module Validation Program. Validation of cryptographic modules under the security management and assurance group of NIST</td>
</tr>
<tr>
<td>CP</td>
<td>Certificate Policy. Defines roles and responsibilities in a PKI</td>
</tr>
<tr>
<td>CPA</td>
<td>Commercial Product Assurance. A CESG assurance service</td>
</tr>
<tr>
<td>CRL</td>
<td>Certificate Revocation List. A list of certificates that may no longer be trusted within a PKI.</td>
</tr>
<tr>
<td>ETSI TS 101 456</td>
<td>EU standards for certification authorities and electronic signature formats</td>
</tr>
<tr>
<td>ETSI TS 101 047</td>
<td>EU standards for certification authorities and electronic signature formats</td>
</tr>
<tr>
<td>ISO 21188:2006</td>
<td>Practice and policy framework for PKI for financial services</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier.</td>
</tr>
<tr>
<td>PGA</td>
<td>Pan Government Accradiator. An individual with authority to accredit for pan-government use, responsible for approving operation of PSN connectivity service providers.</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PSN</td>
<td>Public Services Network. An infrastructure that connects HMG and other public sector organisations.</td>
</tr>
<tr>
<td>PSNA</td>
<td>Public Services Network Authority. The authority responsible for governance of the PSN</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority. Responsible for functions that include approval or rejection of certificate applications and revocation or suspension of certificates.</td>
</tr>
<tr>
<td>RFC5280</td>
<td>Specifies X.509 PKI certificate and CRL profiles</td>
</tr>
<tr>
<td>tScheme</td>
<td>An industry led self regulatory scheme that approves services against assessment criteria that it sets.</td>
</tr>
</tbody>
</table>