Guidance for HMG PKI CP Compliance

Ref. tSi 0274

Issue 1.00

2006-03-31

Executive summary

This document gives guidance to CAs wishing to be assessed for compliance against one or more of the Certificate Policies of the HMG PKI by a *tScheme*-recognised Assessor. It gives guidance on:

1. producing the various sorts of documentation required by *tScheme*;
2. how the Assessors can be expected to interpret some of the CP requirements;
3. the kinds of evidence that should be offered in support of Assessment claims.

DOCUMENT HISTORY

Status	Issue	Date	Comment	Authorised
tSi	Issue 1.00	2006-03-31	First Issued version	*tScheme* Secretariat

CONTENTS

1. INTRODUCTION

This document offers Eligible Certification Authorities guidance as to how they should expect their chosen assessor to perform the compliance assessment and how they should expect the assessors to interpret and make judgements on some of the Certificate Policy criteria.

In doing so, the document also offers guidance on:

- producing the various sorts of documentation required by *tScheme*;
- the kinds of evidence that could usefully be offered in support of assessment claims.

2. SCOPE

The document offers only guidance; it is not definitive. It does not provide additional criteria; it is an aid to the achievement of a successful assessment.

3. GUIDANCE

3.1 Terminology

The terminology in this document is based on the usage and definitions contained in the Certificate Policies of the HMG PKI [HMG CPs].

All other words should be taken in their general English or, if they are technical terms, generally understood technical sense.

3.2 Keeping track of Certificate Policy evolution

Under the terms of this scheme, *tScheme* determines the assessability of certificate policies that are eligible for CAs to be assessed. You must, therefore, ensure that you refer to the specific version of CP that is identified on the *tScheme* website when preparing for an assessment.

3.3 What is being measured

Documentary evidence will be reviewed and assessed to demonstrate that your organization has all of the appropriate processes and procedures in place to support the operation of the CA in compliance with the relevant certificate policies.

This will include manuals, policy statements, third-party agreements, audit trails etc. A fuller discussion on the kind of evidence required for a successful assessment is given later (see §4 Evidence).

In a number of places within the certificate policies, the written permission of the PMA is required. These must be obtained prior to any successful assessment.

Where deemed necessary, as part of a sampling approach, the assessor will confirm by interview and examination of objective evidence that policies, processes and procedures are implemented and effectively manage the operation of the CA.

3.4 What is not being measured

3.4.1 Financial Probity

Since all Eligible Certification Authorities must be UK public sector bodies, the normal *tScheme* requirements for financial probity do not form part of the assessment process as these aspects are already covered by the other processes within local- or central-Government oversight.

However, where the actual operation of the CA or RA is outsourced to a third-party supplier that is not an Eligible Certification Authority, then that third-party must be able to demonstrate approval under a recognised scheme (such as *tScheme*'s CA Profile - tSd 0102), which does cover financial probity amongst its criteria.

3.5 Assessing an Organization's Internal Security

Evaluation of the internal security practices of your organization is an important part of any assessment. An obvious approach to satisfying the assessor in this respect is to offer evidence showing that the guidelines of [ISO/IEC 17799] have been followed, or that [ISO/IEC 27001] has been conformed to, but it is acceptable to base security on other standards. However, assessors can be expected to exercise their judgement in vetting alternatives for suitability. The important overall rule they will apply is that any alternative must form a base from which the organization can furnish the assessor with evidence that relevant risks have been identified and are being effectively managed.

A checklist of topics that an acceptable standard or set of standards should encompass is:

- Security policy;
- Security organization;
- Asset classification and control;
- Personnel security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Systems development and maintenance;
- Business continuity management;
- Compliance with legal and security policy requirements.

3.6 The quality of cryptographic mechanisms

The acceptable parameters for the cryptographic mechanisms are given in the Certificate Policies and any deviation from these values would need the explicit written permission of the PMA.

3.7 Subscriber Agreement

The PMA has produced a template Subscriber Agreement, if, however, you decide to construct your own agreement then you will need to demonstrate to the satisfaction of the assessor that all of the relevant requirements of the given Certificate Policy have been met. This might increase the length, and hence the cost, of any assessment.

3.8 Relying Party Agreement

The PMA has produced a template Relying Party Agreement, if, however, you decide to construct your own agreement then you will need to demonstrate to the satisfaction of the assessor that all of the relevant requirements of the given Certificate Policy have been met. This might increase the length, and hence the cost, of any assessment.

3.9 Reassessments

A reassessment is an assessment performed for any of the following reasons:

- There has been a change in the volume of certificates issued to the extent that the organization's capacity or its risk assessments could be affected.
- The organization has materially changed in terms of location, key personnel or operational-hardware or –software; or its outsourcing arrangements have changed.
- A certificate policy against which the organization was previously assessed has been updated to the degree that the new version has been assigned a new Object Identifier.
- At the request of the PMA.

The extent of the reassessment depends very much on the nature and size of the change. Not all of the kinds of change listed above will result in a complete reassessment.

A reassessment might need to only assess changes, and the extent and cost of a reassessment is strongly related to the nature and size of the change being assessed. However, an assessor should bear in mind that changes in one area can impact, and thereby indirectly change other areas.

It is the organization's responsibility to follow the process outlined in the latest version of the "High Level Processes and Procedures" [HLPP] in all cases where a reassessment may be required.

4. EVIDENCE

This section collects together example forms of evidence that have been identified as being acceptable for demonstrating how the various requirements listed in the Certificate Policies have been complied with. It is intended to act as a checklist and guide. It is by no means definitive, and other forms of evidence may be found equally acceptable by assessors, however, this list is intended to allow assessors to conduct an efficient assessment process and to minimise the duration, and hence the cost, of the assessment.

Any variation in the forms of evidence presented might lead to a longer assessment process as it is up to the organization to demonstrate to the satisfaction of the assessors that the alternative forms of evidence are equivalent.

4.1 Compliance Documentation

4.1.1 General

1. A table cross-referencing the individual requirement statements of the certificate policy against the specific evidence being offered to demonstrate compliance with that requirement;
2. The Certificate Practice Statement;
3. Example agreements (but see §3.7 Subscriber Agreement and §3.8 Relying Party Agreement);
4. Evidence, where appropriate, of relevant PMA approvals (e.g. certificate naming policy).

4.1.2 Management competence

1. Reports from an independent auditing process, with due consideration of their professional status and any qualifications within the report;
2. Demonstration of effective documentation and operation of its relevant policies and procedures;
3. Provision of appropriate dispute resolution policies and procedures;
4. Implementation of a Quality Management System compatible with [ISO 9001].

4.1.3 Acceptable management and security policies and procedures

1. A documented statement of applicability describing the control measures to be implemented and reasons for their selection to meet the base criteria and any additional specific criteria;
2. Presentation of a documented Information Security Management System compatible with [ISO/IEC 17799], supported by a risk analysis.

4.1.4 Assurance of the technical infrastructure

1. A documented statement of applicability describing the control measures to be implemented and reasons for their selection to meet the base criteria and any additional specific criteria;
2. Documented evidence of the implemented security of the technical infrastructure and any procedures adopted to use and apply these controls;
3. Reference to any evaluation criteria, standards, design, development and assurance methods, that might have been used to build and implement.

4.1.5 The suitability of personnel used (skill and competence)

1. Job Descriptions, CVs and training records of the personnel concerned;

2. Auditable records to demonstrate approved definition, modification and application of the required personnel procedures and processes, particularly for those staff in sensitive roles.

4.1.6 Acceptable quality of externally provided CA or RA services

1. A clear description of the relationship and dependencies between the applicant organization and the contractors concerned, with risk analysis;
2. Appropriate contractual documentation;
3. The ISMS and operational procedures to show that communications with the contractors concerned have been secured to the required level;
4. Evidence of an existing successful *tScheme* Assessment of the contractor(s) concerned.

4.1.7 Acceptable quality of suppliers of technology, equipment and general support Services

1. The reputation and track record of the supplier;
2. Appropriate contractual documentation.

5. REFERENCES

[HLPP] "HMG PKI – High Level Processes and Procedures", latest version.

[HMG CPs] "HMG Certificate Policies", latest version.

[ISO 9001] "Quality management systems -- Requirements",
ISO 9001:2000, published 2000-12-15, ISBN 0 580 36837 8.

[ISO/IEC 17799] "Information technology. Security techniques. Code of practice for information security management",
ISO/IEC 17799:2005, published 2005-06-16, ISBN 0 580 46262 5.

[ISO/IEC 27001] "Information technology. Security techniques. Information security management systems. Requirements",
ISO/IEC 27001:2005, published 2000-10-18, ISBN 0 580 46781 3.

