Draft

# Required Compliance Procedures for the HMG PKI

**Ref. tSd 0275**

**Draft 0.01**

**2005-02-08**

## Executive summary

This document sets out the operational steps and processes (procedures) that are related to the overall establishment and operation of the HMG PKI CP Compliance Scheme process. These procedures are required to be followed by all parties participating within the scheme.

# DOCUMENT HISTORY

| Status | Issue | Date | Comment | Authorised |
|---|---|---|---|---|
| tSd | 0.01 | 2005-02-08 | First version, tracked under Document Management procedures. | *tScheme* Secretariat |

 

# CONTENTS



 

 

# PART 0
# INTRODUCTION

## 1 PURPOSE

This document sets out the operational steps and processes (procedures) that are related to the overall establishment and operation of the HMG PKI CP Compliance Scheme process. These procedures are required to be followed by all parties participating within the scheme.

## 2 READERSHIP

This document is **required reading** for all those having a role within this compliance scheme. These are:

- ***tScheme*-recognised Assessors** (who perform compliance assessments);
- **Eligible Certification Authorities** (who are applying to become Certification Authorities within the HMG PKI);
- **Policy Management Team** (the body responsible for generating detailed policy and assisting public bodies in joining the HMG PKI);
- ***tScheme* representatives** (who are responsible for the operation of the scheme and the continued application and maintenance of these, and other, procedures).

Each separate Part of this document states for which of the aforementioned parties that specific Part is required reading. The requirements are summarised in tabular form below. These Parts specifically refer to further *tScheme* documentation all of which is also to be considered as required reading.

This Part of this document is to be read by all.

 

# 3 DOCUMENT STRUCTURE

The document is structured into seven discrete and essentially integral Parts, starting with this Part (0), which provides overall information about the document. The other Parts provide the substantial content of the document and establish a logical sequence of procedures that are to be followed in order for the CP Compliance scheme to function effectively. Not all participants within *tScheme* need be involved in each Part. The following table establishes which Parts are required reading for which parties. The table is linked to and from the respective Parts, to aid readers in moving between Parts within the document:

| Part and Title | | *tScheme*-recognised Assessors | Policy Management Team | Eligible Certification Authorities | *tScheme* representatives |
|---|---|---|---|---|---|
| PART I | Registering for a Compliance Assessment | ✓ | ✓ | ✓ | ✓ |
| PART II | Contracting for a Compliance Assessment | ✓ | ✓ | ✓ | ✓ |
| PART III | Performance of Compliance Assessments | ✓ | ✓ | ✓ | ✓ |
| PART IV | Applying for a Statement of Compliance | ✓ | ✓ | ✓ | ✓ |

# 4 GENERAL REMARKS

At the time of publication of this issue of this document tScheme Limited also operates a voluntary approval scheme, *tScheme,* that provides Grants of Approval for Operational Services that have been independently assessed as meeting the relevant criteria contained in one or more of its Approval Profiles.

As part of that Approval scheme, certification bodies are selected and 'recognised' by *tScheme* as being competent to carry out the necessary Assessments. Further details are to be found in the Required Assessment Procedures document (tSd0244). For the purposes of this Compliance Scheme, assessments may only be carried out by such *tScheme*-recognised Assessors.

Definitions of terms and acronyms not defined in this document may be found in the *tScheme* Glossary of Terms, which itself is **required reading** in order that participating parties understand to the fullest extent the intentions of these procedures.

References to *tScheme* should be interpreted generally to mean the *tScheme* Secretariat, unless specifically otherwise qualified (e.g. *tScheme* Board).

At any time readers of this document may seek clarification and further guidance from the *tScheme* Secretariat.

# 5 FEES DUE

*tScheme* may charge fees for the various services it provides. The collection, timing and value of these fees is not addressed by this document but a scale of fees is published on the *tScheme* website and those parties applying for services will certainly be advised fully at the time they make their application as to the nature of any fees and when they fall due.

# PART I
# REGISTERING FOR A COMPLIANCE ASSESSMENT

This Part consists of §6 to §9 inclusive of the whole document.

## 6 READERSHIP

This part of the *tScheme* Required Compliance Procedures is **required reading** for the following parties and reasons:

- The **Policy Management Team** (**PMT**) who decide whether an organization is eligible to apply to join the HMG PKI, and, if they are, guide them in applying for assessment;
- **Eligible Certification Authorities** (**ECAs**) planning to have the operation of their CA assessed for compliance against one or more of the Certificate Policies of the HMG PKI. Each assessment shall deal only with one Certificate Policy. However, it is conceivable and not impermissible that an applicant might have more than one assessment being conducted in parallel, and gaining some economy from so doing. *tScheme* would treat each on its own specific merits;
- ***tScheme*-recognised Assessors** performing the assessment of **ECAs**, with the objective of the subject of assessment being given the appropriate *tScheme* endorsement, supported by a Compliance Report, to demonstrate to the **PMT** that they comply with the requirements of the stated Certificate Policy(ies);
- ***tScheme*'s representatives** who are responsible for processing registrations and maintaining the appropriate register information.

## 7 WHY BECOME A REGISTERED APPLICANT?

By registering as an applicant, *tScheme* is able to offer the organization support and guidance on being assessed for compliance against one or more of the Certificate Policies.

*tScheme*-recognised Assessors shall not contract for the performance of a CP Compliance assessment unless the applicant can provide evidence of Registered Applicant status.

During the early stages of an application *tScheme* may offer an introductory consultancy service to provide initial advice and guidance to TSPs and Suppliers.

## 8 ADDITIONAL REQUIRED READING

HMG PKI – High Level Processes and Procedures;

Model Compliance Report (tSi 0276);

Guidance for HMG PKI CP Compliance (tSi 0274).

 

# 9 PROCEDURES

## 9.1 Applying for Registered Applicant status

The applicant shall submit to the *tScheme* Secretariat its request for Registered Applicant status, using the proformæ *tScheme* HMG PKI Compliance Applicant letter.

The *tScheme* Board, itself or in delegated committee, will consider all applications at its next scheduled meeting: it may seek supplementary information where it deems appropriate.

Applicants should note that *tScheme* reserves the right not to accept an application that could in *tScheme*'s view, possibly lead to the overall trustworthiness of *tScheme* being brought into disrepute. The decision of the *tScheme* Board shall be final in all respects relating to the discretionary award of *tScheme* Registered Applicant status. Where the Board determines that it is not appropriate to accept the application it will provide a written justification of its decision.

In the case where an application is declined it will not be possible for the applicant to contract for a Compliance assessment.

## 9.2 Registered Applicant agreement

If the application is accepted, *tScheme* will prepare an instantiation of the *tScheme* Model HMG PKI Applicant Agreement, incorporating the details submitted by the applicant in its application letter. This will be sent undated to the applicant, inviting its signature.

After signature by one of its authorised Directors, the applicant shall return the agreement to *tScheme*. *tScheme* will then return a countersigned and dated copy of the agreement as notification of a successful application. The date of the countersigned agreement shall be the date on which *tScheme* Registered Applicant status is granted.

Each agreement shall lapse at the end of the period stated in the *tScheme* HMG PKI Applicant Agreement. A subsequent application may be made in respect of the same or alternative certificate policies, and *tScheme* will consider each application on its merits.

## 9.3 Rights and Obligations

Once the applicant is enrolled as a *tScheme* Registered Applicant, it will be permitted to use this description in connection with the CA that it is submitting for Assessment. The applicant shall not represent nor construe its *tScheme* Registered Applicant status as a form of preliminary or interim approval.

In consideration of the endorsement by *tScheme*, the applicant undertakes to complete the full assessment process within the specified timescale, as stated in its agreement with *tScheme*.

## 9.4 Publication of status

Ordinarily, *tScheme* will publish full details of the applicant's status, including the date of registration, on the *tScheme* website (tScheme-registered Applicants (HMG PKI)). This permits interested parties

to confirm the applicants' claims regarding their status within *tScheme*. *tScheme* shall, at the applicant's express request, withhold from publication in the register notification of the applicant's application[1]. In the event of this request being made, the applicant may make no public reference to such Registered Applicant status.

[1] Some applicants may choose not to publicise their participation until later in the Assessment process, or until a positive Assessment has been achieved, rather than suffer the ignominy of having to withdraw a public declaration of having attempted an Assessment, the results of which were 'unfavourable' or revealing a slippage in their timetable.

 

# PART II
# CONTRACTING FOR A COMPLIANCE ASSESSMENT

This Part consists of §10 to §0 inclusive of the whole document.

## 10 READERSHIP

This part of the *tScheme* Required Compliance Procedures is **required reading** for the following parties and reasons:

- The **Policy Management Team** (**PMT**) who decide whether an organization is eligible to apply to join the HMG PKI, and, if they are, guide them in applying for assessment;
- **Eligible Certification Authorities** (**ECAs**) planning to have the operation of their CA assessed for compliance against one or more of the Certificate Policies of the HMG PKI. Each assessment shall deal only with one Certificate Policy. However, it is conceivable and not impermissible that an applicant might have more than one assessment being conducted in parallel, and gaining some economy from so doing. *tScheme* would treat each on its own specific merits;
- ***tScheme*-recognised Assessors** performing the assessment of **ECAs**, with the objective of the subject of assessment being given the appropriate *tScheme* endorsement, supported by a Compliance Report, to demonstrate to the **PMT** that they comply with the requirements of the stated Certificate Policy(ies);
- ***tScheme*'s representatives** who are responsible for processing registrations and maintaining the appropriate register information.

## 11 WHY CONTRACT FOR AN ASSESSMENT?

It is a condition of acceptance into the HMG PKI that an applicant organization demonstrates compliance against one or more of the relevant certificate policies. tScheme Ltd. has agreed with the Policy Management Authority of the PKI that it will provide the facility within the overall *tScheme* process, for Eligible Certification Authorities to be independently assessed for such compliance.

In order to ensure that the process is being adhered to correctly, it is necessary for the various parties to enter into contractual arrangements.

The point at which a contract is entered into, and under what terms and conditions, is a matter of commercial judgement for the Assessor and the **ECA**, so long as *tScheme*'s express procedures are fulfilled.

During the early stages of an application *tScheme* may offer an introductory consultancy service to provide initial advice and guidance to **ECAs**.

## 12 ADDITIONAL REQUIRED READING

HMG PKI – High Level Processes and Procedures;

 

Model Compliance Report (tSi 0276);

Guidance for HMG PKI CP Compliance (tSi 0274).

# 13 PROCEDURES

## 13.1 Preparing for a Compliance Assessment

In order for applicant organizations to prepare for an assessment, *tScheme* and the **PMT** have produced a guide to the kinds of evidence required - Guidance for HMG PKI CP Compliance (tSi 0274).

## 13.2 Preparation of a Compliance Report

At the conclusion of a successful assessment, the Assessor shall produce a signed Compliance Report that reflects the conduct and outcome of the assessment and provides a statement of satisfaction of the requirements of the selected certificate policy.

The Compliance Report shall fulfil the requirements set out in Model Compliance Report. Note that the Assessor may produce a document of their own format and structure so long as *tScheme*'s information requirements as set out in the Model Compliance Report are satisfied.

In the event that a successful report on the assessment of a CA has qualifications in it, the Assessor shall, by making such qualifications, assert that the CA will be sufficiently trustworthy to comply with the CP requirements if operated as assessed and furthermore that it will review all qualifications within a maximum period of six months and shall report back to *tScheme* the outcome of these reviews and any consequential recommended action that is required to be taken (either by the Assessor itself or by *tScheme*).

In the case that the Assessor is unable to issue a Compliance Report declaring a successful outcome to the assessment, even after the applicant has taken any recommended remedial steps, the applicant shall be unable to apply for *tScheme* endorsement of their application for membership of the HMG PKI.[2] The applicant must notify *tScheme* if this leads to slippage in the timetable agreed in connection with the grant of Registered Applicant status, or if the application is to be withdrawn.

## 13.3 Limitations to contract

Through its agreements with both the Assessor and the Registered Applicant, *tScheme* requires that these parties **shall not** contract for a *tScheme* CP compliance assessment other than for the exclusive purpose of producing a Compliance Report to support the applicant's application for membership of the HMG PKI if the Assessment is successfully concluded.

[2] In the situation where the assessment is not successful the full procedural requirements of *tScheme* need not be satisfied explicitly if the applicant elects to terminate the assessment process, e.g. no Compliance Report need be issued. This entitlement does not affect any contractual obligations between the Assessor and the applicant.

 

# PART III
# PERFORMANCE OF COMPLIANCE ASSESSMENTS

This Part consists of §14 to §0 inclusive of the whole document.

## 14 READERSHIP

This part of the *tScheme* Required Compliance Procedures is aimed primarily at *tScheme*-recognised Assessors, but is intended to be **required reading** for the following parties and reasons:

- The **Policy Management Team** (**PMT**) with the objective that they are satisfied that the process provides sufficient assurance of compliance with the certificate policies of the HMG PKI;
- **Eligible Certification Authorities** (**ECAs**) planning to have the operation of their CA assessed for compliance against one or more of the Certificate Policies of the HMG PKI, with the objective of them understanding the processes that lead to being successfully assessed against the criteria in the chosen Approval Profiles;
- ***tScheme*-recognised Assessors** performing the assessment of **ECAs**, with the objective of them (collectively) producing Compliance Reports based upon a consistent approach to the application of the requirements of the CPs of the HMG PKI;
- ***tScheme*'s representatives** who are responsible for monitoring and tracking the progress of registered applicants' compliance assessments.

## 15 WHY PERFORM A COMPLIANCE ASSESSMENT?

In order to be able to apply for inclusion in the HMG PKI, an **Eligible Certification Authority** must be able to demonstrate, to the satisfaction of the **PMT** that it complies with the requirements of one or more of the Certificate Policies of the HMG PKI. *tScheme* will only support an application for inclusion in the HMG PKI if it is supported by a recent Compliance Report issued by a *tScheme*-recognised Assessor.

Furthermore, the validity of a Report is two years, and it will then be renewed biennially unless the Certification Authority fails to pay its fees or the agreement with *tScheme* is terminated. However, the biennial renewal is dependent upon the production, to *tScheme*, of a recent Compliance Report, which in this context should be taken as being less than three months old.

It is the responsibility of the organization operating the CA to ensure that the Assessor carries out reviews in such a timely manner as to allow submission of renewal reports to *tScheme* one month prior to the anniversary of the initial report. If this is not possible then the organization must notify *tScheme* of the date by which the renewal report will be submitted, which can be no more than one month after the anniversary of the initial report, and the reason for the delay. Upon submission of an acceptable renewal report and subject to payment of the appropriate fees, the validity of the Statement of Compliance will be extended by a further two years to the next anniversary of the initial report.

An Assessor can only prepare a Compliance Report on what it has seen and on evidence judged for itself, and whilst it is required to exercise professional judgement it cannot be expected to second-guess any aspects of the subject of its assessment.

 

# 16 ADDITIONAL REQUIRED READING

HMG PKI – High Level Processes and Procedures;

Model Compliance Report (tSi 0276);

Guidance for HMG PKI CP Compliance (tSi 0274).

# 17 PROCEDURES

## 17.1 Entitlement to perform Assessments

Only those assessors that have been accredited by a recognised Accreditation Body and which have become *tScheme*-recognised Assessors (see Required Assessment Procedures) shall perform Compliance assessments against CPs of the HMG PKI.

## 17.2 Roles and Qualifications

Assessors shall ensure that staff performing assessments have a sufficient working knowledge of the technology being assessed, and an understanding of:

- current PKI security issues, as raised in the IT media, technical development forums, workshops, and conferences;
- third-party perceptions and expectations, in particular, the ability to view the subject of a compliance assessment from the viewpoint of a subscriber or relying party.

Assessors shall not accept a contract to perform a Compliance Assessment unless, having reviewed the Certificate Practice Statement for the assignment, they can confidently field an assessment team that has the experience to address fully all aspects of the subject of the Compliance Assessment.

## 17.3 Assessors' Use of External Experts

Assessors shall also have experts who are specialists in areas where assessment requires specialist knowledge. Whereas it may not always be practicable to have such experts employed as permanent staff it is reasonable for Assessors to make use of external experts where this is required. However the Assessor shall carefully check such experts for experience and track record. They should be considered to be playing a role similar to that of an expert witness in court, and should be checked accordingly. The contractual relationship and method of working between an external expert and an assessing body is a matter for the Assessor to decide.

## 17.4 Certificate Policy Recognition

Part of the *tScheme* CP Compliance process is that compliance can only be assessed against particular versions of specific Certificate Policies (see website) that have been reviewed and determined as assessable. So it is expected that Assessors shall always use the latest available approved versions of the Certificate Policies. Whilst *tScheme* will not approve revisions and developments of Certificate Policies without due process of membership review &c, it remains an Assessor's responsibility to keep

 

track of such developments through liaison with *tScheme*, so as to keep up to date with anticipated changes to the CPs, since this may affect the scheduling of the assessment[3].

Where there is a critical timing between an assessment whose conclusion is imminent and any revisions to Certificate Policies being used in that assessment, the Assessor may request *tScheme* to grant a waiver to the preceding paragraph where it is agreed that the changes shortly to become current do not materially affect the relevance of the assessment. *tScheme* will not be under any obligation to grant such a waiver, and each case will be considered entirely on its own merits. Where practicable, and where a waiver is granted, *tScheme* will encourage informal adoption of any changes in anticipation of the formal change.

Compliance Reports must always refer to the version numbers of the certificate policy actually used by the Assessor in completing the assessment.

[3] In particular it may be appropriate to delay an assessment in order to be able to use an imminent, but not yet available version.

 

# PART IV
# APPLYING FOR A STATEMENT OF COMPLIANCE

This Part consists of §18 to §20 inclusive of the whole document.

## 18 READERSHIP

This part of the *tScheme* Required Compliance Procedures is aimed primarily at assessed TSPs and Suppliers applying for a Grant, but is intended to be **required reading** for the following parties and reasons:

- The **Policy Management Team** (**PMT**) with the objective that they are satisfied that the process provides sufficient assurance of compliance with the certificate policies of the HMG PKI;
- **Eligible Certification Authorities** (**ECAs**) submitting an application for inclusion in the HMG PKI based upon the successful assessment of their CA against the requirements in the chosen certificate policy;
- ***tScheme*-recognised Assessors** who have prepared the Compliance Report supporting the application;
- ***tScheme*'s representatives** who are responsible for monitoring and tracking the progress of registered applicants' compliance assessments.

## 19 WHY APPLY FOR A STATEMENT OF COMPLIANCE?

*tScheme* endorsement of an application for inclusion in the HMG PKI, in the form of a Statement of Compliance, can only be awarded if the organization submits an application that is subsequently accepted by the *tScheme* Approvals Committee and the applicant undertakes, by contract, to abide by the *tScheme* Code of Conduct and other associated conditions. This is the only legitimate route by which an applicant can be supported by *tScheme* in relation to an application for inclusion in the HMG PKI.

## 20 ADDITIONAL REQUIRED READING

HMG PKI – High Level Processes and Procedures;

Model Compliance Report (tSi 0276);

Guidance for HMG PKI CP Compliance (tSi 0274).

 

# 21 PROCEDURES

## 21.1 Submission of an application for a Statement of Compliance

The applicant shall submit to the *tScheme* Secretariat its application, using the electronic forms tScheme SOC Application. The application shall be accompanied by the following supporting documents:

- the Compliance Report, issued by the *tScheme*-recognised Assessor who performed the Compliance Assessment;
- a signed undertaking to abide by the *tScheme* Code of Conduct, should the Statement of Compliance be endorsed, as included in the appropriate electronic application form.
- a signed undertaking to pay the fees associated with the Statement of Compliance, once it is confirmed by *tScheme*.

## 21.2 Consideration of an application

After checking by the *tScheme* Secretariat and any inconsistencies having been resolved with the applicant and/or the Assessor, the application will be passed to the *tScheme* Approvals Committee for consideration at its next meeting. The Committee will ensure that the Assessor is currently recognised and that there is no over-riding reason not to endorse the Statement of Compliance.

## 21.3 Notification of application result

Should the Approvals Committee reject an application, *tScheme* will inform the applicant within 7 days of reaching its decision. In exceptional cases, the applicant may resort to appeal against the decision.

On the decision to endorse the Statement of Compliance, *tScheme* will notify the applicant of its decision and will confirm such to the **PMT**.

### 21.3.1 Successful Compliance Assessment

Once the endorsement of the Statement of Compliance is given, *tScheme* will update its Register of CP Compliant Organizations by adding details of the organization. This register appears on the *tScheme* website as an electronically-signed list and will include the following information for each entry:

- the identity of the organization;
- the specific Certificate Policy for which the Statement of Compliance was given.

This latter item is a hyperlink to the relevant entry in the list of all Compliant and Applicant Organizations listed by Certificate Policy, and that list will include the following information for each entry:

- the identity of the organization, which is a hyperlink giving the relevant contact details for that organization (name, address, email, phone number, website etc.);
- the Assessor (name as used in the register of *tScheme*-recognised Assessors);
- date of successful Compliance Report.

 

## 21.4 Appointment of the Approvals Committee

The Approvals Committee will be appointed by the *tScheme* Board to provide independent adjudication over applications, both for *tScheme* Approvals and for Compliance assessments for the HMG PKI. To ensure impartiality in reaching decisions regarding approvals, the *tScheme* Approvals Committee will consist of individuals who are neither of themselves nor through their employment Trust Service Providers or Component Suppliers. They may be non-TSP / non-Supplier members of *tScheme*, independent user representatives or other appropriate individuals co-opted from time to time. The *tScheme* Board will appoint the chairman of the Approvals Committee.

 