



Model Compliance Report for the HMG PKI

Ref. tSd 0276

Issue 1.00

2006-5-19

Executive summary

This document serves as the model for the production by a *tScheme*-recognised Assessor of a Compliance Report in a form acceptable to the Policy Management Authority of the HMG PKI

Individual copies of this document may be downloaded from <http://www.tScheme.org/>.

The definitive version of this document is the one available for public download from <http://www.tScheme.org/> in Adobe Acrobat Reader format. This document is subject to revision so please check that you have the current version.

Please report errors and address comments to Editors@tScheme.org.

Copyright: This document may be copied in whole or part for private research and study but not otherwise without the express permission of *tScheme* Limited. All copies must acknowledge *tScheme* Limited's copyright. These restrictions apply to copying in all media.

DOCUMENT HISTORY

Status	Issue	Date	Comment	Authorised
tSd	1.00	2006-5-19	First Issued version	<i>tScheme</i> Secretariat

CONTENTS

0. PROLOGUE	4
0.1 PURPOSE	4
0.2 CONFORMANCE ADVISORY	4
0.3 READERSHIP	4
0.4 OVERVIEW, PREPARATION AND REPRESENTATION	5
0.5 CONFIDENTIALITY	5
1. DOCUMENT CONTROL.....	6
1.1 IDENTIFICATION	6
1.2 COPYRIGHT AND ACKNOWLEDGEMENTS	6
1.3 CONTENTS	7
2. CERTIFICATION STATEMENT.....	8
2.1 QUALIFICATIONS TO THE CERTIFICATION	8
3. METHOD AND EVIDENCE EMPLOYED.....	9
4. ASSESSOR COMMENTS	10

0. PROLOGUE

Introductory note:

In this model Compliance Report, the contents of this Prologue and its sub-sections refer solely to this model document description and should not appear as such in any instance of an actual Compliance Report.

0.1 Purpose

This document serves as the model for the production of a Compliance Report by a [tScheme-recognised Assessor](#) when commissioned by an Eligible Certification Authority (ECA) to produce a report certifying compliance with one of the certificate policies (CPs) of the HMG PKI.

This model is intended to be used by *tScheme*-recognised Assessors in regard to the minimum *tScheme*-required format and content for reports that they write.

0.2 Conformance Advisory

Conformance to all aspects of this model on the part of report authors is strongly advised but not mandatory. Where deviation from the advised content in the given format is prohibited, this is marked as such. Where deviation in ordering, layout or wording is permitted, authors shall not use this as cause to omit, in whole or part, otherwise advised content. Authors should generally avoid the inclusion of content beyond that advised where there is any possibility that this may conceal, confuse or dilute the clarity of the report in certifying, and giving sound evidence for certifying, that the subject ECA complies with the chosen certificate policy.

0.3 Readership

This document is required reading for the following parties, as laid down in the [Required Compliance Procedures for the HMG PKI](#):

- **tScheme-recognised Assessors** who will be reporting on the outcome of compliance assessments of the operation of Eligible Certification Authorities;
- the **Policy Management Team (PMT)** of the HMG PKI who will be receiving Compliance Reports with ECAs' applications for inclusion in the HMG PKI.

This document will also be of interest to ECAs who will be given a Compliance Report by their chosen *tScheme*-recognised Assessor in support of their application for inclusion in the HMG PKI.

0.4 Overview, Preparation and Representation

This model provides a framework of sections and sub-headings together with proposed standardised text. The author of a specific instance of a Compliance Report may apply his own styles, phrasing and terminology to the model commensurate with supplying the advised content (including mandatory wording) and structure and otherwise meeting the spirit of what is required. This commonality of presentation assists readers who have to deal with Compliance Reports from many different sources.

tScheme's [Required Compliance Procedures for the HMG PKI](#) is required prior reading for Compliance Report authors. It describes the overall process for applying for tScheme assessment and points to other detailed sources.

Text appearing in sans serif font provides obligatory wording (as per this paragraph) that the author shall provide without variation or augmentation.

Text intended to offer narrative or guidance is in italicised text of this colour, framed within a solid border (as per this paragraph). This text should not appear in an actual report.

Within the obligatory and indicative text, there are placeholders where authors shall substitute the specific details of their actual assessments. These are indicated using «chevrons» as indicated in this sentence. Even where authors can and do choose alternative phrasing, they shall ensure that all of the information items within chevrons still appear.

tScheme requires that each Compliance Report is subject to effective configuration management, which requires that it carries a unique identity and title, including a front title page, table of contents, document history where relevant, and version or issue number. However, tScheme recognises that individual assessors will have their own house styles for documents that will dictate the final visual appearance of their reports. They may also wish to include specific service-related information. Hence an author may substitute an alternative style for the tScheme one used and recommended in this model. It is assumed therefore that any specific instantiation of this model will be subject to the owner's own effective configuration management practices, and hence the model explicitly suggests none of these.

Improvements, enhancements and the provision of additional information to make the Compliance Report more comprehensive, understandable or persuasive are fully encouraged within the constraint of covering the model and the advised content in its entirety.

Definitions of terms and acronyms that are not included in this document appear in the [tScheme Glossary of Terms](#).

0.5 Confidentiality

tScheme undertakes not to place in the public domain any information in the Compliance Report that is not indicated herein as being so destined or else without gaining the ECA's prior consent. However, tScheme will not undertake to restrict access to any of the information in the Compliance Report for its internal purposes. Submission of a Compliance Report to tScheme by an ECA implies that tScheme can use the content for any of tScheme's internal processes relating to applications for inclusion in the HMG PKI.

The following sections and headings are those recommended by this model Compliance Report.

1. DOCUMENT CONTROL

The illustrative text given in this section is written in the singular. Authors should replace with the plural where relevant.

1.1 Identification

This report, reference «optional reference number», relates to the assessment of the Eligible Certification Authority known as «name of organization» that commissioned this report from «name of tScheme-recognised Assessor».

The author of this report is «name of individual» who, together with «optional name(s) of individual(s)», performed the assessment during the period between «date» and «date».

1.2 Copyright and Acknowledgements

Ownership of copyright is a matter of contract between the ECA and the assessor. The text should reflect the chosen arrangement. The granting of copy permission to tScheme Limited is mandatory but the precise wording of the grant is a matter for the owner.

© «name», «year».

All rights reserved. «name of copyright owner» permits tScheme Limited to copy the contents in whole or part for all purposes relating to the processing of, publication of and investigation of the application for the inclusion in the HMG PKI of the Eligible Certification Authority that is the subject of this report, notwithstanding the undertaking given in §0.5.

The following acknowledgement list may be omitted or extended as appropriate.

«trade name» is a trade name of «owning organization».

1.3 Contents

1. DOCUMENT CONTROL.....	6
1.1 IDENTIFICATION.....	6
1.2 COPYRIGHT AND ACKNOWLEDGEMENTS	6
1.3 CONTENTS	7
2. COMPLIANCE STATEMENT.....	8
2.1 QUALIFICATIONS TO THE COMPLIANCE STATEMENT	8
3. METHOD AND EVIDENCE EMPLOYED.....	9
4. ASSESSOR COMMENTS	10

2. COMPLIANCE STATEMENT

We

«name of *tScheme*-recognised Assessor»

of

«registered address»

certify that the Certificate Practice Statement and management system used to deliver the Certification Authority as operated by

«name of organization»

complies with the requirements of the following certificate policy

«name of certificate policy» version «version»

as at the date of this report, being

«date of Compliance Report»

Declaration made by «name of individual», «position or title» on behalf of the above named *tScheme*-recognised Assessor.

2.1 Qualifications to the Compliance Statement

Assessors are encouraged to require ECAs to resolve outstanding issues prior to completion of an assessment rather than issuing a Compliance Report with qualifications and *tScheme* Limited reserves the right to reject a Compliance Report that it deems to include qualifications that prejudice the good standing of the *tScheme* name.

Any outstanding qualifications shall however be stated clearly immediately after the Compliance Statement, each being supported by:

- a reference to the related certificate policy requirement (by clause identity);
- the reason for requiring the qualification;
- a justification for accepting the Certificate Authority as found;
- remedial action agreed between the Assessor and the applicant;
- a resolution date by which remedial action shall be undertaken and the Assessor will have cleared the qualification.

The period for resolution of any qualification shall not exceed six months from the date of the report and will ideally be held to a period of three months from that date. *tScheme* reserves the right, in the event of failure to achieve these dates, to review the situation and take whatever consequential action it deems necessary and justified.

3. METHOD AND EVIDENCE EMPLOYED

This section provides a summary of the procedure that the Assessor followed that led him to conclude that the operation of the Certification Authority complied with the requirements in the specified certificate policy.

The author should consider this content on a clause-by-clause basis for the relevant certificate policy. For each major heading thereof, the Assessor shall state in summary form: the conduct of the Assessment, any significant findings and what relevant evidence he accepted as showing compliance with the requirements.

Where possible, the assessor should adopt a tabular format. A suggested format appears below. However, the assessor is free to substitute its own presentation form.

The summary tables appearing at the end of the Approval Profiles should be used by Assessors to record the specific evidence assessed for each criterion. Although such completed lists may not form part of the Compliance Report itself, tScheme reserves the right to ask for sight of these should it feel that it is necessary.

IMPORTANT NOTE: *tScheme will not accept declarations that depend on future events, intentions or general plans.*

Clause	Action	Evidence
«tag»	«description of inspection action»	«description of evidence»

4. ASSESSOR COMMENTS

Any further information that the Assessor may wish to add about the subject ECA, the Certificate Practice Statement, the Certificate Policy, the third-party agreements, difficulties in operating the process, or anything else. There is no prescribed format.

Such comments may relate to known plans for extension or other significant change to the circumstances of the CA's provision which, whilst not being presently in effect, will when effected, have an impact upon the operation of the CA that would require re-assessment. This will assist all parties in monitoring the occurrence of such events and the early planning to accommodate them.