Approval Profile for Certificate Generation

Ref. tSd 0104

Issue 2.00

2001-11-13

Executive summary

This document defines the *tScheme* criteria against which organisations must be successfully assessed in order to be eligible for approval for the provision of Certificate Generation services.

QC:
Where text appears in the body of the document in a box headed 'QC' (as is this box) that text relates specifically to services claiming to offer Qualified Certificates (QC) as defined in EC Directive 1999/93/EC on a Community framework for electronic signatures, and such services must fulfil the requirements expressed or indicated within that box. In-line text which relates to QCPs is denoted by being enclosed within double brackets, [[QC: … thus…]].

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 Editor@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	Release	Date	Comment	Approved
tS	1.00	2001-07-09	First version ratified by the board. This version produced prior to document management procedures introduced 2001-09-21.	*tScheme* Board
tSd	2.00	2001-11-13	Incorporates the following changes: 1. changes reflecting Disposition tS0163 Version 0.03, 2001-07-24. 2. §2 – removal of reference to the (non existing) Confidentiality Key Pair Management Approval Profile. 3. §3.2 – extension of permitted use of CA's keys to include signing revocation status information. 4. minor editorial changes, including: correction of syntactic errors, incorporation of document maintenance automation, various minor changes in conformance with new document management standards (including the type letter "d" added to the document reference) and the addition of this document history.	*tScheme* Board

© *tScheme* Limited, 2001 - all rights reserved

CONTENTS

1. INTRODUCTION 4

2. SCOPE AND RELATION TO OTHER PROFILES. 5

3. CRITERIA 6

3.1 SERVICE DEFINITION 6
3.2 CREATION OF CERTIFICATES 6
3.3 RECORDS 7

4. ABOUT EVIDENCE 9

5. REFERENCES 10

© *tScheme* Limited, 2001 - all rights reserved

1. INTRODUCTION

This Approval Profile is one of a number developed by *tScheme* against which TSPs offering trust services may be assessed by *tScheme*-recognised Assessors. It addresses the provision of a Certificate Generation service and may be one of a selection which a TSP has identified within the definition of its Service(s) Subject to Assessment. It must, as a minimum, be applied in combination with the Base Approval Profile.

Full details of Approval Profiles and the Approval Process may be found on the *tScheme* website.

Definitions of terms and acronyms not defined in this document may be found in the tScheme Glossary of Terms.

© *tScheme* Limited, 2001 - all rights reserved

2. SCOPE AND RELATION TO OTHER PROFILES.

The criteria given in this Approval Profile are related to the provision of services which result in the creation of an electronic certificate, signed on behalf of an issuing CA in a manner conforming to a published Certificate Policy.

This service component may function in cooperation with:

1. services for the registration and verification of the identity of an entity who is entitled to a certificate, together with any qualifying attributes (date of birth, address, credit rating, etc.) as appropriate to the governing Certificate Policy, such as covered by the Approval Profile for Registration;
2. cryptographic key generation such as covered by the Approval Profile for Signing Key Pair Management.

With the exception of the Base Approval Profile, the criteria given in this Approval Profile are not directly related to any other Approval Profiles for the purposes of assessment, i.e. this Profile may be used in isolation and is not dependent upon a successful assessment against any other Approval Profile.

© *tScheme* Limited, 2001 - all rights reserved

3. CRITERIA

The applicability of this Approval Profile must be described in a Specification of Service(s) Subject to Assessment (S3A), as described in Preparing for an Assessment.

Compliance with this Approval Profile will be achieved by demonstrating compliance with the following criteria:

3.1 Service Definition

The Service Definition must state clearly the following service attributes:

1. which certificate formats it supports;
2. the means by which Certificate Policy requirements relating to the contents of certificates are implemented in the generation process;
3. how the authorisation to generate certificates is authenticated:
4. the response times which it offers to properly authenticated authorisations for certificate generation;
5. what is done with certificates once they have been generated[1];
6. how the CA's signing key is generated, securely managed and applied to completed[2] certificates;
7. which CA algorithms and key lengths are supported;
8. which service levels are provided.

Where the TSP provides the service under more than one Certificate Policy, the identity of the applicable Policy must always be specified.

3.2 Creation of Certificates

The TSP must state clearly the Certificate formats it is capable of creating and the contents with which it will populate Certificates. Typically this would be by reference to appropriate standards defining Certificate contents and formats.

The TSP must ensure that its CA's signing keys are used only for the purposes of generating certificates and/or issuing revocation status information, within physically secure premises.

---

[1] For example they may be returned to the requestor, they may be stored in a database under the control of the TSP or they may be passed directly to a Certificate Dissemination Service, according to the Policy under which the certificates are being issued.

[2] I.e those certificates which have had placed into them, conformant with the specified format, the correct content relating to the Policy under which certificates are being issued, the public key and other details relating to the subscriber, and the certifier's identity.

© *tScheme* Limited, 2001 - all rights reserved

The TSP must ensure that its CA's signing keys are not used beyond the end of their life cycle. In particular, all copies of the CA's signing keys shall be:

1. destroyed such that the private keys cannot be retrieved; or
2. archived in a manner such that they are protected against being put back into use.

The TSP must ensure the security of cryptographic hardware throughout its lifecycle. In particular the TSP must ensure that:

3. certificate signing cryptographic hardware is not tampered with during shipment;
4. certificate signing cryptographic hardware is not tampered with while stored;
5. the use of certificate signing cryptographic hardware requires a minimum of two trusted employees whilst holding valid certification signing keys;
6. certificate signing cryptographic hardware is functioning correctly;
7. The CA's signing keys stored on its cryptographic hardware are destroyed upon device retirement.

The TSP must issue a new certificate using the subscriber's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's intended lifetime and no indications exist that the subscriber's private key has been compromised.

QC:

Where the TSP is claiming that the certificates generated are Qualified Certificates as defined in [DIR.99/93], the Criteria listed in [QCP] Sections 7.2.1 and 7.2.2 must be satisfied in respect of keys used to sign such certificates.

3.3 Records

The TSP must capture and retain records of all actions undertaken or events that occur, and the times at which they occurred. It must also state the period for which such records are to be retained, with a clear justification for the basis of determining the stated period. The records are to include:

1. all certificate generation requests received;
2. whether such requests are fulfilled or rejected;
3. location and movement of all devices used to store the issuing CA's signing keys;
4. all certificates issued (including the identity of the issuing CA);
5. the authentication data relating to the source of a certificate generation authorisation and the information provided with it (e.g. registration data, identity of requesting party, …);
6. all major events in the lifecycle of the CA's private keys;
7. all major events in the lifecycle of the issuing CA's certificates.

Additionally, the TSP must keep records of any service-specific changes in status which may affect their claim of conformance with this *tScheme* Approval Profile (or any on which a claim of conformance is based).

Furthermore, the TSP must show that they have in place appropriate audit procedures to apply self-monitoring and provide evidence of such records where the service is already operational.

© *tScheme* Limited, 2001 - all rights reserved

These records must be protected against unauthorised access and be made available within a reasonable period following a properly justified and authorised request.

© *tScheme* Limited, 2001 - all rights reserved

4. ABOUT EVIDENCE

Most of the evidence required of a TSP is of the same general form whatever the service being assessed. There is some flexibility here, but the specific forms of evidence for each assessment must be agreed with the *tScheme*-recognised Assessor before assessment can start. More information is given in Preparing for an Assessment.

For some Approval Profiles however, there are specific standards[3] that could apply, and to which prior conformance could be demonstrated. Thus, rather than offering point by point evidence, a TSP can offer evidence of already established conformance to appropriate standards. For this Approval Profile, there are no actual standards that are specific to it.

[3] Within *tScheme*'s Approval Profiles the term 'standard' is intended to include both formal (*de jure*) and *de facto* Standards, recognised industry schemes, and other means of demonstrating levels of performance and practice having similar merit.

© *tScheme* Limited, 2001 - all rights reserved

5. REFERENCES

[DIR 99/93] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[QCP] ETSI TS 100 456 "Policy requirements for certification authorities issuing qualified certificates", TS 101 456 December 2000

© *tScheme* Limited, 2001 - all rights reserved