Approval Profile for a Certification Authority [[QC: issuing Qualified Certificates]]

Ref. tSd 0102

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 Certification Authority 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	2001-07-05	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 – recognition of prior *tScheme* Approvals as evidence demonstrating compliance of service components. 3. §3.4.4 – recognition under item 3 (previously (c)) that 'distinguished' names shall not be re-assigned. 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

1.1 CONVENTIONS 4
1.2 GENERAL 4

2. SCOPE AND RELATION TO OTHER PROFILES. 5

3. CRITERIA 7

3.1 SERVICE DEFINITION 7
3.2 CERTIFICATE POLICY 7
3.3 CERTIFICATION PRACTICE STATEMENT 9
3.4 INTERNAL PROCEDURES 9
3.4.1 Authority and Responsibility 9
3.4.2 Subscriber Certificate renewal, rekey and update 9
3.4.3 CA Key Management 9
3.4.4 Certificate Generation 10
3.5 RECORDS 10

4. ABOUT EVIDENCE 11

5. REFERENCES 12

© *tScheme* Limited, 2001 - all rights reserved

1. INTRODUCTION

1.1 Conventions

This Approval Profile defines a high-level service composed of component services, each of which is subject to its own specific Approval Profile. Some of these component services are regarded as being mandatory components of a CA service. Unless they are referred to within 'curly' brackets, { …thus… } any such services, and the implied requirements of any text are mandatory - only optional service components are enclosed within 'curly' brackets, and the TSP must make clear whether they are intending to be assessed against those optional components or not.

This Approval Profile refers to services which either claim or do not claim to be supporting Qualified Certificates (QCs) as defined in EC Directive 1999/93/EC on a Community framework for electronic signatures. Where text refers exclusively to QCs it is shown either within double square brackets [[**QC**: …thus…]] where it is in-line text, or within a separate box, headed 'QC' where a whole sentence or paragraph is concerned.

References to other documents use single square brackets and are easily recognisable by the fact that they contain an abbreviated title rather than natural prose which should not be confused with text within double square brackets.

1.2 General

This Approval Profile is one of a number developed by *tScheme* against which TSPs offering Trust Services may be audited by *tScheme*-recognised Assessors. It addresses the provision of a Certification Authority service [[**QC**: issuing Qualified Certificates]]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 but will more likely require the combination of a number of additional Approval Profiles (refer to §2, Scope and relation to other profiles.).

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

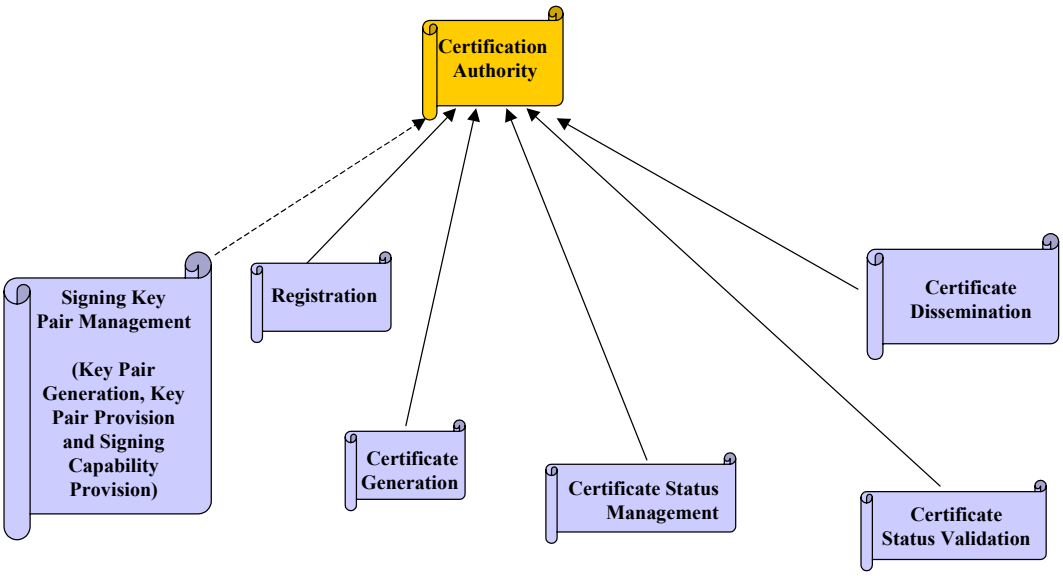
2. SCOPE AND RELATION TO OTHER PROFILES.

The criteria given in this Approval Profile are related to the overall provision and life-cycle management of certification services[[**QC**: issuing Qualified Certificates]]. Life-cycle management provides for services supporting the initial creation and personalisation of encryption keys, tokens and certificates, the secure distribution of keys/tokens and publication of certificates, the maintenance of certificate currency and validity through re-certification and revocation processes.

The components of the service, whether operated directly by the organisation offering the Certification service or whether outsourced to various other third parties, are required to fulfil the criteria defined in the following further Approval Profiles (when used as hyper-links, these will take you to the latest released version, although it is necessary to fix on a specific release for the purposes of scoping the S3A. The formal identification of these documents is given in §5):

Registration
{ Signing Key Management, including
Signing Key Generation
Signing Key Provision
Signature Creation Environment (SCE) Provision }
Certificate Generation
Certificate Dissemination
Certificate Status Management
Certificate Status Validation

The relationships between these profiles is shown in the following diagram. Mandatory APs are shown with a solid connection to the CA Approval Profile, those which are optional are shown with a dashed connecting line.



The TSP acting as the Certification Authority has responsibility for ensuring conformance with the procedures prescribed in the applicable Certification Policy even when the components of the service

© *tScheme* Limited, 2001 - all rights reserved

are outsourced to third parties. This requires the inclusion in its PKI Disclosure Statement of relevant practices undertaken by all parties contributing to the overall service provision.

The TSP acting as the Certification Authority may demonstrate directly the conformance to the appropriate Approval Profiles of the service components or they may refer to prior *tScheme* Approvals awarded to those service components, where they remain current.

© *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 satisfying the following criteria.

QC:

Where the CA is issuing Qualified Certificates the provision of appropriate evidence must demonstrate explicitly compliance with the requirements of [DIR.99/93].

The S3A must address how the components of the service are inter-related and must apportion matters of ownership, management and operational responsibility for the functional components and how they are allocated to other departments of the business or outsourced to third parties.

This information should supplement and make more service-specific the criteria required by the Base Approval Profile.

Note - where components of the services are outsourced to third parties the TSP must bear full liability for the overall service offering. Under these circumstances it is under no obligation to make public how it out-sources these functions, although it may choose to do so.

3.1 Service Definition

The Service Definition must specify how the service's constituent components are delivered and the TSP must, at the time of being assessed, be providing a service which fulfils these statements. The Service Definition must include descriptions of the service elements in a fashion which shows how the criteria of other Approval Profiles will be satisfied by allocating the constituent components to the component Approval Profiles as appropriate.

QC:

Where claiming conformance to one or more specific Qualified Certificate Policies, the policies must be identified.

3.2 Certificate Policy

For each SSA, the TSP must provide a Certificate Policy that states clearly the purpose, conditions and limitations under which certificates issued through its service may be used. Particular emphasis will be given to the topics identified in the following list.

© *tScheme* Limited, 2001 - all rights reserved

QC:

The Qualified Certificate Policy must say how it satisfies the requirements of [DIR.99/93], for example by quoting a standard reference policy identity (OID)[1], such as those given in [QCP] §5, to which it claims conformance.

1. **Registration Policy** –the TSP must state clearly its policy requirements for Registration, and thus verification, of the subscriber's identity or other attributes, in terms of evidence required and forms of presentation. The specific credential documents for identity verification and method of registration must be stated. Where the service offers more than one certificate policy type, the verification requirements must be related to the specific certificate policies, where they differ.

   The Registration process must make clear whether, and under what conditions (e.g. mandatory or optional), the subscriber requires and consents to the publication of its certificate

   If the Subscriber presents with a previously-generated key pair the Registration process must ensure that the Subscriber has possession of the private key associated with the public key presented for certification;

2. **Subscriber Obligations** - the TSP must set out in terms readily understandable and accessible to the subscriber community the obligations with which subscribers must comply if they are issued with a certificate under the identified policy and wish to use the certificate within the terms of its provision. Such terms must:

   a) oblige the Subscriber to submit accurate and complete information as required by the applicable Certificate Policy, and

   b) provide clear instructions as to how the Subscriber should exercise reasonable care to avoid unauthorised use of its private key;

   c) require the Subscriber to notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

   - loss, theft or potential compromise of the subscriber's private key; or

   - control over the subscribers private key through loss due compromise of activation data (e.g. PIN code) or other reasons; and/or

   - any inaccuracies in or changes required to the certificate content.

   The TSP must record the Subscriber's agreement to all their defined obligations.

3. **Relying Party Agreement** - the TSP must provide a plain language explanation of what a relying party can expect, if they are presented with a certificate issued under this policy. This should include information on how to validate certificates issued under the applicable Certificate Policy, including requirements to check the revocation status of the certificate, such that the relying party may "reasonably rely" on the certificate;

4. **Revocation notification** – in addition to the TSP's obligations to revocation status information to Relying Parties, it must also ensure that Subscribers whose certificates are subject to revocation or suspension are notified of the change of status of their certificate, according to the requirements of the Certificate Policy.

---

[1] OID – Object Identifier, A value (distinguishable from all other such values) which is associated with a well-defined piece of information, definition or specification which requires a name in order to identify its use in an instance of communication – source ISO/IEC 8824-1 : 199 (E). In practice an OID is not a name in the normal sense but a value in the form of a multi-part numeric identifier with specific parts indicating specific characteristics, e.g. issuing / owning / approving body, etc.

© *tScheme* Limited, 2001 - all rights reserved

5. **Accessibility** - the TSP must publish the ways in which subscribers and relying parties can contact it in the event of dispute or for general support. It must describe the level of support provided at these contact points and the response times offered. It must offer evidence that its service can achieve these levels in practice.

3.3 Certification Practice Statement

As identified in the Base Approval Profile, the TSP must provide a sufficient description of the practices it employs in delivering the service and in enforcing the Certificate Policy according to which the service is offered, normally referred to as a Certification Practice Statement (CPS). This must satisfy the requirements expressed in the Base Approval Profile.

There is no requirement to make full public disclosure of its practices since this may be to the detriment of the overall security of the service. However, a PKI Disclosure Statement giving an overview of the service provision and how the provisions of the Certificate Policy are implemented must be provided.

The CPS must be consistent with claims made within the service definition.

The TSP must define the processes and responsibilities they use to review and maintain the applicable CPS and must give due notice of changes it intends to make to the CPS and/or the PKI Disclosure Statement which must be promptly published once formally approved.

3.4 Internal Procedures

3.4.1 Authority and Responsibility

The TSP must have a high level management body with final authority and responsibility for approving the certificate policy and certification practice statement, including oversight of its proper implementation.

3.4.2 Subscriber Certificate renewal, rekey and update

The TSP must have in place practices which ensure that requests for a certificate to be issued to a previously-registered subscriber are complete, accurate and duly authorised and that information used to verify the identity and attributes of the subscriber remains valid. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subscriber's attributes.

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

3.4.3 CA Key Management

The TSP must have documented procedures for the generation and storage of its own keys, which address the physical security of the environment, access control procedures which limit access to a minimum number of authorised personnel, and which use system components of demonstrably suitable strength for the claims made for the SSA.

These procedures must ensure that CA signing keys remain confidential and maintain their integrity, including when this includes the passing of these key to the certificate generation function.

© *tScheme* Limited, 2001 - all rights reserved

3.4.4 Certificate Generation

The CA shall ensure that new, renewed and rekeyed certificates are issued securely, in particular ensuring that:

1. the procedure of issuing the certificate is securely linked to the associated Registration, certificate renewal or rekey, including the provision of any subscriber-provided public key;

2. if the TSP generates the subscriber's key:
   - the procedure of issuing the certificate is securely linked to the generation of the key pair by the Key Generation function; and
   - the private key is securely delivered to the registered subscriber;

3. the TSP shall ensure over the life time of the Certification Authority service that any specific distinguished name which has been used in an issued certificate shall never be re-assigned to another entity;

4. the confidentiality and integrity of registration data shall be protected especially when exchanged with the subscriber or between distributed service components;

5. the TSP shall verify that registration information is exchanged with recognised Registration service providers, whose identity is authenticated, in the event that the Registration function is outsourced.

3.5 Records

The TSP must capture and retain records of all actions undertaken, and the time 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. These must include:

1. actions concerning the CA's own keys;
2. adequate records kept in accordance with the requirements of the Approval Profiles applicable to any component functions, covering *inter alia*:
   - the evidence offered to the Registration function and on which was based a decision to either reject a request for a certificate or to accept the request and issue the certificate. This information must identify the point of Registration;
   - {generation of the subscriber's keys;}
   - generation of the subscriber's certificate;
   - dissemination of the subscriber's certificate;
   - any revocation or suspension associated with the subscriber's certificate;
   - any changes in status which may affect the TSP's legitimate claim of conformance with this *tScheme* Approval Profile (or any on which a claim of conformance is based).

Furthermore, the TSP must have in place documented internal audit procedures. Records must be maintained and evidence of their application provided.

These records must be protected against unauthorised access and be made available for audit and dispute resolution purposes 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[2] 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, the standards that *tScheme* has identified as being relevant are:

1. Provision of the TSP's Service Definition and procedures to ensure proper delivery of the service;
   Form:- TSP's own documentation.
2. ISMS relating to the specific aspects of the defined service;
   Form:- BS7799/ISO 47799 or demonstrable equivalent means of defining their ISMS.
3. All evidence relating to testing of the processes involved in authorising and issuing Certificates;
   Form:- conformance with the cited standards;
4. Audit records as required by the assessors;
   Form:- TSP's own documentation.

QC:

Where the TSP claims to be issuing Qualified Certificates in conformance with [DIR.99/93] evidence of such must be provided to fully satisfy the assessors. Such evidence may be provided through demonstrating compliance with [QCP], which has extensive clauses relating to the requirements of this Approval Profile and maps onto [DIR.99/93]. Alternatively the TSP may provide evidence based upon another means of demonstrating conformance to [DIR.99/93] or must itself furnish all evidence and show how compliance with [DIR.99/93] is achieved.

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

© *tScheme* Limited, 2001 - all rights reserved

5. REFERENCES

DIR.99/93 EC Directive 1999/93/EC on a Community framework for electronic signatures

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

© *tScheme* Limited, 2001 - all rights reserved