Issued

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

Ref. tSd 0102

Issue 3.01

2004-10-21

Executive summary

This document defines the *tScheme* criteria against which organisations must be successfully assessed in order to be eligible for a Grant of Approval or *tScheme*-Ready Status 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 or Components claiming to offer Services in support of Qualified Certificates (QC), Advanced Electronic Signatures and/or Secure Signature Creation Devices as defined in [DIR 99/93] on a Community framework for electronic signatures, and such Services or Components must fulfil the requirements expressed or indicated within that box. In-line text that 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 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	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
tSd	3.00	2002-06-21	Incorporates the following changes: Editorial: 1. Removal of §4 'About evidence'. 2. Incorporation of criteria tagging. 3. Addition of a linked Clause compliance table. 4. Incorporation of *tScheme*-Ready text. 5. Minor editorial changes to achieve better consistency across the different Approval Profiles. 6. Reference to 'Model Specification of Service Subject to Assessment' rather than 'Preparing for an Assessment', which also includes removal of opportunity to have more than one Service within the scope of an S3A. Affecting Assessment: 1. Requirements relating to how and to whom Service information is to be presented have been clarified and harmonised across all of the Approval Profiles. Specific forms of presentation are required, and a distinction is now made between information that is to be provided to users and information that is to be provided for the Assessors. The "Service Being Provided" requirement has been relaxed to avoid the Catch 22 situation of *tScheme*	*tScheme* Board

© *tScheme* Limited, 2002 - all rights reserved

Status	Release	Date	Comment	Approved
			requiring a Service to be already in use with customers who may not be prepared to use it until it has acquired *tScheme* approval.	
tSi	3.01	2004-10-21	Amend CR-020/QC to clarify relevance of annex IV of Directive 99/93, in accordance with "tSi0271_1-00 Current Interpretation Responses".	*tScheme* Secretariat

© *tScheme* Limited, 2002 - all rights reserved

CONTENTS

1. INTRODUCTION 5

1.1 CONVENTIONS 5
1.2 GENERAL 5

2. SCOPE AND RELATION TO OTHER PROFILES. 6

3. CRITERIA 8

3.1 PUBLIC SERVICE DESCRIPTION 8
3.2 ASSESSOR'S SERVICE DEFINITION 9
3.3 SERVICE/CERTIFICATE POLICY 9
3.4 SERVICE/CERTIFICATION PRACTICE STATEMENT 11
3.5 INTERNAL PROCEDURES 11
3.5.1 Authority and responsibility 11
3.5.2 Subscriber certificate renewal, rekey and update 11
3.5.3 CA Key Management 12
3.5.4 Certificate issue 12
3.6 RECORDS 13

4. REFERENCES 14

ANNEX 1. CLAUSE COMPLIANCE LIST 15

© *tScheme* Limited, 2002 - all rights reserved

1. INTRODUCTION

1.1 Conventions

This Approval Profile defines a high-level Service composed of multiple constituent parts, each of which is a Service in itself subject to its own specific Approval Profile. Some of these Services are regarded as being mandatory parts 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 Services are enclosed within 'curly' brackets, and the TSP must make clear whether or not they are intending to be assessed against them.

For ease of reference from other documents, each clause is given a tag and a title, adopting the general form of a Common Criteria Protection Profile, as follows:

GENID-000 Text describing the Clause Tag

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 that a TSP has identified within the definition of its Service Subject to Assessment. It shall be applied in combination with the Base Approval Profile and the other Approval Profiles listed in §2, Scope and relation to other Profiles.

Full details of all 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.

Although the wording of this Approval Profile relates to Assessments for *tScheme* Service Approvals, the Profile is also intended to be applicable to *tScheme*-Ready Assessments. For use in the latter context:

- references to "Service Provider" shall be taken to mean "Component Supplier";
- references to "Service" shall be taken to mean "Service Component";
- references to "Service Subject to Assessment", or SSA, shall be taken to mean "Component Subject to Assessment", or CSA;
- references to "Specification of Service Subject to Assessment", or S3A shall be taken to mean "Specification of Service Component Subject to Assessment", or C3A.

© *tScheme* Limited, 2002 - all rights reserved

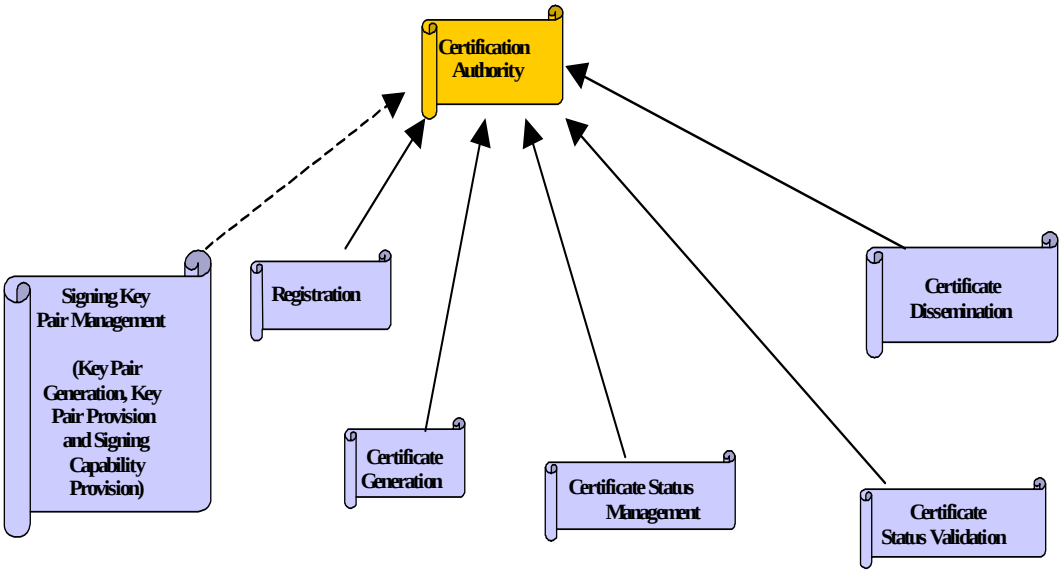
2. SCOPE AND RELATION TO OTHER PROFILES.

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 registration and verification of key holders, 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 Services that together make up the full Certification Authority Service, whether operated directly by the organisation offering the Certification Authority 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):

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.



© *tScheme* Limited, 2002 - all rights reserved

The TSP acting as the Certification Authority has responsibility for ensuring conformance with the procedures prescribed in the applicable Certification Policy even when constituent part Services are outsourced to third parties. This requires the inclusion in its Service Policy Disclosure Statement (normally referred to more specifically as 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 constituent Services or they may refer to prior *tScheme* Approvals awarded to those Services, where they remain current.

© *tScheme* Limited, 2002 - all rights reserved

3. CRITERIA

The applicability of this Approval Profile shall be described in a "Specification of Service Subject to Assessment" (S3A) as defined in "Model Specification of Service Subject to Assessment".

Compliance with this Approval Profile will be achieved by satisfying the following criteria.

CR-010 Operational Service

Each SSA shall be an Operational Service (in the sense defined in the *tScheme* Glossary of Terms) supporting the statements given in response to the criteria listed in the succeeding sections below.

QC: CR-020/QC Evidence of compliance with requirements for QCs

Where the CA is issuing Qualified Certificates the provision of appropriate evidence shall demonstrate explicitly compliance with the requirements of [DIR.99/93] and, if secure signature verification is being provided, including the recommendations of Annex IV or equivalent approach.

CR-030 Interrelationship of constituent parts

The S3A shall address how the constituent parts are interrelated.

CR-040 Apportionment of ownership, management and operational responsibility

The S3A shall apportion matters of ownership, management and operational responsibility for the constituent parts and how they are allocated to other departments of the business or outsourced to third parties. This information shall supplement and make more Service-specific the criteria required by the Base Approval Profile.

NOTE:

Even where constituent Services are outsourced to third parties the TSP shall bear full liability for the overall Service offering. Under these circumstances it is under no obligation to make public how it outsources these functions, although it may choose to do so. Notwithstanding its decision regarding publication, it must make this information available to the Assessor.

3.1 Public Service Description

PSD-010 What the Service is

For each SSA, a Public Service Description shall be provided, which includes information on where to find the SSA's Service Policy and Service Policy Disclosure Statement.

© *tScheme* Limited, 2002 - all rights reserved

3.2 Assessor's Service Definition

ASD-010 How the constituent parts are delivered

For each SSA, the Assessor's Service Definition shall specify how the Service's constituent parts are delivered.

ASD-020 Mapping of Service elements to Approval Profiles

The Assessor's Service Definition shall include definitions of the constituent Services in a fashion which shows, by mapping the constituent Services to the different Approval Profiles as appropriate, how the criteria of other Approval Profiles will be satisfied.

QC: ASD-030/QC Identification of applicable QC Certificate Policy

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

3.3 Service/Certificate Policy

CP-010 Statement of CP usage

For each SSA, the TSP shall provide a Service Policy (in the context of a CA this is normally referred to as 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.

QC: CP-020/QC QCP statement on DIR.99/93 requirements fulfilment

The Qualified Certificate Policy shall 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.

CP-030 Registration policy requirements

- **Registration Policy** –the TSP shall state clearly its policy requirements for Registration and 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 shall be stated. Where the Service offers more than one certificate policy type, the verification requirements shall be related to the specific certificate policies, where they differ.

CP-040 Consent to publication

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

[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 : 1999 (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, 2002 - all rights reserved

CP-050 Possession of private key

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

CP-060 Definition and availability of subscriber obligations

- **Subscriber Obligations** - the TSP shall 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 shall:

  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.

CP-070 Record of subscriber obligations

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

CP-080 Explanation of relying party's expectations

- **Relying Party Agreement** - the TSP shall provide a plain language explanation of what a relying party can expect, if they are presented with a certificate issued under this policy. This shall 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;

CP-090 Notification of revocation of certificates

- **Revocation notification** – in addition to the TSP's obligations to revocation status information to Relying Parties, it shall 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.

CP-100 Access to the TSP

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

© *tScheme* Limited, 2002 - all rights reserved

3.4 Service/Certification Practice Statement

CPS-010 Provision of a CPS

As identified in the Base Approval Profile, the TSP shall 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, the general term for this is a Service Practice Statement, but for a CA it is normally referred to as a Certification Practice Statement (CPS). This shall satisfy the requirements expressed in the Base Approval Profile.

CPS-020 Provision of an SPDS

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 Service Policy Disclosure Statement (normally referred to more specifically as a PKI Disclosure Statement) giving an overview of the Service provision and how the provisions of the Certificate Policy are implemented shall be provided.

CPS-030 Consistency of CPS

The CPS shall be consistent with the Assessor's Service Definition and the Public Service Description.

CPS-040 Maintenance of a CPS

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

3.5 Internal procedures

3.5.1 Authority and responsibility

IPAR-010 Management authority and responsibility

The TSP shall 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.

3.5.2 Subscriber certificate renewal, rekey and update

IPSC-010 Management of subscriber certificates

The TSP shall have in place practices that 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.

IPSC-020 Reissue

The TSP shall 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.

© *tScheme* Limited, 2002 - all rights reserved

3.5.3 CA Key Management

IPCA-010 Definition of procedures for CA's key management

The TSP shall 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 shall 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.

3.5.4 Certificate issue

IPCI-010 Security of certificate issue

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

IPCI-020 Certificate issuing procedures

- 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;

IPCI-030 Certificate issue and security of keys

- 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;

IPCI-040 Reassignment of distinguished names

- 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 reassigned to another entity;

IPCI-050 Protection of registration data

- the confidentiality and integrity of registration data shall be protected especially when exchanged with the subscriber or between distributed Service Components;

IPCI-060 Authentication of registrars

- 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.

© *tScheme* Limited, 2002 - all rights reserved

3.6 Records

RECS-010 Capture and retention of records

The TSP shall capture and retain records of all actions undertaken, and the time at which they occurred. It shall 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 captured shall include:

RECS-020 Actions on CA's keys

- actions concerning the CA's own keys;

RECS-030 Constituent Services

- adequate records kept in accordance with the requirements of the Approval Profiles applicable to any constituent Services, 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 shall 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 that may affect the TSP's legitimate claim of conformance with this *tScheme* Approval Profile (or any on which a claim of conformance is based).

RECS-040 Internal audit records

The TSP shall have in place documented internal audit procedures. Records shall be maintained and evidence of their application provided.

RECS-050 Access to records

These records shall 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, 2002 - all rights reserved

4. 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.

© *tScheme* Limited, 2002 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for a Certification Authority - clause compliance list		
Clause	**Description**	**Compliance**
CR-010	Operational Service	
CR-020/QC	Evidence of compliance with requirements for QCs	
CR-030	Interrelationship of constituent parts	
CR-040	Apportionment of ownership, management and operational responsibility	
PSD-010	What the Service is	
ASD-010	How the constituent parts are delivered	
ASD-020	Mapping of Service elements to Approval Profiles	
ASD-030/QC	Identification of applicable QC Certificate Policy	
CP-010	Statement of CP usage	
CP-020/QC	QCP statement on DIR.99/93 requirements fulfilment	
CP-030	Registration policy requirements	
CP-040	Consent to publication	
CP-050	Possession of private key	
CP-060	Definition and availability of subscriber obligations	
CP-070	Record of subscriber obligations	
CP-080	Explanation of relying party's expectations	
CP-090	Notification of revocation of certificates	
CP-100	Access to the TSP	
CPS-010	Provision of a CPS	
CPS-020	Provision of an SPDS	
CPS-030	Consistency of CPS	

© *tScheme* Limited, 2002 - all rights reserved

Approval Profile for a Certification Authority - clause compliance list

Clause	Description	Compliance
CPS-040	Maintenance of a CPS	
IPAR-010	Management authority and responsibility	
IPSC-010	Management of subscriber certificates	
IPSC-020	Reissue	
IPCA-010	Definition of procedures for CA's key management	
IPCI-010	Security of certificate issue	
IPCI-020	Certificate issuing procedures	
IPCI-030	Certificate issue and security of keys	
IPCI-040	Reassignment of distinguished names	
IPCI-050	Protection of registration data	
IPCI-060	Authentication of registrars	
RECS-010	Capture and retention of records	
RECS-020	Actions on CA's keys	
RECS-030	Constituent Services	
RECS-040	Internal audit records	
RECS-050	Access to records	

© *tScheme* Limited, 2002 - all rights reserved