Issued

Approval Profile for Certificate Generation

Ref. tSd 0104

Draft 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 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 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.

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	2001-07-09	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
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. 2. The "Service Being Provided" requirement has been relaxed to avoid the Catch 22	*tScheme* Board

© *tScheme* Limited, 2002 - all rights reserved

Status	Release	Date	Comment	Approved
			situation of *tScheme* requiring a Service to be already in use with customers who may not be prepared to use it until it has acquired *tScheme* approval.	
tSd	3.01	2004-10-21	Add criterion SI-090 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 7

3.1 SERVICE INFORMATION 7
3.1.1 Information for users 7
3.1.2 Information for Assessors 8
3.2 CREATION OF CERTIFICATES 8
3.3 RECORDS 9

4. REFERENCES 11

ANNEX 1. CLAUSE COMPLIANCE LIST 12

© *tScheme* Limited, 2002 - all rights reserved

1. INTRODUCTION

1.1 Conventions

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 assessed by *tScheme*-recognised Assessors. It addresses the provision of a Certificate Generation Service and may be one of a selection that a TSP has identified within the definition of its Service Subject to Assessment. It shall, 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.

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 provision of Services that 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's function may operate 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, i.e. this Profile may be used in isolation and is not dependent upon a successful Assessment against any other Approval Profile.

© *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 demonstrating compliance with 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.

3.1 Service information

3.1.1 Information for users

The following information shall be made available to potential users of the Service by being present in either the Service's Service Policy, Service Policy Disclosure Statement, Service Practice Statement, or Public Service Description, as appropriate to their purpose.

SI-010 Supported Certificate Formats

- which certificate formats it supports; the TSP shall 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.

SI-030 Certificate Generation Authentication

- how the authorisation to generate certificates is authenticated:

SI-040 Response Time for Certificate Generation

- the response times which it offers to properly authenticated authorisations for certificate generation;

SI-050 Post Generation Process for Certificates

- what is done with certificates once they have been generated[1];

SI-060 CA Algorithm and Key Length Support

- which CA cryptographic algorithms and key lengths are supported;

[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.

© *tScheme* Limited, 2002 - all rights reserved

3.1.2 Information for Assessors

The following information shall appear either in the Service's Service Practice Statement or in the Assessor's Service Definition (*tScheme* does not require it to be made generally available):

SI-070 Implementation of Certificate Contents

- the means by which Certificate Policy requirements relating to the contents of certificates are implemented in the generation process;

SI-075 CA's Signing Key Management

- how the CA's signing key is generated, securely managed and applied to completed[2] certificates;

SI-080 Service Levels Provided

- which Service levels are provided;

SI-090 Choice of Algorithm and Key Length

- justification for the choice of Algorithm and Key Length.

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

3.2 Creation of certificates

CC-020 Control of Signing Key Usage

The TSP shall 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.

CC-030 Signing Key Termination when Life-Cycle completed

The TSP shall ensure that its CA's signing keys are not used beyond the end of their life cycle.

CC-040 Destroyed or Archived Copies of Signing Keys

In particular, all copies of the CA's signing keys shall be:

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

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

CC-050 Tamper-Proof Signing Hardware in Shipment

- certificate signing cryptographic hardware is not tampered with during shipment;

[2] i.e. those certificates that 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, 2002 - all rights reserved

CC-060 Tamper-Proof Signing Hardware in Storage

- certificate signing cryptographic hardware is not tampered with while stored;

CC-070 Dual Control of Signing

- the use of certificate signing cryptographic hardware requires a minimum of two trusted employees whilst holding valid certification signing keys;

CC-080 Correctly Functioning Signing Hardware

- certificate signing cryptographic hardware is functioning correctly;

CC-090 Destruction of Signing Keys

- the CA's signing keys stored on its cryptographic hardware are destroyed upon device retirement.

CC-100 Conditions of issuance of a New Certificate

The TSP shall 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: CC-110/QC Evidence of compliance with requirements for QCs

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 shall be satisfied in respect of keys used to sign such certificates.

3.3 Records

RECS-010 Capture and retention of records

The TSP shall capture and retain records of all actions undertaken or events that occur, and the times 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 Record Certificate Generation Requests

- all certificate generation requests received;

RECS-030 Action Taken on Certificate Generation Requests

- whether such requests are fulfilled or rejected;

RECS-040 Inventory of CA Signing Devices

- location and movement of all devices used to store the issuing CA's signing keys;

© *tScheme* Limited, 2002 - all rights reserved

RECS-050 Identity of Certificates Issued

- all certificates issued (including the identity of the issuing CA);

RECS-060 Authentication Data

- 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, …);

RECS-070 Major Life-Cycle Events re. CA Keys

- all major events in the lifecycle of the CA's private keys;

RECS-080 Major Life-Cycle Events re. CA Certs

- all major events in the lifecycle of the issuing CA's certificates.

RECS-090 Service Changes

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

RECS-100 Internal audit records

Furthermore, the TSP shall 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.

RECS-110 Protection of access to records

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

© *tScheme* Limited, 2002 - all rights reserved

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

© *tScheme* Limited, 2002 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Certificate Generation - clause compliance list

Clause	Description	Compliance
CR-010	Operational Service	
SI-010	Supported Certificate Formats	
SI-030	Certificate Generation Authentication	
SI-040	Response Time for Certificate Generation	
SI-050	Post Generation Process for Certificates	
SI-060	CA Algorithm and Key Length Support	
SI-070	Implementation of Certificate Contents	
SI-075	CA's Signing Key Management	
SI-080	Service Levels Provided	
SI-090	Choice of Algorithm and Key Length	
CC-020	Control of Signing Key Usage	
CC-030	Signing Key Termination when Life-Cycle completed	
CC-040	Destroyed or Archived Copies of Signing Keys	
CC-050	Tamper-Proof Signing Hardware in Shipment	
CC-060	Tamper-Proof Signing Hardware in Storage	
CC-070	Dual Control of Signing	
CC-080	Correctly Functioning Signing Hardware	
CC-090	Destruction of Signing Keys	
CC-100	Conditions of issuance of a New Certificate	
CC-110/QC	Evidence of compliance with requirements for QCs	
RECS-010	Capture and retention of records	
RECS-020	Record Certificate Generation Requests	
RECS-030	Action Taken on Certificate Generation	

© *tScheme* Limited, 2002 - all rights reserved

Approval Profile for Certificate Generation - clause compliance list

Clause	Description	Compliance
	Requests	
RECS-040	Inventory of CA Signing Devices	
RECS-050	Identity of Certificates Issued	
RECS-060	Authentication Data	
RECS-070	Major Life-Cycle Events re. CA Keys	
RECS-080	Major Life-Cycle Events re. CA Certs	
RECS-090	Service Changes	
RECS-100	Internal audit records	
RECS-110	Protection of access to records	

© *tScheme* Limited, 2002 - all rights reserved