Issued

Approval Profile for Certificate Status Management

Ref. tSd 0106

Issue 3.01

2004-08-26

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 Services to individuals, corporate entities and other organisations for the management of the validity status of certificates.

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	Authorised
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 only 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	2002-06-25	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 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.	*tScheme* Board
tSd	3.01	2004-07-28	Correction to footnote to §2 'Scope and relation to other Profiles.'	*tScheme* Secretariat

© *tScheme* Limited, 2004 - all rights reserved

CONTENTS

1 INTRODUCTION 4

1.1 CONVENTIONS 4
1.1 GENERAL 4

2 SCOPE AND RELATION TO OTHER PROFILES. 5

3 CRITERIA 6

3.1 SERVICE INFORMATION 6
3.1.1 Information for users 6
3.1.2 Information for Assessors 7
3.2 INTERNAL PROCEDURES 7
3.3 RECORDS 7

4 REFERENCES 8

ANNEX 1. CLAUSE COMPLIANCE LIST 9

© *tScheme* Limited, 2004 - 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

1.1 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 Status Management 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, 2004 - 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 manage the status of issued certificates. The Services embrace:

1. the receipt of requests to revoke, suspend or otherwise change a certificate's status;
2. the authentication and authorisation of revocation requests;
3. the determination of a decision to revoke and associated actions;
4. notification of status change to certificate owners[1].

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.

1 Notification of status change to relying parties is covered in the Certificate Status Validation Approval Profile.

© *tScheme* Limited, 2004 - 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 then 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.

3.1 Service information

3.1.1 Information for users

The following information shall be made available to potential users of the Service (including relying parties) 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 CAs supported
- which CAs are supported and what types of certificate;

SI-020 Status values supported
- the status values supported[2];

SI-040 Service levels supported
- the Service levels supported[3];

SI-050 Authorised notifiers
- who is authorised to notify the Service of a change of a certificate's status, how they are authenticated and how they communicate with the Service;

SI-080 Method and periodicity of status record amendment
- the method and periodicity for amendment to the status record;

SI-090 Dissemination schedules
- the method and periodicity schedules for disseminating certificate status changes to Certificate Validation Service Providers (if applicable);

SI-100 Acknowledgements of change requests
- any status change acknowledgement/confirmation applicable;

SI-110 Informing the subscriber
- how the subscriber is to be informed of the change of status.

2 For example: valid, revoked, suspended, revocation reasons and revocation scope.

3 In particular, the Service's immediacy, ubiquity and availability.

© *tScheme* Limited, 2004 - 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-120 Assurance of integrity

- how the integrity of the status information is assured;

SI-130 Assumptions relating to Certificate Status Services

- any assumptions relating to the relationship with associated Certificate Status Services;

3.2 Internal procedures

IP-010 Documentation of request registration process

The process for registration of revocation requests shall be fully documented and cover all expected situations, for example how failed requests/notifications are managed, communicated to the originator and recorded.

IP-020 No reinstatement

Once a certificate is definitively revoked (i.e. not suspended), it shall not be reinstated.

IP-030 Suspension period limited

If a certificate is suspended pending possible revocation, suspension shall not be for any longer than required to confirm a certificate's status.

3.3 Records

RECS-010 Records match the Service claim

The Service Provider shall maintain the records stated in the Service claim. These are to include:

RECS-020 Record of time critical transactions

- subject to Service claim, but as a minimum, all transactions that are intended to support time critical validation requirements - such as high value financial transactions;

RECS-030 Trusted time of change request and action

- a trusted time record of when a status change request is received and when it is actioned.

RECS-040 Appropriate media for records

The records are to be stored on media suitable for the record retention period.

© *tScheme* Limited, 2004 - all rights reserved

4 REFERENCES

None

© *tScheme* Limited, 2004 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Certificate Status Management - clause compliance list

Clause	Description	Compliance
CR-010	Operational Service	
SI-010	CAs supported	
SI-020	Status values supported	
SI-040	Service levels supported	
SI-050	Authorised notifiers	
SI-080	Method and periodicity of status record amendment	
SI-090	Dissemination schedules	
SI-100	Acknowledgements of change requests	
SI-110	Informing the subscriber	
SI-120	Assurance of integrity	
SI-130	Assumptions relating to Certificate Status Services	
IP-010	Documentation of request registration process	
IP-020	No reinstatement	
IP-030	Suspension period limited	
RECS-010	Records match the Service claim	
RECS-020	Record of time critical transactions	
RECS-030	Trusted time of change request and action	
RECS-040	Appropriate media for records	

© *tScheme* Limited, 2004 - all rights reserved