Issued

Approval Profile for Certificate Status Validation

Ref. tSd 0107

Issue 3.01

2002-08-26

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, system objects, corporate entities and other organisations for the verification 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

© *tScheme* Limited, 2002 - all rights reserved

tSd	3.01	2002-08-26	Incorporates the following changes: 1. Correct release number in document history, 2.01 is now 3.00; 2. Correct title of criterion RECS-030; 3. Correct hyperlinks from ANNEX 1 to §3.4 - Records collection of criteria.	

© *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 7
3.2 RELYING PARTY AGREEMENT 8
3.3 INTERNAL PROCEDURES 8
3.4 RECORDS 8

4. REFERENCES 9

ANNEX 1. CLAUSE COMPLIANCE LIST 10

© *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 Status Validation 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 enable Service users to determine the validity of a certificate at a defined time. The Services include those that offer access to a published[1] Certificate Revocation List (CRL), those that actively distribute such lists, and those that directly return the certificate's status to a requestor, for example as with the On-line Certificate Status Protocol [OCSP].

This Profile does not assess Certificate Status Management, which would provide the Service with the information to publish.

The scope is limited to only the verification of the status of a certificate and expressly excludes Services that verify the signatures on certificates, signed documents or files.

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 "Published" in this context means "published to the community of interest", which may be the public generally or a restricted community.

© *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 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 Method of publication
- how status information is published and the options available to access it[2];

SI-030 Status values supported
- the status values supported (valid, revoked or suspended, revocation reasons, revocation scope and so on);

SI-040 Service immediacy, ubiquity and availability
- the immediacy, ubiquity and availability of the Service;

SI-050 Authorisation and authentication of requests
- who is authorised to access a certificate's status and how are they authenticated;

SI-070 Update frequency and how indicated
- how often and when the status information is updated, and the method of indicating these things;

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-080 Authorised Certificate Status Management Services
- the rules governing which Certificate Status Management Services are permitted to notify the Service of a change of a certificate's status and how are they authenticated;

2 Examples might be: through the use of published Certificate Revocation Lists, through the mailing of such lists directly to subscribers, or via support of an online certificate status request service.

© *tScheme* Limited, 2002 - all rights reserved

SI-090 Assured Integrity
- how the integrity of the status information is assured;

SI-100 Assured confidentiality
- how the confidentiality of the request and response is assured;

SI-110 Records retained and period
- the records that will be retained and their retention period;

3.2 Relying Party Agreement

RPA-010 Plain language agreement

The Service Provider shall provide a plain language explanation of what a relying party can understand by the validation response and any contractual implications of requesting certificate validation. This may be published directly or indirectly to end-users[3].

3.3 Internal Procedures

IP-010 Process documentation

The validation process shall be fully documented and cover all expected situations, for example how failures are managed and recorded.

3.4 Records

RECS-010 Records as claimed

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

RECS-020 Record of CRLs published
- the publication of CRLs;

RECS-030 Record of time critical transactions
- subject to the Service claim, but as a minimum, all transactions that are intended to support time critical validation requirements - such as high value financial transactions.

RECS-040 Suitable recording media

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

3 This is required, for example, to explain that any status changes made since the last update of published information such as a CRL, will not be reflected in the status response, or to explain that requesting a status may bind the requestor to the terms and conditions associated with the overall Trust Service.

© *tScheme* Limited, 2002 - all rights reserved

4. REFERENCES

[OCSP] RFC 2560 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP" June 1999

© *tScheme* Limited, 2002 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Certificate Status Validation - clause compliance list		
Clause	**Description**	**Compliance**
CR-010	Operational Service	
SI-010	CAs supported	
SI-020	Method of publication	
SI-030	Status values supported	
SI-040	Service immediacy, ubiquity and availability	
SI-050	Authorisation and authentication of requests	
SI-070	Update frequency and how indicated	
SI-080	Authorised Certificate Status Management Services	
SI-090	Assured integrity	
SI-100	Assured confidentiality	
SI-110	Records retained and period	
RPA-010	Plain language agreement	
IP-010	Process documentation	
RECS-010	Records as claimed	
RECS-020	Record of CRLs published	
RECS-030	Record of time critical transactions	
RECS-040	Suitable recording media	

© *tScheme* Limited, 2002 - all rights reserved