Approval Profile
for
Certificate Status Management

Ref. tS 0106

Issue 1.0

2001-07-05

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

© Copyright Notice

This document may be copied for private research and study or for the purpose of any tScheme process.

CONTENTS

1. INTRODUCTION 3

2. SCOPE AND RELATION TO OTHER PROFILES. 4

3. CRITERIA 5

3.1 SERVICE DEFINITION 5
3.2 INTERNAL PROCEDURES 5
3.3 RECORDS 6

4. EVIDENCE 7

5. REFERENCES 8

© *tScheme* Limited, 2001 - all rights reserved

1. INTRODUCTION

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 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.

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 provision of services which 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].

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

© *tScheme* Limited, 2001 - all rights reserved

3. CRITERIA

The applicability of this Profile to the Service Subject to Assessment must be described in a "Specification of the Service Subject to Assessment" (S3A) as defined in "Preparing for an Assessment".

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

3.1 Service Definition

The service definition must clearly state:

1. which CAs are supported and what types of certificate;
2. the status values supported[2];
3. if a certificate is suspended pending possible revocation, suspension should not be for any longer than required to confirm a certificate's status;
4. the service levels supported[3];
5. 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;
6. how the integrity of the status information is assured;
7. any assumptions relating to the relationship with associated Certificate Status Services;
8. the method and periodicity for amendment to the status record;
9. the method and periodicity schedules for disseminating certificate status changes to Certificate Validation Service providers (if applicable);
10. any status change acknowledgement/confirmation applicable;
11. how the subscriber is to be informed of the change of status.

The service provider must at the time of assessment be providing a service which supports these statements.

3.2 Internal Procedures

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

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

---

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

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

© *tScheme* Limited, 2001 - all rights reserved

3.3 Records

The Service provider must maintain the records stated in the service claim. These are to include:

1. 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;
2. a trusted time record of when a status change request is received and when it is actioned.

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

© *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[4] 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. [X.509] - sections on CRLs.

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

© *tScheme* Limited, 2001 - all rights reserved

5. REFERENCES

[X.509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8: "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework"

© *tScheme* Limited, 2001 - all rights reserved