Approval Profile
for
Certificate Status Validation

Ref. tS 0107

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, system objects, corporate entities and other organisations for the verification 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 RELYING PARTY AGREEMENT 6
3.3 INTERNAL PROCEDURES 6
3.4 RECORDS 6

4. ABOUT 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 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 it 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.

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

© *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. how status information is published and the options available to access it[2];
3. the status values supported (valid, revoked or suspended, revocation reasons, revocation scope and so on);
4. the immediacy, ubiquity and availability of the service;
5. who is authorised to access a certificate's status and how are they authenticated;
6. 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;
7. how often and when the status information is updated, and the method of indicating these things;
8. how the integrity of the status information is assured;
9. how the confidentiality of the request and response is assured;
10. The records that will be retained and their retention period;

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

[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, 2001 - all rights reserved

3.2 Relying Party Agreement

The Service Provider must 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

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

3.4 Records

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

1. the publication of CRLs;
2. 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.

The records must 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, 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. Online Certificate Status Protocol [OCSP];
2. PKIX Operational Protocols LDAPv2; [PKOP]
3. [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

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

[PKOP] RFC 2559 "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2" April 1999

[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