Approval Profile
for
Registration Services

Ref. tS0042

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 and registration of identity and other attributes.

© 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 6

3.1 SERVICE DEFINITION 6
3.2 PROXIES 6
3.3 DATA PROTECTION 6
3.4 REGISTRANT AGREEMENT 7
3.5 RELYING PARTY AGREEMENT 7
3.6 DELIVERY OF CREDENTIALS 7
3.7 INTERNAL PROCEDURES 7
3.8 RECORDS 7

4. ABOUT EVIDENCE 9

5. REFERENCES 10

© *tScheme* Limited, 2001 - all rights reserved

1. INTRODUCTION

This Approval Profile is one of a number developed by *tScheme* against which a TSP's service(s) may be assessed by *tScheme*-recognised Assessors. It addresses the provision of a Registration 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.

A Registration Service may be offered for deployment either as a complete service in itself or as part of a multiple component overall service.

In the first case, the TSP may wish to make claims relating to some future overall service of which the Registration Service may either become a part or to which it may become a supplier. For example the TSP may claim that the Registration Service is suitable for playing a part in a Certification Authority Service issuing Qualified Certificates, even though it is not currently be being deployed in that context. In this situation, the tScheme-recognised Assessors would, at the request of the TSP, use the appropriate Approval Profile for the type of Certification Authority identified by the TSP (e.g. Approval Profile for a Certification Authority). Profiles of this type may lay down additional criteria applicable specifically to registration and verification - in fact Approval Profile for a Certification Authority does so by reference to [QCP]. These criteria would then be applied by the tScheme-recognised Assessor in addition to the criteria laid down here.

Alternatively, the TSP may wish to establish a claim that the Registration Service is appropriate for use in trust service contexts for which no Profiles currently exist. In this case, the TSP may specify this context and explicitly identify the additional criteria that it wishes to be applied.

When a Registration Service is to be assessed and deployed only as part of a larger multiple component service for which an Approval Profile has been produced, the additional criteria of the multiple component Approval Profile will automatically be pulled in.

Note also that some of the criteria laid down here, such as the existence of particular procedures or subscriber agreements, may be satisfied by procedures or agreements conducted through the multiple component service of which it is a part.

The criteria given in this Approval Profile are related to the provision of services which verify[1] and register[2] claimed registrant attributes. No specific constraint of scope is intended in this profile on the types of attribute which can potentially be verified using these services, or how they can be verified. In principle, the types of attribute examined in a Registration Service could range widely. For example they could be those:

1. associated with personal identity, such as name, address, and birth date;
2. related to a registrant's employment or position in society, such as name of employee, creditworthiness, bank account number or club membership;
3. belonging to IT system objects such as Virtual Private Network nodes.

Notwithstanding this, *tScheme* does however offer *guidelines* on specific Registration Services. These are provided in separate documents which can be found on the *tScheme* website. In the interests of interoperability and common understanding, providers of Registration Services are recommended to

---

[1] "Verification" is the process of ensuring to some degree of certitude that the attributes claimed are valid, i.e. they exist (a verification step known as "validation") and are possessed by the individual or organisational registrant being represented. Not all attributes need to be expressly validated.

[2] "Registration" is a form of affirmation that the claimed attributes have been successfully verified to some strength. The result of a successful registration process is frequently used as the basis for a request for the creation of a public key certificate, signed by a trusted service provider, indicating (by actual content or by reference), to the appropriate degree of certitude, that the verified attributes are possessed by the holder of the corresponding private key.

© *tScheme* Limited, 2001 - all rights reserved

conform to these *tScheme* service profile guidelines, where they fit the service requirements of their subscribers, relying parties and dependent TSPs.

© *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 state clearly in plain language:

1. why a registrant should use the service;
2. how registration will be conducted;
3. who or what is being verified[3];
4. the attributes being verified;
5. the methods used to complete the verification process and ensure that information used to verify the attributes of the registrant is still valid;
6. the steps necessary to re-verify a registrant at repeat application e.g. certificate renewal;
7. any liability accepted by the service provider in relation to the verification process;
8. disclosure/privacy policy - under what circumstances information will be disclosed to third parties;
9. Minimum retention policy for records.

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

3.2 Proxies[4]

If registration proxies are accepted, it is necessary to verify the authority of the proxy to act for the registrant concerned. The method of proxy verification must be shown to be consistent with that of the registrant proper.

3.3 Data Protection

Personal registrant or registrant proxy information requested during verification must only be that which is needed to perform registration, and it must only be used for this purpose unless explicitly authorised by the registrant.

---

[3] As well as the registrant, other parties may be included in the verification process, for example if an organisation is being registered, attributes of one or more individuals acting as proxies (see footnote 4) may also be subject to verification.

[4] A proxy is an individual who registers on behalf of the registrant whose attributes are being verified. The registrant proper may be either another individual, an organisation or a system object.

© *tScheme* Limited, 2001 - all rights reserved

The service provider must ensure that the requirements of the national data protection legislation are taken into account (including the use of pseudonyms if applicable) within their registration process.

3.4 Registrant Agreement

The TSP must oblige, through agreement, the subscriber or subscriber's proxy to submit accurate and complete information to the registration process in accordance with the requirements of the registration policy.

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP must record this, verify the information and agree it with the subscriber or the subscriber's proxy (see Section 3.2 for a description of a proxy).

3.5 Relying Party Agreement

The Service Provider must provide a plain language explanation of what a relying party can understand by the results of registration. This may be published directly or indirectly to end-users.

3.6 Delivery of Credentials

The resulting credentials must be delivered using an appropriately secure channel. The scope of the ISMS covering the RA component may exclude the delivery of credentials where this is covered by the ISMS of a connected service.

3.7 Internal Procedures

The registration and verification process must be fully documented and cover all expected situations, for example how failed verifications are managed and recorded.

3.8 Records

1. The Service provider must maintain timed and dated records of each registration and verification and secure them from unauthorised alteration or destruction.

2. The record may consist of an electronic or paper tick-sheet type record or copies of source credentials.

3. The record must cover all of the information and documentation used to verify the registrant's identity. Specifically it must include:

    i. document reference numbers;

    ii. any document validity limitations;

    iii. type of document(s) presented;

© *tScheme* Limited, 2001 - all rights reserved

iv. record of unique identification data, numbers, or a combination thereof[5], of identification documents, if applicable;

v. storage location of copies of applications and identification documents,

vi. proof of subscriber acceptance of subscriber agreement[6];

vii. any specific choices in the subscriber agreement (e.g. consent to publication of any resulting certificate);

viii. identity of entity accepting the application;

ix. method used to validate identification documents, if any;

x. name of receiving trust service and/or submitting trust service, if applicable.

4. The service provider must make and document proof of consent from the subscriber regarding record retention.

[5] For example the registrant's driver's licence number

[6] This would commonly be a signed paper or electronic agreement, but other forms of proof acceptable under the applicable data protection legislation would also be suitable.

© *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[7] 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, there are no standards that *tScheme* has identified as being especially relevant.

[7] 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

[QCP] ETSI TS 100 456 "Policy requirements for certification authorities issuing qualified certificates", version 0.0.15, dated 2000-11

© *tScheme* Limited, 2001 - all rights reserved