Approval Profile for Registration Services

Ref. tSd0042

Issue 2.00

2001-11-13

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.

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	1.0	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 the following changes: 1. changes reflecting Disposition tS0163 Version 0.03, 2001-07-24. These comprise various minor changes and the removal of the text describing the interrelationships between Registration and other specific service Profiles (equivalent text has been introduced in generalised form in the Base Approval Profile); 2. changes to Section 3.3 to: (a) permit information other than that needed for registration to be obtained, provided that the registrant gives explicit permission; (b) make clear that certificate management is anyway permitted. This enables the information to be used for revocation purposes among other things; (c) remove the statement of the general requirement to conform to the DPA act (which already appears in the Base Profile); 3. changes to Section 3.5 to: (a) reflect the fact that it is the relying TSP with whom the agreement must be made; (b) bring it into line with text in Section 3.1 of the Base Approval Profile; 4. changes to the references to tScheme guidelines, which have been modified to reflect tScheme's relinquishing of control of guidelines; 5. 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

© *tScheme* Limited, 2001 - all rights reserved

CONTENTS

1. INTRODUCTION 4

2. SCOPE AND RELATION TO OTHER PROFILES. 5

3. CRITERIA 6

3.1 SERVICE DEFINITION 6
3.2 PROXIES 6
3.3 DATA PROTECTION 7
3.4 REGISTRANT AGREEMENT 7
3.5 RELYING TSP 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.

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, guidelines on specific Registration Services do exist, and TSPs may make claims that these guidelines are being followed (see Section 4).

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. it may be used in isolation and is not dependent upon a successful assessment against any other Approval Profile.

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

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 criteria identified in the succeeding subsections:

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 for the TSP 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 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

3.3 Data Protection

In countries where Data Protection legislation has been passed, it will be especially applicable in the case of a TSP offering Registration Services, and the commitment to compliance already identified in the Base Approval Profile will correspondingly be given special emphasis.

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 TSP Agreement

The TSP must provide a plain language explanation of what a relying TSP can understand by the results of registration.

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

The Service provider must maintain timed and dated records of each registration and verification and secure them from loss, destruction, unauthorised amendment and falsification.

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

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

1. document reference numbers;
2. any document validity limitations;
3. type of document(s) presented;

© *tScheme* Limited, 2001 - all rights reserved

4. record of unique identification data, numbers, or a combination thereof[5], of identification documents, if applicable;
5. storage location of copies of applications and identification documents,
6. proof of subscriber acceptance of subscriber agreement[6];
7. any specific choices in the subscriber agreement (e.g. consent to publication of any resulting certificate);
8. identity of entity accepting the application;
9. method used to validate identification documents, if any;
10. name of receiving trust service and/or submitting trust service, if applicable.

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, though guidelines for the validation of identity of individuals [GOVID] and organisations [GOVORG] have been produced by the UK government for use with government services.

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

[GOVID] Guidelines for the Verification of Identity of Individuals, Pilot Version 2000-11-01, Editor: Martin Leverington, CCTA.

[GOVORG] Guidelines for the Verification of Identity of Organisations, Pilot Version 2000-11-01, Editor: Martin Leverington, CCTA.

© *tScheme* Limited, 2001 - all rights reserved