Issued

Approval Profile for Registration Services

Ref. tSd 0042

Issue 3.02

2004-08-26

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 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, 2004 - all rights reserved

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. Mention of how conformance to external guidelines can be claimed is now deleted, as this matter is now extensively covered elsewhere. 6. Minor editorial changes to achieve better consistency across the different Approval Profiles. 7. 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
tSd	3.01	2003-03-20	Update 'Date completed' in document properties to put correct date on front page.	*tScheme* Secretariat
tSd	3.02	2004-08-26	Incorporate the following changes: 1. Clause SI-050, delete the word 'still'; 2. Add clause RA-015; 3. Clause RECS-010, emphasise that records are kept both initially and as a result of changes.	*tScheme* Secretariat

© *tScheme* Limited, 2004 - 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 8
3.2 PROXIES 8
3.3 DATA PROTECTION 8
3.4 REGISTRANT AGREEMENT 8
3.5 RELYING TSP AGREEMENT 9
3.6 DELIVERY OF CREDENTIALS 9
3.7 INTERNAL PROCEDURES 9
3.8 RECORDS 9

4. REFERENCES 11

ANNEX 1. CLAUSE COMPLIANCE LIST 12

© *tScheme* Limited, 2004 - 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 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 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, 2004 - 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 verify[1] and register[2] claimed registrant attributes. No specific constraint of scope is intended in this Profile on the types of attribute that 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.

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 "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 Trust 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, 2004 - 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 criteria identified in the succeeding subsections:

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 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 Reason for use of Service
- why a registrant should use the Service;

SI-020 Conduct of registration
- how registration will be conducted;

SI-030 Scope of verification
- who or what is being verified[3];

SI-040 Attributes verified
- the attributes being verified;

SI-050 Verification process and verification validity assurance method
- the methods used to complete the verification process and ensure that information used to verify the attributes of the registrant is valid;

SI-060 Repeat verification methods
- the steps necessary to re-verify a registrant at repeat application e.g. certificate renewal;

SI-070 Liability accepted
- any liability accepted by the Service Provider in relation to the verification process;

SI-080 Disclosure/privacy policy
- disclosure/privacy policy - under what circumstances information will be disclosed to third parties;

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.

© *tScheme* Limited, 2004 - all rights reserved

SI-090 Minimum record retention policy

- Minimum retention policy for records.

3.1.2 Information for Assessors

No specific additional information identified

3.2 Proxies[4]

PROX-010 Proxy verification

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 shall be shown to be consistent with that of the registrant proper.

3.3 Data Protection

DP-010 Emphasis on Data Protection compliance

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

RA-010 Registrant obligation to be accurate and complete

The TSP shall 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.

RA-015 Registrant obligation to notify information changes

The TSP shall oblige, through agreement, the subscriber or subscriber's proxy to notify the TSP whenever there are any changes to the registrant's registration information.

RA-020 Record of registration information changes

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP shall record this.

RA-030 Verification of registration information changes

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP shall verify the information.

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, 2004 - all rights reserved

RA-040 Agreement on registration information changes

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP shall 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

RTA-010 Explanation to relying TSP of meaning of results

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

3.6 Delivery of credentials

DC-010 Secure credential delivery

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

3.7 Internal procedures

IP-010 All processes and expected situations documented

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

3.8 Records

RECS-010 Maintenance of records

The TSP shall maintain timed and dated records of each registration and verification, both initially and as a result of changes to registration information.

RECS-020 Security of records

The Service Provider shall secure from loss, destruction, unauthorised amendment and falsification all records of registration and verification. These records may consist of an electronic or paper tick-sheet type records or copies of source credentials.

RECS-030 Record of all information and documentation used

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

RECS-040 Record of document reference numbers

- document reference numbers;

© *tScheme* Limited, 2004 - all rights reserved

RECS-050 Record of document validity limitations

- any document validity limitations;

RECS-060 Record of type of document(s) presented

- type of document(s) presented;

RECS-070 Record of documentation identification

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

RECS-080 Record where applications and document copies stored

- storage location of copies of applications and identification documents,

RECS-090 Record of proof of agreement

- proof of subscriber acceptance of subscriber agreement[6];

RECS-100 Record of agreement choices made

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

RECS-110 Record of identity of who accepted the application

- identity of entity accepting the application;

RECS-120 Record of document validation method

- method used to validate identification documents, if any;

RECS-130 Record of receiving and/or transmitting Trust Services

- name of receiving Trust Service and/or submitting Trust Service, if applicable.

RECS-140 Proof of consent regarding record retention

The Service Provider shall 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, 2004 - all rights reserved

4. REFERENCES

None.

© *tScheme* Limited, 2004 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Registration Services - clause compliance list

Clause	Description	Compliance
CR-010	Operational Service	
SI-010	Reason for use of Service	
SI-020	Conduct of registration	
SI-030	Scope of verification	
SI-040	Attributes verified	
SI-050	Verification process and verification validity assurance method	
SI-060	Repeat verification methods	
SI-070	Liability accepted	
SI-080	Disclosure/privacy policy	
SI-090	Minimum record retention policy	
PROX-010	Proxy verification	
DP-010	Emphasis on Data Protection compliance	
RA-010	Registrant obligation to be accurate and complete	
RA-015	Registrant obligation to notify information changes	
RA-020	Record of registration information changes	
RA-030	Verification of registration information changes	
RA-040	Agreement on registration information changes	
RTA-010	Explanation to relying TSP of meaning of results	
DC-010	Secure credential delivery	
IP-010	All processes and expected situations documented	
RECS-010	Maintenance of records	

© *tScheme* Limited, 2004 - all rights reserved

Approval Profile for Registration Services - clause compliance list

Clause	Description	Compliance
RECS-020	Security of records	
RECS-030	Record of all information and documentation used	
RECS-040	Record of document reference numbers	
RECS-050	Record of document validity limitations	
RECS-060	Record of type of document(s) presented	
RECS-070	Record of documentation identification	
RECS-080	Record where applications and document copies stored	
RECS-090	Record of proof of agreement	
RECS-100	Record of agreement choices made	
RECS-110	Record of identity of who accepted the application	
RECS-120	Record of document validation method	
RECS-130	Record of receiving and/or transmitting Trust Services	
RECS-140	Proof of consent regarding record retention	

© *tScheme* Limited, 2004 - all rights reserved