Issued

Approval Profile for Identity Registration Services

Ref. tSd 0108

Issue 2.06

2009-09-15

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 Government, individuals, system objects, corporate entities and other relying parties for the verification and registration of identity attributes.

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	Version	Date	Comment	Authorised
tSd	1.00	2003-09-04	First version, tracked under Document Management procedures.	*tScheme* Board
tSd	2.00	2004-05-08	Incorporate the following changes: 1. Change title of document and broaden scope given in executive summary on front cover; 2. §1.2 – General: remove specific reference to [HMGVInd] and introduce concept of RVR; 3. Add §1.3 - Glossary for terms used just in this Profile; 4. Extensive changes to §2 - Scope and relation to other Profiles, including addition of diagram; 5. §3 - Criteria: remove specific reference to [HMGVInd] and introduce concept of RVR; 6. §3.1.1 - Information for users: changes to reflect use of RVR; 7. §3.2 - Proxies: emphasise verification of proxies must be at least as rigorous as for registrants; 8. §3.4 - Registrant agreement: reorder some criteria and add new criterion on agreement to notification of changes to relying parties; 9. §3.5 - Relying TSP agreement: add new criteria; 10. §3.6 - Credential Lifecycle: title changed from 'Delivery of credentials' and new criteria added to cover entire lifecycle not just delivery; 11. §3.7 - Internal procedures: add new criterion relating to pre-existing credentials; 12. §3.9 - Records: changes to reflect use of RVR; 13. Throughout: minor changes to reflect consistent usage of new terminology as defined in the glossary.	*tScheme* Board
tSd	2.01	2008-08-04	Change title to fit into broader set of IdP services and remove §1.3 – Glossary.	*tScheme* secretariat
tSd	2.02	2008-12-24	Changes as a result of discussions with EAS project	*tScheme* secretariat
tSd	2.03	2009-01-07	§3.2 - Proxies: clarify criteria must cover both identity and authority of proxy.	*tScheme* secretariat

© *tScheme* Limited, 2009 - all rights reserved

tSd	2.04	2009-02-06	SI-100: require clarification about conditions required for pre-approval credentials to be still valid.	*tScheme* secretariat
tSd	2.05	2009-08-07	Incorporate the following changes: 1. All external *tScheme* document references now added to References section; 2. Embolden all terms that are in Glossary document; 3. Wording for steps 2 & 3 in diagram in Scope section modified to be more generic; 4. In Scope section, remove apparent restriction that Identity Providers are only large organisations; 5. Reword DP-010 on Data Protection compliance.	*tScheme* secretariat
tSd	2.06	2009-09-15	Ratified by Board for Issue status	*tScheme* board

© *tScheme* Limited, 2009 - 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 8

3.1 SERVICE INFORMATION 8
3.1.1 Information for users 8
3.1.2 Information for Assessors 9
3.2 PROXIES 9
3.3 DATA PROTECTION 9
3.4 REGISTRANT AGREEMENT 9
3.5 RELYING TSP AGREEMENT 10
3.6 CREDENTIAL LIFECYCLE 10
3.7 DELIVERY OF CREDENTIALS 10
3.8 INTERNAL PROCEDURES 11
3.9 RECORDS 11

4. REFERENCES 13

ANNEX 1. CLAUSE COMPLIANCE LIST 14

© *tScheme* Limited, 2009 - 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

Use of bold text indicates that the word or phrase is defined within the *tScheme* Glossary of Terms [Glossary].

For the purposes of this document, any organisation providing services that enhance or supply trusted information in order to support electronic transactions is referred to as a **Trust-Service Provider**, hereafter abbreviated to **TSP**. The term **Trust-Service Provider** or **TSP** includes the more specific term **Identity Service Provider**, which applies to providers of **Services** such as are addressed by this **Profile**.

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 an Identity Registration Service and may be one of a selection that a **TSP** has identified within the definition of its **Service Subject to Assessment**.

Since a large proportion of the criteria that are assessed for a *tScheme* **Approval** are not service specific, they have been separated from the service-specific elements and are maintained in a document called the Base Approval Profile [Base]. Therefore, during a *tScheme* **Assessment**, the criteria defined herein shall, as a minimum, be applied in combination with the Base Approval Profile [Base] (unless it is a ***tScheme*-Ready Assessment**).

Full details of all Approval Profiles and the Approval Process may be found on the *tScheme* website.

This document is designed to be applied in conjunction with one of a number of alternative '**Recognised Verification Requirements** (**RVR**)' documents, which are available in the secure directory area of the *tScheme* website. Each of these documents lays down the minimum set of requirements that are appropriate to a particular relying party or community of relying parties.

All of these **RVR** documents on the website have been assessed and recognised by *tScheme* as being capable of being used as an 'External standard or guideline' as defined in our Required Assessment Procedures document [RAP].

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:

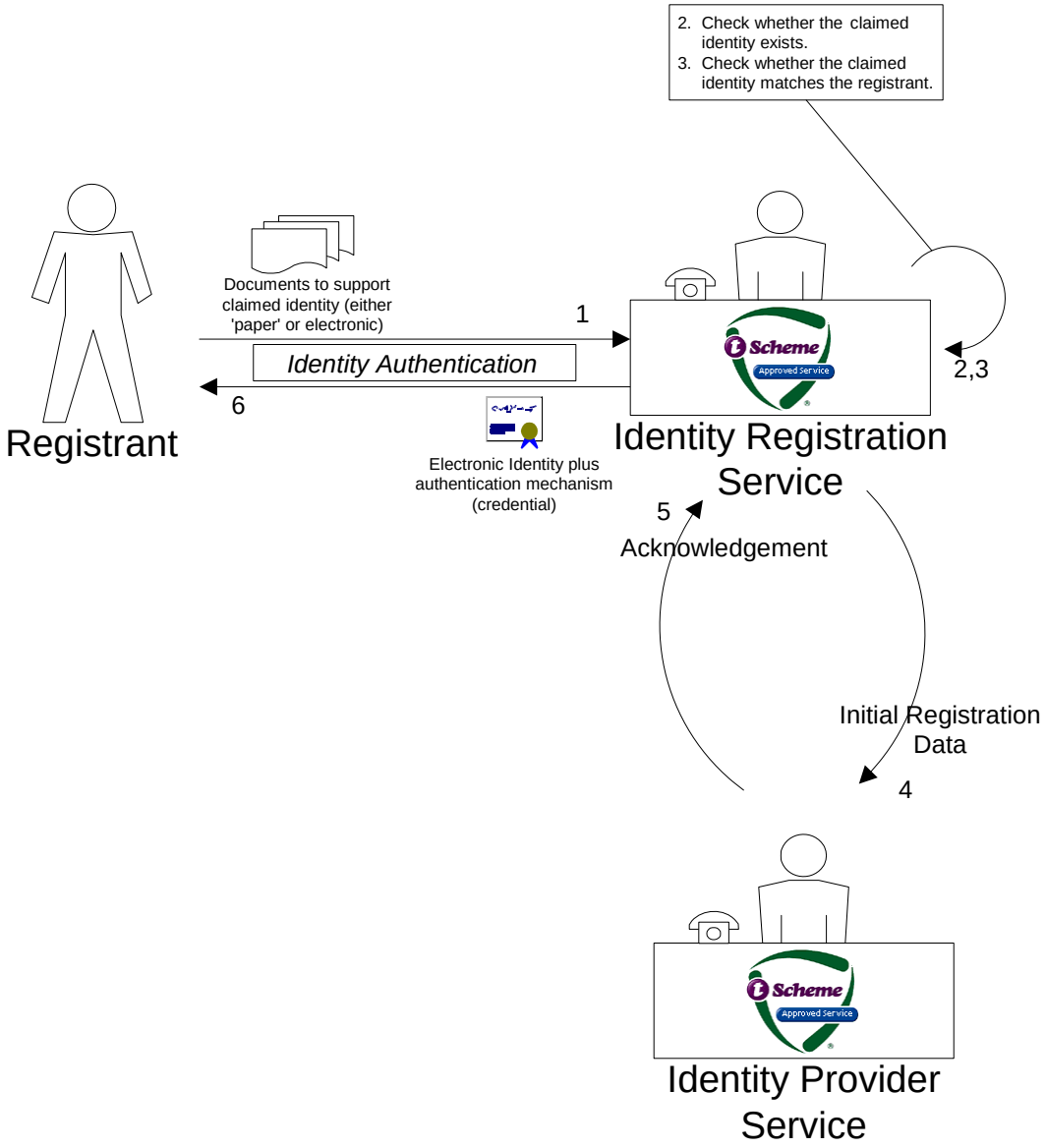
- references to "**Service Provider** or **TSP**" shall be taken to mean "**Component supplier**";
- references to "**Service**" shall be taken to mean "**Service Component**";
- references to "**Service Subject to Assessment**", or **SSA**, shall be taken to mean "**Service Component Subject to Assessment**", 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, 2009 - all rights reserved

2. SCOPE AND RELATION TO OTHER PROFILES

The criteria given in this **Approval Profile** are related to **Services** that are established to enable an individual to register with an **Identity Provider** in order to gain the means of transacting electronically with relying parties. These relying parties, who will be either **Trust Service Providers** or some other kind of service providers, need to be able to trust that ultimately they are transacting with the individual from whom the electronic transaction appears to originate.

An overview of the processes involved can be seen in the following diagram:



As can be seen, the **Identity Registration Service** links an **electronic identity** with a **real-world identity**. The **registrant** presents proof of their **real-world identity** (e.g. **documentation** such as Passport, Driving Licence or pre-existing electronic evidence) to the **Identity Registration Service** so that they can **validate** and **verify** the **registrant**'s claimed **real-world identity**. No specific constraint of scope is intended in this **Profile** on how these processes could be carried out.

© *tScheme* Limited, 2009 - all rights reserved

The **verification** process must, as a minimum, comply with the requirements laid down by one of the **Recognised Verification Requirements** on the ***tScheme*** website, for example, the UK government's minimum requirements for the verification of the identity of individuals [HMGVInd].

As a result of a successful **identity authentication**, the **registrant** will be allocated an **electronic identity**, which might be the name of the **registrant**, a pseudonym or some other identifier (or combination thereof). They will then be issued with the means to authenticate themselves against this **electronic identity**; hereafter such means are termed a **credential**. In principle, the types of **credential** used by an **Identity Provider** could range widely and might involve an electronic or physical **credential**. Examples of such **credentials** could include:

1. a PIN and/or password (virtual **credential**);
2. a one-time password generator or smartcard (physical **credential**);
3. a biometric token (biometric **credential**).

Note that any further uses of the **credential** other than for **credential authentication** against the **electronic identity** are out of scope of this **Profile**.

Finally, the **Identity Registration Service** must also provide, directly or indirectly, the means by which the lifecycle of the **credential** can be managed. For example, recovering or replacing lost PINs and passwords or revoking public-key certificates. The characteristics of this process are covered by the Credential Management Profile [CrdM].

This **Profile** is intended to support both organisations that act as **Identity Providers** and apply a defined set of requirements when **validating** and **verifying** identities of individuals already known to them, either as customers or employees etc, who then wish to provide these individuals with **credentials** that can be used to access online services from, amongst others, the UK government; and also commercial **Identity Providers** who are providing such **credentials** as a **Service** to a given community.

The criteria given in this **Approval Profile** are in addition to those given in the Base Approval Profile [Base] but are not directly related to any other service-specific **Approval Profiles**, i.e. this **Profile** may be used in isolation and is not dependent upon a successful **Assessment** against any other service-specific **Approval Profile**.

© *tScheme* Limited, 2009 - 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 the "Model Specification of Service Subject to Assessment" document [ModelS3A]. In particular, this **S3A** must state, amongst other things (as detailed below), the **validation** and **verification** policy that is to be applied when checking a **registrant**'s real-world identity, including, if applicable, the registration level (in the case of incremental alternatives) or category (in the case of discrete alternatives) that is being applied from the specified **RVR** document(s); the type of credential used to allow authentication of the electronic identity; and the lifecycle processes employed to manage the electronic identity and related credential.

Compliance with this **Approval Profile** will then be achieved by satisfying the criteria identified in the following subsections.

CR-010 **Operational Service**

Each **SSA** shall be an **Operational Service** (in the sense defined in the *tScheme* Glossary of Terms [Glossary]) supporting the statements given in response to the criteria listed 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 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 Applicable **RVR**
- identification of the relevant **Recognised Verification Requirements** to be used;

SI-040 Registration level or category
- if applicable, either the level (incremental) or category (discrete) of registration checks to be applied from the specified **RVR** document;

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 real-world identity of the **registrant** is **valid**;

SI-060 Repeat **verification** methods
- where offered, the steps necessary to re-**verify** a **registrant** at repeat application;

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

© *tScheme* Limited, 2009 - all rights reserved

SI-080 Disclosure/privacy policy

- under what circumstances information will be disclosed to third parties;

SI-090 Minimum record retention policy

- minimum retention policy for records;

SI-100 Validity of pre-**Approval credentials**

- conditions under which **credentials** established prior to initial *tScheme* **Approval** will still be valid.

3.1.2 Information for Assessors

No specific additional information identified.

3.2 Proxies

PROX-010 **Proxy verification**

If registration **proxies** are accepted, it is necessary for the **Identity Registration Service** to verify the identity of the **proxy** and their authority to act for the **registrant** concerned. The method of **proxy verification** shall be shown to be consistent with, and at least as rigorous as, that of the **registrant** proper.

3.3 Data Protection

DP-010 Emphasis on Data Protection compliance

In countries where Data Protection legislation is in force the commitment to compliance already identified in the Base Approval Profile [Base] will be given special emphasis.

3.4 Registrant agreement[1]

RA-010 **Registrant** obligation to be accurate and complete

The **Identity Registration Service Provider** shall oblige, through agreement, the **registrant** or **registrant**'s **proxy** to submit accurate and complete information to the registration process in accordance with the requirements of the relevant **RVR**.

RA-020 **Registrant** obligation to notify information changes

The **Identity Registration Service Provider** shall oblige, through agreement, the **registrant** or **registrant**'s **proxy** to notify the **Identity Registration Service Provider** whenever there are any changes to the **registrant**'s **registration information**.

[1] This section requires an ongoing agreement between the **Identity Service Provider** and the **registrant**. Such an agreement may be limited in time, but must last throughout the validity period of any **credential** issued subject to that agreement (see Section 3.6, DC-020).

© *tScheme* Limited, 2009 - all rights reserved

RA-030 **Verification** of **registration information** changes

If, subsequent to initial registration and **verification**, the **Identity Registration Service Provider** is notified that any **registration information** has changed, the **Identity Registration Service Provider** shall determine the authenticity of the notification and, where required, **verify** the changed information.

RA-040 Record of **registration information** changes

If, subsequent to initial registration and **verification**, the **Identity Registration Service Provider** is informed that any **registration information** has changed, the **Identity Registration Service Provider** shall record this changed information.

RA-050 Agreement on **registration information** changes

If, subsequent to initial registration and **verification**, the **Identity Registration Service Provider** is informed that any **registration information** has changed, the **Identity Registration Service Provider** shall agree the changes with the **registrant** or the **registrant**'s **proxy**. The **Identity Registration Service Provider** shall record this agreement.

RA-060 Agreement on notification to RPs

The **Identity Registration Service Provider** shall oblige, through agreement, the **registrant** or **registrant**'s **proxy** to allow the notification of **registration information** to be passed to relying parties.

3.5 Relying TSP agreement

RTA-010 Explanation to relying TSP of meaning of results

The **Identity Registration Service Provider** shall provide a plain language explanation of what a relying TSP can understand by the results of registration.

3.6 Credential Lifecycle

CL-010 Creation of electronic identity and credential

The **Identity Registration Service Provider** shall record details of the e**lectronic identity** chosen by the **registrant** or created by the relevant **Identity Service Provider**, including details of any associated **credential**. Details shall be stored in a manner that minimises risk of compromise, e.g. by using a one-way hash function. If appropriate, procedures should be in place to ensure that **credentials** are unique and that they are not reused.

3.7 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 Identity Registration function may exclude the delivery of credentials where this is covered by the ISMS of a connected Service.

© *tScheme* Limited, 2009 - all rights reserved

3.8 Internal procedures

IP-010 All processes and expected situations documented

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

IP-020 Registration procedures must comply with requirements of relevant **RVR**

The **identity authentication** process must, as a minimum, comply with the requirements laid down by the relevant **Recognised Verification Requirements**, as appropriate for the registration level or category stated in the Public Service Description.

3.9 Records

RECS-010 Maintenance of records

The **Identity Registration Service Provider** shall maintain timed and dated records of each **identity authentication**, both at initial registration and when any changes to the **registration information** are processed.

RECS-020 Security of records

The **Identity Registration Service Provider** shall secure from loss, destruction, unauthorised release or amendment and falsification all records of **identity authentication**.

RECS-030 Proof of consent regarding record retention

The **Identity Registration Service Provider** shall make and document proof of consent from the **registrant** regarding record retention.

RECS-040 Record of all information and **documentation** used

The record shall cover all of the information and **documentation** used to **verify** the **registrant**'s identity. The details of what must be retained and the period of retention are as specified in the current version of the relevant **Recognised Verification Requirements**.

Specifically it shall include:

RECS-050 Record of document reference numbers
- any reference numbers applicable to the **documentation**;

RECS-060 Record of document validity limitations
- any validity limitations for the **documentation**;

RECS-070 Record of type of **documentation** presented
- type of **documentation** presented;

RECS-080 Record of evidence of claimed **real-world identity**
- record of unique identification data, numbers, or a combination thereof[2], of **documentation** supplied as evidence of the claimed **real-world identity**, if applicable;

2 For example the **registrant**'s passport or driver's licence number

© *tScheme* Limited, 2009 - all rights reserved

RECS-090 Record of where copies stored

- storage location of copies of applications and **documentation** supplied as evidence of the claimed **real-world identity**,

RECS-100 Record of proof of agreement

- proof of **registrant**'s acceptance of **registrant** agreement[3];

RECS-110 Record of agreement choices made

- any specific choices in the **registrant** agreement;

RECS-120 Record of process of acceptance of the application

- audit trail of the process leading to acceptance of evidence supplied to support claimed **real-world identity**;

RECS-130 Record of document **validation** method

- method used to **validate** identification **documentation**, if any;

3 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, 2009 - all rights reserved

4. REFERENCES

[Base] tSd0111 – Base Approval Profile

[CrdM] tSd0113 – Approval Profile for Credential Management Services

[Glossary] tSd0226 - tScheme Glossary of Terms

[HMGVInd] HMG's Minimum Requirements for the Verification of the Identity of Individuals v2.0

[ModelS3A] tSd0230 – Model Specification of Service Subject to Assessment

[RAP] tSd0244 - Required Assessment Procedures

© *tScheme* Limited, 2009 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Identity 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	Applicable **RVR**	
SI-040	Registration level or category	
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	
SI-100	Validity of pre-**Approval credentials**	
PROX-010	**Proxy verification**	
DP-010	Emphasis on Data Protection compliance	
RA-010	**Registrant** obligation to be accurate and complete	
RA-020	**Registrant** obligation to notify information changes	
RA-030	**Verification** of **registration information** changes	
RA-040	Record of **registration information** changes	
RA-050	Agreement on **registration information** changes	
RA-060	Agreement on notification to RPs	
RTA-010	Explanation to relying TSP of meaning of results	
CL-010	Creation of electronic identity and credential	

© *tScheme* Limited, 2009 - all rights reserved

Approval Profile for Identity Services - clause compliance list

Clause	Description	Compliance
DC-010	Secure **credential** delivery	
IP-010	All processes and expected situations documented	
IP-020	Registration procedures must comply with requirements of relevant **RVR**	
RECS-010	Maintenance of records	
RECS-020	Security of records	
RECS-030	Proof of consent regarding record retention	
RECS-040	Record of all information and **documentation** used	
RECS-050	Record of document reference numbers	
RECS-060	Record of document validity limitations	
RECS-070	Record of type of **documentation** presented	
RECS-080	Record of evidence of claimed **real-world identity**	
RECS-090	Record of where copies stored	
RECS-100	Record of proof of agreement	
RECS-110	Record of agreement choices made	
RECS-120	Record of process of acceptance of the application	
RECS-130	Record of document **validation** method	

© *tScheme* Limited, 2009 - all rights reserved