Issued

Approval Profile for Attribute Registration Services

Ref. tSd 0110

Issue 1.00

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 correlation of qualification evidence with an electronic identity sufficient to support addition of relevant attributes to the entity represented by the electronic identity.

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	0.01	2008-11-14	First draft for comment.	*tScheme* secretariat
tSd	0.02	2008-12-24	Changes as a result of discussions with EAS project	*tScheme* secretariat
tSd	0.03	2009-02-18	Renumber RECS-040 as RECS-035, then amend subsequent numbers and re-title new RECS-040 so that they align with same criteria in the Identity Registration Profile tSd0108.	*tScheme* secretariat
tSd	0.04	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. Reword DP-010 on Data Protection compliance; 4. Reword RA-040 to clarify that changes are recorded after they have been verified; 5. Reword RA-050 to require notification of changes not agreement.	*tScheme* secretariat
tSd	1.00	2009-09-15	Ratified by Board for Issue status	*tScheme* board

© *tScheme* Limited, 2009 - all rights reserved

CONTENTS

1. INTRODUCTION 4

1.1 CONVENTIONS 4
1.2 GENERAL 4

2. SCOPE AND RELATION TO OTHER PROFILES 5

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 INTERNAL PROCEDURES 9
3.7 RECORDS 9

4. REFERENCES 12

ANNEX 1. CLAUSE COMPLIANCE LIST 13

© *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 Attribute 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.

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:

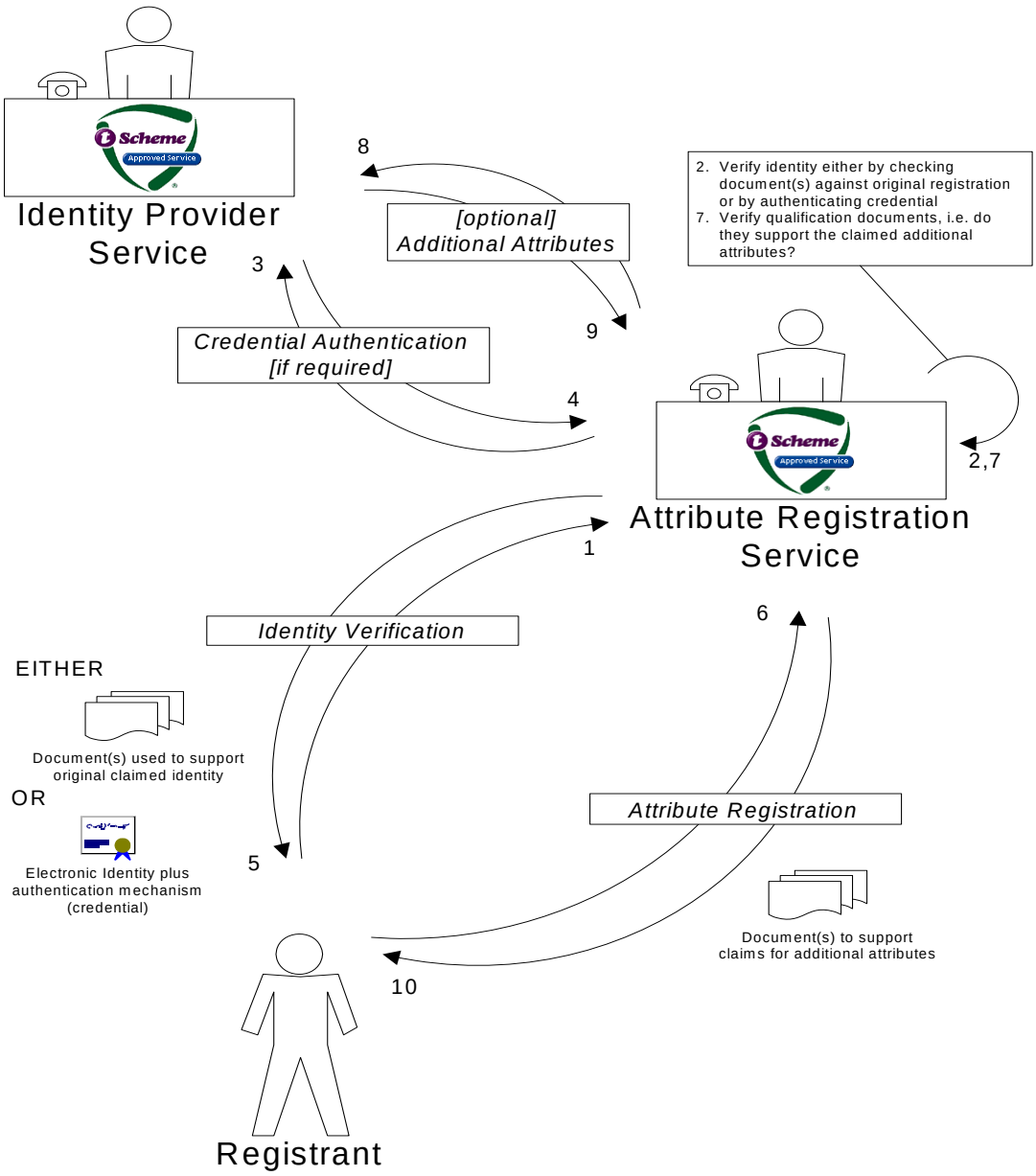
- references to "**Service Provider** or **TSP**" shall be taken to mean "**Component supplier**";
- references to "**Service**" shall be taken to mean "**Service Component**";
- references to "**Service Subject to Assessment**", or **SSA**, shall be taken to mean "**Service Component Subject to Assessment**", 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 in possession of a **credential** to associate additional attributes with that **credential** in order to be able assert those attributes to 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:



In order to be able to assert additional attributes within a **scheme** or community, an individual will make use of an **Attribute Registration Service** in order to demonstrate their right to assert such

attributes (such as educational qualifications, proof of successful training, affiliation to a society or professional body, etc).

The **registrants** will identify themselves to the **Attribute Registration Service**, and then apply for additional attributes to be associated with their **electronic identity**. To identify themselves, the **registrants** will either use the appropriate **credential** or, if the process is within a **scheme**, present proof of their **real-world identity** sufficient to identify themselves within the **scheme**. No specific constraint of scope is intended in this **Profile** on how these processes could be carried out.

Having identified themselves, the **registrants** will then produce evidence to support their claim that they are entitled to assert additional attributes. This **attribute verification** process must comply with rules published and understood by the **scheme** or community.

Referring to the earlier process-flow diagram, in the case where **registrants** identify themselves to the **Attribute Registration Service** using proof of their **real-world identity** steps 3 & 4 would not take place. Similarly, the **Attribute Registration Service** may either relay the additional attributes back to the **Identity Provider Service** or they may stay local to the **scheme** (in which case steps 8 & 9 would not take place). However, the **scheme** must ensure that it can manage these additional attributes either directly or via the **Attribute Registration Service** or, if appropriate, via the **Identity Provider Service**.

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 refer to the **attribute registration** policy that is to be applied when checking a **registrant**'s evidence to support their claim that they are entitled to assert additional attributes, and the lifecycle processes employed to manage these additional attributes. This policy must be published so as to be available to all relying parties.

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 identity verification
- how identity verification will be conducted;

SI-030 Conduct of attribute registration
- how attribute registration will be conducted;

SI-040 Applicable **attribute registration** policy
- reference to the **attribute registration** policy to be used when checking a claim to assert additional attributes;

SI-050 Liability accepted
- any liability accepted by the **Attribute Registration Service** in relation to the **attribute registration** process;

SI-060 Disclosure/privacy policy
- under what circumstances information will be disclosed to third parties;

SI-070 Minimum record retention policy
- minimum retention policy for records;

© *tScheme* Limited, 2009 - all rights reserved

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 **Attribute 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 original **identity verification** 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 **Attribute Registration Service** 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 **attribute registration** policy.

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

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

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

If, subsequent to initial **attribute registration**, the **Attribute Registration Service** is notified that any **attribute registration information** has changed, the **Attribute Registration Service** shall determine the authenticity of the notification and, as appropriate, verify the changed information.

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

Following verification of any **attribute registration information** changes, the **Attribute Registration Service** shall record this changed 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.

© *tScheme* Limited, 2009 - all rights reserved

RA-050 Notification of **attribute registration information** changes

Following verification of any **attribute registration information** changes, the **Attribute Registration Service** shall notify the **registrant** or the **registrant**'s **proxy** of the changes. The **Attribute Registration Service** shall record this notification.

RA-060 Agreement on notification to RPs

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

3.5 Relying TSP agreement

RTA-010 Explanation to relying TSP of meaning of results

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

3.6 Attribute Lifecycle

AL-010 Association of additional attributes to an **electronic identity**

The **Attribute Registration Service Provider** shall ensure that attributes verified during the **attribute registration** process are associated with the e**lectronic identity** of the **registrant**. Details shall be stored in a manner that minimises risk of compromise, e.g. by using a one-way hash function.

3.7 Internal procedures

IP-010 All processes and expected situations documented

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

IP-020 Registration procedures must comply with requirements of relevant policy

The **attribute registration** process must, as a minimum, comply with the requirements laid down by the relevant **attribute registration** policy as stated in the Public Service Description.

3.8 Records

RECS-010 Maintenance of records

The **Attribute Registration Service** shall maintain timed and dated records of initial **attribute registration** and of any changes to the **attribute registration information** that are processed.

© *tScheme* Limited, 2009 - all rights reserved

RECS-020 Security of records

The **Attribute Registration Service** shall secure from loss, destruction, unauthorised release or amendment and falsification all records of **identity verification** and **attribute registration**.

RECS-030 Proof of consent regarding record retention

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

RECS-035 Record of all **identity verification** information used

The record shall cover all of the **identity verification** information used to verify the **registrant**'s identity. The details of what must be retained and the period of retention shall be specified in the current version of the relevant **attribute registration** policy.

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

The record shall cover all of the **attribute registration information** used to verify the **registrant**'s claim to additional attributes. The details of what must be retained and the period of retention shall be specified in the current version of the relevant **attribute registration** policy.

Specifically it shall include:

RECS-050 Record of document reference numbers
- any reference numbers applicable to the **attribute registration information**;

RECS-060 Record of document validity limitations
- any validity limitations for the **attribute registration information**;

RECS-070 Record of type of **documentation** presented
- type of attribute registration information 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;

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**;

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

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

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

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

© *tScheme* Limited, 2009 - all rights reserved

4. REFERENCES

[Base] tSd0111 – Base Approval Profile

[Glossary] tSd0226 - tScheme Glossary of Terms

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

© *tScheme* Limited, 2009 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Approval Profile for Attribute Registration Services - clause compliance list		
Clause	**Description**	**Compliance**
CR-010	**Operational Service**	
SI-010	Reason for use of **Service**	
SI-020	Conduct of identity verification	
SI-030	Conduct of attribute registration	
SI-040	Applicable **attribute registration** policy	
SI-050	Liability accepted	
SI-060	Disclosure/privacy policy	
SI-070	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-020	**Registrant** obligation to notify information changes	
RA-030	Verification of **attribute registration information** changes	
RA-040	Record of **attribute registration information** changes	
RA-050	Notification of **attribute registration information** changes	
RA-060	Agreement on notification to RPs	
RTA-010	Explanation to relying TSP of meaning of results	
AL-010	Association of additional attributes to an **electronic identity**	
IP-010	All processes and expected situations documented	
IP-020	Registration procedures must comply with requirements of relevant policy	

© *tScheme* Limited, 2009 - all rights reserved

Approval Profile for Attribute Registration Services - clause compliance list

Clause	Description	Compliance
RECS-010	Maintenance of records	
RECS-020	Security of records	
RECS-030	Proof of consent regarding record retention	
RECS-035	Record of all **identity verification** information used	
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