Issued

Approval Profile for Identity Services

Ref. tSd 0108

Issue 2.00

2004-08-05

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 provision of credentials to enable the authentication of the identity of individuals.

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 Party 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. §3.8 - 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

© *tScheme* Limited, 2003 - all rights reserved

CONTENTS

1. INTRODUCTION 4

1.1 CONVENTIONS 4
1.2 GENERAL 4
1.3 GLOSSARY 5

2. SCOPE AND RELATION TO OTHER PROFILES 7

3. CRITERIA 9

3.1 SERVICE INFORMATION 9
3.1.1 Information for users 9
3.1.2 Information for Assessors 10
3.2 PROXIES 10
3.3 DATA PROTECTION 10
3.4 REGISTRANT AGREEMENT 10
3.5 RELYING PARTY AGREEMENT 11
3.6 CREDENTIAL LIFECYCLE 12
3.7 INTERNAL PROCEDURES 13
3.8 RECORDS 13

4. REFERENCES 15

ANNEX 1. CLAUSE COMPLIANCE LIST 16

© *tScheme* Limited, 2003 - 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 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** 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 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. Therefore, during a *tScheme* **Assessment**, the criteria defined herein 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.

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 (tSd0244).

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, 2003 - all rights reserved

1.3 Glossary

tScheme employs its own specialised use of terms. This **Approval Profile** and other Definitive documents create a vocabulary that, while in itself internally self-consistent, is easily capable of misuse to the confusion of readers and listeners. This section provides a guide to the correct usage within the *tScheme* process for terms relating solely to this **Profile**. Definitions of terms and acronyms not defined in this document may be found in the *tScheme* Glossary of Terms.

210	Credential	A mechanism used by an individual to prove that they 'own' a given **electronic identity**.
310	Credential authentication	The process by which a relying party confirms that an individual is using a genuine **credential** as proof of a claimed **electronic identity**.
510	Documentation	Physical or electronic data used to provide evidence to support a claimed **real-world identity**.
110	Electronic identity	A name or similar identifier that can be used in electronic transactions and that is capable of being linked to a **real-world identity**.
710	Identity authentication	The procedure used by an **Identity Service Provider** to **validate** and **verify** a **registrant**'s **real-world identity**.
320	Identity Service	An **Electronic Trust Service** that allocates unique **electronic identities** to users of the service and provides **credentials** to enable relying parties to authenticate a user against their assigned **electronic identity**.
410	Identity Service Provider	A body operating or offering one or more **Identity Services**.
610	Proxy	An individual who registers on behalf of the **registrant** whose identity is being **verified**.
10	Real-world identity	A set of attributes (e.g. name, date of birth, physical characteristic) which together uniquely identify an individual.
520	Registrant	The individual who is registering with the **Identity Service Provider** in order to gain the means for transacting electronically.
620	Registration information	This is the **documentation** required by the relevant Recognised Verification Requirements to support the claimed **real-world identity**. It does not cover any other, supplementary information required by the **Identity Service Provider** when providing the **Service** to the **registrant**.
120	Validate	Demonstrate that a claimed **real-world identity** exists (i.e. that a person, who has certain attributes, exists).

© *tScheme* Limited, 2003 - all rights reserved

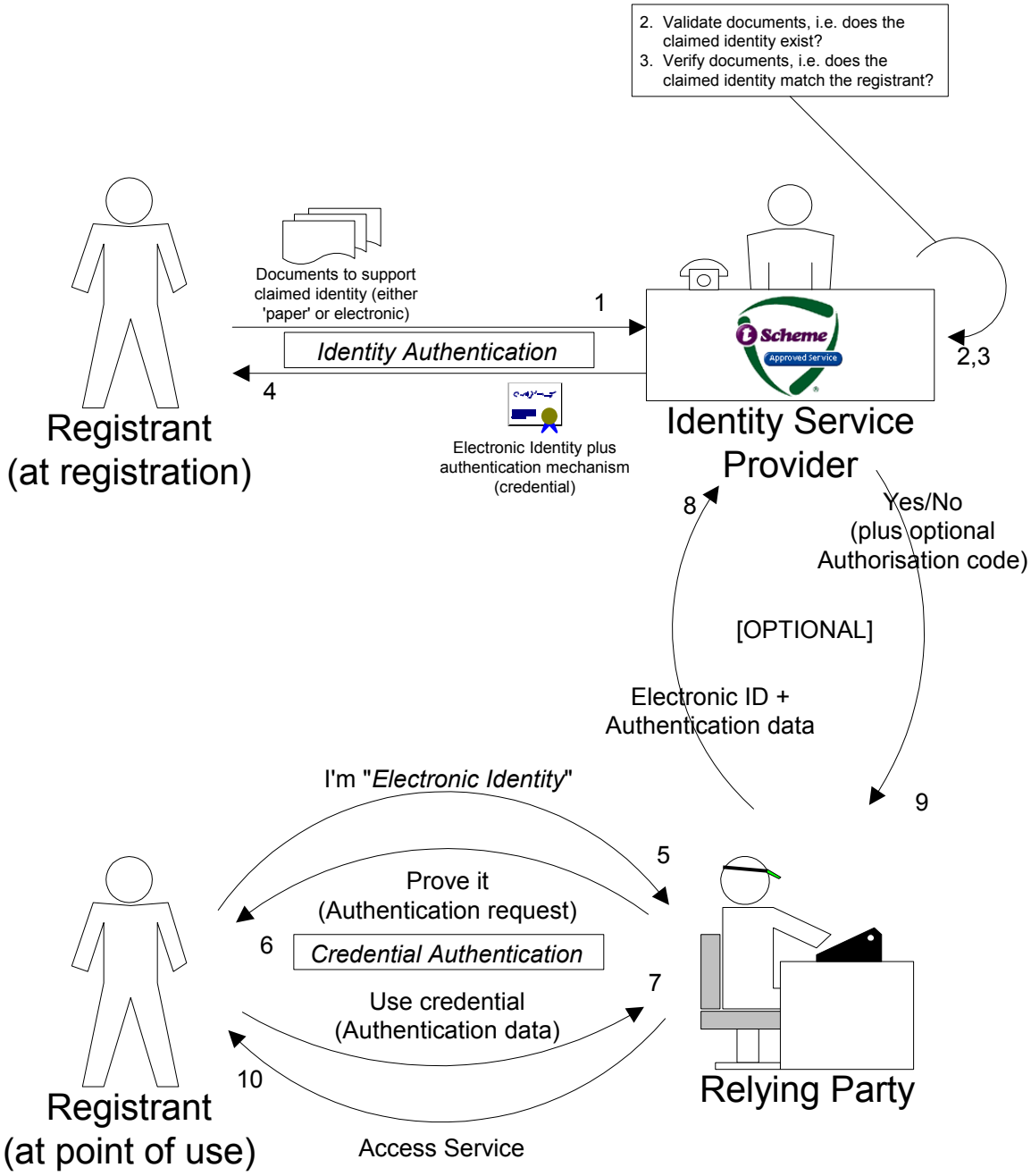
630	Verify	Demonstrate that the **registrant** is who they claim to be (i.e. that the person purporting to hold these attributes is not impersonating the actual owner of the **real-world identity**).

© *tScheme* Limited, 2003 - 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 the **Identity Service 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 Service Provider** 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 Service Provider** 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.

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 (e.g. National Insurance Number) 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 Service Provider** could range widely and might involve an electronic or physical **credential**. Examples of such **credentials** could include:

1. a PIN and/or password (knowledge **credential**);
2. a public-key certificate (electronic **credential**);
3. a biometric token (physical **credential**);
4. an electronic token (virtual **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**.

Referring to the earlier process-flow diagram, in the case where a virtual (one-off use) **credential** is issued the steps 1 & 4 would not take place, as the interaction would be between the individual, the relying party and the Identity Service Provider i.e. steps 5,6,7,8,2,3,9,10. Step 7 would allow the individual to supply paper documents and / or the key to access electronic data (e.g. name & address and their consent).

Finally, the **Identity Service Provider** 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.

This **Profile** is intended both for large organisations that 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 for **Identity Service 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 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, 2003 - 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". 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 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 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 e.g. credential renewal;

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

© *tScheme* Limited, 2003 - 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**

- whether **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 Service Provider** 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, 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, it will be especially applicable in the case of an **Identity Service Provider**, and the commitment to compliance already identified in the Base Approval Profile will correspondingly be given special emphasis.

3.4 Registrant agreement[1]

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

The **Identity 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 Service Provider** shall oblige, through agreement, the **registrant** or **registrant**'s **proxy** to notify the **Identity 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, 2003 - all rights reserved

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

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

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

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

RA-060 Agreement on notification to RPs

The **Identity 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 Party agreement

RPA-010 Explanation of means of authenticating credential

The **Identity Service Provider** shall provide a plain language explanation of what a relying party needs to do in order to authenticate a credential, including requirements for securing the authentication process to minimise the risk of compromising the credential.

RPA-020 Information passed to RP

The **Identity Service Provider** must agree with the relying party if there is any personal information that needs to be passed from the **Identity Service Provider** to the relying party on initial registration or on subsequent change or during the process of **credential authentication**.

RPA-030 Record of notification of information to RP

The **Identity Service Provider** shall record any information passed to relying parties at initial registration or on subsequent change or during **credential authentication**.

RPA-040 Use of Information passed to RP

The **Identity Service Provider** must agree with the relying party the contractual and regulatory conditions of use of any personal information passed to the relying party.

© *tScheme* Limited, 2003 - all rights reserved

3.6 Credential Lifecycle

DC-005 Creation of **electronic identity** and **credential**

The **Identity Service Provider** shall record details of the **electronic identity** chosen by the **registrant** or created by the **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, similarly to ensure that they are not reused.

DC-010 Secure **credential** delivery

If relevant to the type of **credential**, any resultant **credentials** shall be delivered using an appropriately secure channel. If there is an access control mechanism associated with the **credential**, then this must also be delivered separately using an appropriately secure channel.

DC-020 Validity period of **credential**

If there is a validity period associated with the **credential**, then this must be made known to the **registrant** together with their responsibilities in this concern.

DC-030 Renewal of **credential**

The procedure involved in the renewal of a **credential** at the end of its validity period must be clearly defined and made known to the **registrant**.

DC-040 Issuance of new **credential** on information change

Where the **credential** contains **registration information** and subsequent to initial registration and **verification** but within the agreed lifetime of the **credential**, the **Identity Service Provider** is informed that any **registration information** that was previously contained in the **credential** has changed, then a new **credential** should be issued.

DC-050 Actions on compromise

If the **credential** has an associated access control method that is or is believed to be compromised or if the **credential** itself is or is believed to be compromised, then there must be a clearly defined procedure for dealing with the compromise. This must be made known to the **registrant** and, if appropriate, to relying parties together with their responsibilities in this concern.

DC-060 Termination of validity of **credential**

There must be a clearly defined procedure for dealing with the termination of validity of **credential** and destruction of **credential** (if relevant) and this must be made known to the **registrant** together with their responsibilities in this concern.

DC-070 Maintenance of status of **credential**

The **Identity Service Provider** must maintain the status of the **credential**.

DC-080 Record of lifecycle events

All major events in the lifecycle of the **credential** shall be recorded.

© *tScheme* Limited, 2003 - all rights reserved

3.7 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 Requirement, as appropriate for the registration level or category stated in the Public Service Description.

IP-030 Pre-existing **credentials**

For **credentials** previously established and now intended for use in connection with the **Identity Service**, the **Identity Service Provider** must show that the level of assurance achieved by the registration process at the time of issue, combined with the level of assurance gained through consistent use of the **credential** since that time, together constitute full equivalence to the relevant Recognised Verification Requirement. The **Identity Service Provider** must also show that all relevant **registration information** currently held is fully up to date. In the absence of such full equivalence being shown, additional forms of evidence of identity not previously submitted by the **registrant** must be used in re-establishing the **credential**.

3.8 Records

RECS-010 Maintenance of records

The **Identity 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 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 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**;

© *tScheme* Limited, 2003 - all rights reserved

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;

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;

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, 2003 - all rights reserved

4. REFERENCES

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

© *tScheme* Limited, 2003 - 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	
RPA-010	Explanation of means of authenticating credential	
RPA-020	Information passed to RP	

© *tScheme* Limited, 2003 - all rights reserved

Approval Profile for Identity Services - clause compliance list

Clause	Description	Compliance
RPA-030	Record of notification of information to RP	
RPA-040	Use of Information passed to RP	
DC-005	Creation of **electronic identity** and **credential**	
DC-010	Secure **credential** delivery	
DC-020	Validity period of **credential**	
DC-030	Renewal of **credential**	
DC-040	Issuance of new **credential** on information change	
DC-050	Actions on compromise	
DC-060	Termination of validity of **credential**	
DC-070	Maintenance of status of **credential**	
DC-080	Record of lifecycle events	
IP-010	All processes and expected situations documented	
IP-020	Registration procedures must comply with requirements of relevant RVR	
IP-030	Pre-existing **credentials**	
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**	

© *tScheme* Limited, 2003 - all rights reserved

Approval Profile for Identity Services - clause compliance list		
Clause	**Description**	**Compliance**
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, 2003 - all rights reserved