Issued

Approval Profile for an Identity Provider

Ref. tSd 0112

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 an Identity Provider (IdP) Service.

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
tSd	0.01	2008-06-25	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	2009-01-07	Changes to glossary to harmonise with changes to Credential Validation Service Profile. Update Scope to allow for outsourced Credential Management.	*tScheme* secretariat
tSd	0.04	2009-08-07	Incorporate the following changes: 1. All external tScheme document references now added to References section; 2. Remove Glossary section and merge into existing tScheme document 3. Embolden all terms that are in Glossary document; 4. Wording for steps 2 & 3 in flow-diagram in Scope section modified to be more generic.	*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 8

3.1 PUBLIC SERVICE DESCRIPTION 8
3.2 ASSESSOR'S SERVICE DEFINITION 9
3.3 SERVICE POLICY 9
3.4 SERVICE PRACTICE STATEMENT 11
3.5 INTERNAL PROCEDURES 11
3.5.1 Authority and responsibility 11
3.5.2 Credential renewal and update 11
3.5.3 Credential issuance 11
3.5.4 Pre-existing Credentials 12
3.6 RECORDS 12

4. REFERENCES 14

ANNEX 1. CLAUSE COMPLIANCE LIST 15

© *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** addressed by this **Profile** and the other related **Profiles** listed in §2 - Scope and relation to other Profiles.

This **Approval Profile** is one of a number developed by *tScheme* against which **TSP**s offering **Trust Services** may be audited by ***tScheme*-recognised Assessors**. It addresses the provision of an Identity Provider 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] and the other **Approval Profiles** listed in §2 - Scope and relation to other Profiles (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 the overall provision and life-cycle management of an Identity **Credential** (other than a PKI certificate, which is covered in the Approval Profile for a Certification Authority). Life-cycle management provides for the registration and verification of the particular identity attributes of the subject; initial creation and personalisation of **credentials** and/or **tokens** (as appropriate); the secure distribution of **credentials**/**tokens**, the maintenance of **credential** status; the potential for adding additional, verified attributes and the provision of suspension/revocation processes.

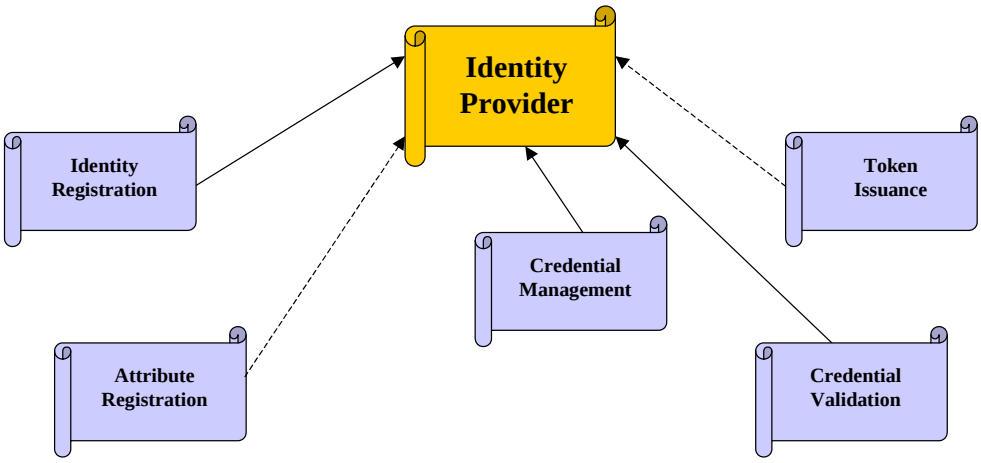
Some of these functions could be offered as stand-alone **Services** so, to avoid repetition of the related criteria, they have been removed from this **Approval Profile** and placed in appropriate service-specific **Approval Profiles**. Nevertheless they are still part of the provision of an **Identity Provider Service**.

The **Services** that together make up the full **Identity Provider Service**, whether operated directly by the organisation offering the **Identity Provider Service** or whether outsourced to various other third parties, are required to fulfil the criteria defined in the following further **Approval Profiles** (when used as hyper-links, these will take you to the latest released version, although it is necessary to fix on a specific release for the purposes of scoping the **S3A**):

Identity Registration
{Attribute Registration}
Credential Validation
Credential Management
{Token Issuance}

Some of these **Services** are regarded as being mandatory parts of an **Identity Provider Service**. Unless they are referred to within 'curly' brackets, { …thus… }, any such **Services**, and the implied requirements of any text are mandatory - only optional **Services** are enclosed within 'curly' brackets, and the **TSP** must make clear whether or not they are intending to be assessed against them.

The relationships between these **Profiles** is shown in the following diagram. Mandatory **Approval Profiles** are shown with a solid connection to the **Identity Provider Approval Profile**, those that are optional are shown with a dashed connecting line.

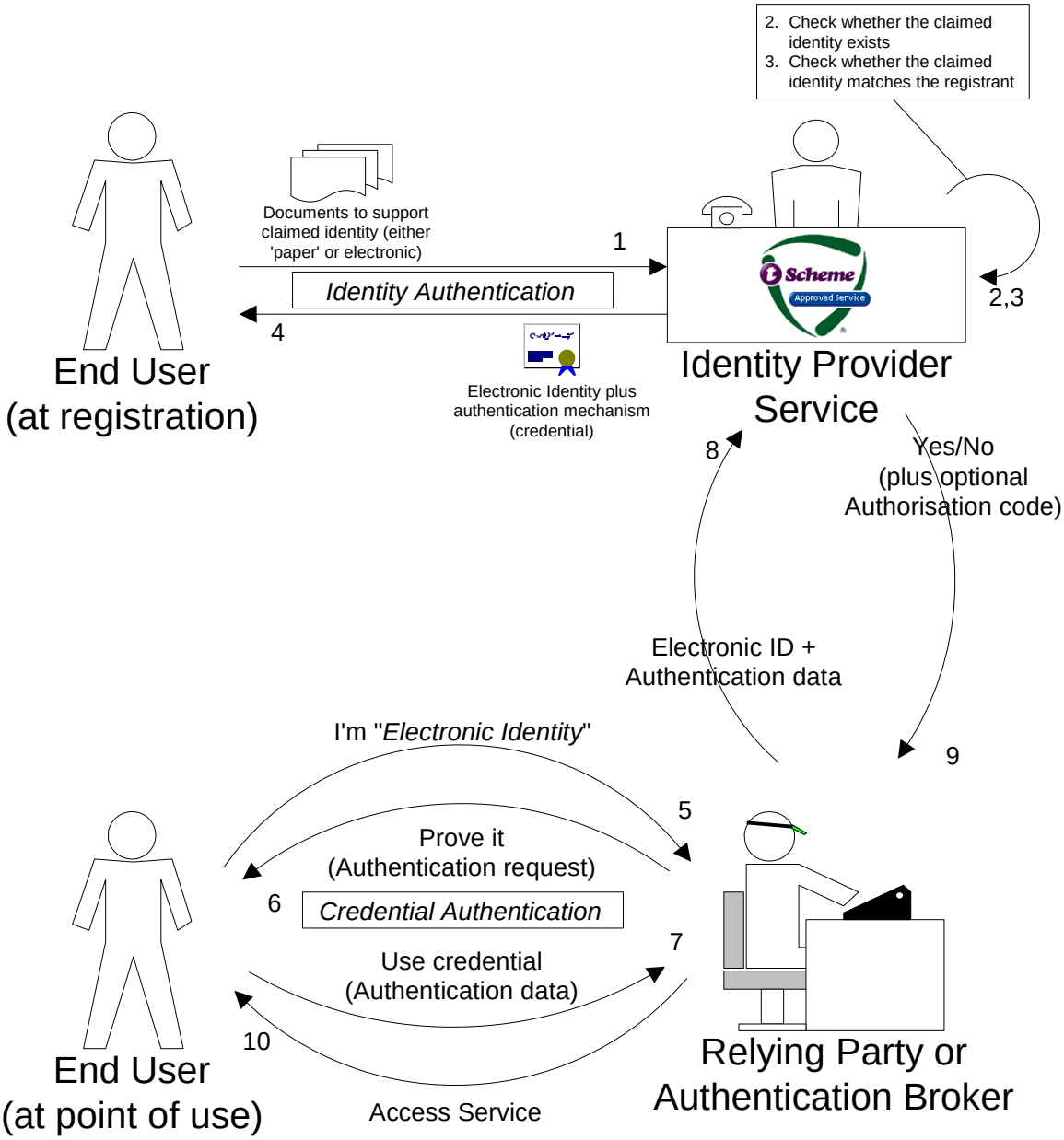


© *tScheme* Limited, 2009 - all rights reserved

The **TSP** acting as the **Identity Provider** has responsibility for ensuring conformance with the procedures prescribed in the applicable **Service Policy** even when constituent part-**Services** are outsourced to third parties. This requires the inclusion in its **Service Policy Disclosure Statement** of relevant practices undertaken by all parties contributing to the overall **Service** provision.

The **TSP** acting as the **Identity Provider** may demonstrate directly the conformance to the appropriate **Approval Profiles** of the constituent **Services** or they may refer to prior ***tScheme*** **Approvals** awarded to those **Services**, where they remain current.

An overview of the scope of the overall **Identity Provider Service** is illustrated here (note, more detailed interactions are shown in the related constituent service **Approval Profiles**):



Note, throughout this document references are made to **credentials** and **tokens**. Whereas a **credential**

might be usable purely as electronic data e.g. a username with associated PIN as its authentication mechanism or a user-id with an associated cryptographic key and a shared secret as its authentication mechanism, for technical reasons or to provide additional security, the **credential** and/or its related authentication mechanism might need to be provided on a physical device – this device is then referred to as a **Token** e.g. a smartcard.

© *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].

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.

CR-020 Interrelationship of constituent parts

The **S3A** shall address how the constituent parts are interrelated.

CR-030 Apportionment of ownership, management and operational responsibility

The **S3A** shall apportion matters of ownership, management and operational responsibility for the constituent parts and how they are allocated to other departments of the business or outsourced to third parties. This information shall supplement and make more Service-specific the criteria required by the Base Approval Profile [Base].

NOTE:

Even where constituent **Services** are outsourced to third parties the **TSP** shall bear full liability for the overall **Service** offering. Under these circumstances it is under no obligation to make public how it outsources these functions, although it may choose to do so. Notwithstanding its decision regarding publication, it must make this information available to the **Assessor**.

3.1 Public Service Description

PSD-010 What the Service is

For each **SSA**, a **Public Service Description** shall be provided, which includes information on where to find the **SSA**'s **Service Policy** and **Service Policy Disclosure Statement**.

© *tScheme* Limited, 2009 - all rights reserved

3.2 Assessor's Service Definition

ASD-010 How the constituent parts are delivered

For each **SSA**, the **Assessor's Service Definition** shall specify how the **Service**'s constituent parts are delivered.

ASD-020 Mapping of **Service** elements to **Approval Profiles**

The **Assessor's Service Definition** shall include definitions of the constituent **Services** in a fashion that shows, by mapping the constituent **Services** to the different **Approval Profiles** as appropriate, how the criteria of other **Approval Profiles** will be satisfied.

3.3 Service Policy

SP-010 Statement of **Credential** usage

For each **SSA**, the **TSP** shall provide a **Service Policy** that states clearly the purpose, conditions and limitations under which **credentials** (and related **tokens**, if applicable) issued through its **Service** may be used. Particular emphasis will be given to the topics identified in the following list:

SP-020 Identity Registration policy requirements

- Identity Registration policy - the TSP shall state clearly its policy requirements for authentication of the subject's identity, in terms of attributes being verified, evidence required and forms of presentation. The specific **documentation** for **identity authentication** and applicable **Recognised Verification Requirements** shall be stated. Where the **Service** offers more than one **Identity Authentication** policy type, the verification requirements shall be related to the specific identity policies, where they differ.

SP-030 Attribute Registration policy requirements

- Attribute Registration policy (if applicable) - the TSP shall state clearly its policy requirements for authentication of any additional attributes to be linked to the subject, in terms of attributes being verified, evidence required and forms of presentation. The specific **documentation** for attribute registration shall be stated. Where the **Service** offers more than one attribute registration policy type, the verification requirements shall be related to the specific attribute registration policies, where they differ.

SP-040 Consent to publication

- The above registration processes shall make clear whether, and under what conditions (e.g. mandatory or optional), the subject requires and consents to the publication of the status of his/her credential.

SP-050 Definition and availability of subject obligations

- Subject Obligations - the TSP shall set out in terms readily understandable and accessible to the user community the obligations with which subjects must comply if they are issued with a credential under the identified policy and wish to use the credential within the terms of its provision. Such terms shall:
    a) oblige the Subject to submit accurate and complete information as required by the applicable Registration Policy, and
    b) provide clear instructions as to how the Subject should exercise reasonable care to avoid unauthorised use of its credential;

© *tScheme* Limited, 2009 - all rights reserved

c) require the Subject to notify the **Identity Provider,** without any unreasonable delay, if any of the following occur up to the end of the validity period connected with the credential:

- loss, theft or potential compromise of the Subject's **credential**;
- risk of loss of control over the Subject's **credential** and /or **token** due to compromise of activation data (e.g. PIN code) or other reasons; and/or
- any inaccuracies in or changes required to the **credential** or **token** content.

SP-060 Record of subject obligations

➢ The TSP shall record the Subject's agreement to all their defined obligations.

SP-070 Explanation of relying party's expectations

➢ Relying Party Agreement - the TSP shall provide a plain language explanation of what a relying party can expect, if they are presented with a **credential** issued under this policy. This shall include information on how to validate **credentials** issued under the applicable Service Policy, including requirements to check the revocation status of the **credential**, such that the relying party may "reasonably rely" on the **credential**;

SP-080 Notification of revocation of credentials

➢ Revocation notification – in addition to the TSP's obligations to provide revocation status information to Relying Parties, it shall also ensure that Subjects whose **credentials** are subject to revocation or suspension are notified of the change of status of their **credential**, according to the requirements of the Service Policy.

SP-090 Access to the TSP

➢ Accessibility - the TSP shall publish the ways in which Subjects and Relying Parties can contact it in the event of dispute or for general support. It shall describe the level of support provided at these contact points and the response times offered. It shall offer evidence that its Service can achieve these levels in practice.

© *tScheme* Limited, 2009 - all rights reserved

3.4 Service Practice Statement

SPS-010 Provision of an SPS

As identified in the Base Approval Profile [Base], the TSP shall provide a sufficient description of the practices it employs in delivering the Service and in enforcing the Service Policy according to which the Service is offered, the general term for this is a Service Practice Statement. This shall satisfy the requirements expressed in the Base Approval Profile [Base].

SPS-020 Provision of an SPDS

There is no requirement to make full public disclosure of its practices since this may be to the detriment of the overall security of the Service. However, a Service Policy Disclosure Statement giving an overview of the Service provision and how the provisions of the Service Policy are implemented shall be provided if the SPS is not published in full.

SPS-030 Consistency of the SPS

The SPS shall be consistent with the Assessor's Service Definition and the Public Service Description.

SPS-040 Maintenance of the SPS

The TSP shall define the processes and responsibilities they use to review and maintain the applicable SPS and shall give due notice of changes it intends to make to the SPS and/or the SPDS, which shall be promptly published once formally approved.

3.5 Internal procedures

3.5.1 Authority and responsibility

IPAR-010 Management authority and responsibility

The TSP shall have a high-level management body with final authority and responsibility for approving the Service Policy, Service Practice Statement and the Service Policy Disclosure Statement (if applicable) - including oversight of their proper implementation.

3.5.2 Credential renewal and update

IPSC-010 Management of subject credentials

The TSP shall have in place practices that ensure that requests for a credential to be issued to a previously registered subject are complete, accurate and duly authorised and that information used to verify the identity and attributes of the subject remains valid. This includes credential renewals following revocation or prior to expiration, or update due to change to the subject's attributes.

3.5.3 Credential issuance

IPCI-010 Security of **credential** issuance

The **Identity Provider** shall ensure that new and renewed **credentials** are issued securely, in particular ensuring that:

IPCI-020 **Credential** issuance procedures

- the procedure for issuing the **credential** is securely linked to the associated Identity Registration or **credential** renewal;

IPCI-030 Reassignment of **electronic identity**

- the TSP shall ensure that, over the lifetime of the **Identity Provider Service**, any specific identifier or **electronic identity** that has been used in an issued **credential** shall never be reassigned to another subject;

IPCI-040 Protection of registration data

- the confidentiality and integrity of registration data (both identity registration and attribute registration, if applicable) shall be protected especially when exchanged with the subject or between distributed Service Components;

IPCI-050 Authentication of registrars

- the TSP shall verify that registration information is only exchanged with approved Registration Service Providers, whose identity is clearly established, in the event that the Registration function is outsourced.

3.5.4 Pre-existing Credentials

IPPC-010 Pre-existing **credentials**

For **credentials** previously established and now intended for use in connection with the **Identity Provider Service**, the **Identity 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 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**. The **registrant** must also be able to demonstrate a current and continuing entitlement to use the **credential**.

3.6 Records

RECS-010 Capture and retention of records

The TSP shall capture and retain records of all actions undertaken, and the time at which they occurred. It shall also state the period for which such records are to be retained, with a clear justification for the basis of determining the stated period.

The records captured shall include:

RECS-020 Constituent Services

- adequate records kept in accordance with the requirements of the **Approval Profiles** applicable to any constituent Services, covering inter alia:

© *tScheme* Limited, 2009 - all rights reserved

- the evidence offered to the Identity Registration function and on which was based a decision to either reject a request for a credential or to accept the request and issue the credential. This information shall identify the point of Registration;
- {the evidence offered to the Attribute Registration function and on which was based a decision to either accept or reject a request for a additional attributes to be associated with a credential. This information shall identify the point of Registration;}
- dissemination of the authentication data for a subject's **credential**;
- any revocation or suspension associated with the subject's **credential**;
- any changes in status that may affect the TSP's legitimate claim of conformance with this *tScheme* Approval Profile (or any on which a claim of conformance is based).

RECS-030 Internal audit records

The TSP shall have in place documented internal audit procedures. Records shall be maintained and evidence of their application provided.

RECS-040 Access to records

These records shall be protected against unauthorised access and be made available for audit and dispute resolution purposes within a reasonable period following a properly justified and authorised request.

© *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 an Identity Provider - clause compliance list		
Clause	**Description**	**Compliance**
CR-010	Operational Service	
CR-020	Interrelationship of constituent parts	
CR-030	Apportionment of ownership, management and operational responsibility	
PSD-010	What the Service is	
ASD-010	How the constituent parts are delivered	
ASD-020	Mapping of **Service** elements to **Approval Profiles**	
SP-010	Statement of **Credential** usage	
SP-020	Identity Registration policy requirements	
SP-030	Attribute Registration policy requirements	
SP-040	Consent to publication	
SP-050	Definition and availability of subject obligations	
SP-060	Record of subject obligations	
SP-070	Explanation of relying party's expectations	
SP-080	Notification of revocation of credentials	
SP-090	Access to the TSP	
SPS-010	Provision of an SPS	
SPS-020	Provision of an SPDS	
SPS-030	Consistency of the SPS	
SPS-040	Maintenance of the SPS	
IPAR-010	Management authority and responsibility	
IPSC-010	Management of subject credentials	
IPCI-010	Security of **credential** issuance	

© *tScheme* Limited, 2009 - all rights reserved

Approval Profile for an Identity Provider - clause compliance list		
Clause	**Description**	**Compliance**
IPCI-020	**Credential** issuance procedures	
IPCI-030	Reassignment of **electronic identity**	
IPCI-040	Protection of registration data	
IPCI-050	Authentication of registrars	
IPPC-010	Pre-existing **credentials**	
RECS-010	Capture and retention of records	
RECS-020	Constituent Services	
RECS-030	Internal audit records	
RECS-040	Access to records	

© *tScheme* Limited, 2009 - all rights reserved