Issued

Approval Profile for Credential Validation Services

Ref. tSd 0109

1.04

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 validation 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	2008-06-10	First version, tracked under Document Management procedures.	*tScheme* Board
tSd	1.01	2008-07-25	Remove redundant entry 'PROX-010' from Annex 1 – the clause compliance list.	*tScheme* Secretariat
tSd	1.02	2009-01-07	Changes as a result of discussions with EAS project	*tScheme* Secretariat
tSd	1.03	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 first diagram in Scope section modified to be more generic; 4. Expand acronym in footnote in second diagram in Scope section; 5. Remove duplicate text at the end of SI-170; 6. Reword DP-010 on Data Protection compliance; 7. Remove clause at the end of RPA-010; 8. Modify RPA-030 to allow for situation when cryptographic keys are not exchanged; 9. Clarify that DC-050 covers all circumstances in which a credential's validity is terminated.	*tScheme* Secretariat
tSd	1.04	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 SERVICE INFORMATION 8
3.1.1 Information for users 8
3.1.2 Information for Assessors 9
3.2 DATA PROTECTION 9
3.3 AUTHENTICATION BROKER AGREEMENT 9
3.4 RELYING PARTY AGREEMENT 10
3.5 CREDENTIAL LIFECYCLE 11
3.6 INTERNAL PROCEDURES 11
3.7 RECORDS 12

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 a **Credential Validation 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:

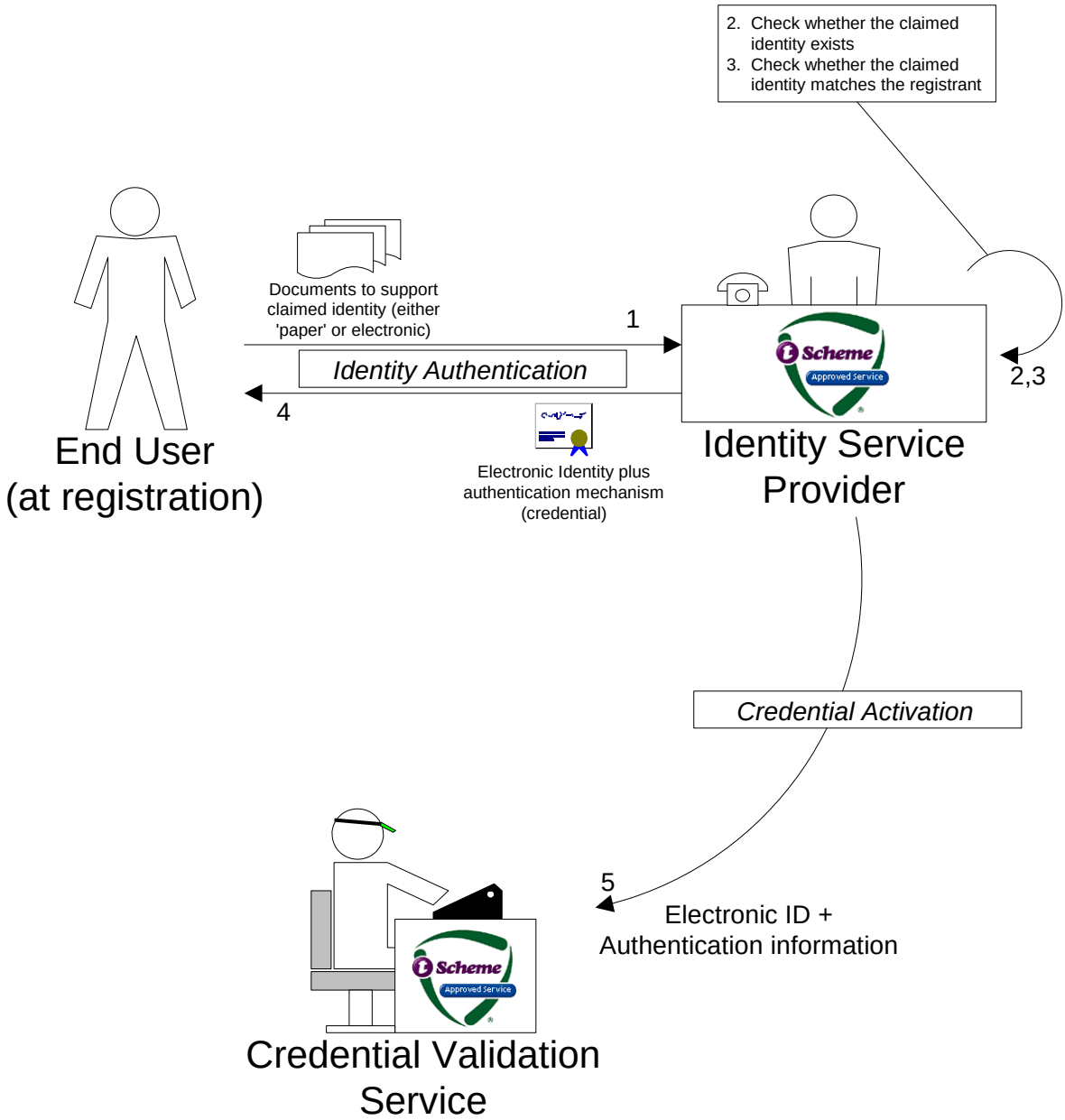
- references to "**Service Provider** or **TSP**" shall be taken to mean "**Component supplier**";
- references to "**Service**" shall be taken to mean "**Service Component**";
- references to "**Service Subject to Assessment**", or **SSA**, shall be taken to mean "**Service Component Subject to Assessment**", 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 to register with an **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.

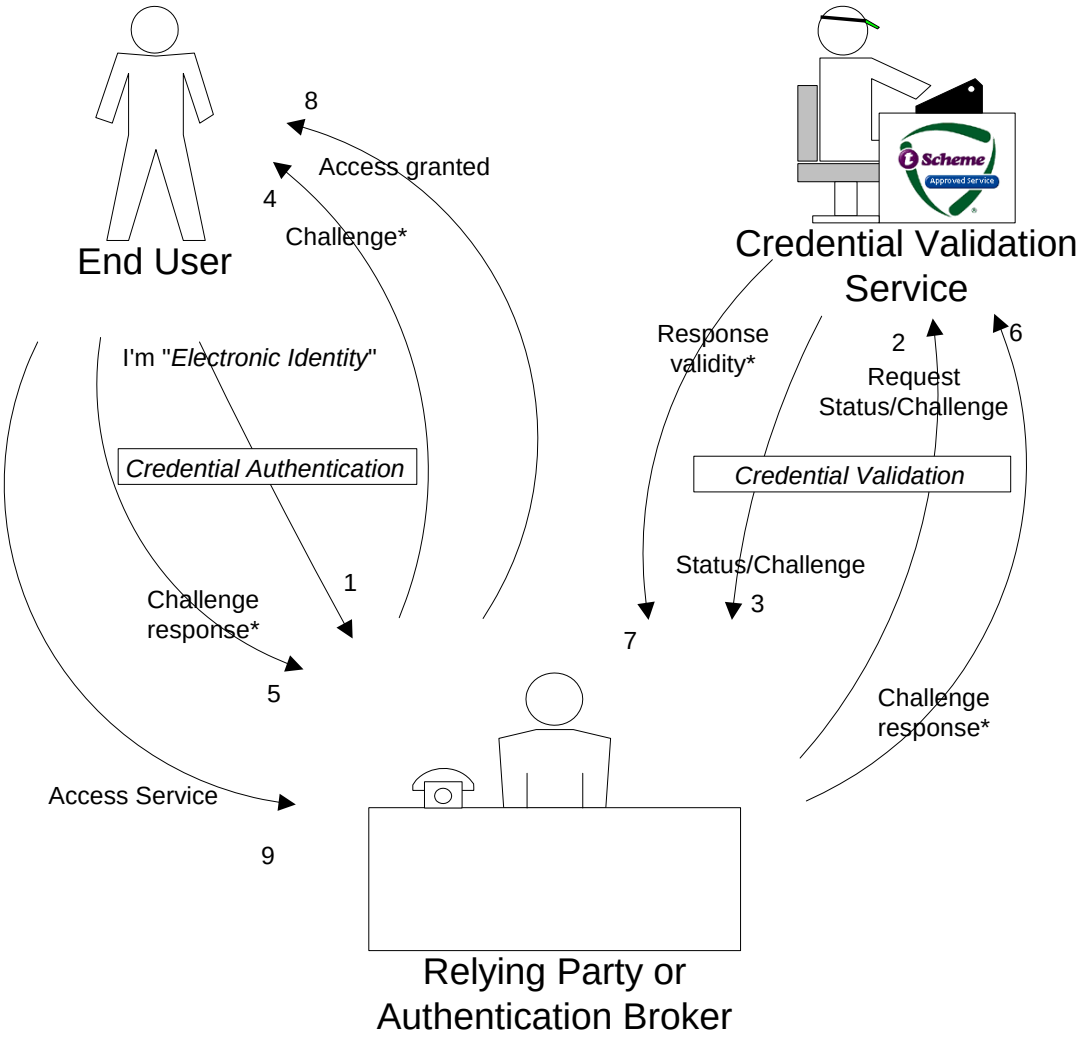
An overview of the processes involved can be seen in the following diagram:



As can be seen, the **Identity Service Provider** links an **electronic identity** with a **real-world identity**.

The **End User** 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**, issue them with a **credential** and then (if appropriate) pass **authentication information** to support **credential validation** to a **Credential Validation Service Provider**. No specific constraint of scope is intended in this **Profile** on how these processes could be carried out.

Then, when the **End User** wants to gain access to a service, they will use their **credential** and an overview of the processes involved can be seen in the following diagram:



* Steps 4, 5, 6 & 7 are optional if the Credential Validation Service just provides a status and does not require a challenge/response mechanism

For some simple **credentials**, such as those based on PIN & password, all that the **credential validation service** does is to confirm that the **credential** is valid and has not been suspended or revoked; for more sophisticated **credentials**, such as Chip & PIN smartcards, the **credential validation service** can support a Challenge/Response function to provide additional assurance that the **credential** is being used by an **End User** that knows how to access the **credential**. However, assurance that it is

© *tScheme* Limited, 2009 - all rights reserved

the correct **End user** depends on the strength of the registration process and on the security applied to prevent improper access to the **credential**. These factors are out of scope for the **credential validation 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].

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 **relying party** should use the **Service**;

SI-020 Service immediacy, ubiquity and availability
- the immediacy, ubiquity and availability of the Service;

SI-030 Status values supported
- the status values supported (valid, revoked or suspended, revocation reasons, revocation scope and so on);

SI-040 Authorisation and authentication of requests
- who is authorised to access a credential's status and how are they authenticated;

SI-050 Activation process
- the methods used to carry out credential activation, including the messages that are exchanged;

SI-060 Revocation process
- the methods used to carry out credential revocation, including the messages that are exchanged;

SI-070 Validation process and verification validity assurance method
- the methods used to complete the validation process, including the messages that are exchanged;

SI-080 Liability accepted
- any liability accepted by the **Credential Validation Service Provider** in relation to the **credential validation** process;

SI-090 Disclosure/privacy policy
- under what circumstances information will be disclosed to third parties;

© *tScheme* Limited, 2009 - all rights reserved

SI-100 Minimum record retention policy
- minimum retention policy for records;

SI-110 Information sensitivity
- the maximum **Impact Level** associated with the information processed as part of the service;

SI-120 Incident reporting and management
- the processes used by the **Credential Validation Service Provider** to declare and manage an incident which may affect the security of the service;

SI-130 Secure channel
- the processes and mechanisms used by the **Credential Validation Service Provider** to provide a secure channel for exchanges of information;

SI-140 Validity of pre-Approval credentials
- whether **credentials** established prior to initial *tScheme* **Approval** will still be valid.

3.1.2 Information for Assessors

The following information shall appear either in the Service's Service Practice Statement or in the Assessor's Service Definition (*tScheme* does not require it to be made generally available).

SI-150 Assured integrity
- how the integrity of the status information is assured;

SI-160 Assured confidentiality
- how the confidentiality of the request and response is assured;

SI-170 Records retained and period
- the records that will be retained and their retention period;

SI-180 Service availability
- the availability levels associated with the Service.

3.2 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.

3.3 Authentication Broker agreement

This section is only applicable in architectures where relying parties (typically more than one) are making use of an **Authentication Broker** as a means of mediating requests from **End Users** (again, typically, where they have **credentials** provided by a variety of **Identity Providers**).

© *tScheme* Limited, 2009 - all rights reserved

ABA-010 Plain language agreement

The **Credential Validation Service Provider** shall provide a plain language explanation of what an **Authentication Broker** can understand by the validation response and any contractual implications of requesting credential validation.

ABA-020 Information passed

The **Credential Validation Service Provider** must agree with the **Authentication Broker** operator on the information that needs to be passed to the **Credential Validation Service Provider** by the relying party or by the **Identity Provider Service**, as appropriate, on initial registration of the **End User** and on subsequent change (**authentication information**) and by the **Authentication Broker** during the process of **credential authentication** (**authentication data**).

ABA-030 Record of notification of Authentication Information

The **Credential Validation Service Provider** shall record any **authentication information** passed at initial registration of the **End User,** on subsequent change and during credential authentication.

ABA-040 Record of Authentication Information changes

If, subsequent to initial provisioning, the **Credential Validation Service Provider** is informed that any **authentication information** has changed, the **Credential Validation Service Provider** shall record this changed information.

ABA-050 Record of notification of Authentication Data

The **Credential Validation Service Provider** shall record any **authentication data** passed during **credential authentication**.

3.4 Relying Party agreement

RPA-010 Explanation of means of authenticating credential

The **Credential Validation Service Provider** shall provide a plain language explanation of what a relying party needs to do in order to perform **credential authentication**.

RPA-020 Use of Information passed to RP

The **Credential Validation Service Provider** must agree with the relying party the contractual and regulatory conditions of use of any information passed by the relying party.

RPA-030 Key management

The **Credential Validation Service Provider** shall, if relevant, provide a secure means of key management for exchanges of cryptographic keys with relying parties.

© *tScheme* Limited, 2009 - all rights reserved

3.5 Credential Lifecycle

DC-010 Storage of electronic identity and credential

The **Credential Validation Service Provider** shall record appropriate details of the **electronic identities** and related **credentials** provided by the **Identity Service Provider** or the **Authentication Broker**, as appropriate. Details shall be stored in a manner that minimises risk of compromise, e.g. by using a one-way hash function.

DC-020 Secure credential receipt

The **Credential Validation Service Provider** shall provide a mechanism for acceptance of **electronic identities** and **credentials** using an appropriately secure channel.

DC-030 Change in status of credential

The **Credential Validation Service Provider** shall provide a mechanism for changes in status of **electronic identities** and **credentials** using an appropriately secure channel.

DC-040 Actions on compromise

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 appropriate parties, according to their contractual arrangements, together with their responsibilities in this concern.

DC-050 Termination of validity of credential

There must be a clearly defined procedure for dealing with the termination of validity of a **credential** for whatever reason, including revocation, expiry, etc.

DC-060 Record of lifecycle events

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

3.6 Internal procedures

IP-010 All processes and expected situations documented

The **credential validation** process shall be fully documented and cover all expected situations, for example how failed validations are managed and recorded.

IP-020 Validation procedures must comply with requirements of the service

The **credential validation** process must comply with the requirements necessary to support the validation process and verification validity assurance method as stated in the Public Service Description.

© *tScheme* Limited, 2009 - all rights reserved

3.7 Records

RECS-010 Maintenance of records

The **Credential Validation Service Provider** shall maintain timed and dated records of each **credential validation** and when any changes to the **authentication information** are processed.

RECS-020 Security of records

The **Credential Validation Service Provider** shall secure from loss, destruction, unauthorised release or amendment and falsification all records of **credential validation**.

© *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 Credential Validation Services - clause compliance list		
Clause	**Description**	**Compliance**
CR-010	Operational Service	
SI-010	Reason for use of Service	
SI-020	Service immediacy, ubiquity and availability	
SI-030	Status values supported	
SI-040	Authorisation and authentication of requests	
SI-050	Activation process	
SI-060	Revocation process	
SI-070	Validation process and verification validity assurance method	
SI-080	Liability accepted	
SI-090	Disclosure/privacy policy	
SI-100	Minimum record retention policy	
SI-110	Information sensitivity	
SI-120	Incident reporting and management	
SI-130	Secure channel	
SI-140	Validity of pre-Approval credentials	
SI-150	Assured integrity	
SI-160	Assured confidentiality	
SI-170	Records retained and period	
SI-180	Service availability	
DP-010	Emphasis on Data Protection compliance	
ABA-010	Plain language agreement	
ABA-020	Information passed	
ABA-030	Record of notification of Authentication Information	

© *tScheme* Limited, 2009 - all rights reserved

Approval Profile for Credential Validation Services - clause compliance list

Clause	Description	Compliance
ABA-040	Record of Authentication Information changes	
ABA-050	Record of notification of Authentication Data	
RPA-010	Explanation of means of authenticating credential	
RPA-020	Use of Information passed to RP	
RPA-030	Key management	
DC-010	Storage of electronic identity and credential	
DC-020	Secure credential receipt	
DC-030	Change in status of credential	
DC-040	Actions on compromise	
DC-050	Termination of validity of credential	
DC-060	Record of lifecycle events	
IP-010	All processes and expected situations documented	
IP-020	Validation procedures must comply with requirements of the service	
RECS-010	Maintenance of records	
RECS-020	Security of records	

© *tScheme* Limited, 2009 - all rights reserved