Issued

Approval Profile for Credential Management Services

Ref. tSd 0113

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 management of the lifecycle of credentials used 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	0.01	2008-12-24	First draft for comment	*tScheme* Secretariat
tSd	0.02	2009-01-07	Amend all references to Credential Validation Service to be Credential Management Service.	*tScheme* Secretariat
tSd	0.03	2009-02-06	Add new criterion CL-060 to cover suspension and reactivation of credential. Adjust numbering of subsequent criteria in section	*tScheme* Secretariat
tSd	0.04	2009-03-11	Remove SI-070 that was incorrectly left in from CVS Profile and, similarly, update header of clause compliance table.	*tScheme* Secretariat
tSd	0.05	2009-08-07	Incorporate the following changes: 1. All external *tScheme* document references now added to References section; 2. Embolden all terms that are in Glossary document; 3. Clarify first paragraph of Scope section to cover all changes in a credential's status not just on revocation; 4. Wording for steps 2 & 3 in diagram in Scope section modified to be more generic; 5. Correct RTA-010 to refer to credential status not registration.	*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 6

3.1 SERVICE INFORMATION 6
3.1.1 Information for users 6
3.1.2 Information for Assessors 7
3.2 RELYING TSP AGREEMENT 7
3.3 CREDENTIAL LIFECYCLE 7
3.4 ATTRIBUTE LIFECYCLE 8
3.5 INTERNAL PROCEDURES 9
3.6 RECORDS 10

4. REFERENCES 11

ANNEX 1. CLAUSE COMPLIANCE LIST 12

© *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 Management 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 the provision of **Services** that manage the lifecycle of issued **credentials**. Such **Services** cover:

1. the receipt of requests to revoke, suspend or otherwise change a **credential**'s status;
2. the authentication and authorisation of such requests;
3. the determination of a decision to change a **credential**'s status and associated actions;
4. notification of status change to **credential** owners.

In the overall design of an **Identity Provider Service** there is likely to be some flexibility as to where the lifecycle management of **credentials** and, if applicable, additional attributes is performed. It will either be part of the **Identity Provider Service** itself or it will be performed by the appropriate registration service. It could also be a mixture of both with some registration service providers managing the lifecycle of credentials/attributes of their **registrants** with the remaining **registrants** managed by the overall **Identity Provider Service**.

It is thus up to the **Identity Provider Service** to demonstrate that, as part of its overall **Assessment,** the relevant criteria in this **Profile** are satisfied for all their issued **credentials** and, if applicable, all associated additional attributes.

© *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-080 Liability accepted
- any liability accepted by the Credential Management Service Provider in relation to the credential management process;

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

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

© *tScheme* Limited, 2009 - all rights reserved

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 Management 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 Management 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; the availability levels associated with the Service;

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

3.2 Relying TSP agreement

RTA-010 Explanation to relying TSP of meaning of results

The Credential Management Service Provider shall provide a plain language explanation of what a relying **TSP** can understand by the status of a credential.

3.3 Credential Lifecycle

CL-010 Creation of **electronic identity** and **credential**

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

© *tScheme* Limited, 2009 - all rights reserved

CL-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.

CL-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**.

CL-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.

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

CL-060 Suspension and reactivation of **credential**

There must be a clearly defined procedure for dealing with the suspension and reactivation of the validity of **credential,** if this is relevant, and this must be made known to the **registrant** together with their responsibilities in this concern.

CL-070 Termination of validity of **credential**

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

CL-080 www.aaa.com - _Hlk217464794Maintenance of status of **credential**

The Credential Management Service Provider must maintain the status of the **credential**.

CL-090 Record of **credential** lifecycle events

All deliveries and change of status events in the lifecycle of the **credential** shall be recorded.

3.4 Attribute Lifecycle

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

The Credential Management 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.

© *tScheme* Limited, 2009 - all rights reserved

AL-020 Validity period of additional attributes

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

AL-030 Renewal of additional attributes

The procedure involved in the renewal of additional attributes at the end of their validity period must be clearly defined and made known to the **registrant**.

AL-040 Issuance of new **credential** on attribute 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.

AL-050 *Not used*

[In order to maintain parity of clause numbering between credential lifecycle criteria and attribute lifecycle criteria, this item is not used.]

AL-060 Suspension and reactivation of additional attributes

There must be a clearly defined procedure for dealing with the suspension and reactivation of any additional attributes**,** and this must be made known to the **registrant** together with their responsibilities in this concern.

AL-070 Termination of validity of additional attributes

There must be a clearly defined procedure for dealing with the termination of validity of additional attributes, for whatever reason, and this must be made known to the **registrant** together with their responsibilities in this concern.

AL-080 www.aaa.com - _Hlk217464794Maintenance of status of additional attributes

The Credential Management Service Provider must maintain the status of any additional attributes.

AL-090 Record of attribute lifecycle events

All major events in the lifecycle of the additional attributes shall be recorded.

3.5 Internal procedures

IP-010 All processes and expected situations documented

The **credential** management process shall be fully documented and cover all expected situations.

© *tScheme* Limited, 2009 - all rights reserved

3.6 Records

RECS-010 Maintenance of records

The Credential Management Service Provider shall maintain timed and dated records of all significant management activity.

RECS-020 Security of records

The Credential Management Service Provider shall secure from loss, destruction, unauthorised release or amendment and falsification all records of **credential** and **attribute** lifecycle events.

© *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 Management 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-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	
RTA-010	Explanation to relying TSP of meaning of results	
CL-010	Creation of **electronic identity** and **credential**	
CL-020	Validity period of **credential**	
CL-030	Renewal of **credential**	
CL-040	Issuance of new **credential** on information change	

© *tScheme* Limited, 2009 - all rights reserved

Approval Profile for Credential Management Services - clause compliance list

Clause	Description	Compliance
CL-050	Actions on compromise	
CL-060	Suspension and reactivation of **credential**	
CL-070	Termination of validity of **credential**	
CL-080	Maintenance of status of **credential**	
CL-090	Record of **credential** lifecycle events	
AL-010	Association of additional attributes to an **electronic identity**	
AL-020	Validity period of additional attributes	
AL-030	Renewal of additional attributes	
AL-040	Issuance of new **credential** on attribute information change	
AL-060	Suspension and reactivation of additional attributes	
AL-070	Termination of validity of additional attributes	
AL-080	Maintenance of status of additional attributes	
AL-090	Record of attribute lifecycle events	
IP-010	All processes and expected situations documented	
RECS-010	Maintenance of records	
RECS-020	Security of records	

© *tScheme* Limited, 2009 - all rights reserved