# Approval Profile for Verified Identity Services

**Ref. tSd 0108**

**Issue 1.00**

**2003-09-04**

## 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 and other relying parties for the verification 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 | 2004-09-04 | First version, tracked under Document Management procedures. | *tScheme* Board |

© *tScheme* Limited, 2003 - all rights reserved

# CONTENTS

**1. INTRODUCTION ..... 4**

1.1 CONVENTIONS ..... 4
1.2 GENERAL ..... 4

**2. SCOPE AND RELATION TO OTHER PROFILES ..... 6**

**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 PARTY AGREEMENT ..... 9
3.6 DELIVERY OF CREDENTIALS ..... 9
3.7 INTERNAL PROCEDURES ..... 9
3.8 RECORDS ..... 9

**4. REFERENCES ..... 11**

**ANNEX 1. CLAUSE COMPLIANCE LIST ..... 12**

© *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

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.

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 Verification 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.

Definitions of terms and acronyms not defined in this document may be found in the *tScheme* Glossary of Terms.

This document must be read in conjunction with "e-Government Strategy Framework Policy and Guidelines, Registration and Authentication v3.0" [RegAuth] and "HMG's Minimum Requirements for the Verification of the Identity of Individuals" [HMGVInd]. In the context of these documents, identity means a set of attributes that together uniquely identify a person. The minimum set of attributes acceptable to government for specifying the identity of an individual is:

a) Full name or names by which a person is or has been known (including all other names used);

b) Residential Address at which he/she can be located;

c) Date of birth.

The process covered by this Profile is called registration, and hence the person whose identity is being verified is referred to as the 'registrant'.

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";

© *tScheme* Limited, 2003 - all rights reserved 

- references to "Service Subject to Assessment", or SSA, shall be taken to mean "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 

# 2. SCOPE AND RELATION TO OTHER PROFILES

The criteria given in this Approval Profile are related to the provision of Services that verify[1] and authenticate the claimed registrant identity. No specific constraint of scope is intended in this Profile on how this can be verified. As a result of a successful verification and authentication, the registrant will be issued with a credential with which they can assert their identity to any relying parties. In principle, the types of credential provided by an Verified Identity Service could range widely. Examples of such credentials could include:

1. a PIN and password;
2. a public-key certificate;
3. a biometric token.

The verification process must, as a minimum, comply with the requirements laid down by the UK government for the verification of the identity of individuals [HMGVInd].

This profile is intended for large organisations that apply [HMGVInd] requirements to 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 then be used to access online services from, amongst others, the UK government.

The criteria given in this Approval Profile are in addition to those given in the Base 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.

1 "Verification" is the process of ensuring to some degree of certitude that the attributes claimed are valid, i.e. they exist (a verification step known as "validation") and are possessed by the individual or organisational registrant being represented. Not all attributes need to be expressly validated.

© *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 the authentication checks that are employed when verifying a user's credentials (see [RegAuth]) as well as the Registration Level from [HMGVInd] that is being applied.

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 Verification process and verification validity assurance method
- the methods used to complete the verification process and ensure that information used to verify the identity of the registrant is valid;

SI-040 Repeat verification methods
- the steps necessary to re-verify a registrant at repeat application e.g. credential renewal;

SI-050 Liability accepted
- any liability accepted by the TSP in relation to the verification process;

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

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

SI-080 Authentication checks
- authentication checks are carried out in accordance with [RegAuth].

SI-090 Registration Level
- Registration Level requirements to be applied from [HMGVInd].

© *tScheme* Limited, 2003 - all rights reserved 

### 3.1.2 Information for Assessors

No specific additional information identified

## 3.2 Proxies[2]

PROX-010 Proxy verification

If registration proxies are accepted, it is necessary for the TSP 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 that of the registrant proper.

## 3.3 Data Protection

DP-010 Emphasis on Data Protection compliance

In countries where Data Protection legislation has been passed, it will be especially applicable in the case of a TSP offering Verified Identity Services, and the commitment to compliance already identified in the Base Approval Profile will correspondingly be given special emphasis.

## 3.4 Registrant agreement

RA-010 Registrant obligation to be accurate and complete

The TSP 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 registration policy.

RA-020 Registrant obligation to notify information changes

The TSP shall oblige, through agreement, the registrant or registrant's proxy to notify the TSP whenever there are any changes to the registrant's registration information.

RA-030 Record of registration information changes

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP shall record this.

RA-040 Verification of registration information changes

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP shall verify the information.

RA-050 Agreement on registration information changes

If, subsequent to initial registration and verification, the TSP is informed that any registration information has changed, the TSP shall agree it with the registrant or the registrant's proxy (see Section 3.2 for a description of a proxy).

2 A proxy is an individual who registers on behalf of the registrant whose identity is being verified.

© *tScheme* Limited, 2003 - all rights reserved 

## 3.5 Relying Party agreement

RPA-010 Explanation to relying party of meaning of results

The TSP shall provide a plain language explanation of what a relying party can understand by the results of registration.

## 3.6 Delivery of credentials

DC-010 Secure credential delivery

The resulting credentials shall be delivered using an appropriately secure channel.

## 3.7 Internal procedures

IP-010 All processes and expected situations documented

The registration and verification 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 [HMGVInd]

The registration and verification process must, as a minimum, comply with the requirements laid down by the UK government for the verification of the identity of individuals [HMGVInd] as appropriate for the registration level stated in the Public Service Description.

## 3.8 Records

RECS-010 Maintenance of records

The TSP shall maintain timed and dated records of each registration and verification, both at initial registration and when any changes to the registrant's information are processed.

RECS-020 Security of records

The TSP shall secure from loss, destruction, unauthorised amendment and falsification all records of registration and verification.

RECS-030 Proof of consent regarding record retention

The TSP 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 information must retained and the period of retention are as specified in the current version of [HMGVInd].

Specifically it shall include:

© *tScheme* Limited, 2003 - all rights reserved 

RECS-050 Record of document reference numbers
- document reference numbers;

RECS-060 Record of document validity limitations
- any document validity limitations;

RECS-070 Record of type of document(s) presented
- type of document(s) presented;

RECS-080 Record of documentation identification
- record of unique identification data, numbers, or a combination thereof[3], of identification documents, if applicable;

RECS-090 Record where applications and document copies stored
- storage location of copies of applications and identification documents,

RECS-100 Record of proof of agreement
- proof of registrant's acceptance of registrant agreement[4];

RECS-110 Record of agreement choices made
- any specific choices in the registrant agreement;

RECS-120 Record of identity of who accepted the application
- identity of entity accepting the application;

RECS-130 Record of document validation method
- method used to validate identification documents, if any;

3 For example the registrant's driver's licence number

4 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

[RegAuth] e-Government Strategy Framework Policy and Guidelines, Registration and Authentication v3.0

© *tScheme* Limited, 2003 - all rights reserved

# ANNEX 1. CLAUSE COMPLIANCE LIST

**Approval Profile for Authenticated 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 | Verification process and verification validity assurance method | |
| SI-040 | Repeat verification methods | |
| SI-050 | Liability accepted | |
| SI-060 | Disclosure/privacy policy | |
| SI-070 | Minimum record retention policy | |
| SI-080 | Authentication checks | |
| SI-090 | Registration Level | |
| 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 | Record of registration information changes | |
| RA-040 | Verification of registration information changes | |
| RA-050 | Agreement on registration information changes | |
| RPA-010 | Explanation to relying party of meaning of results | |
| DC-010 | Secure credential delivery | |
| IP-010 | All processes and expected situations documented | |
| IP-020 | Registration procedures must comply with requirements of [HMGVInd] | |

© *tScheme* Limited, 2003 - all rights reserved

| **Approval Profile for Authenticated Identity 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-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 document(s) presented | |
| RECS-080 | Record of documentation identification | |
| RECS-090 | Record where applications and document copies stored | |
| RECS-100 | Record of proof of agreement | |
| RECS-110 | Record of agreement choices made | |
| RECS-120 | Record of identity of who accepted the application | |
| RECS-130 | Record of document validation method | |

© *tScheme* Limited, 2003 - all rights reserved