

Draft



## Model Specification of Service Subject to Assessment

Ref. tSd 0230

Draft 4.02

2009-04-22

### Executive summary

This document serves as a model for the production of a Specification of a Service Subject to Assessment (S3A) by any Trust Service Provider wishing to achieve *tScheme* Registered Applicant status and/or apply for *tScheme* Approval.

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](mailto: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	Approved
tSi	1.00	2001-10-25	First version, tracked under <i>tScheme</i> document management procedures.	<i>tScheme</i> Secretariat
tSi	2.00	2002-01-17	Approved version for Issue.	CEO
tSi	3.00	2002-02-25	Approved version for Issue, with correct Executive summary and minor typographic amendments.	CEO
tSd	4.00	2002-09-09	Revisions to accommodate concurrent revisions to the Glossary and the Required Assessment Procedures, and to elevate the document to 'definitive' status.  Principal other changes are: <ul style="list-style-type: none"><li>• removal of opportunity to have more than one service within the scope of an S3A;</li><li>• use of first capitals for Glossary terms;</li><li>• conformance with document becomes mandatory;</li><li>• separate section for the Assessor's Service Definition;</li><li>• align version, history and filename.</li></ul>	<i>tScheme</i> Board
tSd	4.01	2004-08-26	Add tSd0108 to tables in §4.1 and §4.3 and remove actual issue numbers.	<i>tScheme</i> Secretariat
tSd	4.02	2009-04-22	Add specific statement re services issuing Qualified Certificates. Clarify the contents of the table listing external standards and guidelines in §4.2	<i>tScheme</i> Secretariat

# CONTENTS

<b>1. INTRODUCTION .....</b>	<b>4</b>
1.1 PURPOSE .....	4
1.2 READERSHIP .....	4
1.3 OVERVIEW & PREPARATION .....	5
<b>2. PURPOSE &amp; READERSHIP .....</b>	<b>7</b>
<b>3. SERVICE DESCRIPTION .....</b>	<b>8</b>
3.1 SERVICE PROVIDER .....	8
3.2 PUBLIC SERVICE DESCRIPTION .....	9
3.3 SERVICE TOPOLOGY .....	10
3.4 SERVICE PLATFORM .....	10
3.5 ASSESSOR'S SERVICE DEFINITION .....	10
<b>4. APPROVAL PROFILES, RECOGNISED STANDARDS, GUIDELINES AND EVIDENCE .....</b>	<b>11</b>
4.1 APPLICABLE APPROVAL PROFILES .....	11
4.2 RECOGNISED STANDARDS AND GUIDELINES .....	12
4.3 SERVICE AND APPROVAL PROFILES MAPPING .....	12
4.4 EVIDENCE .....	13
4.5 DOCUMENT HIERARCHY .....	13
4.6 EVIDENCE AND APPROVAL PROFILE CRITERIA MAPPING .....	14
<b>5. ADDITIONAL INFORMATION .....</b>	<b>15</b>

## 1. INTRODUCTION

*Introductory note:*

*In this model Specification of a Service Subject to Assessment (hereafter simply the 'S3A') the sub-sections of the Introduction refer explicitly to this document.*

*In preparing their own specific instantiation of the model S3A, the applicant's own text to explain their reasons for preparing the document and seeking tScheme Registered Applicant status and/or Approval, as required, should be placed in the Introduction. They should also add any other introductory material they feel they require and the following tScheme text within this section should be deleted in its entirety.*

### 1.1 Purpose

This document serves as a model for the production of a Specification of a Service Subject to Assessment (S3A) by any Trust Service Provider wishing to achieve Registered Applicant status and/or apply for tScheme Approval.

This document is intended to be used by TSPs who are preparing an S3A, as the model for their own documents defining their own specific Services and the basis on which they intend having them assessed.

Conformance with this document is mandatory.

### 1.2 Readership

This document is required reading for the following parties, whose awareness of it is a requirement of the [Required Assessment Procedures](#):

- **Accreditation bodies** which have established with tScheme a agreement, in order to understand the specific tScheme requirements upon the tScheme-recognised Assessors which the Accreditation Body are responsible for accrediting;
- **tScheme-recognised Assessors** who will be performing the Assessment of an **Electronic Trust Service** and its **Provider**, as defined by an S3A;
- **TSPs** who wish to have a Service submitted for an Assessment as the basis for seeking a tScheme Grant of Approval;
- **tScheme's representatives** who are available to offer guidance during the Assessment and approval processes.

This document is intended for use as a template by Providers of Electronic Trust Services when preparing an S3A as a prerequisite to making an application for Registered Applicant status and who will use the S3A as the basis for contracting with a tScheme-recognised Assessor for the conduct of an Assessment with the intention of applying to have their service(s) accepted for tScheme Approval.

### 1.3 Overview & preparation

The document provides a framework of sections and sub-headings together with proposed standardised text. Authors of specific S3As are invited to adopt the style, phrasing and terminology of this model to the fullest extent practical within the context of their own organisations. This will assist readers who have to deal with S3As from a number of different sources.

As stated above, tScheme's [Required Assessment Procedures](#) is required prior reading for S3A authors (amongst others). It sets out explicit requirements across the overall process of the tScheme Approval procedures and points to other detailed sources. A further document, [Preparing for an Assessment](#) includes guidance on how to select a [tScheme-recognised Assessor](#).

*Text intended to offer narrative or guidance is in italicised dark red (brown) text framed within a dark red border (as per this paragraph).*

Within the suggested text there are a number of place-holders where authors should substitute the details of their own organisations and Services. These are indicated using «chevrons» as indicated in this sentence.

Throughout this document a distinction is made between an **Outline S3A** associated with a request for Registered Applicant status, and a **Full S3A**, which will become the focus of the Assessment itself.

Only the Outline S3A should be submitted to tScheme. The Full S3A is likely to be designated 'Commercial In Confidence', its confidentiality protected within the context of an independent agreement signed with the chosen Assessor. However, certain parts of the Full S3A will be taken directly and used in preparing the Assessment Report and ultimately in tScheme's Grant of Approval.

*In order to alert the TSP as to which parts of their S3A will be taken directly when preparing their Assessment Report those parts of this model document are framed in green without background shading (as per this paragraph). tScheme will then copy such text from the Assessment Report and use it when preparing their Grant of Approval.*

It is recommended that the S3A be agreed with the chosen Assessor prior to the Assessment. This will assist the Assessor in understanding the Service to be assessed and will ensure a sufficient and mutually acceptable level of detail is documented. It is further a requirement that the S3A be revised as necessary to accurately define the Service as actually assessed.

It is recognised that individual companies will have their own house styles and possibly specific service-related requirements that will dictate the final appearance of their own S3A, and hence it is understood that the tScheme styling of this model document may be substituted by the owner's own style. It is assumed therefore that any specific instantiation of this model will be subject to the owner's own configuration management practices, and hence none of these are explicitly suggested within this model.

Improvements, enhancements and the provision of additional information to support the explanation of the SSA are fully encouraged within the constraint of following the model format as much as possible.

Definitions of terms and acronyms that are not defined in this document may be found in the [tScheme Glossary of Terms](#).

Within the following Sections, an indication is given as to whether the heading and related text is applicable to either an Outline S3A, a Full S3A or both.

## 2. PURPOSE & READERSHIP

*The following text is suggested for those seeking tScheme Registered Applicant status, i.e. preparing an Outline S3A.*

This document is the primary reference governing «company»'s application for tScheme Registered Applicant status in respect of their «name of service» Service.

It provides the necessary high-level service description, target customer market, and outline technical specification required by tScheme.

The document is intended to give:

- «company»'s management an understanding of what it is they are committing to;
- the chosen Assessor, «assessor», an understanding of the scope of Assessment that «company» requires to have conducted, and;
- the tScheme Approvals Committee the basis for considering and accepting «company»'s application for tScheme Registered Applicant status.

*The following text is suggested for those wishing to have their services assessed and submitted for tScheme Approval, i.e. a Full S3A.*

This document is the primary reference governing the Assessment and submission for tScheme Approval of «company»'s «name of service» Service.

The document is intended to:

- give «company»'s management an understanding of what it is they are committing to;
- define the full scope of the Assessment to be undertaken;
- define what evidence is to be provided and how it demonstrates compliance of the Service as a whole;
- form the central technical scoping of the contract between «company» and its chosen Assessor, «assessor»;
- support «company»'s submission to the tScheme Approvals Committee for a Grant of Approval;

### 3. SERVICE DESCRIPTION

#### 3.1 Service Provider

*The following text is required in all S3As*

*This document relates to «company», registered in «place of registration» under «registration reference / details» whose registered office is at «registered address». «company» is «status, e.g. independent corporation / wholly owned subsidiary of etc.».*

*«company»'s additional contact details are as follows:*

*Contact person for the purposes of this Assessment:*

*Primary contact:*

*«name, title»*

*«address»*

*«telephone»*

*«email»*

*Secondary contact:*

*«name, title»*

*«address»*

*«telephone»*

*«email»*

*The following **additional** text is suggested for those wishing to have their services assessed and submitted for tScheme Approval (i.e. Full S3A).*

*Contact points with regard to the service (e.g. Customer Support etc):*

*Contact 1:*

*«functional title»*

*«address»*

*«telephone»*

*«email»*

*«url»*

*Contact 2:*

*«functional title»*

*«address»*

*«telephone»*

*«email»*

*«url»*

*«... additional contacts as required»*

## 3.2 Public Service Description

*The following text is required in all S3As*

*This S3A relates to «company»'s service known as «name of service».*

*«name of service» is a «Public Service Description of service».*

*The Public Service Description will be preserved throughout the Assessment process, will be included in the Assessment Report and used subsequently by tScheme when preparing the Grant of Approval.*

*The Public Service Description should describe the principal features of the Service by setting out the purpose of the Service followed by additional detail, including, inter alia:*

*features and functions incorporated;  
intended class(es) of users (subscribers and relying parties, as appropriate);  
list of tasks and usage;  
checks performed on supplied data;  
applicable restrictions;  
assumed user community characteristics;  
nature of provision / contracting with users & relying parties;  
etc.*

*This description must be a concise and accurate description of the scope and content of the SSA. It must be:*

- *suitable for unlimited public release;*
- *free of any jargon and marketing-hype;*
- *understandable to the non-specialist;*
- *suitable for prospective and actual customers of the service and for parties relying on the service;*
- *include a reference to the Service Policy and Service Policy Disclosure Statement<sup>1</sup>, giving a specific version number or date of publication.*

*If the Service wishes to claim that it will be issuing Qualified Certificates conforming to the requirements of [DIR 99/93], then this MUST be explicitly stated in the Public Service Description. In particular and if appropriate, details of any SSCDs used and whether secure signature verification is being provided as part of the Service.*

*Furthermore, any claims of conformance to an external standard or guideline must be for one that has been recognised by tScheme and is identified in 4.2.*

<sup>1</sup> Inclusion of a reference to these documents in this description does not automatically require that they too are fully public – the TSP may impose access controls over them. However, their inclusion does demonstrate that they exist (because the assessor will validate this).

*Before an Assessment can commence the full S3A must be extended to provide an Assessor's Service Definition. This is addressed in Section 3.5.*

### 3.3 Service topology

*For those seeking tScheme Registered Applicant status (i.e. Outline S3A), a system-level diagram (or diagrams) should be provided showing physical sites (geographic locations), where specific service components are located and what interconnectivity is employed. Brief supporting narrative should be provided to describe the elements of the diagrams.*

*For an Assessor's Service Definition (i.e. Full S3A), a system-level diagram (or diagrams) should be provided showing physical sites (geographic locations), where specific service components are located and what interconnectivity is employed. Supporting narrative should be provided to describe the elements of the diagrams to a further level of detail, such that the way in which the Service is managed and delivered is explained, plus indications of levels of redundancy and resilience that are built into the architecture>.*

### 3.4 Service platform

*In an Outline S3A the level of detail provided under this heading need only be a generalised description.*

*For a Full S3A, the level of detail provided should include specific descriptions of physical premises, hardware installations and software versions and configurations, such that the intended assessing body can plan the assessment required of them.*

### 3.5 Assessor's Service Definition

*This section is only required in a Full S3A. It must give a comprehensive, precise definition of the Service, its constituent parts and its internal functions, suitable for tScheme-recognised Assessors to identify and scope the Service for the purpose of the Assessment. It must provide information beyond the extent of that which would be found in the Service (Certification) Policy, Service Practice Statement and Service Policy Disclosure Statement, and which an assessor would need to know about the SSA in order to effectively conduct the Assessment. The Assessor's Service Definition is not aimed at customers and is not primarily intended for public dissemination.*

*This definition may be in a separate document but it is catered for in this Model S3A, and should consist of an extension to the detail given in the Outline S3A, in §3.2 to §3.4 inclusive*

## **4. APPROVAL PROFILES, RECOGNISED STANDARDS, GUIDELINES AND EVIDENCE**

### **4.1 Applicable Approval Profiles**

*The following table includes all existing Approval Profiles at their latest published status.*

*All authors should delete those that are not applicable*

*In an Outline S3A the columns headed 'Issue' and 'Abbrvn' should be deleted (since the actual versions used will be determined according to those current at the time the Assessment is undertaken).*

*In a Full S3A, in the column headed 'Issue', replace the term '<latest>' with the actual version number that is current at the time the Assessment is undertaken.*

The applicable tScheme Approval Profiles are:			
<i>Title</i>	<i>Identity</i>	<i>Issue</i>	<i>Abbrvn</i>
<b>Base Approval Profile (mandatory)</b>	<b>tSd0111</b>	<b>&lt;latest&gt;</b>	<b>Base</b>
Approval Profile for a Certification Authority [[issQCs]] < <b>including</b> Qualified Certificates > <i>delete if not applicable</i>	tSd0102	<latest>	CA
Approval Profile for Signing Key Pair Management < <b>including</b> Qualified Certificates > <i>delete if not applicable</i>	tSd0103	<latest>	SKPM
Approval Profile for Certificate Generation < <b>including</b> Qualified Certificates > <i>delete if not applicable</i>	tSd0104	<latest>	CGen
Approval Profile for Certificate Dissemination	tSd0105	<latest>	CDis
Approval Profile for Certificate Status Management	tSd0106	<latest>	CSM
Approval Profile for Certificate Status Validation	tSd0107	<latest>	CSV
Approval Profile for Registration Services	tSd0042	<latest>	Regn
Approval Profile for Identity Services	tSd0108	<latest>	ID

*NB – in the above table, the column headed 'Abbrvn' will not be included within the Grant of Approval and hence does not appear within the green border.*

## 4.2 Recognised standards and guidelines

*Both forms of S3A should specify here to which recognised standards and guidelines the author wishes tScheme to endorse conformance, within its Grant of Approval. Such external standards or guidelines must have been recognised by tScheme for this purpose and listed on the [tScheme website](#).*

*A table in the same format as that for the Approval Profiles should be used.*

*The following table may be used to list the standards or guidelines against which conformance is claimed. NB. This does not need to refer to either ISO 9000 or ISO 27001 (or equivalents), which are implicit in the tScheme Base Profile.*

*In an Outline S3A the columns headed 'Issue' and 'Abbrvn' should be deleted (since the actual versions used will be determined according to those current at the time the Assessment is undertaken).*

The applicable tScheme-recognised standards and guidelines are:

<i>Title</i>	<i>Identity</i>	<i>Issue</i>	<i>Abbrvn</i>
<title>			
<title>			
<title>			

*The information in the remainder of this section need only be provided in a Full S3A.*

## 4.3 Service and Approval Profiles mapping

The high-level mapping between the Service functional elements and the selected Approval Profiles is as follows:

*In the following table the document owner should enter in the left-hand column the identifiable functional elements of their Service, deleting the columns for those Approval Profiles they have not selected.*

*In each entry where there is a correspondence between the Service and the selected Approval Profiles there should be a reference or linkage to a following sub-section that describes the nature of the relationship and identifies the evidence that will be offered to demonstrate compliance with the*

*Approval Profiles' criteria. This reference should be to 4.4, 4.5, 4.6, or additional sub-sections if required.*

<i>Service functional element/Site</i>	<i>Base</i>	<i>CA</i>	<i>SKPM</i>	<i>CGen</i>	<i>CDis</i>	<i>CSM</i>	<i>CSV</i>	<i>Regn</i>	<i>ID</i>	<i>other</i>

## 4.4 Evidence

*A general description of the available evidence and documents, covering:*

- Formal status of «company»;*
- Formal quality certifications held;*
- The procedures and standards that govern the management and operation of the Service;*

*Documents in the above category could include, inter alia:*

*Corporate Security Policies and procedures, Service Policies, Service Practice Statements, SPDS;  
 Legal compliance, Insurance policies;*

*Technical standards and specifications, other supporting material (both de facto and de jure);*

*Documents in the above category could include, inter alia:*

*Service, System and Web design documentation; Test & Integration plans, schedules, scripts, results;*

*Contractual arrangements for support services and outsourcing, together with related risk analysis and contractual arrangements for Assessment;*

*Pre-existing approvals or evaluations, certifications, technical reports, industry-scheme recognition, other tScheme Approvals, site inspections;*

*The format and source of these documents should be indicated (paper, electronic).*

## 4.5 Document hierarchy

*Include a graphic or other effective means of identifying the documents being provided as evidence and their relationship to one another (including title and formal reference or identity).*

## 4.6 Evidence and Approval Profile criteria mapping

*In this section the document owner should insert, or provide reference to a further document giving, the identity/title of documents intended to be offered as evidence in relation to the chosen Approval Profiles and their respective criteria. tScheme recommends the following method for accomplishing this, although document owners are free to accomplish this by other means so long as the requirements are satisfied and the Assessor finds it to be a workable solution. The recommended approach is:*

*From each of the chosen Approval Profiles, insert or cut & paste §3 and Annex I into this section of the S3A (or into the alternative document if preferred). This will bring in the explicit criteria (§3) and the Clause Compliance List (Annex I) – the intervening §4 should be deleted – it serves little purpose here. It would be sufficient for the purposes of this section of the present document to just import the Clause Compliance List, but by also importing the criteria themselves a convenient feature of the Approval profiles, the ability to follow bi-directional linking between criteria clauses and their corresponding compliance list entries, is preserved. This will facilitate the Assessment later on.*

*Then, in the compliance lists, for each criterion in each Approval Profile, the document owner should insert a reference to the form of evidence that will show compliance with that criterion. This process may be facilitated by allocating convenient abbreviations to specific evidential documents when describing them in either of the preceding sections of the present document.*

*The document owner will need to attend to imported headings to structure and contain the imported text within this section of the present document which, since they will have a good degree of competence in using MS Word, need not be spelled out for them»*

## 5. ADDITIONAL INFORMATION

*The owner may provide here whatever additional information is felt necessary or useful to support the S3A, whether being used for an application for tScheme Registered Applicant status (Outline S3A) or for formal tScheme Approval (i.e. Full S3A)*

*The owner may, furthermore, express additional requirements for the Assessors to address that take the Assessment beyond the scope of the selected Approval Profiles. It is recommended that the necessary additional parts of the document be placed in the most appropriate section (e.g. additional criteria against which to be assessed might go under §4.1, with the proposed evidence under §4.4).*

*Annexes may also be added where required, and may be an alternative holding place for the table entries required in the 'Applicable Approval Profiles, Recognised standards and guidelines and Evidence' sections if, for example, a landscape presentation is more suitable.*

## 6. REFERENCES

[DIR 99/93]      [EC Directive 1999/93/EC on a Community framework for electronic signatures.](#)