Issued

Guidance for Assessments

Ref. tSi 0250

Issue 2.03

2004-10-21

Executive summary

This document gives guidance to TSPs wishing to be assessed by a *tScheme*-recognised Assessor. It gives guidance on:

1. how to choose the right kind of Assessment that is most suitable for the Service or Trust Service Component they are offering for Assessment;
2. producing the various sorts of documentation required by *tScheme*;
3. how the Assessors can be expected to interpret some of the Profile criteria;
4. the kinds of evidence that could usefully be offered in support of Assessment claims.

It is expected that, as experience in operating *tScheme* develops and the number of Assessments undertaken increases, so this document will be extended to provide interpretative guidance arising out of practical experience.

DOCUMENT HISTORY

Status	Issue	Date	Comment	Authorised
tSi	1.00	2001-10-08	First version, tracked under Document Management procedures.	Chief Executive
tSi	2.00	2002-09-09	The focus of the document has been shifted so that the main target audience for the document is now the TSPs. This new purpose is described in the Executive Summary on the front sheet. Assessors already have knowledge of much of what is in this document. The title of the document has changed to reflect this new focus, though its reference number remains the same and the version numbering has not been restarted. The shift in focus has had a major impact on the wording, with the majority of the existing text having been altered or deleted. The document is best viewed as a rewrite of issue 1.00. The main changes are listed below. 1. A new section has been added on recognition of other Trust Service Assessment schemes. 2. Amendments needed to cover *tScheme*-Ready have been made. In particular, new guidance on whether an offering is suitable for recognition as *tScheme*-Ready has been added. 3. A new Section explaining trust-enabled Service approvals has been added. 4. The sections offering specific advice on the individual Approval Profiles have been removed and the text there put into the Approval Profiles themselves. 5. Extensive new guidance on how to produce a Service Description has been added. 6. A number of items, although offered as guidance, were really intended to be taken as mandatory. Some of them have been retained here, perhaps with slight rewording, since they also constitute useful advice to TSPs, but others have simply been moved out into the relevant definitive documents. 7. The Section on the relation to the [DIR 99/93] has been removed as it is not offering guidance to TSPs. Much of what was said there is already said elsewhere.	CEO

Status	Issue	Date	Comment	Authorised
			8. The Section on the S3A has been removed as this topic is now extensively covered elsewhere. 9. A major new Section on Evidence has been added. It contains all of the information that previously appeared in the Approval Profiles themselves. 10. The subsection on Internationalisation has been deleted as it is inaccurate and not thought to be helpful.	
tSi	2.01	2002-10-21	Update References Section to reflect new issue of BS 7799 part 2 in September 2002. Also add ISBN for ISO 17799.	CEO
tSi	2.02	2004-08-26	Update References section to correct errors	*tScheme* Secretariat
tSi	2.03	2004-10-21	Update in line with PPC response on Qualified Certificates as detailed in "tSi0271_1-00 Current Interpretation Responses"	*tScheme* Secretariat

CONTENTS

1. INTRODUCTION

It is *tScheme*'s task to lay down the detailed criteria against which a Trust Service and its Provider can be approved and, by having TSPs assessed against those criteria, consider applications for Approval of specific Trust Services offered by Providers.

It is the task of a *tScheme*-recognised Assessor to perform these Assessments against a TSP's nominated Services, and to certify compliance with the *tScheme* criteria, from which *tScheme* will, subject to the Approvals Committee's sanction and on subsequently establishing acceptable contractual arrangements with the TSP, issue a Grant of Approval.

This document offers TSPs and Suppliers of Service Components guidance as to how they should expect their chosen Assessor to perform the Assessment and how they should expect the Assessors to interpret and make judgements on some of the Approval Profile criteria.

In doing so, the document also offers guidance on:

- producing the various sorts of documentation required by *tScheme*;
- how to choose the kind of Assessment that is most suitable for the Trust Service or Trust Service Component they wish to have assessed;
- the kinds of evidence that could usefully be offered in support of Assessment claims.

2. SCOPE

The document offers only guidance; it is not definitive. It does not provide additional criteria; it is an aid to the achievement of a successful Assessment.

Although much of the wording of this document relates to Assessments for *tScheme* Service Approvals, the document is also intended to be widely applicable to *tScheme*-Ready Assessments. For use in the latter context:

- references to "Service Provider" shall be taken to mean "Component Supplier";
- references to "Service" should be taken to mean "Service Component";
- references to "Service Subject to Assessment", or SSA should be taken to mean "Service Component Subject to Assessment", or CSA;
- references to "Specification of Service Subject to Assessment", or S3A should be taken to mean "Specification of Service Component Subject to Assessment", or C3A.

Where there are distinctions to be drawn between Assessments for *tScheme* Service Approval and *tScheme*-Ready status, this is either self-evident or made explicit.

3. GUIDANCE

3.1 Terminology

Many of the technical terms used in the Approval Profiles are defined in the *tScheme* Glossary of Terms. If a word used in an Approval Profile appears in the *tScheme* Glossary of Terms, the specific meaning given there is always intended. All other words should be taken in their general English or, if they are technical terms, generally understood technical sense.

3.1.1 The Public Service Description, Assessor's Service Definition, SPS, SP and SPDS

There are five general terms in the Glossary that relate to descriptions of how a TSP goes about doing things. Refer to the Glossary itself for the formal definitions of these terms. Below is a general description of their import:

- **Public Service Description**, which is a concise description of a Trust Service or Trust Service Component, understandable to the non-specialist, suitable for prospective and actual customers of the Service and for parties relying on the Service. It contains or refers to the specific Service Policy and Service Policy Disclosure Statements that apply to the Service. It is intended for public dissemination;
- **Assessor's Service Definition**, which is a comprehensive definition of a Trust Service or Trust Service Component suitable for *tScheme*-recognised Assessors to identify and scope the Service for the purpose of an Assessment. It contains or refers to the specific Service Policy, Service Policy Disclosure Statement and Service Practice Statement that apply to the Service, and provides additional detail sufficient to enable the Assessors to understand the S3A. It is not aimed at customers and is not primarily intended for public dissemination;
- **Service Practice Statement** (SPS), which is a statement of the practices that an Electronic Trust Service Provider employs in providing its Electronic Trust Service;
- **Service Policy** (SP), which is a named set of rules indicating the applicability of an Electronic Trust Service's deliverables to a particular community and/or class of applications with common security requirements;
- **Service Policy Disclosure Statement** (SPDS), which is a statement of aspects of an Electronic Trust Service most important to an Electronic Trust Service Provider's subscribers and relying parties, in a form that is unambiguous and conspicuous to them.

Similar terms are also defined, which are more specific to a particular Service being offered; for example a **Certification Policy** is a **Service Policy** for a **Certification Service**. These terms are simply ways of expressing the same things in a more specific context.

Together the terms denote statements, perhaps in the form of formal documents, that form the core of a TSP's description of what it does and how it goes about doing it. In assessing their quality, Assessors will take into account the different objectives of these statements; they can be characterised as follows:

- The purpose of the **Public Service Description** is to inform potential customers of what is on offer. It must do this clearly and fairly. The wording of the description will appear in the Grant of Approval, so it must be free of marketing hyperbole. It must be a straightforward factual statement of what the Service offers. Section 3.2 gives more detailed guidance on how to write a Public Service Description that will be acceptable to *tScheme*;

- The purpose of the **Assessor's Service Definition** is to tell the Assessors what is to be assessed. It scopes and precisely defines the Service. It contains additional technical detail required by the Assessor that may not be present in any of the Public Service Description, SPS, SP or SPDS;
- The **SPS** has two main audiences: the customer and the Assessor. The customer needs to see only those parts of the SPS that indicate what to do to use the Service. The Assessor needs to see how things are done in order to evaluate their appropriateness for the SP being supported. The SPS contains information about the security practices of the TSP. A TSP may or may not choose to make the document publicly available;
- The **SP** is primarily for the customer and relying parties. It is what they use to get a full picture of the nature of the Service they are being offered. It is about what the Service is for and what the world can expect of it, rather than how it operates. The SP must be unambiguous. It must be complete in the sense that all visible aspects of the Service, including the consequences of failure, need to be described. The SP may be long and involved - there is usually a lot to say;
- The **SPDS** cuts through the verbosity of the SP and SPS, picking from them the essentials, with particular emphasis on the legal, administrative and contractual issues, and rephrasing them in readily understandable terms. Its aim is to inform up front, avoiding "small print" legalese. It should provide the subscriber and relying party with all of the main things they need to know to get a basic picture of what they should expect, and their rights and obligations. It should be short. Semantically it should contain nothing that the SP and SPS do not already contain, but its aim in life is clarity and fairness of expression. The Base Approval Profile lays down in detail requirements for its content.

3.2 Writing the Public Service Description and the Assessor's Service Definition

For a Service to gain its Grant of Approval, *tScheme* requires its Provider (the TSP) to produce both a **Public Service Description** and an **Assessor's Service Definition**. Both of these terms have specific meanings defined in the *tScheme* Glossary of Terms. Although they describe the same subject – the Service – they serve different purposes and appeal to different audiences. The challenge is to make both of them serve their purposes while remaining consistent with each other and with the realities of the Service as actually offered and operated.

As a generality, the longer, more technical and the more prescribed the Assessor's Service Definition is, the easier it is to write. Typically, a long technical definition like this is written by experts for experts and tends to be well validated in the course of its use as a guide to implementation and operation. Moreover, the language is usually highly technical, using words drawn from a technical lexicon, which have meaning familiar only to domain experts. This guidance offers no further counsel to experts writing their long, technical definition.

It is much harder (and nearly as time consuming) to write a short description aimed at the non-expert, typical user of the Service. Technical words and phrases now serve to confuse rather than to enlighten. Brevity demands careful selection of what really matters. There is a temptation to highlight what differentiates the Service from its competitors at the expense of the fundamentals. Perhaps worst of all, the Service's sales brochure suddenly appears to be the short cut to just what is needed when in truth it certainly is not. The guidance that follows is about writing a short description for lay readers - the Public Service Description.

1. **Construct the description as a short answer to the question from the typical user: "What is your Service and what does it do for me?"**

Any valid answer must use the vocabulary and the context of that typical user. This may well not entail the complete avoidance of technical words and phrases. For example, even the most lay of lay

users should know what a "browser" is. Nevertheless, the writer should validate carefully that the vocabulary that he perceives as safe really is so. For example, many users have heard the phrase "digital certificate" but almost none would be capable of describing one in any detail, even less in terms of, say, X.509 conformance. On the other hand, the elimination of all technical content may prove equally inappropriate – technical language retains the benefits of precision and compactness. The key message to authors is to validate their descriptions with typical users and to make as few assumptions as possible.

2. Consider the description as a promise to deliver the features of the Service.

An author could do a great deal worse than to list all the features of the Service, to put them into order of importance and to concentrate on describing the first few. The important point is the identification of features rather than benefits. A feature is a property of the Service that remains however the Service is used. It is easy to prove whether it is present or absent. A benefit depends on usage and circumstance and cannot be guaranteed. Features go in the contract; benefits go in the brochure.

3. Avoid all boastful, content-free and inherently unprovable phrases.

Brochurese contains much that has no meaning – competitive, state-of-the-art, cost-effective, leading-edge and the like. Such words and phrases have no place in a factual, sober description. The first test of acceptability for any word or phrase is that it is reasonably capable of proof if challenged; this means observable, measurable, countable or other objective evidence as appropriate. The second test is that it remains true after the passage of time; this generally ensures that the description is not a market comparison.

4. Replace all words about how it works under the covers with words about what it achieves for the end user.

Only experts should know or need to know what causes a feature to work as it does. Any description of how a feature works is either superfluous, because the feature is already adequately described, or a substitute for a proper description, perhaps indicating that the author does not know what to write.

5. Encompass all the features not just the technical ones.

The author should consider all the features of the Service rather than just those that appear on the computer screen. If there is a manned help desk then this is a feature too. If there is a no-quibble compensation scheme for certain types of faults then this is also a feature. For many users, such non-technical features can be just as important as any of the technical ones.

6. State clearly the limitations and boundaries.

Successful use of any Service depends as much on the user as the Supplier. A user who unwittingly attempts to exceed the limitations of a Service is going to be unhappy whether he then attempts to blame the Supplier or not. This is particularly important in the context of a Trust Service where a user could turn any untoward discovery of a limitation, constraint or boundary into a loss of trust. The author should not therefore hide relevant things that the Service cannot do, or should not be used to do, as part of the trust-building process where there is any realistic danger of misuse.

Clearly, there is no standard formula for creating a good non-technical, short description of something that is inherently complex and esoteric, other than hard work, attention to detail and careful checking. Doing such a thing well should not be treated lightly. For Trust Services it is vital.

7. Refer to the definitive detail

For those readers who do wish to dig deeper into the features and rules of the Service and see the small print, the description should point at the definitive documents. The Service Policy, the Service Practice Statement and the Service Policy Disclosure Statement constitute the basic set that should be referenced from the Public Service Description.

3.3 Keeping track of Approval Profile evolution

Every authorised Approval Profile contains a Document History section. This records the main differences between the current and previous authorised issues and will be used by Assessors to identify more easily the differences between successive Profile issues.

At any time the *tScheme* website will hold for public access only the most recently ratified Approval Profiles.

3.4 Variance of Criteria values

The *tScheme* criteria are required to be applicable across a broad range of Service types and policies operated by TSPs ranging in size from a single individual to an industrial giant. For these reasons it is not always possible for the criteria to prescribe specific quantitative values.

The examples below may help:

- a measure such as "timeliness" might need to be applied differently for a low reliance stable Service to the way it needs to be applied for a Service certifying fast changing attributes on which there is a high level of reliance;
- the type of organisational risk Assessment that is suitable for a one-person Registration Authority will be quite different from that expected from a large organisation;
- if a TSP has chosen to use well known, widely accepted, tried and tested in practice security technology to support its activities, the Assessors will see fitness for purpose as the main issue in assessing its suitability. The main question will be: is the technology functionally capable of doing the job asked of it? A TSP is unlikely to have to justify such a choice on security and quality grounds as rigorously as if it had chosen relatively unknown technology whose security, quality and functionality would be more difficult to assess. This will be especially so if some kind of Assessment has been previously undertaken on the technology, e.g. a formal evaluation, the results of which are offered as evidence.

Differences like those listed above mean that Assessors can be expected to make judgements on many of the *tScheme* criteria, according to the context in which they are being assessed. Indeed, *tScheme* considers the competence to make such judgements to be an important characteristic of a *tScheme*-recognised Assessor, and an important factor in their Accreditation.

3.5 Interpretation

tScheme encourages Assessors to achieve mutually balanced approaches to their Assessments. A TSP should be able to be confident that it will be examined with similar rigour and to a similar depth no matter which Assessor it chooses. To this end, the *tScheme* Approval Profiles and the Required Assessment Procedures documents remain definitive, and can be expected to be consistently applied in

all Assessments. However, in difficult judgement situations, or where a decision cannot safely be made by the Assessor, particularly a decision having a major effect on the result of an Assessment, *tScheme* has encouraged Assessors to communicate this to *tScheme*, and to approach the *tScheme* Secretariat for specific guidance when they feel it would help. If they wish it, TSPs can require anonymity to be preserved throughout this process, so that *tScheme* can, without prejudice, assist the Assessors by confirming the original intent of the specific criteria concerned. Also, *tScheme* may have the advantage of experience of other Assessment judgements made by other Assessors in similar circumstances.

This 'Interpretation Library' of experience[1] is contained in document reference "tSi0271 Current Interpretation Responses.doc", which can be found in the library pages of the *tScheme* website. This document is also intended to be especially valuable in clarifying current intentions, where issues have arisen that may require amendments to the Profiles at the next review date.

3.6 What is being measured

3.6.1 Quality of Service and Service provider

tScheme approval is represented by the *tScheme* Mark. The meaning of the *tScheme* Mark can be summarised as follows:

1. the Service has been thoroughly evaluated against rigorous criteria by independent experts;
2. the Service Provider has agreed to keep to these criteria;
3. the Service Provider subscribes to the *tScheme* Code of Conduct; and
4. the Service Provider has agreed to act promptly and fairly to remedy faults.

tScheme Approval Profiles require Service Providers to describe their Services in clear, simple, unambiguous language that allows those who rely on their Services to reach informed decisions about the suitability of those Services. In particular, *tScheme* does not grant approval to any Service if its investigations show that the Service Provider conceals important factors, seeks to confuse or otherwise attempts to mislead users. A potential user of an approved Service is therefore better equipped to choose a Service appropriate for his purposes.

Note also that the language and method of communication of information must be appropriate to the user community.

Assessors' judgements will be coloured by the need to satisfy the above quality criteria.

The above applies equally well to *tScheme*-Ready Assessments.

3.7 What is not being measured

3.7.1 Suitability

It is always up to the Service's customer and any relying parties to decide whether a Trust Service is useful and appropriate for them or not. *tScheme* cannot, and does not offer any guarantees on this. The Grant of Approval may say that the Service conforms to certain externally produced and widely recognised functional standards or guidelines laid down for particular intended usage contexts, and this

[1] Along the lines built up in Europe for ITSEC interpretation.

in many cases will give potential customers and relying parties a strong steer on suitability, but the final onus is on them to decide.

3.7.2 Financial Probity

In the IT and dot-com business world, financial soundness is particularly difficult to assess, many businesses operating with high levels of financial loss and yet still often considered to be viable. With the exception of specific criteria identified explicitly in the Approval Profiles, such as a TSP's ability to underwrite its liabilities, Assessors will not be assessing financial probity.

So general financial probity is not an Assessment factor, although a TSP's ability to underwrite its liabilities **is** assessed (See Section 3.15).

3.7.3 Interworking

The Assessment of functional interworking is out of scope of *tScheme* and therefore out of scope of an Assessment. *tScheme* will not approve claims of functional interworking, and any such claims will be explicitly excluded in any Assessment report and in any Grant of Approval.

3.8 Recognition of other Trust Service approval schemes

As *tScheme* evolves it will increasingly find itself being asked to establish recognition arrangements with other Trust Service evaluation/approval/accreditation schemes (referred to simply as "schemes" from hereon). When assessing Trust Services approved under an approval scheme recognised by *tScheme*, Assessors will use the *tScheme* Approval documents relating to that scheme. For some schemes, immediate recognition may be feasible, but where this is not possible the scheme-specific recognition documents analyse the differences between the recognised schemes and *tScheme* itself to establish the *tScheme* criteria that have not been assessed by each scheme. Procedural differences may also be identified; the documents will also spell out the impact of this on the *tScheme* Assessment process.

3.9 Relationship to external standards and guidelines

Although a direct Assessment of suitability is out of scope, TSPs may, if they wish, offer Services that claim to conform to particular external standards or guidelines, and may ask *tScheme* to positively endorse (in the Grant of Approval) their Service's conformance to them. One example is the government guideline for Registration Authorities on the verification of the identity of individuals [HMGVInd] (for the purpose of such individuals interacting with government Services).

- *tScheme* states the criteria it will apply in deciding on what it considers to be acceptable for this sort of treatment in its Required Assessment Procedures.

3.10 Assessing a TSP's Internal Security

Evaluation of the internal security practices of a TSP is an important part of any Assessment. An obvious approach to satisfying the Assessor in this respect is to offer evidence showing that the guidelines of [ISO/IEC 17799] have been followed, or that [BS 7799-2] has been conformed to, but it is acceptable to base security on other standards. However, Assessors can be expected to exercise their judgement in vetting alternatives for suitability. The important overall rule they will apply is that any

alternative must form a base from which the TSP can furnish the Assessor with evidence that relevant risks have been identified and are being effectively managed.

A checklist of topics that an acceptable standard or set of standards should encompass is:

- Security policy;
- Security organization;
- Asset classification and control;
- Personnel security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Systems development and maintenance;
- Business continuity management;
- Compliance with legal and security policy requirements.

3.11 The quality of cryptographic mechanisms

Use of cryptography is a common theme across the great majority of Trust Services in terms of deliverables, Service delivery methods and preservation of internal security. Quality requirements will vary according to the level of reliance that the Service claims, but questions of key length and algorithm choice will be asked by Assessors. Although, strictly speaking, Assessment of these things demands specialised knowledge, there are generally agreed industry norms. It is only if either a TSP diverges from such norms, or especially strong protection is needed, that the issue of specific expert validation would arise. In such a case, the TSP can expect to have to provide specialist evidence to convince the Assessor of the suitability of the approach being followed for the security requirements of the SSA.

3.12 Assessment under multiple Approval Profiles

This section confines itself to Operational Services being offered for *tScheme* Approval. The recognition of Trust Service Components as being *tScheme*-Ready is covered in Section 3.13.

In a multi-Profile Assessment, the appropriateness of the choice of the Approval Profiles nominated by the TSP should be reasonably clear. For a Service offering the full range of Certification Authority functions, the Approval Profile for a Certification Authority would be nominated, and this itself automatically pulls in the required individual functional Approval Profiles. For a Service offering only a subset of this functionality, the TSP must nominate in its S3A the specific functional Approval Profiles applicable to the subset being offered. How this is done may depend on the business model within which the TSP is operating.

In either case, the Specification of Service Subject to Assessment (S3A) will need to describe how the different functional parts fit together. During the Assessment, the Assessor will pay particular attention to their secure interworking.

The examples below show how multiple Approval Profiles could be handled under just two of the many possible different business models. The examples are relatively simple, but not all business

models offer such straightforward choices. In general, TSPs are strongly recommended to engage in discussions with *tScheme* to determine, and agree with *tScheme*, the best approach. This should be done as part of the process of becoming a *tScheme*-registered Applicant. This will also help the TSP to decide whether it really is providing an Operational Trust Service, or whether it is in fact best seen through *tScheme*'s eyes as a supplier of a Trust Service Component eligible for Assessment as *tScheme*-Ready. What distinguishes a *tScheme*-Ready Component from an Operational Trust Service is discussed in the Section 3.13.

Example 1. A Registration Authority subcontracting Certification Services but retaining overall authority (a common closed solution case).

This might occur if an organisation wished to act as a Certification Authority providing Certification Services for its staff. This is a Service being run and controlled by the organisation (and which is, therefore, the 'issuing authority' for those certificates). The organisation would naturally wish to handle its own staff registration, but might wish to outsource the specialist technical tasks of certificate generation and management to an outside agency.

This leads to a reasonably straightforward Assessment choice. The S3A would describe the full Service, so it would be subject to Assessment under the Approval Profile for a Certification Authority and the required functional Profiles identified there.

In the language of Schedule 1 of the Base Approval Profile, the organisation performing the RA functions is both the Service offerer and the operational enterprise. The Certification Services are "Externally Provided Trust Service Components". The Base Approval Profile requires the organisation to establish appropriate contractual relationships with the Certification Service providers. The S3A would identify the organisation as being in control and taking any liability to subscribers that might apply and to relying parties.

Example 2. A provider of one or more Certification Service functions, without a registration function.

This might occur if a commercial back-end Certification Services provider wishes to gain market advantage by having its Services carry the *tScheme* Mark, but does not wish any particular Registration Services to be assessed, even though its own Services are currently operating with a number of different Registration Services.

In this case the Service being assessed is simply handling the Certification end of the full possible functional range and would be assessed under an appropriate selection from the various back-end functional Approval Profiles, the selection depending on exactly what was being offered. Although the Service to be assessed must be Operational[2], ready to supply Services to one or more external Registration Services, the Registration Services themselves would remain out of scope of the Assessment. An important feature of this Service is that its customers are the operators of the Registration Services, not the subscribers to the Registration Services. The Service's policy and practice statements would therefore need to be expressed in terms of the operators of the Registration Services as its customers.

So the Registration Services would not be treated as being outsourced in any way; they are not being assessed.

In the language of Schedule 1 of the Base Approval Profile, for the purpose of the Assessment the Certification Services provider is the operational enterprise. It is also a Service offerer in the sense that it is offering its Services to a Registration Authority (the back-end provider does not see or know the end user subscribers who are the customers of the Registration Authority). The

[2] Note that *tScheme*'s use of the term "Operational" is very specific. See the definition in the Glossary

Certification Services provider would be directly liable to its customer RAs, not to the subscribers of the RAs. The S3A would identify only the back-end Service as being in scope for Assessment.

Future Registration Authorities may now find the Certification Services package attractive, since only their Registration Service and its links with the previously approved back-end Service would now need to be assessed in order to obtain use of the *tScheme* Mark for the full combined CA Service.

3.13 *tScheme*-Ready

Any Operational Trust Service that can be assessed against all of the criteria in the Approval Profiles that apply to it can potentially be assessed for eligibility to become *tScheme* Approved and carry the *tScheme* Mark. There are, however, some Trust Service Component offerings that are never themselves provided to end-customers as a stand alone Service, and would therefore not be able to be assessed against all of the criteria in the relevant Approval Profiles. The concept of "*tScheme*-Ready" was conceived to address this issue by permitting the invariant features of the offering to be assessed out of context of the Services within which it is designed to be deployed.

3.13.1 What makes something *tScheme*-Ready?

In the limit, *tScheme*'s customers are the customers of the Trust Services approved by *tScheme*, and the parties relying on the deliverables of the Service (who may, but need not be, customers of the Service). Safeguarding their interests is *tScheme*'s main purpose; it is to them that *tScheme*'s ultimate responsibility lies. Customers and relying parties use the TSP's description of its Service, its rules and its operation as the basis for deciding whether the Service is functionally and legally acceptable to them and whether it is sufficiently reliable and trustworthy. They cannot make this decision unless these descriptions are made available to them, so it is not simply enough that such descriptions exist. The presentation of Service information is as important to a *tScheme* approval as its existence.

Continuing the theme of safeguarding customer interests, another distinguishing feature of *tScheme*'s approvals is that a TSP's ability to deliver on its Service promises, according to its Service description and policy, has to be independently assessed. This can only be done if the Service being assessed is deployed and open for business[3]. TSPs have to show by deed, not promise, that they can deliver.

All of the above means that a Trust Service being offered as a candidate for a Grant of *tScheme* Approval must at the time of submission be deployed and open for business using an identified Service Policy (SP), a Service Practice Statement (SPS) and a Service Policy Disclosure Statement (SPDS), all of which are advertised to and available (except perhaps some possible confidential parts of the SPS) to the Service's customers and relying parties.

So in assessing suitability for Grant of Approval, the first question to be asked is: is the Service currently Operational?

If it is not, then the Service cannot be obtain a Grant of Approval, though may still be a candidate, as a Trust Service Component, for a Grant of *tScheme*-Ready Status.

tScheme-Ready enables Trust Service related Components to be assessed under the *tScheme* banner as being suitable for incorporation within *tScheme* approved Trust Services. *tScheme*-Ready is not intended to be used to obtain a partial Assessment of a not-quite-Operational Service, nor of a Service Component intended to be developed later into a self-contained Trust Service. The customers of a

[3] More formally, the Service must be "Operational" as defined in the *tScheme* Glossary of Terms

tScheme-Ready Service Component are always the TSPs responsible for the Trust Service containing it.

There is one other critical question to ask. If the *tScheme*-Ready candidate Service Component is intended to form the basis of all or part of a number of separate deployed Services, are there sufficient aspects of the candidate that remain invariant from deployment to deployment, and that can be tested against the *tScheme* criteria in the relevant Approval Profiles?

To make an Assessment worthwhile, a substantial proportion of the criteria in the Profiles relevant to the candidate offering must apply, and those that do apply must all be satisfied independent of any particular deployment. Judgement of what is substantial will be made both by *tScheme* and the Assessor, following separate discussions between the Component Supplier, *tScheme* and the Assessor. These must take place when the Supplier registers as a *tScheme*-registered Applicant. Both must feel that the Assessment and resulting recognition will be sufficiently substantial and hence not misleading. If these conditions are satisfied, the Service is a candidate for *tScheme*-Ready status.

3.14 Trust-enabled Services

The concept of a Trust-enabled Service has not yet been fully developed, and at the time of writing it is not possible to request that a trust-enabled application, offered as an application Service to customers, be assessed by *tScheme*. However, the description below is provided to give TSPs some idea of what *tScheme* has in mind for the future.

A Trust-enabled Service is an application level Service that interfaces with and relies upon underlying Trust Services. The *tScheme* Mark will be able to be applied to a trust-enabled Service. *tScheme* will not approve the application level functionality of such Services; it will simply approve the provider of the application, and the application's choice and use of the Trust Services it relies upon. So an approved trust-enabled Service:

- is being operated by an organisation satisfying the *tScheme* probity criteria in the Base Approval Profile;
- uses only *tScheme* approved Trust Services;
- interfaces with them in a manner satisfying the *tScheme* criteria applied to ensure the secure and trustworthy use of those Services.

3.15 TSP Liability

The reasonableness of the level of liability accepted by a TSP is not being assessed under *tScheme*, except when a TSP is claiming conformance to [DIR 99/93], for which specific requirements apply (and even so, there are no explicit levels cited). What is important is that the TSP declares conspicuously, clearly and fairly, exactly what liability it accepts.

The level of liability accepted can however affect the depth of examination required, since the more liability that is accepted, the more it is that the TSP suffers as a result of any failures than the subscriber or relying party. However a reasonable balance must be struck, as reflected in the meaning of the *tScheme* Mark (outlined in Section 3.6); *tScheme* will not approve patently poor Services, even though they say they will accept all liability themselves (see also Section 3.7.2).

3.16 Subscriber Agreement

What constitutes an acceptable subscriber agreement depends very much on what the subscriber is being asked to agree to. The greater the commitment the subscriber is making and the greater the level of reliance on the Service being provided to the subscriber, the better the proof of agreement is required to be. For example does a record of subscribers "clicking through" to a web page, having been presented with terms and conditions to which they are asked to agree, provide sufficient proof of agreement? At low levels of commitment it may be judged to do so ("the subscriber can't get through to the next stage without a click-through from the terms page. This page requests the subscriber to click through only if he or she agrees to the terms displayed, so therefore the subscriber must have seen, and by implication agreed to them."), but for more sensitive subscriber agreements, a stronger indication of agreement with better evidence of acceptance of terms is likely to be required, both to protect the subscriber from accidental agreement and to protect the TSP in case of dispute.

3.17 Evidence

TSPs should reach an agreement with the Assessors early in the Assessment process on the types of evidence they will be presenting. This should happen naturally since the S3A is required to indicate the evidence the TSP is planning to offer. It may be necessary to work with the Assessor to develop a mutually acceptable list.

Remember that evidence of Service promises made will not be considered sufficient. Evidence is also required that actual practice is in line with promises. This may require site visits.

A TSP may offer evidence of a previous assessment of some kind for all or part of its Service (not necessarily a *tScheme* Assessment). If this happens, *tScheme*-recognised Assessors will form a judgement of the status and, if not *tScheme*-recognised, competence of the previous Assessor. In due course, agreements are expected to be established between *tScheme* and other assessment agencies on mutual recognition. Until then however, each case will be looked at on its individual merits, though a case history of comparison conclusions may build up over time.

3.18 Reassessments

A Reassessment[4] is an Assessment performed for any of the following reasons:

- The previously assessed Service has materially changed;
- There has been a change in the volume of business to the extent that the TSP's Service capacity or its financial guarantees could be affected;
- The organisation offering the Service has materially changed, or its outsourcing arrangements have changed
- An Approval Profile under which the Service was previously assessed has been updated[5], and the existing approval has come up for renewal, or the TSP wishes independently to obtain approval under the new Profile.

---

4 As distinct from renewal of an approval, whose aim is to ensure that the Service still possesses Service properties that have previously been assessed. However, any renewal will require Assessment against the currently ratified versions of the selected Approval Profiles (see last bullet in this subsection).

5 Note that profiles are not changed in a manner that would affect existing Assessments except either at notified revision dates or in direct response to external events.

The extent of the Reassessment depends very much on the nature and size of the change. Not all of the kinds of change listed above will result in a Reassessment. If a different but well-known organisation, which already has a number of approved Trust Services under its wing, takes over the TSP's ownership, it may be that no Reassessment is needed. If a single simple additional criterion has been added to one of the Service's Approval Profiles, the extra check that this has been satisfied may be trivially small. On the other hand, if a Service is being significantly extended with a major new Service policy options, or a major Profile rewrite has been undertaken, the Reassessment could be extensive.

A Reassessment will only assess changes, and the extent and cost of a Reassessment is strongly related to the nature and size of the change being assessed. However, an Assessor should bear in mind that changes in one area can impact, and thereby indirectly change other areas.

It is the TSP's responsibility[6] to inform *tScheme* of all significant changes of the kinds identified above as soon as they are known about. Assessors will also be apprised of the changes in sufficient detail to enable the points of Reassessment and evidential requirements to be determined. If *tScheme* decides that a Reassessment is indeed needed[7], the TSP should be asked to provide an amended S3A or an addendum to the existing one to capture these details.

6 Indeed it is in *tScheme's* contract with the TSP.

7 *tScheme* may take guidance from Assessors here.

4. EVIDENCE

This section collects together example forms of evidence that have been identified as being acceptable for demonstrating how the various criteria listed in the Approval Profiles have been satisfied. It is intended to act as a checklist and guide. It is by no means definitive, and other forms of evidence may be found equally acceptable by Assessors. Specific forms of evidence for each Assessment should be agreed with the *tScheme*-recognised Assessor before Assessment starts.

Most of the evidence required of a TSP is of the same general form whatever the Service being assessed. Guidance on this is offered below in relation to the criteria of the Base Approval Profile.

For some Approval Profiles however, there are specific standards[8] that could apply, and to which prior conformance could be demonstrated. Thus, rather than offering point by point evidence, a TSP can offer evidence of already established conformance to such standards. For many of the functional Approval Profiles, *tScheme* has identified some candidates. They are listed below under the appropriate profile headings.

4.1 tSd0111 - Base

4.1.1 General

1. Any TSP approval, certification achieved, and for what Services/policies[9].

4.1.2 Business probity and management competence

1. Reports from independent auditing bodies, with due consideration of their professional status and any qualifications within the report;
2. Information from relevant regulatory bodies, such as the FSA or OFTEL, pertinent to the provision of Trust Services;
3. Demonstration of effective documentation and operation of those parts of its Service related policies and procedures required;
4. Implementation of a QMS compatible with [ISO 9001-2000].

4.1.3 Acceptable management and security policies and procedures

1. A documented statement of applicability describing the control measures to be implemented and reasons for their selection to meet the base criteria and any additional specific criteria;
2. Presentation of a documented ISMS, supported by a risk analysis, and an unqualified (i.e. having no reservations) opinion of a qualified external Assessor;
3. Examples of widely recognised standards against which evidence may be offered are:

- [ISO/IEC 17799],
- [BS 7799-2],

8 Within *tScheme*'s Approval Profiles the term 'standard' is intended to include both formal (*de jure*) and *de facto* Standards, recognised industry schemes, and other means of demonstrating levels of performance and practice having similar merit.

9 For example if a Certification Authority has been certified to be conformant with an identified Qualified Certificate policy, whether through *tScheme* or another body.

- [QCP] Sections 7.4.5 to 7.4.7,
- [ANSI X9.79].

4.1.4 Assurance of the technical infrastructure

1. A documented statement of applicability describing the control measures to be implemented and reasons for their selection to meet the base criteria and any additional specific criteria;
2. Documented evidence of the implemented security of the technical infrastructure and any procedures adopted to use and apply these controls;
3. Reference to any evaluation criteria, standards, design, development and assurance methods, that might have been used to build and implement;
4. If an evaluation of any product used was carried out by an independent test house then any documents/certificates relating to this evaluation;
5. If the assurance provided depends on a product Supplier's own declaration of conformity to *tScheme* criteria or equivalent, or if any self-testing or evaluation has been done, then the documented evidence of this.

4.1.5 The suitability of personnel used (skill and competence)

1. Job Descriptions, CVs and training records of the personnel concerned;
2. Auditable records to demonstrate approved definition, modification and application of the required personnel procedures and processes, particularly for those staff in sensitive rôles (with regard to the provision of the Service).

4.1.6 Acceptable quality of externally provided Trust Service Components

1. A clear description of the relationship and dependencies between the SSA and the agents concerned, with risk analysis;
2. Appropriate contract, management and Trust Service documents;
3. The ISMS and operational procedures to show that communications with the agents concerned have been secured to the required level;
4. Evidence of an existing successful *tScheme* Assessment of the agent(s) concerned.

4.1.7 Acceptable quality of suppliers of technology, equipment and general support Services

1. The reputation and track record of the supplier;
2. Appropriate contractual documentation.

4.1.8 Conformance to Service policy and procedure criteria

1. Presentation of appropriate documents, and demonstration of conformant working practices and internal processes to Assessors during on-site visits;
2. Audit records, made available for inspection, which satisfy the Assessors that the necessary audit trails containing appropriate information have been recorded and retained.

4.2 tSd0042 - Registration

There are no standards that tScheme has identified as being especially relevant, though guidelines for the validation of identity of individuals and organisations are being produced by the UK government for use with Government Services (see Government gateway policy documents).

4.3 tSd0102 - Certificate Authority

Where the TSP claims to be issuing Qualified Certificates in conformance with [DIR 99/93], evidence of such must be provided to fully satisfy the Assessors. Such evidence may be provided through demonstrating compliance with [QCP], which has extensive clauses relating to the requirements of this Approval Profile and maps onto [DIR 99/93]. Alternatively the TSP may provide evidence based upon another means of demonstrating conformance to [DIR 99/93] or must itself furnish all evidence and show how compliance with [DIR 99/93] is achieved (but note the related procedure mandated for Assessors by the Required Assessment Procedures).

Compliance with Annex IV of [DIR 99/93] can be demonstrated by conformance to the following or equivalent standards:

1. [CWA14171].

4.4 tSd0103 - Signing Key Pair Management

Compliance with Annex III of [DIR 99/93] can be demonstrated by conformance to the following or equivalent standards:

1. [CWA14167-3] - parts related to the SSCD only;
2. [CWA14169];
3. [PKCS #5] - for the interface between the signing capability provision and the Signature Creation System;
4. [FIPS-140].

4.5 tSd0104 - Certificate Generation

Justification of choice of cryptographic algorithms, together with the requirements on their parameters, can be made by reference to the following or equivalent documents:

1. [ALGO paper].

4.6 tSd0105 - Certificate Dissemination

No specific standards identified.

4.7 tSd0106 - Certificate Status Management

1. [X.509] – sections on CRLs.

4.8 tSd107 - Certificate Status Validation

1. [OCSP];
2. [X.509] - sections on CRLs.

5. REFERENCES

[ALGO paper] ESI Special Report SR 002 176 "Algorithms and Parameters for Secure Electronic Signatures", published March 2003.

[ANSI X9.79] "American National Standard for Financial Services - Part 1: PKI Practices and Policy Framework", ANS X9.79-1: 2001.

[BS 7799-2] "Information Security Management - Part 2: Specification for information security management systems", 2002, published by the BSI, ISBN 0 580 40250 9.

[CWA14167-3] CEN Workshop Agreement 14167-3; Cryptographic Module for CSP Key Generation Services – Protection Profile CMCKG-PP, 2002.

[CWA14169] CEN Workshop Agreement 14169; Secure Signature Creation Devices, version 'EAL 4+', 2002.

[CWA14171] CEN Workshop Agreement 14171; Procedures for Electronic Signature Verification.

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

[FIPS-140] "Security Requirements For Cryptographic Modules", Federal Information Processing Standard Publication 140-2, 1999.

[HMGVInd] "HMG's Minimum Requirements for the Verification of the Identity of Individuals v2.0"

[ISO 9001-2000] "Quality management systems -- Requirements" 2000-12-08

[ISO/IEC 17799] "Information technology - Code of practice for information security management", ISO/IEC 17799:2000, first edition 2000-12-01, ISBN 0 580 36958 7.

[OCSP] "Internet X.509 Public Key Infrastructure Online Certificate Status Profile" (RFC 2560) Feb 2002.

[PKCS #5] "Password-Based Cryptography Standard", RSA Laboratories, v2.0, March 25, 1999.

[QCP] "Policy requirements for certification authorities issuing qualified certificates", ETSI TS 101 456.

[X.509] "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU Recommendation X.509 (03/00).

