Base Approval Profile

Ref. tSd 0111

Issue 3.00

2002-06-25

Executive summary

This document defines the base *tScheme* criteria against which Trust Services and the organisations which provide them must be successfully assessed in order to be eligible for a Grant of Approval or *tScheme*-Ready Status. It is intended to be used in conjunction with individual Approval Profiles specific to particular Service types.

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.
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	Issue	Date	Comment	Authorised
tS	1.00	2001-07-20	First version ratified by the board. This version produced prior to document management procedures introduced 2001-09-21.	*tScheme* Board
tSd	2.00	2001-11-13	Incorporates the following changes: 1. changes reflecting Disposition tS0163 Version 0.03, 2001-07-24. These comprise various minor changes and the addition of text describing the interrelationships between specific Service Profiles, moved and generalised from similar more specific text in the Registration Profile; 2. changes proposed at the P&PC meeting on 2001-10-25 as follows: (a) reference added to ISO 9001:2000; (b) Paragraph 3 of Section 2.1 deleted; (c) change to 3.1 to generalise the requirement for legal conformance and emphasise that it is commitment to complince that is required - *tScheme* Assessors cannot test actual compliance; 3. minor editorial changes, including: correction of syntactic errors, incorporation of document maintenance automation, various minor changes in conformance with new document management standards (including the type letter "d" added to the document reference) and the addition of this document history.	*tScheme* Board
tSd	3-00	2002-06-25	Incorporates the following changes: Editorial: 1. All non-normative text has been removed, including all the guidance text on evidence, which can now be found in Guidance for Assessments. 2. Incorporation of criteria tagging. 3. Addition of a linked Clause compliance table. 4. Incorporation of *tScheme*-Ready text. 5. Normative footnotes have been changed to become in-line notes in order to give them greater prominence. 6. Minor editorial changes to achieve better consistency across the different Approval Profiles. Affecting Assessment: 1. The requirement for regular external audit has been modified to make clear that a *tScheme*-recognised	*tScheme* Board

© *tScheme* Limited, 2002 - all rights reserved

Status	Issue	Date	Comment	Authorised
			assessor is viewed as a suitable external organisation to perform the audit. (BPMC-030). 2. A TSP is now required to show that it understands the legal requirements that apply to it, as well as simply being committed to compliance with them. (BPMC-035) 3. TSP management must now be responsible for actually defining the TSP's information security policy rather than just providing a clear line of responsibility for doing it. (MSPP-030) 4. A requirement for a record of subscriber agreement to be made has been brought in from the CA Profile, where a similar requirement is already present. (SRPP-025) 5. Requirements relating to how and to whom Service information is to be presented have been clarified and harmonised across all of the Approval Profiles. Specific forms of presentation are required, and a distinction is now made between information that is to be provided to users and information that is to be provided for the Assessors. (Sections 3.6.1, 3.6.2 and specifically criteria SRPP-035 and SRPP-290) 6. The "Service Being Provided" requirement has been relaxed to avoid the Catch 22 situation of *tScheme* requiring a Service to be already in use with customers who may not be prepared to use it until it has acquired *tScheme* approval. (SRPP-005) 7. Text on the following topics, originally provided in Guidance for Assessors has now been moved here, as it is now viewed as contributing in a normative manner: • instructions not to assess financial probity; (ELC-060) • a rule about assessing liability; (SRPP-090) • rules about timestamping; (MSPP-130) • rules to help decide whether the right things are being recorded; (MSPP-040) • what constitutes an acceptable subscriber agreement; (SRPP-025) • instruction to Assessors relating to legal issues; (SRPP-310 and at the start of Schedule 1) • clarification of what is meant by "Job Description"; (SPU-040) • text on assessing external agents; (at the start of Section 3.5.1) • what is meant when information is required to be "made available" and "communicated"; (SRPP-010) • elaboration of what is meant by "appropriate" in Schedule 1.	

© *tScheme* Limited, 2002 - all rights reserved

CONTENTS

1. INTRODUCTION 5

1.1 CONVENTIONS 5
1.2 GENERAL 5

2. SCOPE AND RELATION TO SPECIFIC SERVICE PROFILES. 6

3. THE BASE CRITERIA 7

3.1 BUSINESS PROBITY AND MANAGEMENT COMPETENCE 7
3.2 MANAGEMENT AND SECURITY POLICIES AND PROCEDURES 8
3.3 ASSURANCE OF TECHNICAL INFRASTRUCTURE 10
3.4 SUITABILITY OF PERSONNEL USED 10
3.5 EXTERNAL RELATIONSHIPS 12
3.5.1 Externally provided Trust Services and Trust Service Components 12
3.5.2 Suppliers of technology, equipment and general support services 14
3.6 SERVICE RELATED POLICIES AND PROCEDURES 14
3.6.1 Information for users 15
3.6.2 Information for Assessors 18

SCHEDULE 1. ENTERPRISE LEVEL CRITERIA 20

SCHEDULE 2. SERVICE POLICY DISCLOSURE STATEMENT 22

4. REFERENCES 23

ANNEX 1. CLAUSE COMPLIANCE LIST 24

© *tScheme* Limited, 2002 - 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

This Approval Profile is one of a number developed by *tScheme* against which TSPs offering Trust Services may be assessed by *tScheme*-recognised Assessors. It addresses the basic criteria that all TSPs must satisfy in order to provide an approved Trust Service. It shall, as a minimum, be applied in combination with one of the Service specific Approval Profiles.

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.

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" shall be taken to mean "Component Supplier";
- references to "Service" shall be taken to mean "Service Component";
- references to "Service Subject to Assessment", or SSA, shall be taken to mean "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, 2002 - all rights reserved

2. SCOPE AND RELATION TO SPECIFIC SERVICE PROFILES.

The criteria laid down here do not by themselves form the full basis for an Assessment under *tScheme*. This document shall be used in conjunction with one or more individual Service-related Approval Profiles. Each of these focuses on a particular indivisible set of Trust Service functions, though the full Service actually provided by any given TSP will commonly be constructed from more than one of these. The *tScheme* website lists the functions for which Profiles have been developed. An individual Trust Service offered for Assessment under these Profiles is known as the Service Subject to Assessment, or SSA.

© *tScheme* Limited, 2002 - all rights reserved

3. THE BASE CRITERIA

Criteria are listed under assessment topics. For each topic, the basic assessment criteria are identified.

The topics are:

- business probity and management competence;
- management and security policies and procedure;
- assurance of technical infrastructure;
- suitability of personnel use;
- external relationships, including:
  - externally provided Trust Services and Service Components;
  - relationships with suppliers of technology, equipment and general support services;
- Service related policies and procedures.

Compliance with this Approval Profile will then be achieved by satisfying the criteria in the succeeding sub-sections.

3.1 Business probity and management competence

BPMC-010 Proper and sound organisation - see Schedule 1

The TSP shall be competent and shown to be a fit, proper and sound organisation to carry out its role. It shall be a legitimate organisation, adequately resourced for the nature of the work undertaken and with trustworthy and capable management. These "Enterprise Level" criteria are detailed in Schedule 1 to this document.

BPMC-020 Regular internal audit

To demonstrate a continued acceptable level of competence, and adequate resource levels, the TSP's working methods, policies, procedures and management shall be regularly audited for effective execution by internal audit functions independent of the parts of the organisation being *tScheme* assessed.

BPMC-030 Regular independent external audit

To demonstrate a continued acceptable level of competence, and adequate resource levels, the TSP's working methods, policies, procedures and management shall be regularly audited for effective execution at least annually by an independent organisation of qualified and approved auditors, or a *tScheme*-recognised Assessor.

© *tScheme* Limited, 2002 - all rights reserved

BPMC-035 Understanding of, and commitment to legal requirements

The TSP shall show that it understands the legal requirements that are applicable to the Service, and shall demonstrate its commitment to comply with them[1]. These are very likely to include:

BPMC-040 Compliance with data retention legislation

- Data Retention: laws relating to the protection of important information from loss, destruction, unauthorised amendment and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities;

- Data Protection: many countries have enacted data protection legislation. Issues especially likely to be emphasised are:

BPMC-050 Technical compliance with data protection legislation

  - the technical and organisational measures that must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;

BPMC-060 Disclosure compliance with data protection legislation

  - assurance that the information that subscribers contribute to the TSP is protected from disclosure unless with their agreement or by court order or other legal requirement.

3.2 Management and security policies and procedures

MSPP-010 Documented risk assessment

The TSP shall carry out a risk assessment to evaluate business risks and determine the security requirements and operational controls necessary to manage and reduce risk to a level commensurate with the Trust Service being assessed. The risks identified and the countermeasures implemented to mitigate and manage those risks shall be documented.

MSPP-020 Adequacy of administrative and management procedures

The TSP shall ensure that administrative and management procedures (sometimes known as an Information Security Management System or ISMS) are applied that are adequate and are based upon recognised standards.

In particular:

MSPP-030 Defined InfoSec Policy

- the TSP management shall provide direction on information security by defining the TSP's information security policy and ensuring publication and communication of the policy to all employees who are affected by the policy;

1 Although this requirement might seem obvious, its purpose is to ensure that the TSP demonstrates to the Assessors its commitment to compliance.

© *tScheme* Limited, 2002 - all rights reserved

MSPP-040 Maintenance of InfoSec infrastructure

- the information security infrastructure necessary to manage the risks within the TSP shall be maintained at all times. Any changes that will affect the level of security provided shall be approved by the TSP management;

MSPP-050 Security controls and operating procedures

- the security controls and operating procedures for TSP facilities, systems and information assets providing the Trust Services shall be documented, implemented and maintained. This documentation shall identify all relevant targets, objects and potential threats related to the Services provided and the safeguards required to avoid or limit the effects of those threats. It shall describe the rules, directives and procedures regarding how the specified Services and the associated security assurance are granted in addition to stating policy on incidents and disasters.

MSPP-060 Best practice ISMS

The process of Risk Assessment and the development of the ISMS shall be fit for purpose. It is therefore recommended that the process used aligns with current best practice as accepted by the information security industry.

Because of the nature of the Services offered by TSPs, it is considered especially important that policies and procedures are put in place to cover the following areas (where applicable), which are not normally sufficiently emphasized in more general recommendations:

MSPP-070 Management of cryptographic hardware

- management of cryptographic hardware, including uninitialised personal hardware tokens and those that have been personalised prior to delivery to the subscriber, etc.;

MSPP-080 Usage of non-trusted channels

- usage of non-trusted channels for exchange of information with subscribers and agents (for example postal, telephone, and so on);

MSPP-100 Duress events

- detection and management of events by subscribers under duress.

- Specific criteria are applied in the following areas:

MSPP-110 Contingency plans

- contingency plans shall be drawn up, which show how, in the event of a disaster, including compromise of the TSP's own confidential data[2], operations will be able to be restored;

MSPP-120 Confidentiality & integrity of records

- the confidentiality and integrity of current and archived records concerning Service deliverables shall be preserved where appropriate;

2 For example the TSP's private cryptographic signing key(s).

© *tScheme* Limited, 2002 - all rights reserved

MSPP-130 Recording of time of events

- the precise time of significant TSP management events[3] shall be recorded;

NOTE:

In general, the time of a recorded event will be part of the record of the event. The TSP shall state in its practices the accuracy of the clock used in timing of events, and how this accuracy is ensured. Any difference from actual time shall not affect either the value of the event record when used in evidence in a court of law, or any reliance decision based on knowing when the event took place. The TSP shall make the degree of precision clear.

MSPP-140 Logging of events

- recorded events shall be logged and retained, with appropriate protection according to regulatory obligations and risk management requirements.

NOTE:

Criteria relating to which operational Service-related events must be recorded are laid down in the specific Service Approval Profiles, but there are also more general events related to the security and general management of the Service. Assessors shall bear in mind the purpose of this record keeping in deciding whether a particular record needs to be kept. Specifically they shall ask themselves "is the record needed as part of the Assessor's Service Definition, either implicit or explicit?".

Also of special interest here is the question of the level of proof needed that some event has or has not occurred, and the implications on how, and what details about, an event is recorded. What is reasonable depends on the level of reliance on the event, both by the TSP itself (guarding itself against litigation) and by other parties who might be involved, such as the subscriber or relying party. Assessors shall ask themselves:

- Will the record be needed in evidence should a dispute arise?
- Will the record be valuable in a forensic examination should a security breach be detected or suspected?
- Does the law require the record to be kept? Although it could be argued that it is the authorities' task to ensure compliance with the law in this respect is not an Assessor's, in general this is not *tScheme*'s position. Legal compliance is a quality issue - a particularly serious one. The *tScheme* Mark is a quality mark so this compliance needs to be looked at.

3.3 Assurance of technical infrastructure

ATI-010 Inclusion of security control measures

The TSP shall build security control measures into the technical infrastructure that, in conjunction with physical and administrative measures, will provide the level of protection and degree of assurance required to manage the areas of risk identified in conformance with the ISMS.

3.4 Suitability of personnel used

SPU-020 Personnel trustworthiness assessed within risk assessment

The security requirements and operational controls associated with the trustworthiness of personnel shall be addressed within the risk assessment.

3 For example environmental, key management and certificate management events.

© *tScheme* Limited, 2002 - all rights reserved

The TSP shall ensure that personnel and hiring practices enhance and support the trustworthiness of the TSP's operations. In particular:

SPU-030 Personnel skills re. job function

- the TSP shall employ personnel who possess the expert knowledge, experience and qualifications necessary for the offered Services and as appropriate to the job function;

SPU-040 Defined security rôles

- security rôles and responsibilities, as specified in the TSP's security policy, shall be documented in job descriptions. Trusted rôles, on which the security of the TSP's operation is dependent, shall be clearly identified;

NOTE:

Where the term "job description" appears in this document it shall be interpreted by Assessors with some latitude. There is no intent to mandate a formal document with that title, rather it shall be interpreted as requiring that the scope and content of the jobs in question shall be clearly documented in some form.

SPU-050 Separation of duties and privileges

- TSP personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and TSP specific functions. These shall include skills and experience requirements;

SPU-060 Exercise of procedures and processes in line with ISMS

- personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures;

SPU-070 No conflicts of interest

- TSP personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the TSP operations.

© *tScheme* Limited, 2002 - all rights reserved

3.5 External relationships

The criteria in this section relate to the use of externally provided Trust Services operating within the SSA, Service Components operating within the SSA, and suppliers of technology, equipment and general support services.

3.5.1 Externally provided Trust Services and Trust Service Components

A TSP may offer for *tScheme* Assessment an SSA that is dependent on externally provided Trust Services or Trust Service Components. For example, a TSP may submit for *tScheme* Assessment a Certification Authority Service that uses a Registration Service supplied by one or more external agents[4]. However, while operations may be delegated, responsibility and liability for Service provision cannot. The criteria below are identified to enable *tScheme*'s recognised Assessors to ensure that the overall quality and security of the SSA being offered is not prejudiced by any insecurities in the Services or Components upon which it depends.

A full assessment of an agent could in principle be as large a task as the Assessment of the controlling TSP itself and in some cases this level of assessment will be necessary. However there are also situations in which this expense can be avoided. The extent and nature of the requirement for an external agent assessment depends on a number of factors:

- their existing assessment status and track record.

  An agent may already have been assessed for *tScheme* approval, either through a formal Assessment or in some other way. Assessors shall use their judgement as to the applicability and scope of such assessments. They shall also be careful to ensure that the operational interface to the agent and the management relationship with the agent satisfy the *tScheme* criteria.

- the results of the risk analysis.

  The more critical the role of the agent, the more important it is to ensure that the agent is performing properly and the wider the area of assessment. Two examples may illuminate:

  - If a Registration Authority is outsourcing Certification Services and it wishes these Services to be included in the Service being assessed, then the Certification Services and the agent providing them will need to be assessed (or to have been assessed) to the same depth as the registration functions - they are equally important.

  - If a Certificate Status Validation Service outsources its CRL database servers to an external agent, the dependency is much lower. The prime need would be to assess the external agent only in terms of the denial of service threat.

- the number, type and size of the agents.

  In some cases, particularly in the case of Registration Authority agents, there may be a large number of small agents operating a part of the Service. It is clearly not feasible to perform in-depth assessments of each of many thousand agents. In this situation a spot check approach is appropriate, the percentage of agents examined depending both on the other factors identified above and the results of the spot check; if the spot check raises an unexpected number of

4 The term "agent" is intended here to include all forms of external supplier, ranging from an individual person to a fully fledged independent TSP.

© *tScheme* Limited, 2002 - all rights reserved

concerns, coverage may have to be extended to get a more reliable sample. It may be useful for the TSP to categorise agents in terms of the value of Service that can be provided through them. The Assessor can then take special steps to assess the agents through which the higher Service values can be obtained[5].

When a TSP offers for *tScheme* Assessment an SSA that is dependent on one or more Trust Services or Trust Service Components provided by external agents, the TSP shall provide a risk assessment to include analysis of:

XPTC-010 Risk assessment of inter-organisational communications security

- inter-organisational communications security;

XPTC-020 Risk assessment of dependence upon agents

- the degree of dependence on the agents concerned;

XPTC-030 Risk assessment of error or malice by agents

- the likelihood and consequences to the SSA of agent error or malice.

Then, to a level appropriate to the conclusions of that analysis[6], the TSP shall:

XPTC-040 Legal status and probity of agent

- verify that the agent is an organisation of a legal status and probity consistent with the criteria laid down in Schedule 1;

XPTC-050 Agents' admin and security policy & procedures

- agree by contract that the agent will apply administrative and security policies and procedures consistent with *tScheme* approval of the type of Service or Component it is providing;

XPTC-060 Agents' Admin and Service Policy & Practices

- agree by contract that the agent will apply and publish Service Policy and Practice Statements consistent with *tScheme* approval of the type of Service or Component it is providing;

XPTC-070 Verification of agents' adherence to contractual commitments

- verify that the above contractual commitments are being honoured by the agent on a regular or spot check basis appropriate to the number and size of providers involved;

XPTC-080 Agent's agreement to *tScheme* Assessment

- contract with the agent that it agrees to subject its Service or Component to a *tScheme* Assessment or follow-on Assessment check, should the *tScheme*-recognised Assessor decide to do this. Such a check will not be necessary if either the agent's Service has already been *tScheme* approved, or the agent's Component is already recognised as being *tScheme*-Ready, or the Assessor can otherwise be convinced that no Assessment of the agent's Service or Component will be required[7];

5 For example, only a few registration authority agents from the thousands being used may be explicitly identified as being able to support the provision of specific, especially valuable certificate types. Such agents may even be persuaded to help pay for the special attention they will be receiving, on the grounds that their marketability will thereby be raised.

6 Details will be discussed on a case by case basis early in the Assessment process, and agreed between the *tScheme*-recognised Assessors and the TSP.

7 For example if the risk assessment has shown that the level of dependence on it is sufficiently low, or it has been approved in some way under another approval scheme recognised in whole or in part by *tScheme*.

© *tScheme* Limited, 2002 - all rights reserved

XPTC-090 Suitability of agents' personnel

- ensure that the agent will satisfy *tScheme* criteria in relation to the suitability of personnel used;

XPTC -100 Agents' technical assurance level

- ensure that the agent's technical infrastructure assurance levels are compatible with those of the Service or Component jointly being provided;

XPTC-110 Agent TSP communications security

- implement an appropriate level of inter-organisational communications security;

XPTC-120 Agents' accountability

- monitor and record agent actions in such a manner that for each SSA deliverable, the identity of, and actions taken by, the agent(s) contributing to that deliverable can be traced (accountability is the issue here).

XPTC-130 Agents providing higher levels of trust

A TSP may nominate specific external agents for use in the provision of higher levels of SSA trust. Depending on the trust level required and the agent related risk analysis described above, such agents may all be required to be *tScheme* assessed. Approval of the SSA would then require the achievement of the higher trust level to be conditional on use of these agents.

3.5.2 Suppliers of technology, equipment and general support services

Suppliers of underlying Trust Service technology, such as cryptographic software, hardware and communications fall into this category, as well as more general service suppliers such as office services and physical security services.

STES-010 Include suppliers in Service risk assessment

To the extent that the security of the SSA is dependent on such suppliers, the TSP shall consider them in the Service risk analysis and take appropriate steps[8] to ensure that their probity, competence and security matches the risks they might pose.

3.6 Service related policies and procedures

This section gives criteria which, although Service orientated, can be expressed in general terms and, although the responses will often be Service specific, are generally applicable across a wide range of functionality.

A "Specification of Service Subject to Assessment" (S3A) as defined in "Model Specification of Service Subject to Assessment" shall be produced.

SRPP-005 Operational Service

Each SSA must be an Operational Service (in the sense defined in the *tScheme* Glossary of Terms) supporting the statements given for it in response to the criteria listed in Subsections 3.6.1 and 3.6.2 below.

8 In practice, the appropriate step will mainly be choosing an appropriate supplier, but contractual steps can also be taken to ensure product quality and help underwrite risk.

© *tScheme* Limited, 2002 - all rights reserved

3.6.1 Information for users

SRPP-010 Public Service Description

A description of the scope and content of each SSA, the Public Service Description (PSD), which shall also include a description of the subscriber and expected relying party community to which the Service applies, shall be made publicly available by the TSP.

NOTE:

There is a distinction between information that must be "made available" to other parties and information that must be "communicated" to them. These shall be interpreted as follows:

Making information available.	Information is made available to a party if it is published in a form accessible to the party in a place that the party might reasonably expect to find it, for example in a clearly identifiable page on the TSP's website. It is also made available if it is provided promptly on request through a mechanism that is widely published and easy to find and use. Finally, it is also made available if it is directly communicated to the party (see next).
Communicating information.	Information is communicated to a party if it is passed to them directly, for example by hand, by email or by post.

In order to better interpret the distinction, it is helpful to understand the rationale behind it. The assumption is that a TSP cannot be expected to communicate information to parties the TSP does not know about, though it can be expected to make it available to them through publication. Also, in some cases, although the TSP may know the party, for some types of information, the party may not wish it to be pushed at them, so publication will suffice. If the TSP does know the parties concerned, and the information should certainly be known to them, it is reasonable to expect that the TSP make sure they get the information by having it 'communicated' (i.e. passed) to them directly.

SRPP-020 Communication of decisions and deliverables

Service decisions and deliverables shall be communicated (see note above) with integrity and, where appropriate to the Service being provided, confidentiality, to the subscriber, to any other approved third parties[9] and to any follow-on dependent Trust Services.

9 Examples are: relying parties, and other Trust Service Providers with whom peer relationships have been established such as might happen in a cross-certification situation.

© *tScheme* Limited, 2002 - all rights reserved

SRPP-025 Record of subscriber agreement

The TSP shall record the Subscriber's agreement to the terms and conditions of the Service.

NOTE:

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 (the 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 required, both to protect the subscriber from accidental agreement and to protect the TSP in case of dispute.

SRPP-030 Communication of changes to Service

If any terms and conditions have changed for a subscriber revisiting a Trust Service, the changes shall be communicated to the subscriber and agreed as if for a new subscriber.

SRPP-035 Service Policy and Service Practice Statement

A Service Policy (SP) and a Service Practice Statement[10] (SPS) shall be produced. Although they need not be in separate publications, if they are in the same publication they must be distinctly identifiable as separate parts of the publication.

The following information shall be present in either the Service's SP, SPS or PSD, as appropriate to the nature of the information and the objectives of an SP, SPS or PSD:

SRPP-040 TSP normal obligations

- obligations of the TSP in normal operation;

SRPP-050 TSP unavailability obligations

- obligations of the TSP in the event of Service unavailability;

SRPP-060 Jurisdiction under which Service provided

- the legal system by which the Service Provider will be bound;

SRPP-070 Subscriber's obligations

- obligations of the subscriber, primarily in respect of contracted subscriber liability, and subscriber actions that would absolve the Service Provider from liability;

SRPP-080 Notifications to relying parties

- notifications and advice given to relying parties, primarily in respect of steps that relying parties are expected to take (e.g. verification steps) for any liability to be enforced on the subscriber or accepted by the Service Provider;

10 As defined in the *tScheme* Glossary of Terms.

© *tScheme* Limited, 2002 - all rights reserved

SRPP-090 Statement of liability

- liability accepted and liability limitations (the stated accepted liabilities shall at least match the legally enforceable minimum);

NOTE:

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. What is important is that the TSP declares conspicuously, clearly and fairly, exactly what liability it accepts.

SRPP-100 Statement of warranty

- warranties to subscribers;

SRPP-120 Applicable privacy and data protection provisions

- subscriber privacy and relevant national Data Protection legislation provisions;

SRPP-130 Principles of Service operation

- principles of operation of Service specific procedures;

SRPP-140 Subscriber Service usage

- how a subscriber initiates use of, and continues to use the Service;

SRPP-150 Acceptance of subscriber change of status notification

- procedures for acceptance of notification of subscriber status change;

SRPP-160 Publication of subscriber change of status

- procedures for publication of subscriber status change to subscribers and other dependants;

SRPP-170 Changes to policy & practice

- procedures for changes in Service Policy and Practice;

SRPP-180 Service termination

- procedures in case of Service termination;

NOTE:

Suitable procedures are outlined in Section 7.4.9 of [QCP].

SRPP-190 Contact details for the TSP

- how and when subscribers can contact the TSP;

SRPP-210 Physical access to the Service

- any obligation of the TSP to supply physical access to Service;

SRPP-230 Conditions for notification of decisions

- conditions under which Service decisions will be notified to third parties;

© *tScheme* Limited, 2002 - all rights reserved

SRPP-240 Methods of notification of decisions

- description of methods by which Service decisions and deliverables will be notified to third parties;

SRPP-250 Query & complaint procedures

- policy and procedures for dealing with queries and complaints;

SRPP-280 Availability of information to interested parties

The Service Policy and Public Service Description shall clearly and conspicuously be made available to potential users of the Service (including relying parties) through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language. Those parts of the Service Practice Statement intended for users shall similarly be made conspicuously available.

SRPP-290 Publication of a Service Policy Disclosure Statement

Of these items, the ones listed below in Schedule 2 shall clearly and conspicuously be made available by the TSP in a separate Service Policy Disclosure Statement (SPDS)[11] to its community of users, for each SSA it provides[12].

3.6.2 Information for Assessors

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

SRPP-300 Processes for audit of TSP

- audit processes, i.e. the ways in which the correct operation of Service processes are audited;

SRPP-310 Retention of audit records

- policies and procedures for maintaining and retaining secure evidence and audit trail records of Service specific operations. Records shall be sufficient to be able to provide evidence of Service delivery for the purposes of legal proceedings;

NOTES:

- Legal proceedings may arise after a considerable period (e.g. long term contracts such as pensions).
- If a record is related to a Service deliverable, it shall be kept long enough to cover declared usage of that deliverable (for example the declared supported lifetime of signed data).
- The appropriate life of a forensic record is a matter of judgement, though there may also be a legal minimum life for such a record.

11 Note that the SPDS is merely a generalised form of what is known as a PKI Disclosure Statement. It contains essentially the same contents, but depending on the type of Service, may be expressed in any of a number of different forms.

12 This may result in these items being documented in more than one place, since they will commonly appear in the full Service Policy and Practice Statement, but the underlying objective remains to ensure that users will find this information easy to obtain and understand, by it being separated out and expressed in suitable terms for user consumption. In some legislative regimes TSPs may find that they are obliged by law to provide much of this information in a separate document.

© *tScheme* Limited, 2002 - all rights reserved

SRPP-320 Contracts with other TSPs

- contractual relationships with other TSPs (although the details of these contracts may be largely confidential, evidence of any required features specified in Section 3.5 shall be provided);

SRPP-330 Confirmation of completion

- procedures to ensure secure and timely confirmation of Service completion.

© *tScheme* Limited, 2002 - all rights reserved

SCHEDULE 1. ENTERPRISE LEVEL CRITERIA

Whenever the term "enterprise" is used in this Schedule, it is qualified to refer either to:

- the enterprise which, or individual who, is actively performing the Trust Service and is responsible for its day to day operation, i.e. the operational enterprise;

OR

- the enterprise which controls the operational enterprise, i.e. the controlling parent enterprise;

OR

- the enterprise with which the subscriber has a contractual relationship, i.e. the Service offerer.

These distinctions may merely reflect aspects of the same single enterprise, or they may refer to truly separate ones. The criteria laid out below are couched in terms of these different enterprise aspects or enterprises.

Either the operational enterprise or its parent enterprise shall be able to demonstrate that it has an appropriate legal status.

NOTE:

The size and sophistication of organisations applying for *tScheme* approval may vary from being one single individual, for example a Notary Public applying for approval as a registration authority, to being a large multinational corporation applying for approval of multiple complex Trust Services. The word "appropriate" is used here to permit Assessors to use their judgement in deciding on requirements relating to legal status, the sophistication of the TSP's ISMS, contractual arrangements, and level and type of documentation.

Specifically, it shall provide:

ELC-010 Registration of the business

- evidence of its establishment / registration (as required by the law of the territory in which it is established);

ELC-020 Relationship to parent

- in the case of a separately identifiable parent organisation, evidence of the specific relationship between this parent entity and the operational enterprise[13].

ELC-030 Legal status

If the Service offerer is neither the operational enterprise nor its parent, it shall similarly demonstrate its legal status.

The operational enterprise shall demonstrate that:

ELC-040 Distinct management structure and operations

- it safeguards impartiality of operations by having a documented and distinct management structure and a separately documented set of management policies, controls and procedures for the Trust Services provided;

13 The purpose of this requirement is to ensure that the Provider is sufficiently identifiable to enable it to be made legally accountable for its actions.

© *tScheme* Limited, 2001 - all rights reserved

NOTE:

Issues of management autonomy, financial independence and parental responsibility need to be covered. The operational enterprise may be dependent on the parent for provision of premises, IT systems, recruitment etc. It is possible for it to be subject to corporate policies which conflict with *tScheme*, therefore there needs to be recognition and acceptance of such obligations by the parent.

ELC-050 Appropriate quality management system

- it has a quality management system appropriate for the Trust Services it is providing;

ELC-060 Appropriate information security management system

- it has a information security management system appropriate for the Trust Services it is providing;

ELC-070 Stability and resources

- it has the stability and resources required for supplying electronic Trust Services;

NOTE:

Financial soundness is not in scope. 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 considered to be viable (by some). With the exception of specific criteria identified explicitly in the Approval Profiles, such as a TSP's ability to underwrite its liabilities, Assessors shall not assess financial probity.

ELC-080 Sufficiency of personnel

- it employs a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide electronic Trust Services to the published availability;

ELC-090 Outsourcing agreements

- it has a properly documented agreement and contractual relationship in place where the provisioning of Services involves subcontracting, outsourcing or other third party arrangements (see Section 3.5 for more details of this requirement).

The Service offerer shall demonstrate that:

ELC-100 Query & complaint procedures

- it has policies and procedures for the resolution of complaints and disputes from customers received from customers or other parties about the provisioning of electronic Trust Services or any other related matters;

ELC-110 Liability underwritten

- it has adequate arrangements to cover liabilities arising from its operations and/or activities.

ELC-120 Address for serving legal notices

The Service offerer shall supply an address at which legal notices can be served.

© *tScheme* Limited, 2001 - all rights reserved

SCHEDULE 2. SERVICE POLICY DISCLOSURE STATEMENT

For each SSA, the following information shall clearly and conspicuously be made available by the TSP to its community of subscribers and relying parties. It shall be sufficiently up-to-date and accurate as to not, at any time, mislead subscribers or relying parties:

STATEMENT TYPES	STATEMENT DESCRIPTIONS
TSP contact information:	The name, location and relevant contact information for the TSP
Relying Party validation procedures and usage:	A description of the different classes of Service offered by the TSP, corresponding validation procedures[14], and any restrictions on usage of the Service deliverables[15].
Reliance limits:	The reliance limits, if any.
Obligations of subscribers:	The description of, or reference to, the critical subscriber obligations[16].
Checking obligations of relying parties:	The extent to which relying parties are obliged to check the status of Service deliverables, and references to further explanation[17].
Limited warranty & disclaimer/Limitation of liability:	Summary of the warranty[18], disclaimers, limitations of liability and any applicable warranty or insurance programs.
Applicable agreements, Service Practice Statement, Service Policy:	Identification and references to applicable agreements[19] and Service Policy and Practice statements.
Privacy policy:	A description of and reference to the applicable privacy policy, if any.
Refund policy:	A description of and reference to the applicable refund policy, if any.
Applicable law and dispute resolution	Statement of the choice of law and dispute resolution mechanism.
TSP and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs and a description of the audit process[20] and, if applicable, the audit firm

14 This refers to validation procedures to be followed by relying parties, including any Trust Services relying on the SSA. In the case of a certificate service, this may simply reference the X.509 certificate processing rules.

15 Including the requirements to qualify as a subscriber or relying party and any restrictions on the applications for which the Service deliverables (such as registered subscriber credentials, or certificates, or time-stamps) are approved to be used.

16 Including the requirement to protect the confidentiality of the subscriber's private information used in the SSA (such as a private key or password or private personal data), and report actual or suspected compromise or change of material circumstances.

17 There are two aspects to this: a requirement, where applicable, to check that the relied upon Service deliverable has not been revoked for any reason, and a requirement to protect the integrity of the means of verification of the deliverable (for example, in the case of a certification authority, its public key). Optionally, instructions for retrieving Service deliverables (e.g. certificates issued by the CA) should be given.

18 Including whether, and the extent to which, the TSP warrants the accuracy of the information contained in the Service deliverable.

19 Including the Service Practice Statement and the Service Policy, particularly the latter if the Service Policy Disclosure Statement is simply an extract from the Service Policy.

20 Including a reference to current specific *tScheme* and other audit reports.

© *tScheme* Limited, 2001 - all rights reserved

4. REFERENCES

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

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

© *tScheme* Limited, 2001 - all rights reserved

ANNEX 1. CLAUSE COMPLIANCE LIST

Base Approval Profile - clause compliance list

Clause	Description	Compliance
BPMC-010	Proper and sound organisation - see Schedule 1	
BPMC-020	Regular internal audit	
BPMC-030	Regular independent external audit	
BPMC-035	Understanding of, and commitment to legal requirements	
BPMC-040	Compliance with data retention legislation	
BPMC-050	Technical compliance with data protection legislation	
BPMC-060	Disclosure compliance with data protection legislation	
MSPP-010	Documented risk assessment	
MSPP-020	Adequacy of administrative and management procedures	
MSPP-030	Defined InfoSec Policy	
MSPP-040	Maintenance of InfoSec infrastructure	
MSPP-050	Security controls and operating procedures	
MSPP-060	Best practice ISMS	
MSPP-070	Management of cryptographic hardware	
MSPP-080	Usage of non-trusted channels	
MSPP-100	Duress events	
MSPP-110	Contingency plans	
MSPP-120	Confidentiality & integrity of records	
MSPP-130	Recording of time of events	
MSPP-140	Logging of events	
ATI-010	Inclusion of security control measures	

© *tScheme* Limited, 2001 - all rights reserved

Base Approval Profile - clause compliance list

Clause	Description	Compliance
SPU-020	Personnel trustworthiness assessed within risk assessment	
SPU-030	Personnel skills re. job function	
SPU-040	Defined security rôles	
SPU-050	Separation of duties and privileges	
SPU-060	Exercise of procedures and processes in line with ISMS	
SPU-070	No conflicts of interest	
XPTC-010	Risk assessment of inter-organisational communications security	
XPTC-020	Risk assessment of dependence upon agents	
XPTC-030	Risk assessment of error or malice by agents	
XPTC-040	Legal status and probity of agent	
XPTC-050	Agents' admin and security policy & procedures	
XPTC-060	Agents' admin and Service policy & practices	
XPTC-070	Verification of agents' adherence to contractual commitments	
XPTC-080	Agent's agreement to *tScheme* Assessment	
XPTC-090	Suitability of agents' personnel	
XPTC -100	Agents' technical assurance level	
XPTC-110	Agent TSP communications security	
XPTC-120	Agents' accountability	
XPTC-130	Agents providing higher levels of trust	
STES-010	Include suppliers in Service risk assessment	
SRPP-005	Operational Service	
SRPP-010	Public Service Description	

© *tScheme* Limited, 2001 - all rights reserved

Base Approval Profile - clause compliance list

Clause	Description	Compliance
SRPP-020	Communication of decisions and deliverables	
SRPP-025	Record of subscriber agreement	
SRPP-030	Communication of changes to Service	
SRPP-035	Service Policy and Service Practice Statement	
SRPP-040	TSP normal obligations	
SRPP-050	TSP unavailability obligations	
SRPP-060	Jurisdiction under which Service provided	
SRPP-070	Subscriber's obligations	
SRPP-080	Notifications to relying parties	
SRPP-090	Statement of liability	
SRPP-100	Statement of warranty	
SRPP-120	Applicable privacy and data protection provisions	
SRPP-130	Principles of Service operation	
SRPP-140	Subscriber Service usage	
SRPP-150	Acceptance of subscriber change of status notification	
SRPP-160	Publication of subscriber change of status	
SRPP-170	Changes to policy & practice	
SRPP-180	Service termination	
SRPP-190	Contact details for the TSP	
SRPP-210	Physical access to the Service	
SRPP-230	Conditions for notification of decisions	
SRPP-240	Methods of notification of decisions	
SRPP-250	Query & complaint procedures	

© *tScheme* Limited, 2001 - all rights reserved

Base Approval Profile - clause compliance list

Clause	Description	Compliance
SRPP-280	Availability of information to interested parties	
SRPP-290	Publication of a Service Policy Disclosure Statement	
SRPP-300	Processes for audit of TSP	
SRPP-310	Retention of audit records	
SRPP-320	Contracts with other TSPs	
SRPP-330	Confirmation of completion	
ELC-010	Registration of the business	
ELC-020	Relationship to parent	
ELC-030	Legal status	
ELC-040	Distinct management structure and operations	
ELC-050	Appropriate quality management system	
ELC-060	Appropriate information security management system	
ELC-070	Stability and resources	
ELC-080	Sufficiency of personnel	
ELC-090	Outsourcing agreements	
ELC-100	Query & complaint procedures	
ELC-110	Liability underwritten	
ELC-120	Address for serving legal notices	

© *tScheme* Limited, 2001 - all rights reserved