Base Approval Profile

Ref. tSd0111

Issue 2.00

2001-11-13

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 approval. 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 interrelation-ships 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 compliance 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

© *tScheme* Limited, 2001 - all rights reserved

CONTENTS

1. INTRODUCTION **4**

2. SCOPE AND RELATION TO SPECIFIC SERVICE PROFILES **5**

2.1 SPECIFIC SERVICE PROFILES AND THEIR INTERRELATIONSHIPS 5

3. THE BASE CRITERIA **6**

3.1 BUSINESS PROBITY AND MANAGEMENT COMPETENCE 6
3.1.1 Criteria: *6*
3.1.2 Example evidence: *7*
3.2 MANAGEMENT AND SECURITY POLICIES AND PROCEDURES 7
3.2.1 Criteria: *7*
3.2.2 Example evidence: *8*
3.3 ASSURANCE OF TECHNICAL INFRASTRUCTURE 8
3.3.1 Criteria: *8*
3.3.2 Example evidence: *8*
3.4 SUITABILITY OF PERSONNEL USED 9
3.4.1 Criteria: *9*
3.4.2 Example evidence: *9*
3.5 EXTERNAL RELATIONSHIPS 10
3.5.1 Externally provided Trust Service components *10*
3.5.2 Suppliers of technology, equipment and general support services *11*
3.6 SERVICE RELATED POLICIES AND PROCEDURES 11
3.6.1 Criteria: *11*
3.6.2 Example evidence: *13*

SCHEDULE 1. ENTERPRISE LEVEL CRITERIA **14**

SCHEDULE 2. SERVICE POLICY DISCLOSURE STATEMENT **15**

SCHEDULE 3. CONSOLIDATED LIST OF FORMS OF EVIDENCE **16**

4. REFERENCES **18**

© *tScheme* Limited, 2001 - all rights reserved

1. INTRODUCTION

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 must, 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

© *tScheme* Limited, 2001 - 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 must be used in conjunction with one or more individual service related Approval Profiles. Each of these focuses on a particular indivisible Trust Service component, though the full service actually provided by any given TSP will commonly be constructed from multiple component parts. The *tScheme* website lists the components for which Profiles have been developed. The individual Trust Services offered for assessment under these Profiles are known as Services Subject to Assessment, or SSA.

2.1 Specific service Profiles and their interrelationships

Some types of service may be offered for deployment either as a complete service in itself or as part of a multiple component overall service.

In the first case, the TSP may wish to make claims relating to an overall type of service of which the offered service may either in future become a part or to which it may become a supplier. For example a TSP may claim that its offered Registration Service is suitable for playing a part in Certification Authority Services issuing Qualified Certificates, even though it is not currently being deployed in that context. In this situation, the *tScheme*-recognised Assessors would, at the request of the TSP, include the relevant criteria from the appropriate Approval Profile for the type of Certification Authority identified by the TSP, for example the Approval Profile for a Certification Authority with the QC options nominated[1]. These criteria would then be applied by the assessor in addition to the criteria laid down in the Approval Profile for the offered component itself.

When an offered component service is to be assessed and deployed only as part of a full multiple-component service for which an Approval Profile has been produced, the additional criteria of the multiple component Approval Profile will naturally be applied, since this is the Profile that would be directly nominated for the assessment. The relevant individual component Approval Profile criteria would then pulled in by reference from the encompassing Profile.

Note also that some of the criteria laid down here, such as the existence of particular procedures or subscriber agreements, may be satisfied by procedures or agreements conducted through the multiple component service of which an offered service is a part.

1 Such a Profile would lay down any additional criteria applicable specifically to the offered service component - in fact for the example of a Registration Authority component, the Approval Profile for a Certification Authority does do this via reference to [QCP]

© *tScheme* Limited, 2001 - all rights reserved

3. THE BASE CRITERIA

Criteria are listed under assessment topics. For each topic, the basic assessment criteria are identified. These are followed by examples of the typical forms of evidence that could be provided to an assessor. The evidence indication, while being as comprehensive as possible, is intended neither to be exhaustive nor mandatory. In all cases, the actual evidence to be provided must be agreed in advance between the TSP and the *tScheme*-recognised Assessor.

The topics are:

1. business probity and management competence;
2. management and security policies and procedure;
3. assurance of technical infrastructure;
4. suitability of personnel use;
5. external relationships, including:
   - externally provided service components;
   - relationships with suppliers of technology, equipment and general support services;
6. service related policies and procedures.

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

Each sub-section identifies forms of evidence that a *tScheme*-recognised *Ass*essor will find appropriate. However, the specific forms of evidence for each assessment must be agreed with the Assessor before assessment can start. More information is given in Contracting with an Assessor.

3.1 Business probity and management competence

3.1.1 Criteria:

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

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

The TSP must demonstrate its commitment to comply with applicable legal requirements[2]. These are very likely to include:

1. 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;

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

© *tScheme* Limited, 2001 - all rights reserved

2. Data Protection: many countries have enacted data protection legislation. Issues especially likely to be emphasised are:
   - 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;
   - assurance that the information subscribers contribute to the TSP is protected from disclosure unless with their agreement or by court order or other legal requirement.

3.1.2 Example evidence:

1. Demonstration of compliance with Schedule 1 can be based on information from the following sources:
   - reports from independent auditing bodies, with due consideration of their professional status and any qualifications within the report;
   - information from relevant regulatory bodies, such as the FSA or OFTEL, pertinent to the provision of trust services;
   - demonstration to the *tScheme*-recognised Assessors of effective documentation and operation of those parts of its service related policies and procedures required by the Schedule.

2. Implementation of a QMS compatible with ISO 9001-2000.

3.2 Management and security policies and procedures

3.2.1 Criteria:

The TSP must 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(s) being assessed.

The risks identified and the countermeasures implemented to mitigate and manage those risks must be documented.

The TSP must ensure that administrative and management procedures (sometimes known as an Information Security Management System or ISMS) are applied that are adequate and correspond to recognized standards.

In particular:

1. the TSP management must provide direction on information security with a clear line of responsibility for defining the TSP's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy;
2. the information security infrastructure necessary to manage the risks within the TSP must be maintained at all times. Any changes that will impact on the level of security provided must be approved by the TSP management;
3. the security controls and operating procedures for TSP facilities, systems and information assets providing the trust services must be documented, implemented and maintained. This documentation should 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 should 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.

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

© *tScheme* Limited, 2001 - all rights reserved

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:

4. management of cryptographic hardware, including uninitialised personal hardware tokens and those that have been personalised prior to delivery to the subscriber, etc.;
5. usage of non-trusted channels for exchange of information with subscribers and agents (for example postal, telephone, and so on);
6. detection and management of events initiated by remote agents and by subscribers under duress.
7. Specific criteria are applied in the following areas:
8. contingency plans must be drawn up, which show how, in the event of a disaster, including compromise of the TSP's own confidential data[3], operations will be able to be restored;
9. the confidentiality and integrity of current and archived records concerning service deliverables must be preserved where appropriate;
10. the precise time[4] of significant TSP management events[5] must be recorded;
11. recorded events must be logged and retained, with appropriate protection according to regulatory obligations and risk management requirements.

In addition, the *tScheme*-recognised Assessors will use Sections 7.4.4 to 7.4.7 inclusive of [QCP] as guidelines to be applied as appropriate to the service being offered.

3.2.2 Example evidence:

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. Management systems can be demonstrated to exist and be effectively exercised.

Examples of widely recognised standards against which evidence may be offered are [ISO/IEC 17799], [BS 7799-2] and [ANSI X9.79], though any other forms of evidence that the assessor determines to fulfil the *tScheme* criteria will be acceptable.

3.3 Assurance of technical Infrastructure

3.3.1 Criteria:

The TSP must build security control measures into the technical infrastructure, which 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.

3.3.2 Example evidence:

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

4 The TSP should state in its practices the accuracy the clock used in timing of events, and how this accuracy is ensured.

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

© *tScheme* Limited, 2001 - all rights reserved

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 authority then any documents/certificates relating to this evaluation must be provided.
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 documented evidence must be provided.

3.4 Suitability of personnel used

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

3.4.1 Criteria:

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

1. the TSP must employ personnel who possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function;
2. security roles and responsibilities, as specified in the TSP's security policy, must be documented in job descriptions. Trusted roles, on which the security of the TSP's operation is dependent, must be clearly identified;
3. TSP personnel (both temporary and permanent) must 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 must differentiate between general functions and TSP specific functions. These should include skills and experience requirements;
4. personnel must exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures;
5. TSP personnel in trusted roles must be free from conflicting interests that might prejudice the impartiality of the TSP operations.

3.4.2 Example evidence:

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

© *tScheme* Limited, 2001 - all rights reserved

3.5 External relationships

The criteria in this section relate to the use of externally provided Trust Service components and suppliers of technology, equipment and general support services.

3.5.1 Externally provided Trust Service components

A TSP may offer for *tScheme* assessment an SSA which is dependent on externally provided Trust Service components. For example a Certification Authority service may be offered for *tScheme* assessment, which uses a Registration component service supplied by one or more external agents[6], 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 Trust Service components it depends upon.

Criteria:

When a TSP offers for *tScheme* assessment an SSA which is dependent on one or more Trust Service components provided by external agents, the TSP must provide a risk analysis to include analysis of:

1. inter-organisational communications security;
2. the degree of dependence on the agents concerned;
3. and the likelihood and consequences to the SSA of agent error or malice.

Then, to a level appropriate to the conclusions of that analysis[7], the TSP must:

4. verify that the provider is an organisation of a legal status and probity consistent with the criteria laid down in Schedule 1;
5. agree by contract that the provider will apply administrative and security policies and procedures consistent with tScheme approval of the type of service component it is providing;
6. agree by contract that the provider will apply and publish service policy and practice statements consistent with tScheme approval of the type of service component it is providing;
7. verify that the above contractual commitments are being honoured by the TSP on a regular or spot check basis appropriate to the number and size of providers involved;
8. contract with the provider that it agrees to subject itself to a tScheme assessment or follow-on assessment check, should the tScheme-recognised Assessor decide to do this. Such a check would not be necessary if either the agent has already been tScheme approved, or the assessor can otherwise be convinced that no assessment of the agent will be required;
9. ensure that the provider will satisfy tScheme criteria in relation to the suitability of personnel used;
10. ensure that the agent's technical infrastructure assurance levels are compatible with those of the service jointly being provided;
11. implement an appropriate level of inter-organisational communications security;
12. 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[8].

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

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

7 Details will be discussed on a case by case basis early in the audit process, and agreed between the *tScheme* auditors and the TSP.

8 Accountability is the issue here.

© *tScheme* Limited, 2001 - all rights reserved

may be required all 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.

Example evidence:

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 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.

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.

Criteria:

To the extent that the security of the SSA is dependent on such suppliers, the TSP must consider them in the service risk analysis and take appropriate steps[9] to ensure that their probity, competence and security matches the risks they might pose.

Example evidence:

1. Their contribution is considered where relevant in risk analysis documentation.
2. The reputation and track record of the supplier.
3. Appropriate contractual documentation.

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 applicable to any SSA.

3.6.1 Criteria:

A "Specification of the Service(s) Subject to Assessment" (S3A) as defined in "Preparing for an Assessment" must be produced.

A definition of the scope and content of each SSA (the SSA's Service Definition), which must also include a definition of the subscriber and expected relying party community to which the service applies, must be made available by the TSP to all potential users of the service.

Service decisions and deliverables must be communicated with integrity and, where appropriate to the service being provided, confidentiality, to the subscriber, to any other approved third parties[10] and to any follow-on dependent Trust Services.

---

9 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.

10 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, 2001 - all rights reserved

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.

One or more documented statements[11], containing the following information, must be made available to all interested parties for each service. The statements must be made available through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language:

1. obligations of the TSP in normal operation;
2. obligations of the TSP in the event of service unavailability;
3. the legal system by which the provider will be bound;
4. obligations of the subscriber[12];
5. obligations of relying parties[13];
6. liability accepted and liability limitations (the stated accepted liabilities must at least match the legally enforceable minimum);
7. warranties to subscribers;
8. any TSP approval, accreditation or certification achieved, and for what services/policies[14];
9. subscriber privacy and relevant national Data Protection Act provisions;
10. principles of operation of service specific procedures;
11. how a subscriber initiates use of, and continues to use the service;
12. procedures for acceptance of notification of subscriber status change;
13. procedures for publication of subscriber status change to subscribers and other dependants;
14. procedures for changes in service policy and practice;
15. procedures in case of service termination[15];
16. how and when subscribers can access the TSP;
17. audit processes[16];
18. any obligation of the TSP to supply physical access to service;
19. policies and procedures for maintaining and retaining secure evidence and audit trail of service specific operations. Records must be sufficient to be able to provide evidence of service delivery for the purposes of legal proceedings[17];
20. conditions under which service decisions will be conveyed to third parties;
21. description of methods by which service decisions and deliverables will be conveyed to third parties;

---

11 These will commonly take the form of Service Policy statements and Service Practice Statements and/or be part of the Service Definition *tScheme* recommends, but does not does not require that this document structure is used.

12 Primarily in respect of contracted subscriber liability, and subscriber actions that would absolve the service provider from liability.

13 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.

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

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

16 The ways in which the correct operation of service processes are audited.

17 These may arise after a considerable period (e.g. long term contracts such as pensions and wills)

© *tScheme* Limited, 2001 - all rights reserved

22. policy and procedures for dealing with queries and complaints;
23. contractual relationship with other TSPs[18];
24. procedures to ensure secure and timely confirmation of service completion;

The TSP must at the time of assessment be providing a service which supports these statements.

Of these items, the ones listed in Schedule 2 must clearly and conspicuously be made available by the TSP, preferably[19] in a separate Service Policy Disclosure statement to its community of users, for each SSA it provides.

3.6.2 Example evidence:

1. Presentation of appropriate documents, and demonstration of conformant working practices and internal processes to *tScheme*-recognised 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.
3. Evidence of the presence and efficacy of complaints procedures.
4. Evidence that any liability accepted has been adequately underwritten.

18 Although the details of these contracts may be largely confidential, evidence of any required features specified in Section 3.5 must be provided.

19 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, 2001 - all rights reserved

SCHEDULE 1. ENTERPRISE LEVEL CRITERIA

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

1. 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

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

OR

3. 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.

4. Either the operational enterprise or its parent enterprise must be able to demonstrate that it has an appropriate[20] legal status and must provide:
   - evidence of its establishment / registration (as required by the law of the territory in which it is established);
   - in the case of a separately identifiable parent organisation, the specific relationship between this parent entity and the operational enterprise[21].

5. If the service offerer is neither the operational enterprise nor its parent, it must similarly demonstrate its legal status.

6. The operational enterprise must demonstrate that:
   - 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[22];
   - it has quality management and information security management systems appropriate for the Trust Services it is providing;
   - it has the stability and resources required for supplying electronic Trust Services;
   - 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;
   - 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).

7. The service offerer must demonstrate that:
   - 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;
   - it has adequate arrangements to cover liabilities arising from its operations and/or activities.

8. The service offerer must supply an address at which legal notices can be served.

---

20 The "organisation" may be an individual such as a Notary Public.

21 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.

22 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.

© *tScheme* Limited, 2001 - all rights reserved

SCHEDULE 2. SERVICE POLICY DISCLOSURE STATEMENT

For each SSA, the following information must clearly and conspicuously be made available by the TSP to its community of subscribers and relying parties. It must 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[23], and any restrictions on usage of the service deliverables[24].
Reliance limits:	The reliance limits, if any.
Obligations of subscribers:	The description of, or reference to, the critical subscriber obligations[25].
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[26].
Limited warranty & disclaimer/Limitation of liability:	Summary of the warranty[27], disclaimers, limitations of liability and any applicable warranty or insurance programs.
Applicable agreements, Service Practice Statement, Service Policy:	Identification and references to applicable agreements[28] 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[29] and, if applicable, the audit firm

23 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.

24 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.

25 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.

26 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.

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

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

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

© *tScheme* Limited, 2001 - all rights reserved

SCHEDULE 3. CONSOLIDATED LIST OF FORMS OF EVIDENCE

This Schedule collects together the example forms of evidence that have been identified in the main body of this Approval Profile as being acceptable for demonstrating how the various criteria listed there have been satisfied. It is intended to act as a checklist for use both in the context of this Profile and as a guide to forms of evidence that may be suitable for use in the context of the service specific Approval Profiles. However, the specific forms of evidence for each assessment must be agreed with the *tScheme*-recognised Assessor before assessment can start. More information is given in Contracting with an Assessor.

1. Business probity and management competence is evidenced by:
   - Demonstration of compliance with Schedule 1. This can be based on information from the following sources:
   - reports from independent auditing bodies, with due consideration of their professional status and any qualifications within the report;
   - information from relevant regulatory bodies, such as the FSA or OFTEL, pertinent to the provision of trust services;
   - demonstration to the *tScheme*-recognised Assessors of effective documentation and operation of those parts of its service related policies and procedures required by the Schedule.
   - Schedule 1 also specifically requires evidence of establishment / registration (as required by the law of the territory in which it is established);
   - implementation of a QMS compatible with ISO 9001-2000.

2. Acceptable management and security policies and procedures is evidenced by:
   - 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;
   - presentation of a documented ISMS, supported by a risk analysis, and an unqualified (i.e. having no reservations) opinion of a qualified external assessor;
   - management systems can be demonstrated to exist and be effectively exercised.

   Examples of widely recognised standards against which evidence may be offered are [ISO/IEC 17799], [BS 7799-2] and [ANSI X9.79], though any other forms of evidence that the assessor determines to fulfil the *tScheme* criteria will be acceptable.

3. Assurance of the technical infrastructure is evidenced by:
   - 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;
   - documented evidence of the implemented security of the technical infrastructure and any procedures adopted to use and apply these controls;
   - reference to any evaluation criteria, standards, design, development and assurance methods, that might have been used to build and implement;
   - if an evaluation of any product used was carried out by an independent test house then any documents/certificates relating to this evaluation must be provided;
   - 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 documented evidence must be provided.

4. The suitability of personnel used, in terms of skill and competence is evidenced by
   - Job Descriptions, CVs and training records of the personnel concerned;
   - 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).

© *tScheme* Limited, 2001 - all rights reserved

5. The acceptability of the quality of externally provided Trust Service components is evidenced by:
   - a clear description of the relationship and dependencies between the SSA and the agents concerned, with risk analysis and:
   - appropriate contract, management and Trust Service documents;
   - The ISMS and operational procedures show that communications with the agents concerned have been secured to the required level;
   - evidence of an existing successful *tScheme* assessment of the agent(s) concerned.

6. The quality of suppliers of technology, equipment and general support services is evidenced by the following:
   - their contribution is considered where relevant in risk analysis documentation;
   - the reputation and track record of the supplier;
   - appropriate contractual documentation.

7. Conformance to service policy and procedure criteria is evidenced by:
   - presentation of appropriate documents, and demonstration of conformant working practices and internal processes to *tScheme*-recognised Assessors during on-site visits;
   - audit records, made available for inspection, which satisfy the Assessors that the necessary audit trails containing appropriate information have been recorded and retained;
   - evidence of the presence and efficacy of complaints procedures;
   - evidence that any liability accepted has been adequately underwritten.

© *tScheme* Limited, 2001 - all rights reserved

4. REFERENCES

[ANSI X9.79] "Part 1: PKI Practices and Policy Framework" Ref: ANS X9.79-1:2001.

[ISO/IEC 17799] "Information technology - Code of practice for information security management", First edition, 2000-12-01, Reference Number ISO/IEC 17799:2000.

[BS 7799-2] "Information Security Management - Part 2: Specification for information security management systems", 1999, published by the BSI, ISBN 0 580 28280 5.

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

[QCP] "Policy Requirements for certification authorities issuing qualified certificates" ETSI TS 101 456 V1.1.1 (2000-12).

© *tScheme* Limited, 2001 - all rights reserved