

EC DGXIII/0.7 ETS//  
Project *SEDUCER* (23186)

Document Identification

<b>Title:</b>	<b>D03: Trust Framework Model</b>
<b>Ref.:</b>	<b>ETS/23186/D03/2.0</b>
<b>Status:</b>	<b>2.0</b>
<b>Date:</b>	<b>98 12 18</b>

Approvals

<b>Author/Editor:</b> .....	<b>Date:</b> 1998 12 18
D.F.C. Brewer, Gamma Secure Systems Ltd.	
<b>Quality Review:</b> .....	<b>Date:</b> 1998 12 18
R.G. Wilsher, the Zygma partnership	



The opinions expressed in this document do not necessarily reflect the official views and policies of the European Commission

## Amendment Record

<u>Status</u>	<u>Issue Date</u>	<u>Comments</u>
1.0	1998 10 30	Submission to EC as Deliverable D03
1.1	1998 11 11	Revisions prior to validation and Web release
1.2	1998 12 10	Revisions made as result of review feedback
1.3	1998 12 16	Final version of document for internal review prior to submission
2.0	1998 12 18	Submission to EC as Revised Deliverable D03

## CONTENTS

<b>1. EXECUTIVE SUMMARY</b>	<b>6</b>
<b>2. DOCUMENT PURPOSE</b>	<b>7</b>
2.1 Objectives	7
2.2 Scope	7
2.3 Terminology	7
2.4 A Taxonomy of Service Provision	8
2.5 The Players	9
<b>3. BACKGROUND</b>	<b>10</b>
<b>4. THE ‘UNIVERSAL’ USER RISKS</b>	<b>11</b>
<b>5. FRAMEWORK SELECTION CRITERIA</b>	<b>14</b>
5.1 General Framework Principles	14
5.2 Framework Element Criteria	15
<b>6. TRUST INDICATORS</b>	<b>16</b>
<b>6.1 Liability</b>	<b>16</b>
6.1.1 L-Insurance	16
6.1.2 L-Financial Standing	17
<b>6.2 Credibility</b>	<b>17</b>
6.2.1 C-Financial Background	17
6.2.2 C-Independence	17
6.2.3 C-Overall Image	17
6.2.4 C-Technical Competence	18
6.2.5 C-Professional Ethics	18
<b>6.3 Policy</b>	<b>18</b>
6.3.1 P-Standards Compliance	18
6.3.2 P-Legal Compliance	19
6.3.3 P-Information Security Management	19
6.3.4 P-Accountability	19
<b>7. TRUST FRAMEWORK</b>	<b>20</b>
<b>7.1 Phases</b>	<b>20</b>
7.1.1 Pre-Operation	20
7.1.2 Operation	20
7.1.3 Maintenance	20
7.1.4 Termination	21
7.1.5 Service Succession	21
<b>7.2 Domains</b>	<b>22</b>
7.2.1 Technical	22
7.2.2 Operational	22

7.2.3	Physical Infrastructure-----	23
7.2.4	Personnel-----	23
7.2.5	Legal-----	23
<b>7.3</b>	<b>Trust Indicator Matrix-----</b>	<b>23</b>
<b>8.</b>	<b>ASSURANCE METHODS-----</b>	<b>26</b>
<b>8.1</b>	<b>Available Methods-----</b>	<b>26</b>
8.1.1	Testing-----	26
8.1.2	Self-Assessment-----	27
8.1.3	Self-Declaration-----	27
8.1.4	Audit-----	27
8.1.5	Certification-----	27
8.1.6	Independent Assessment-----	27
8.1.7	Independent Testing-----	28
8.1.8	Independent Accreditation-----	28
<b>8.2</b>	<b>Standards and Criteria-----</b>	<b>28</b>
<b>8.3</b>	<b>Selecting Assurance Methods-----</b>	<b>29</b>
<b>8.4</b>	<b>Assurance Profiles-----</b>	<b>33</b>
<b>8.5</b>	<b>Assurance Levels-----</b>	<b>34</b>
<b>8.6</b>	<b>An Assurance Path-----</b>	<b>36</b>
<b>9.</b>	<b>TRUST ASSURANCE PLAN-----</b>	<b>37</b>
<b>9.1</b>	<b>Providing the Glue – the Trust Assurance Specification-----</b>	<b>37</b>
9.1.1	Structure of the Trust Assurance Specification-----	39
<b>9.2</b>	<b>Alignment with Licensing and Accreditation-----</b>	<b>43</b>
<b>9.3</b>	<b>Trust Assurance Planning-----</b>	<b>45</b>
9.3.1	Applying the Trust Assurance Specification-----	45
9.3.2	Applying the Trust Assurance Plan-----	45
<b>10.</b>	<b>BENEFITS OF ADOPTION OF THIS FRAMEWORK-----</b>	<b>47</b>
<b>10.1</b>	<b>Flexibility-----</b>	<b>47</b>
<b>10.2</b>	<b>Methodology-----</b>	<b>47</b>
<b>10.3</b>	<b>Widespread Service Applicability-----</b>	<b>47</b>
<b>10.4</b>	<b>Open model-----</b>	<b>47</b>
<b>10.5</b>	<b>Extensibility-----</b>	<b>48</b>
<b>10.6</b>	<b>Adaptability-----</b>	<b>48</b>
<b>10.7</b>	<b>Binding qualities-----</b>	<b>48</b>
<b>10.8</b>	<b>Comparative Trust-----</b>	<b>48</b>
<b>10.9</b>	<b>Guidance-----</b>	<b>49</b>

**APPENDIX I - APPLYING THE 'UNIVERSAL' RISKS ----- 50**

**1. EXAMPLES ----- 50**

**1.1 Example 1: Key Generation Service (Public - Private key pairs) ----- 51**

- 1.1.1 Non timely delivery of the service ----- 51
- 1.1.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user 51
- 1.1.3 Service provider stopping to deliver the service ----- 51
- 1.1.4 Misuse of information ----- 52

**1.2 Example 2: Certification Service ----- 53**

- 1.2.1 Non timely delivery of the service ----- 53
- 1.2.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user 53
- 1.2.3 Service Provider stops the service ----- 54
- 1.2.4 Misuse of information by the Service Provider ----- 55

**1.3 Example 3: Key Escrow or Key Recovery Service ----- 56**

- 1.3.1 Non timely delivery of the service ----- 56
- 1.3.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user 57
- 1.3.3 Service provider stopping to deliver the service ----- 58
- 1.3.4 Misuse of information ----- 58

**1.4 Example 4: Time Stamping Service ----- 60**

- 1.4.1 Non timely delivery of the service ----- 60
- 1.4.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user 61
- 1.4.3 Service provider stopping to deliver the service ----- 61
- 1.4.4 Misuse of information ----- 61

**1.5 Conclusion ----- 62**

**APPENDIX II - APPLYING THE 'UNIVERSAL' RISKS ----- 63**

**1. OVERVIEW ----- 63**

**2. OBJECTIVES ----- 63**

**3. THE METHOD ----- 65**

**4. WORKSHEETS ----- 66**

**1.**

## **EXECUTIVE SUMMARY**

This report defines a Trust Framework Model which provides a structured approach towards the issues of understanding Users' expectations of Trust and the provision of some form of Assurance that their Trust is well-placed. The Model is scoped to address all aspects of a business and its provision of Trust Services – it is by no means limited only to technical issues.

The report identifies the 'universal' risks of using third-party services, as generically perceived by Users, and shows how to interpret these in terms of specific Trust Services. The Model then shows how these Service-specific User Risks (SPURs) can be related to the Service Providers' internal risk assessment and policy.

The Model goes on to describe how, through the selection of appropriate Trust Indicators which support the Users' need for Trust in response to the SPURs, the security measures within the service can be identified and for each of them an appropriate Assurance Method chosen with specific Standards or Criteria nominated as the basis of the Assessment. Since this approach is unlikely to lead to the identification of a single Assurance Method or Standard which suits all types of Security Measures in which Trust is required, the Model describes a specific document, the 'Trust Assurance Specification', which acts as the 'glue' between potentially disparate Assurance Methods and Results.

Hence, the application of this Model delivers business-focused Trust based upon a methodology which addresses Risks in User-orientated terms, using Assurance Methods which can be as detailed and specific as required, including in the technical domain, and which presents Assurance based upon a single overall assessment (i.e. through the Trust Assurance Specification). The model has been developed from a process-orientated point of view. No claims are made as to its cost-effectiveness: such judgements would need to be made on a case-by case basis, but the fact that validation has indicated that it is well suited to the needs and practices of actual Service Providers suggests that it can be economically applied in some circumstances.

This model has been developed jointly by four organisations with extensive experience in the Information Security Management domain. It is already being used in real-world situations by some of the project partners and will shortly be validated by a small group of selected participants.

All feedback on this report will be welcomed, and readers are invited to contact the *Zygya* partnership (the Project Co-ordinators) or to email [SeducerPj@aol.com](mailto:SeducerPj@aol.com), or to contact any of the other project partners.

## **2.**

## DOCUMENT PURPOSE

### 2.1 Objectives





The development of a sound Trust Framework Model (TFM), based upon the work initially produced as this project's Deliverable D02 ("Trust Framework Elements"), that can be validated both internally and by a sufficiently representative external audience.

### 2.2 Scope




This Trust Framework Model must be applicable across a multi-domain global environment, and embrace those mechanisms and components required to support and enable the creation of internationally-recognised processes for the assessment and seamless recognition of Electronic Trust Services. The Model must be User-orientated so as to deliver to Users, who in the main will not be technical experts, the means of having trust and confidence in services which form a crucial part of their business and personal electronic affairs.

### 2.3 Terminology


Since the phrase 'Trusted Third Party' is heavily loaded with assumptions and pre-conceptions, this report has tried to use clear terminology in the discussion presented by this report. Hence:

-  **Assessment** is a generic term for evaluation, verification- and inspection-type activities, rather than the term **Evaluation**, which is sometimes perceived to imply the style of an ITSEC Evaluation;
-  **Evaluation** is used to refer to a specific approach according to a scheme such as ITSEC, Common Criteria, etc.
-  **Certification** is the process reviewing the application of a formally-recognised method (e.g. ITSEC) to ensure its application has conformed to the standardised approach and that results were obtained through the objective application of defined criteria.
-  **Accreditation** is the process leading to a formal statement that an **Assessment** has been undertaken across the broad scope of a business' information security needs and a satisfactory result obtained (with specified criteria being met);

When referring to actions taken by the various parties who may be involved in the provision of TTP services;


-  **Self-Assessment** is used rather than '**First-Party Assessment**' when referring to owners, operators and providers of Trusted Services and;
-  **Independent** is used to refer to parties acting with no vested interests in the subject or outcome of their actions, rather than as '**Third Parties**', e.g. we would use the term '**Independent Assessment**';
-  **Assurance** is used to mean trust in a broad sense, rather than a literal sense (since it is understood that in calling certain bodies '**Trusted Third Parties**' the broader sense applies and includes the literal)

We have also defined two further terms of vital importance to this report, and whilst we have not made any radical changes to the general meaning of these terms we have qualified them to ensure that readers understand them in the context in which they are used within this study. These terms are:

 **TRUST** is the belief, based frequently on evidence, that the Risks of using a TTP Service are acceptable.

*This definition has to be understood in the context of the following qualifying notes:*

- 1) For a Service Provider, it is **their** view of **their** risks in providing the specific service(s);
- 2) For a User, it is **their** view of **their** risks in using the specific service(s);
- 3) Neither Service Provider nor User has any entitlement to form a view of risk, or make a judgement on risks on behalf of the other party. However, a Service Provider will try to form a view in order to be able to offer some indication of trustworthiness covering the most likely risks Users have when using the service (although in most cases the Service Provider will not know in detail what the assets of the User actually are, and must therefore make some reasoned assumptions about the Users' risks);

 a **RISK** is any potential event associated with the use of or dependence upon TTP Services which has the potential to adversely affect the business' objectives.

*This definition has to be understood in the context of the risks which the application of the TFM has the ability to address. It is recognised that a business may face many other risks from sources having no relationship with the provision of TTP Services.*

Some other key definitions are included within the report, as they become necessary.

## 2.4 A Taxonomy of Service Provision

During a study undertaken for the UK's Department of Trade and Industry we developed a taxonomy of TTPS. Briefly, this taxonomy considered services to be of either the Primary Value (PV) or Added Value (AV) type, and suggests that the operational environment in which these services may be employed can be described as either Private, Syndicated or Public. Certain combinations of these lead to four major classifications being identified, and these are shown in the following table.

	Private AV	Syndicated AV	Public AV
Private PV	Class 1		
Syndicated PV		Class 2	
Public PV		Class 3	Class 4

To date, most TTP and TTPS are of the PV type. Further, a very large proportion of AV services are used within 'Syndicated' operational environments which means they are quite tightly bound to the supporting PV services.



So far as our survey suggested, the likely development of the market place appeared to be as follows:

- Σ Within Private service provision, PV and AV functions will be developed to be mutually supporting - we called this Class 1;
- Σ Within Syndicated services, the nature of their operation suggests that AV functions will be provided internally, but these may be based upon internally provided PV services (which we labelled Class 2) or by externally provided PV functions from an independent provider in the Public domain (which we labelled Class 3);
- Σ Public AV services based upon Public PV functions (which we have called Class 4) will be more likely to address the high volume, low value, market with a correspondingly low level of trust required of them (since the risk per transaction should be relatively limited).

Within SEDUCER we are addressing the provision of public services, i.e. Classes 3 and 4 in the table above. This is the primary focus of the project, although the results could equally be applied within Class 1 and Class 2 situations, to provide internal assurance, and we are equally open to contribution of ideas and suggestions from those domains as valid input to the SEDUCER framework.

## 2.5 The Players

We refer to Service Providers and Users. These can be described in terms of the SEDUCER scope, as follows: Service Providers are those providers offering one or more of the Primary-Value PKI services we have defined. Users are the consumers of the PV services: they may be public administrations, large corporates down through SMEs and micro-enterprises (less than five employees, by our definition). These Users could be operating in Business-Business, Business-Retail (Consumer), Business-Administration (Government) or Private Individual-Administration contexts, and indeed some of them could be delivering Added-Value services built upon the PKI on which we are primarily focusing.

## 3.

## **BACKGROUND**

### The relevance of basic work undertaken in D02 “Trust Framework Elements”

In its deliverable D02 this project set out a number of discrete views on what constitutes trust and what available means there are for demonstrating it, or rather, for demonstrating the trustworthiness of a service. These Trust Framework Elements were effectively catalogued but not structured in any way which could be called a model for demonstrating trustworthiness. In this report (D03) those framework elements are considered further in terms of how they can contribute to a homogenous Trust Framework Model (TFM) which provides a clear path from the need for trust (from the User’s perspective, one of the key elements of this project) to the means to provide evidence of trustworthiness.

### The need to look at things from the Users’ perspectives

The need to consider the User’s perspective is paramount – the provision of trusted services stands to have a significant rôle within global electronic commerce. Understanding the needs of the players in this marketplace is key to the success of trusted services. A significantly large proportion of the users of these services will neither have the time, nor probably the desire or ability, to learn of their internal functioning and how the service is managed and delivered in detail. However, they should have a clear view of what they gain from using the service, and how it fits into their personal lives and business activities. This project assumes their perspective and identifies a model which Service Providers can put into place to deliver this trust. What this project does not seek to do is to solve either the Service Provider’s or the User’s own internal risk assessment challenges.

### Recognising that most Users will be business, not technically, -orientated and the need to express the Model in terms they can understand

The TFM which the project proposes is therefore based upon these basic trust requirements which Users have, and establishes a set of indicators which are initially generic but which can be used by a User to understand the degree of trust on offer without having detailed knowledge of the ‘internals’ of the service. This approach, as stated, recognises the need for internal asset valuation and risk analysis by both Service Provider and User, and describes how these activities relate to the TFM. The report then identifies the available assessment methods, relates these to the trust indicators and enables a comprehensive matrix to be developed which takes into consideration all aspects of the Service provision. After considering the appropriate means of assessing the trust which the matrix has shown to be necessary, the model enables the expression of assessment profiles, one for each selected approach. Finally, the TFM supports the combination of approaches by providing the overall framework for their assessment and the glue between the individual assessment (part)s.

The coherence of this approach is being demonstrated already by the consortium concerned, in two independent assignments for private clients;

## **4.**

## THE 'UNIVERSAL' USER RISKS

Today's view of Information Security is more mature, and has more of a business perspective than the stereotypical 'CIA' approach

Up to even the last ten years, the 'classical' domain of IT Security was principally in the Defence and Governmental sectors, with some notable exceptions in the form of some large corporate bodies (e.g. Wells Fargo Bank, 1983). Even so, there were few exceptions in the commercial sector to the view that security was generally technical, being expressed in terms of 'CIA': Confidentiality, Integrity and Availability. This approach failed frequently to take into account the real business objectives (where even the workings of governmental departments can be regarded as 'businesses' with missions to achieve, services to deliver and budgets to keep within).

With a more mature view which one can hold today, the concept of Information Security (Risk) Management is more commonly espoused. The idea behind this is that the security of a business' information needs to be driven by the business objectives, the assets required to support the successful achievement of those objectives and the measures needed to provide that protection. There is recognition in that view that the security of the business is met by considering all the domains across which the business operates, not just the technical domain.

Users of Trusted Services will increasingly take this view, and therefore their perception of the risks they might be subject to by using these services will be based upon some fundamental, or 'universal', concerns.

Service Providers must, therefore, take into consideration the potential risk for the Users of their service. Generally speaking, Users want their risks to be covered appropriately without knowing in detail how the Service Provider has addressed these risks. The User wants to be ensured that the Service Provider has taken all necessary precautions against any failure to deliver the service in the way which results in loss of assets or image to the User. Users also want financial compensation when the Service Provider fails to deliver the service in the defined way or when he suffers from financial losses due to failures in the Service Provider's environment. In addition they want to be assured that the service is delivered in compliance with existing and relevant laws and regulations. However, since User will generally be unable to check for themselves the effectiveness and adequacy of the security measures implemented by the Provider they have to trust the Provider. As our definition of trust points out, Users expect some evidence that this trust is not misplaced. The framework therefore defines methods which support the provision of this evidence and defines which aspect and phase in the life cycle of the service for which they can be applied.

The idea of basic, service-orientated, generic risks from the Users' perspective and the need to express them in terms of a specific service

As a starting point for the TFM we can consider the general risks a User faces when he uses a TTP service. These will be potential problems due to:

1. Unreliable provision of the service or the results not of the quality that is expected;
2. Disruption to provision of the service;
3. Non-provision (suspension /termination) of the service;
4. Misuse by the Service Provider of information he should protect resulting in a Loss of User assets and/or image.

The relevance of these risks for each individual User depends on the type of the service and the User's intended use of it. The User will want to know whether the Service Provider has covered the risks he (the User) sees with the use of the service and how he can be assured that those risks either will not

materialise or will be covered by the liability of the Service Provider. The User will be generally uninterested in what may cause those risks to materialise in the Service Provider's environment, but will be concerned that the Service Provider manages those risks effectively. This suggest that for certain services, probably more so in the case of Added-Value services, the provider needs to have a sound understanding of the Users business and how they will use the service.

The generic risks that are inherent to specific types of services can be used as a starting point for a risk analysis as well as for the definition of a scheme (licensing, accreditation, certification) aimed to define some minimum set of security measures and the associated assessment techniques that should provide the trust necessary.

As an example, in the case where a User would be satisfied with financial compensation for any problems that arose with delivery of the service (i.e. so long as compensated, he didn't care about the temporary problems) he may be satisfied with appropriate contractual conditions giving him assurance that his losses will be covered. If financial compensation is not appropriate or when it could be difficult to prove a provider's failure or misuse of information, assurance will be needed to demonstrate that the provider has taken sufficient and effective precautions to prevent critical risks from happening becoming actual events. The main purpose of the TFM is therefore to define and explain the manner of implementation of the set of assurance methods needed to protect the consumer of a critical TTP service.

Since the criticality of the service depends on the User's application of it, a Service Provider should state in the information he presents to the User the security objectives of the service he is providing. This can be accomplished by making available a document describing the general features of the service (the Service Description).

This document should not only contain a description of the functional aspects of the service but also the obligations upon Users of the service, limitations in the use of the service, the Service Provider's liability conditions as well as the assessments that have been undertaken to ensure the effectiveness of the necessary security measures.

The Service Provider can make its own judgement as to the specific risks which a User will perceive in their use of a service, or otherwise by using the Service Description as a vehicle for communication with the Users, and building a deeper understanding of their perceptions. This User-focussed understanding of the risk allows the Service Provider to better judge the ways in which he can assure the Users that their trust in them is well-placed. This is dealt with in the following section.

**Looking at the Risks from the User's perspective is important but the Service Provider must also perform their own internal risk assessment and provide combined security solutions and assurances for all parties**

However, before moving on it is important to make again the observation that this framework serves to allow the Service Provider to judge the User's perception of risk associated with the use of the service. What it does not do is to support explicitly the Service Provider's own internal asset valuation, risk assessment and security policy. Although the model suggests how this can be accomplished in the context of the TFM, it is not this project's intention to become another essay on risk assessment, many fine examples of which are readily available. Neither does it address the other side of the question, and offer a solution to all the information security management questions which may face the Users. These too need to addressed in the context of the overall business objectives and operations of the User, whether private citizens or major corporations, and in this the use of the specific Service would be just one factor, although possibly a critical one depending on the specific type of service.

However, one can make some broad comment on the risk analysis aspect of applying the TFM to a Service. In deciding to offer a service the provider will have defined their service model (the Service Description). This will have defined the scope. After considering things from the Users' perspective

the Provider needs to take an introspective view – what are the incumbent obligations in terms of legislation, licensing and internal policies with which they are obliged to comply? What are their own assets, the components and resources supporting the service, what are the threats ranged against them, and what therefore are the vulnerabilities?

By considering a Risk to be the product of the defined Threat, the Vulnerability and the Asset (value), one can see that the effect of a safeguard is to mitigate one of the threat, vulnerability or asset (whether this be achieved by technical or non-technical measures, or the application of a specific assessment method which improves understanding and confidence). We can consider three examples to illustrate this point: use of encryption can mitigate the value of an Asset (by making the encrypted version far less valuable than the plain text equivalent); a software patch on an operating system might mitigate against an identified vulnerability; the presence of physical measures (walls, physical access control, reception staff) and staff vetting procedures can serve to mitigate the threat. The combined application of all these measures serves to reduce the original (unprotected) risk by the cumulative effect of all the various Security Measures: the skilled application of risk analysis will achieve a balance between cost of the measures and the benefits gained, i.e. the point where the Residual Risk is acceptable.

Therefore, in parallel with the application of the TFM, the Service Provider needs to develop his own detailed risk analysis and to ensure that in doing so he can explain the interpretation of the Universal risks in the context of the service being provided. For such a program to be successful, the risk analysis/assessment offered by Service Provider's should conform to some standards and use a recognised knowledgebase. As a result of their Risk Analysis they can then deduce what Trust Indicators and Assurance Methods are required. How they do that we now explain.

## 5.

## **FRAMEWORK SELECTION CRITERIA**

The components of the framework have been validated against the following criteria, established at the beginning of this report as being the principles against which the framework elements would be justified.

### **5.1 General Framework Principles**

The selection of each framework element shall be justifiable in terms of its contribution to the following principles of the TFM:

1. The framework shall be constructed and populated so as to give adequate and proportional coverage to all principal operational domains viz.: Technical, Organisational, Physical, Personnel and Legal.
2. The framework shall be constructed and populated so as to give adequate and proportional coverage to all principal operational phases (Set-up, Operation, Maintenance, Termination).
3. Framework elements should use as high a proportion of current practices as possible, with excursions from this principle being fully justified.
4. There should be a clear relationship between the elements, and any isolated relationship-groups of elements should be justifiable in terms of the application of the model.
5. Within each relationship-group any notion of 'level of trust/assurance' must be discernible throughout all elements of the group.
6. There should be clear justification for any empty parts of the framework (i.e. empty cells in matrix of operational domains and operational phases).
7. There should be a coupling between relevant operational domains for the Operation and Maintenance phases.
8. To the extent practical and in a broad sense, ensure alternative approaches exist where a given approach may be inappropriate or unacceptable to some sectors or TTP providers (e.g. only appropriate for large enterprises and not for SMEs).
9. Ensure alternative approaches exist where a given approach may be unacceptable to certain member states.

## 5.2 Framework Element Criteria

In order for Framework Elements to qualify for inclusion in the TFM, they should be:

1. Not in contravention of any national laws of any EU Member State, nor so far as is practical, of those of other jurisdictions world-wide (and indeed should be able to satisfy to the fullest extent any or all relevant legal requirements).<sup>1</sup>
2. Directly or readily applicable to the provision of TTP services, either for a specific sector or in general.
3. Flexible enough to be applicable to both Primary Value and Added Value TTP services.
4. Clearly able to contribute towards evidence that can be seen and used by a potential user of the service to assess and make comparisons concerning the level of trust that can be placed in the service.
5. A means whereby a provider can define and have measured the trust in the TTP services they provide.
6. Flexible enough to support different levels of trust.

## 6.

---

<sup>1</sup> The need for legal neutrality is exemplified in the requirement to develop a framework equally applicable in, say, France where the use of encryption for confidentiality purposes is licensed (but not prohibited outright) and the UK where there are no significant prohibitions. Thus, the framework needs to recognise this but need not itself be in conflict with legal circumstances, i.e. the framework cannot itself mandate or prohibit encryption for confidentiality.



## **TRUST INDICATORS**

### Important and relevant work undertaken for UK DTI

A study in 1997, conducted on behalf of the UK Department of Trade and Industry by this consortium, looked at the meaning of trust in electronic third party services. It addressed this issue not only in the UK, but also in four other EU Member States.


Its findings were used in the preparatory work undertaken in D02, and allowed the creation of a matrix which looked across all aspects of the operation of a Trust Service.

### Reappraisal of the results of D02 leads to separation of key elements into trust indicators and methods for assessing

Within D02, a number of Trust framework Elements were identified, following the review of thirty-seven documents covering techniques methods and standards, legislation, policy and practical studies and experience. Further consideration of these elements during the preparation of this report has identified these elements as being in two distinct groups – those elements which indicate trust(worthiness) and those which can be used to assess it.

These trust indicators are now defined, in their three groups.

## **6.1 Liability**

 Liability is the ability and willingness (and under certain circumstances, the obligation) of a Service Provider to cover financial losses suffered by its users as a result of its failure to deliver service in accordance with an agreed service definition.

Whilst liability does not directly contribute to trust in a service, it is an important element to identify and limit the potential risk associated with either the use or the provision of a TTP service. A clear definition of liability may effectively lower the level of trust one needs in a service. It is this aspect that makes liability an important element of a trust framework for TTP services.

In some countries there are legal requirements for the minimum liability conditions a Service Provider has to offer his customers. These may quite broad and relate to all kinds of services, not only TTP services, and in these cases the interpretation of these minimum conditions in the light of a specific type of TTP service may be difficult.

Liability is clearly linked with the financial standing of the Service Provider's organisation. A user of a TTP service has to be sure that the Service Provider is able to cover the financial obligations associated with his liability conditions. Associated with liability are two indicators:

### **6.1.1 L-Insurance**

Whenever a Service Provider is either not able or is not willing to take the complete risk associated with the liability conditions in relation to his customers, he can take out insurance. With this he can transfer the risk to the insurance company and can provide the customer with the confidence that financial losses will be covered (to the extent that they are defined in the contract or relevant regulation, etc.) if the Service Provider fails to provide the service as defined in the service agreement with the customer.


There are, however, some legal aspects that need to be addressed in conjunction with insurance. Most insurance companies limit the scope of the insurance and don't cover cases where the Service Provider deliberately fails to fulfil his contractual obligations or misuses the information provided to him by his customers. Insurance is therefore not able to cover the liability issue completely.



### 6.1.2 L-Financial Standing

This element is defined as the ability of a Service Provider to manage any failure in their operations and to cover liability cases using their own financial resources. The financial resources of the Service Provider from which liability cases can be covered are therefore another important aspect. These financial resources will also be used in those cases that are not or can not be covered by insurance, e.g. in cases of deliberate misuse of the service or customer data by the Service Provider or one of his employees. A good financial standing will on the one side provide the customer with a high level of confidence that the Service Provider will cover his liability and on the other side give some confidence that the Service Provider himself will set up appropriate security controls to prohibit such deliberate misuse because of the high financial loss he may have to face.

## 6.2 Credibility

 **Credibility**, i.e. a ‘good’ reputation, is an important market factor and Service Providers will use it as one of their main marketing arguments. Where an organisation has an image and reputation that can be damaged, then failure adequately to perform its obligations towards its customers can result in a loss of credibility. Credibility is therefore perhaps one of the most important User selection criteria, particularly for business-critical services.

Associated with credibility are a number of indicators:

### 6.2.1 C-Financial Background

This aspect has already been addressed under Liability. In terms of credibility, the financial background is a factor that a customer would consider when it comes to compensation if the Service Provider fails to provide the service and where the liability clauses don’t hold. With a good financial background and a good reputation a customer can reasonably expect the Service Provider to compensate for losses in such cases as a matter of ‘customer care’ to maintain his reputation.

### 6.2.2 C-Independence

Another important aspect of credibility is the independence of the Service Provider from organisations or activities that potentially have a conflict of interest with the service provided. From a customers point of view such an independence limits the threat of misuse of the service.

The degree of Independence will be influenced by several elements, such as:

- Σ Management independence in decisions regarding the provision of the service;
- Σ Technical independence from the providers of software, hardware and support services;
- Σ Organisational independence from any organisations with conflicting interests;
- Σ Personal qualifications and character of senior management;
- Σ Financial independence, i.e. the financial backing is sufficient and financial decisions are made by the Service Provider himself;
- Σ Service independence, i.e. the extent to which the provision of the service relies upon a service from a different Service Provider;
- Σ The ability to select alternative support services rather than be tied to a specific provider.

### 6.2.3 C-Overall Image

A more general aspect of credibility is the overall image which the Service Provider commands. This is of course very subjective but a Service Provider may improve its image significantly by publishing

information about its overall security policy, financial background, customer support etc. In general one can say that the overall image is, amongst other items, dependent on the information the Service Provider makes available to its customers or the general public, concerning how it implements the other trust framework elements.

#### 6.2.4 C-Technical Competence

The competence of the Service Provider regarding the technical aspects associated with the provision of the service. This includes not only the competence with respect to the technical equipment needed to run the service but also includes the level of understanding for the technical needs and problems of a customer. Customers expect several elements where a Service Provider should show technical competence:

- Σ Competence regarding their own technical equipment and infrastructure needed to provide the service;
- Σ Competence regarding the technical equipment and infrastructure a customer needs to use the service appropriately;
- Σ Competence regarding the type, installation and use of technical security measures needed within the Service Provider's domain to protect the service from failure and attack;
- Σ Competence to provide the customer with sufficient assistance to solve technical problems when using the service;
- Σ Competence to identify, understand, and effectively mitigate the risks associated with the services offered and the resources required to offer them.

#### 6.2.5 C-Professional Ethics

In addition to these other credibility indicators, the evidence of a Code of Ethics issued by the provider organisation and to which its employees demonstrably adhere, can be a significant trust indicator where the User may be dependent upon the provision of the services across a wide range of their business activities, yet do not directly control themselves (and of course, many businesses will be focussing on doing what they do best and leaving others to deliver these specialised services). Clear evidence of the effective pursuit of ethical practices will be a positive indicator.

### 6.3 Policy



**Policy** has been considered, in this report as well as in the preceding studies, to have the broader definition of “*the set of rules and practices that regulate how the service, including its security provisions, is managed and how the trustworthiness of the service is assessed*”. The Security Policy enforced by an organisation can play an important role in an overall trust framework.:

In this report policy is considered to have a broader definition than in some other documents. Policy is regarded as the set of rules and practices that regulate how the service, including its security provisions, is managed and how the trustworthiness of the service is assessed. The Security Policy enforced by an organisation can play an important role in an overall trust framework. The Security Policy will describe how the Service Provider manages and protects all security-critical information and systems that are involved in the provision of the service. The indicators for the policy aspect are:

#### 6.3.1 P-Standards Compliance

Within this element a Service Provider defines the set of standards to which he claims compliance. Such standards may include:

- Σ Technical Standards for data formats, protocols and messages;
- Σ Technical Standards for equipment and equipment safety/security;
- Σ Standards regarding the overall operation and management of the service;
- Σ Standards regarding the security provisions associated with the service.

### 6.3.2 P-Legal Compliance

This element describes the laws and official regulations with which the service has to comply with and how this compliance is achieved. This includes general laws and regulations for the delivery of commercial services as well as laws and regulations specific for the type of service provided, or specific to the sector or jurisdiction in which the service is delivered.

### 6.3.3 P-Information Security Management

This element includes all areas that define how the Service Provider manages security critical information and security critical equipment. It includes the definition of technical, organisational, physical, personnel and legal compliance security provisions and how they are managed. This is generally defined as the security policy for the service. The basis for such a security policy is the security objectives defined to support the service's business plan. Depending on those stated objectives, a security policy then should contain, inter alia, descriptions of the following elements:

- Σ How a service user is authenticated;
- Σ How the correct usage of the service is verified;
- Σ How data associated with the service usage and critical user data are protected;
- Σ How misuse of the service by legitimate users is dealt with;
- Σ How the availability of the service is guaranteed;
- Σ What criteria are applied to enable cross-certification with other Service Providers<sup>2</sup>.

To define those elements a Service Provider usually describes the security measures he has in place. Most security policies are structured into chapters describing the technical, organisational, physical, personnel and legal security measures and how they contribute to the security objectives.

### 6.3.4 P-Accountability

This element describes the provisions a Service Provider has taken to trace (down to the originator) security critical events as well as activities relevant for billing processes. It includes accountability for activities by personnel within its responsibility as well as activities of service users and activities by third parties that may interfere with the service (e.g. maintenance activities). The Service Provider has to define which are the relevant events and activities and which data are collected to provide and fulfil the accountability requirements. In addition he should state how this data is authenticated and protected.

## 7.

---

<sup>2</sup> This is based upon the mutual trust between the two service providers, over and above the technical inter-operability issue, which is dealt with in the following section.

## **TRUST FRAMEWORK**

The need to address all Phases and Domains of Service Provision and of operation of the business

Deliverable D02 used as one of the paradigms for its initial analysis a matrix which related the phases of operation of a (trusted) service to the domains in which the management of the service could be considered. This provided the basis for assessing thirty-seven source documents, from which were derived the trust elements described in that report (and now further analysed into the trust indicators, previously described herein, and the trust assessment methods, to be described further in this report).

### **7.1 Phases**

The principal life-cycle stages of the initiation, operation and termination of a trust service (and equally applicable to most services, in fact) were considered to be: Pre-Operation, Operation, Maintenance and Termination. In fact, D02 considered another level of detail for each of these but this is no longer a necessary contributor to the development of the framework. Although we have identified four phases, each of which must be considered, it is the expectation that the bulk of the provision or demonstration of trust will be during the Operational and Maintenance phases. The Phases considered were:

#### **7.1.1 Pre-Operation**

The defines the period up to the formal initiation of services. This is largely concerned with, inter alia: the definition of the service (Service Description, as already referred to); putting in place the organisational structure; securing any necessary financial backing; defining the Corporate Security Policy; setting up the Service Security Management; recruiting; establishing premises; fulfilling legal and legislative pre-requisites; recruiting staff; training; developing or selecting technical equipment; procuring systems and services; installing and integrating systems; and performing trials to establish the service, possibly with a group of pilot Users. And of course, integrated into this activity would be the definition of the security aspects of the service, in all domains of its operation, through the preparation of the security policy and the provisioning of necessary security products, systems and services, etc. As stated already, there is much guidance on the mechanics of these steps, and it is not the objective of this project to describe them anew. However, what is important to establish is that, during this phase, the initial application of the TFM would take place, so as to establish the means by which the trust in the service could be demonstrated.

#### **7.1.2 Operation**

Once the service is in operation this phase is concerned with the ongoing provision of service and the monitoring of services for any necessary changes to perhaps the way in which it is delivered and possibly the way in which trust in it is maintained. So, this phase would be concerned with, amongst other responsibilities, ensuring that all defined security procedures and measures are effectively applied as required and are not overlooked through familiarity or contempt, checking for security relevant incidents, analysing if the assumptions made in the risk analysis continue to hold. The upholding of the trusted status of the service is, in terms of the TFM, the goal of this phase.

#### **7.1.3 Maintenance**

As the service continues upgrades will be required for a variety of reasons, amongst which might be: revision to software to amend any short-comings; addition of new services; changes to the legal, regulatory or any licensing environment; change of physical location of service elements, re-organisation of the business, changes affecting the use of external services. During such events,

maintenance of the validity of the basis of trust in the service needs to be considered, as does changes to the way in which trust indicators are assessed (or possibly the choice of trust indicators) according to the severity of the change. Some, such as ongoing upgrade of software, could be quite straightforward; others such as moving to another physical site could be quite dramatic, requiring substantial re-assessment of many of the trust indicators.

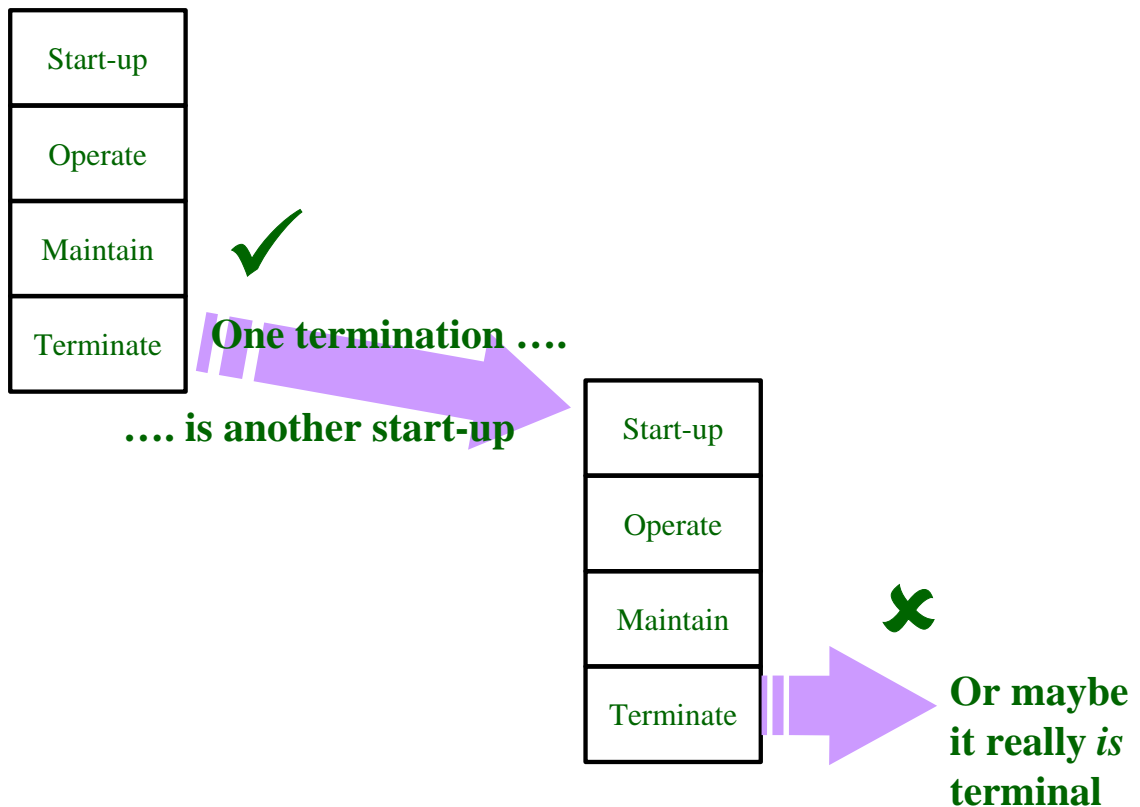
#### **7.1.4 Termination**

This phase becomes active whenever there is effectively a cessation in the provision of the service by the recognised Service Provider. A number of factors could initiate this, inter alia, bankruptcy, withdrawal of license, legal injunction, decline in market share, major loss of User confidence, generally falling demand for the type of service, transfer of services (to another Provider) or take-over (with continuity of services). Depending on the nature of circumstances, the cessation may be temporary or permanent, and its impact will vary according to the service affected. As brief examples, cessation of a Certification service may simply mean that another CA needs to be used, and the loss of service is transient and inconvenient but not critical. Loss of a Directory Service may be more inconvenient because of the inability to authenticate certificates, and this could have repercussions upon businesses. Loss of a Key Escrow / Recovery service and possibly Added-Value services such as electronic cash or electronic registries could be much more severe. In particular, laws and regulations regarding a business which is under receivership may prohibit from having access the owners of property held by the Service Provider (in this case their private keys, their Ecash or perhaps electronically-held negotiable instruments). Such a situation could have much more far-reaching implications.

For Users to be confident when initially subscribing to a service in which they will have great reliability (and hence trust), they will seek assurances as to the provisions made for the termination of the service under any of these contemplated circumstances. The application of the TFM during the Set-up phase has therefore to consider all other phases of operation.

#### **7.1.5 Service Succession**

We can visualise the four phases quite simply as follows, fig X. It is important to recognise how the phase elements of the matrix relate when Termination arises, since as we have suggested above, Termination can be absolute or there can be a continuation of service under different circumstances. Hence as the figure suggests Termination in the case of some form of continued operation is effectively re-entry into the life-cycle at the Set-up phase. Thus the basis of the TFM covers these eventualities.



## 7.2 Domains

The second axis of the initial Trust Framework identified five principal domains in which trust could be said to be required. Each of these is fundamental to the overall assessment of security, and specifically, to the determination of trustworthiness; none exist without some influence from the other domains, and cannot be considered truly in isolation. These were: Technical, Operational, Physical Infrastructure, Personnel, Legal. In D02 we noted that there was already a project in the same programme which was dealing with legal aspects of Electronic Trusted Services, and elected to initially omit this domain from our study. However, because of the interrelationship within the domains, and the fact that we felt sure that these other studies were not considering legal matters from the same perspective as was SEDUCER, we re-introduced that domain into D03. These domains are now briefly described.

### 7.2.1 Technical

This domain is clearly the ‘stereo-typed’ security domain, and would include all of the technical components of the service: computers, software, other hardware such as routers, exchanges, networks etc.; it would also address the technical procedures, e.g. back-up and safe-store procedures, change-over procedures where used, etc. It would also address the technical issues affecting any outsourced or bought-in services.

### 7.2.2 Operational

Largely concerned with the organisation, operation and management of the business and the service delivery. This is perhaps the central domain into which and through which all other domains interact.



This domain is therefore concerned with, at the high level: determination of the business objectives; putting into practice the business' security plan; applying the TFM to provide the trust assurance; the provision of overall policies; management; conformance to external requirements, etc. At the service level, matters such as the day-to-day operation of the service, application of procedures, provision of consumables etc. and oversight of maintenance would be covered. Provision of outsourced services would be considered here, from a non-technical point of view.

### 7.2.3 Physical Infrastructure

This is concerned with the premises from which the services are operated and the accommodation provided for the related systems and machinery. Physical protection and access would fall into this domain, as would storage and the provision of utilities and alternative sources of supply (e.g. power, telecommunications, ...); protection against theft, vandalism and natural disaster.

### 7.2.4 Personnel

The manner by which staff are recruited, trained, facilitated and monitored would be relevant in this domain. The obligations imposed upon them would be addressed, e.g. contractual terms, client and business confidentiality, code of ethics, etc.

### 7.2.5 Legal

Any trust services will be operating within some kind of legal and regulatory environment, both in general terms and in the specific context of trust services. A growing number of states, both in the EU and world-wide, have or are proposing regulation or licensing affecting the provision of trust services. There are also other multi-national industry-led initiatives which may require conformance to remain as a licensed Service Provider. Thus consideration of this domain is important to ensure conformance with appropriate legislative requirements, although this project does not set out to define what those specific statutes should be, since this was the specific scope of the 'LEGAL' sister-study..

## 7.3 Trust Indicator Matrix

Trust Indicators are a general group which need to be related  
to the specific domains and phases of the Service

In D02 the Phase vs. Domain matrix was used as a paradigm for the analysis of the review of the reference documents. Further analysis of these findings during the preparation of D03 has led the project team to separate the results of that analysis into the two groups of trust indicators and assessment methods. In developing the model to define the method of applying these, the trust indicators have been considered to be in effect global to the overall Phase / Domain matrix. This leads to the following form of the matrix.

L-Insurance	✓	✓	✓	✓	✓
L-Financial Standing		✓			
C-Financial Background		✓			
C-Independence		✓			
C-Overall Image		✓			
C-Technical Competence				✓	
C-Professional Ethics		✓		✓	
P-Standards Compliance	✓	✓	✓		
P-Legal Compliance					✓
P-Information Security Management		✓			
P-Accountability		✓		✓	
	Tech.	Org.	Physical	Personnel	Legal
Start-up					
Operate					
Maintain					
Terminate					

The purpose of this table is to provide the basis for mapping into the Phase – Domain matrix (green cells) the Trust Indicators which the Service Provider feels are appropriate to fit the Users’ (perceived) view of the risks in using the service. The ‘reference’ matrix bearing the Trust Indicators shows the domains in which each Indicator has a meaning, or more accurately, a validity.

The process of mapping Trust Indicators requires that each User Risk ‘URn’ is considered against each of the cells in the Phase – Domain matrix and, where it has some relevance the risk (reference) is entered. This process should proceed with a record maintained of the justification for each time any risk is associated with any cell. A consistency check is required to ensure that all risks are considered and that each one appears in the matrix at least once (Whilst there can be no guarantee as to how many times a risk might justifiably be placed into the matrix, its absence should cause some concern; it may be that on reflection when populating the table, there is actually no justification for the considering the risk).

A second parse over the table should then consider each risk in each cell against the Trust indicators arranged above the domain in question. The Trust Indicator(s) considered to be appropriate to demonstrate trust for the risk should be noted in the cell, related to the risk they address. The following figure indicates how this will proceed.



L-Insurance	✓	✓	✓	✓	✓
L-Financial Standing		✓			
C-Financial Background		✓			
C-Independence		✓			
C-Overall Image		✓			
C-Technical Competence				✓	
C-Professional Ethics		✓		✓	
P-Standards Compliance	✓	✓	✓		
P-Legal Compliance					✓
P-Information Security Management		✓			
P-Accountability		✓		✓	
	Tech.		Physical	Personnel	Legal
Start-up					
Operate					
Maintain					
Terminate					

Allocate to Phase as appropriate (indicator may apply to several phases)

The mapping may include blank cells but the absence of any mappings needs to be fully justified

The mapping of Trust Indicators needs also to be verified for any risk to which no TI has been associated. As with the mapping of risks, there is no proof of completeness and no ‘right’ number of mappings. However, the absence of any relationship between a risk and any TI could imply one of three possible situations: 1) the risk is not appropriate to the domain and has been wrongly mapped – if it cannot be found an appropriate place in any cell then perhaps it is not a risk which the User would be concerned with; 2) the risk is perhaps mapped into a number of domains and can be more adequately addressed in one of these (and hence can be removed from the mapping question); 3) there is a need for a new Trust Indicator which can deal with the particular type of risk concerned. Whilst at this stage the TFM still requires validation through use, and hence cannot be claimed to be either absolutely correct, nor absolutely complete, such a circumstance should be considered an exception.

At the end of this process, the matrix should be populated with a number of risk – TI couplings. In some cases a risk may be associated with more than one TI in the same cell. So long as this can be rationalised, there should be no fundamental objection to this. Likewise, whilst there should always be cautioned exercised should a cell in the matrix be completely empty or significantly more lightly populated than others, there is no absolute rule which can be expressed to suggest that all cells must always be populated. Effectively, the matrix shows what Service-sPecific User Risks can be shown to be countered by demonstration of trust in particular Trust Indicators. Just how those indicators are actually assessed is the subject of the next section.

8.

## **ASSURANCE METHODS**

There is a choice of methods and measures, some of which can be performed by internal resources. Others are intended to be performed by independent parties, and the Service Provider has to make decisions

There is a range of assessment methods available for the assurance of information services and systems, and within these methods, an even broader range of standards and criteria which can be applied. Some of these are formal and recognised at the highest international level, yet at the other end of the scale, they could be bespoke and informal, drawn up by a particular Provider organisation.

The decision facing the Service Provider is to determine the degree of assurance which his customers will expect or demand, and to select methods which deliver this degree of assurance. The Provider must exercise judgement as to the degree of trade-off between delivering assurance which is sufficient to satisfy the User needs, and the degree of investment they must make in achieving that assurance.

Unquestionably, using external sources to provide independent advice and opinion will appear to cost more, but by employing specialist services the degree of trust will in all likelihood be higher, the risk of error of judgement will be lower and there may be a degree of risk transfer for the Provider himself through the implicit or expressly-stated liability of the external source. Furthermore, beyond the Users' needs (as external parties) there may be specific imposed requirements either by industry self-regulation or in general by other providers of Trusted services with whom a Provider may wish to inter-operate.

Specific considerations when choosing assessment criteria –  
subjectivity rather than objectivity, and counterbalancing factors

The choice of assurance methods may also be determined by the nature of the User risks which the Provider is addressing or the status of the Provider. As an example, a start-up Service Provider may be expected to provide a high degree of evidence of their financial standing, possibly by external auditors, against an established and prominent organisation, who may carry a perception of their good standing, and hence subjected to much lighter demands for evidence. Their track record and their word may be good enough.

Such issues are in fact quite subjective, and would need to be judged by the Provider or their advisors in each specific case. The TFM provides the means to select methods and criteria and to justify that choice (i.e. to justify the degree of subjectivity), such that an independent reviewer could make a reasonable assessment as to whether the methods specified are adequate for the perceived need.

### **8.1 Available Methods**

A wide choice, with some methods suited to particular aspects but not others,  
and nothing today which provides an all-embracing solution (until the SEDUCER TFM)

#### **8.1.1 Testing**

One element to provide trust is to test the security measures using defined test cases. A key facet of testing is that the tests should be repeatable. Testing can not only be applied to technical equipment but also to operational procedures in order to check if they produce the expected results. For example an organisation can test its recovery procedures from time to time to verify that recovery from a specific

failure situation is possible. Different types of testing can be applied for different purposes. Examples are:

- Σ Functional testing;
- Σ Compliance testing;
- Σ Penetration testing.

### **8.1.2 Self-Assessment**

This is essentially the technical assessment of security measures used within the service. An assessment uses a specified set of criteria that define the assessment activities and the checks that have to be performed (essentially established by the Provider organisation, although external expertise could be used in their drafting). With self assessment the Service Provider performs the assessment activities himself and provides the results as well as evidence on the performance of the necessary activities either directly to his customers or to an independent body that checks the evidence and results and confirms the correct performance of the assessment procedure. Examples of potential subjects of an assessment are:

- Σ Technical equipment;
- Σ Operational procedures;
- Σ Development and Maintenance processes;
- Σ Physical Security measures

### **8.1.3 Self-Declaration**

Declaring compliance with a predefined set of criteria may be a method to increase the trust a customer has in the Service Provider. But this requires that the self declaration carries as a consequence the legal obligation to conform to the criteria defined in the declaration. A self declaration may be regulated by a scheme which then may require some additional form of either self or independent assessment or audit to be performed.

### **8.1.4 Audit**

Auditing is another method to check the technical, operational, physical, personnel security and legal compliance measures. But in contrast to an assessment or accreditation process it is normally used to check if the required measures are applied in a correct way during operation. An auditing procedure therefore relies heavily on evidence that has to be provided to demonstrate how the security measures are implemented.

### **8.1.5 Certification**

Certification within this context is an official statement of compliance to the requirements defined in a certification scheme by a certification body. Within Europe the operation of a certification scheme is regulated by the EN45000 series of standards. Certification usually requires that the compliance is checked independently before the certificate is issued.

### **8.1.6 Independent Assessment**

As with self assessment, independent assessment is viewed as the technical assessment of security measures used within the service. The potential targets for an independent assessment are the same as for a self assessment. However, with an independent assessment the criteria used in the assessment process, as well as the activities performed, need to be defined clearly in documents that are at least available to the assessment body and the Service Provider. Independent assessment by a recognised

assessment body can provide a much higher level of objectivity within the assessment process thereby allowing a direct comparison between different evaluated objects provided they are evaluated with the same level of rigour against the same set of criteria. The consistency and objectivity which this delivers can enhance significantly the trust in the service. Further, because of their broader experience on a range of systems and services, an external assessment team may be more capable than an internal team.

### 8.1.7 Independent Testing

Usually independent testing is performed for compliance testing (resulting in some kind of official statement of compliance with a standard) or for penetration testing which requires specific skill that the Provider's organisation usually doesn't have. It is important that independent testing be carried out by qualified personnel and that it can be repeated and that results are accurately recorded.

### 8.1.8 Independent Accreditation

Independent Accreditation has the same objective as self accreditation, i.e. to provide sufficient evidence for the persons responsible for operating a service to allow the service to become operational. The difference with independent accreditation is that this process needs a more clearly defined scheme. This will then allow the comparison of the results of different accreditation processes. Independent accreditation can also be important when a licensing or regulatory body party has to approve a service as being fit for operation. Independent assessment is likely to make the results more trustworthy by parties outside of the accredited system / organisation.

## 8.2 Standards and Criteria

The potential list of standards and recognised criteria which could be applied are beyond the scope of this project, and even a comprehensive list at the time of publication would not remain up-to-date for very long, such is the level of activity in this particular area. Furthermore, subject to the acceptability of any particular standard or basis of assessment by the User community, by any licensing or legislative regime and possibly by other Providers, there is no reason to limit the choice of methods to any particular list, and even bespoke criteria should not be discouraged as a de facto policy. Indeed, the idea of a Trust Assurance Specification will seek to provide, where necessary, a controlled measure of bespoke criteria. Thus, we mention a small number of recognised assessment standards and criteria as well as prominent legislation, as an illustrative aid only. No claim of completeness nor of implied suitability or relative importance is intended by the inclusion or exclusion from this list of any particular reference.

### Technical Standards

ITSEC 1992

US Federal Information Processing Standard (FIPS PUB 140-1)

BS7799 "Information Security Management" Part I: 1995

SEI Capability Maturity Model (CMM)

System Security Engineering Capability Maturity Model [SSE-CMM]

Common Criteria Version 2.0 Draft

EN45000 Series

IEC 1508 Safety Critical standard

ISO 9000 series - specifically

- ISO 9000-1 : 1994
- ISO 9000-2 : 1997
- ISO 9000-3 : 1991
- ISO 9001: 1994
- ISO 9002: 1994
- ISO 9003 : 1994
- ISO 9004-1 : 1994

Chip-Secured Electronic Transaction (C-SET) Security Architecture, Vers. 1.0, 29th January 1997

NIST Federal Public Key Infrastructure

TTAP

Legislation:

Deutsches Signaturgesetz

FR encryption law, 96-659 dated 960726, article 17

Leggere Bassanini Regulation, March 23rd 1997

EC COM (97) 503

American Bar Association 'Legal Infrastructure for Certification Authorities and Secure Electronic Commerce', published August 1, 1996

BXA Interim Rule

Utah Ruling

UK Govt Secure Electronic Commerce Statement, April 1998

EC COM (98) 297 on Common Framework for Electronic Signatures (in draft form)

Policies:

BelSign's - Version 1.0 5 October 1996

Verisign Certification Practice Statement, Published May 15<sup>th</sup>, 1997.

Anonymous Service Provider's CPS - 1998

Deutsches Forschungsnetz Certification Practice Statement for the Policy Certification Authority, 1997

### 8.3 Selecting Assurance Methods

The relationship between the Trust Indicators and the Assurance Method(s) has to be carefully explained and justified to support the Trust. At least one Assurance Method has to be used

It is important to keep in mind that the purpose of applying the TFM is to develop the means of conveying trustworthiness at the point in time at which a User subscribes to the service, and to maintain it thereafter. This could be either when the Service itself is starting up or when a new User is subscribing after the Service has become established. In either case, the objective is to give trust to the User. Therefore, even such 'distant' events as Termination have to be dealt with at the time of

applying the TFM, so as to give the User confidence that the whole life-cycle of the service has been considered. This stage of the process

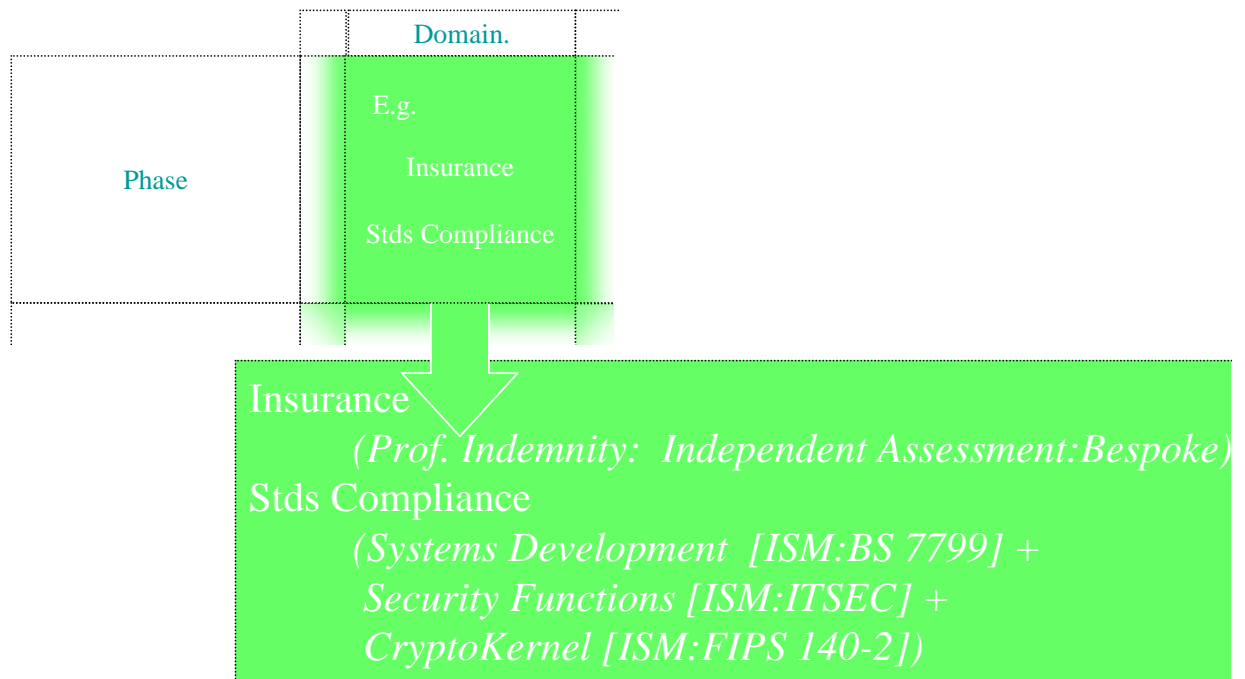
The selection of Assurance Methods starts with consideration in turn of each SPUR / Trust Indicator in each cell of the matrix.

For each SPUR / Trust Indicator pair, there must be identified some aspect of the overall service provision that can be assessed to support the selected Trust Indicator.

As already described, the Service Provider should make in parallel their own risk assessment considering their internal objectives and policies, which will lead to the selection of various Security Measures, be they procedures, physical means or technological components. These will be mapped into the SPURs as well as to other internal risks. Through these it is therefore possible to establish a mapping between Trust Indicators and related Security Measures. Therefore, to achieve this, in each cell of the matrix the related Security Measures should be noted, retaining their relationship to the SPUR / Trust Indicator pairs.

The extent to which these Measures can counter the risk should be assessed, and the level of risk reduction used as the basis for selecting the level of assurance required: the greater the contribution to overall risk reduction, the greater the level of assurance that will be required.

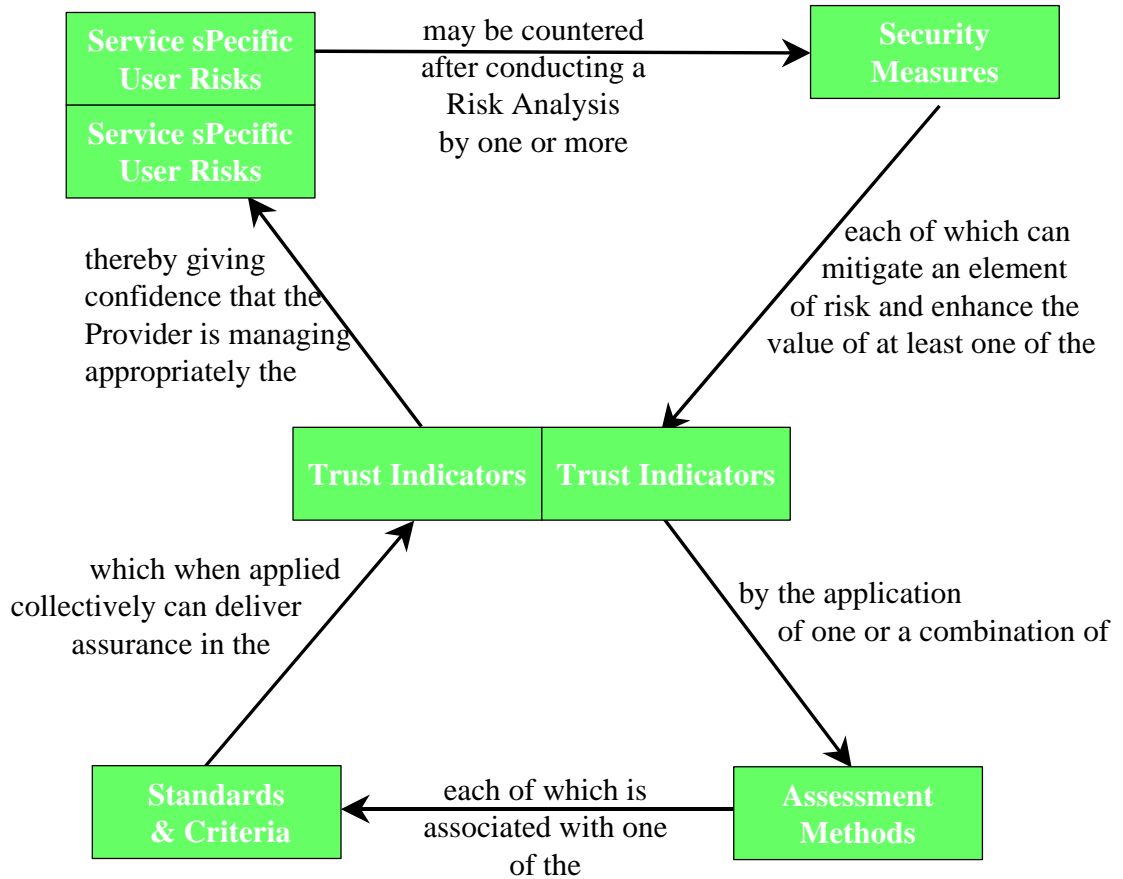
For each identified Security Measure, at least one Assurance Method should be selected, and at the same time a suitable Standard or Criteria specified. A brief justification for the choice should be made, both as an aide mémoire for the author, and to support any analysis of the choices made by another party. Thus for each Security Measure the matrix will in one direction provide a mapping to the Trust Indicator which it supports, and in the other the Assessment which should be performed to demonstrate risk reduction and hence justify the trust placed in the Trust Indicator. The Level of Assurance required from the Assessment process should be defined, determined by the degree to which the identified Security Measures mitigate specific risks. The following figure illustrates the concept.



At the conclusion of this Assessment selection process, some Security Measures may justify more than one Assurance Method and/or different Standards or Criteria being nominated. This could typically be where a technical component required detailed security analysis in order to contribute to a higher-level form of Assessment, such as is suggested in the preceding figure. By such a means we will also find different Security Measures being assessed by quite different criteria, but for those assessments to then be taken into consideration in other assessments performed on a broader basis. This intended relationship should be indicated when the mapping process is applied. For that reason, the ordering of the different Assurance Methods should suggest to the reader and implementor the intended relationships, e.g. A + B would suggest that Assurance Method ‘A’ takes account of Method ‘B’.

The relationship between SPURs, Service Aspects, Trust Indicators, Assurance Methods and Standards/Criteria can be illustrated, if somewhat simplistically, as in the following Boonogram.





Application of the TFM involves much justification of choices and analysis – this is necessary to allow others to understand why certain methods are chosen, and the relationship between methods

Part of the provision of Trust will stem from the rationale for the particular choice of Assurance Method(s). If a choice can be well-explained in the context of the particular service, risk and Security Measure, then greater Assurance will be taken from the evidence of conformance or compliance.

When the selection of Assurance Methods has been completed, it will be necessary to perform another consistency check. This time the objective is to identify whether any SPUR / Trust Indicator pair has been omitted from the mapping. As with the matching of SPURs to Trust Indicators, whilst there is no correct number of Security Measures to support a SPUR, there is clearly either an oversight or an error of understanding, if any SPUR / Trust Indicator pair remains without at least one related Security Measure and accompanying Assurance Method. Wherever this occurs, the circumstances must be reviewed to determine whether the situation is genuine, and therefore there must be a related Security Measure requiring an Assurance Method, or it is an error undetected in the preceding process (Referring to the Trust Indicator Matrix). In the former case, the solution may be to add some bespoke methodology and criteria within the TAS (see later).

The conclusion of this process should provide a matrix which is populated with a comprehensive description of the relationships from Trust Indicators through SPURs to Security Measures and the related Assurance Methods and Standards or Criteria used to demonstrate the trustworthiness of the service.

The available information can be analysed in two important ways – these are each now described.





## 8.5 Assurance Levels

There is no ‘natural’ and consistent measure of assurance across the scope of the SEDUCER TFM

The concept of Level of Assurance is quite a natural one, and implies a question which will frequently be asked. However, taking into consideration the range of possible services, the various facets of the service which have to be trusted (e.g. technical *versus* legal *versus* personnel, ...), the different phases of the life-cycle, the existing standards or criteria which can be used to assess trust, and other factors it becomes clear that the overall trust for a TTP service is actually multi-dimensional. Reducing this in total to a single dimensional scheme like a set of levels will not address adequately all aspects of trust in Trusted Services.

For example, several standards deal with the assessment of technical equipment, organisations or even the qualification of personnel define a set of hierarchical levels. Such levels do not naturally relate to other aspects such as physical security or personnel. The framework defined in this document has identified a whole set of trust indicators that hardly can be measured on the basis of a single scale. The definition of a single set of trust levels that can be applied to all different types of TTP services, cover the whole life cycle of such a service, is suitable for all trust indicators and is also independent of details of the implementation of the service is therefore extremely difficult to define, and it is doubtful whether doing so would not destroy any utility by the degree of ‘normalisation’ required.

Looking at the framework defined in this document one also can see that some of the trust indicators are not actually designed to increase the level of trust one can place in the delivery of a service, but are designed to *decrease* the level of trust *needed* in order to use a service. Liability is the most evident one of those indicators. The framework also includes very subjective indicators, such as the reputation of a Service Provider, that cannot practicably be expressed in terms of levels which have the goal of defining (as far as possible) an objective way of measuring trust. It is clear therefore that most assurance methods can be used only for the assessment of a few trust indicators.

Nevertheless, can the definition of a set of levels be useful, if not necessary, when addressing a specific type of service. Within an overall licensing scheme (whether governmental or industry-driven) a possible approach might be to prepare such a definition for each of the services which fall within the scheme. A scheme adopting such an approach would usually define limitations for the application of the service, require mandatory security measures and make a pre-selection of assurance methods from the set defined in the framework. In this case the definition of levels makes sense and we will just describe briefly, how the framework can used to define such levels.

Looking at existing standards that define trust or assurance levels (e. g. the Common Criteria, ITSEC, FIPS 140-1, IEC 1508) one can see some commonality in their definition. They all define their own levels from a limited set of assurance methods by increasingly more stringent demands, and it is possible to provide a mapping between them. These levels are based upon:

- Σ the type of assurance methods used;
- Σ the number of assurance methods used;
- Σ the degree of rigour used for a specific method;
- Σ the degree of independence of the assessor from the target of assessment;
- Σ the degree of competence of the assessor or assessment team.

However, none of these standards gives a satisfactory justification why a specific combination of assurance methods provides a higher level of assurance or trust than other ones. Furthermore, these standards address only a subset of the trust indicators mentioned in the framework. This

acknowledges the fact that all these standards try to approximate a multi-dimensional problem by a single set of hierarchical levels thereby focusing on specific trust indicators and specific functional aspects of the target of assessment. Nevertheless those levels can provide a useful guidance for the comparison of different targets of assessment and for the selection of assurance methods.

**A preliminary means to define minimum assurance profiles can be shown**

The framework defined in this document can be used to define an accreditation or licensing scheme and can also be used to define levels in much the same way as the other standards. Based on the type of service covered by the scheme and the mandatory security functions required one can define a set of levels by:

- Σ selecting those trust indicators that are to be measured by the levels;
- Σ selecting an appropriate set of assurance methods for the trust indicators. Usually the set for a higher level should be a superset of those for lower levels;
- Σ provide additional details on how to apply the methods for the type of service addressed;
- Σ define the degree of rigour for the assurance method;
- Σ define requirements for the skill and independence of the assessors.

By this means, a set of minima can be defined for notional levels of assurance. Within a particular scheme, a specific qualification could be stated for each aspect in which trust was required, to effectively provide a minimum profile, for each level of assurance to be defined (e.g. Basic, Moderate, High, Very High). Anyone claiming to satisfy the criteria for any given level would need to demonstrate their fulfilment of the criteria. Because of the complexity of this aspect of trust we propose that rather than demanding absolute compliance with minima there is a degree of qualified subjectivity permitted, which would allow a claimed assurance to contain some elements which did not meet the minima for the level claimed but which had justified balancing measures in place which counter-acted any perceived deficiency in achievement.

Additional complexity is added by the fact that the framework covers the whole life cycle of a service. Most of the above mentioned standards that define trust or assurance levels do this for a static target of assessment. Maintaining this level over the life cycle has not been addressed by any of them. While such a simplified static view may be acceptable for the assessment of products, it is vitally important to address the whole life cycle when the target of assessment is a service. To do this it is necessary to either select assurance methods that cover all life cycle or to define a set of different assurance methods for each life cycle phase and justify why these different combinations define a comparable level of assurance.

These remarks give just a simplified perspective on the definition of levels of trust for TTP services. Defining useful detailed levels for such a complex target like a TTP service requires a significant amount of work as the existing standards for the assessment of comparatively simpler things like IT-products have demonstrated. The purpose of this framework is just to give some guidance how such levels may be defined, but clearly further practical application of the framework is required to bring out the detail solutions which can make it an effective tool

## 8.6 An Assurance Path

### Providing for traceability within the assurance process

A key interpretation of the matrix is to identify all instances of each SPUR in turn, and to illustrate what Security Measures are in place to counter which of these SPURs and to show how trust is provided. In other words, this analysis provides a thread from each SPUR to the actual Trust Indicators which support trust that the SPUR has been adequately addressed, and behind that, should the User or any other party with a legitimate interest so wish, is the opposite path to specific Security Measures and the actual methods and criteria employed.

## 9.

## **TRUST ASSURANCE PLAN**

The need to address all aspects of a service's provision, probably requiring at least a small number of different methods, presents certain challenges when attempting to perform a broad assessment which delivers an overall opinion

In this section we introduce the Trust Assurance Plan which allows a Service Provider to define how the assessment steps required to fulfil the TFM can actually be implemented. Its major component is the Trust Assurance Specification (TAS), already mentioned in preceding Sections. We also show how the concept of a TAS can support the definition of licensing and regulation schemes.

### **9.1 Providing the Glue – the Trust Assurance Specification**

Work done previously by this consortium has identified needs for wider application of certain methods, principally ITSEC, and the way in which much broader assessments can be carried out

During the earlier phases of DGXIII's INFOSEC / ETS Programme members of this consortium undertook studies into the relationship between ITSEC and such practical issues as the evaluation of telecommunication services, its applicability to distributed services and the accreditation of commercial systems. Without exception, each of those studies commented upon the limitations of the ITSEC process alone, not just in its ability to cover important security aspects of systems and businesses, but also in its shortcomings in being able to handle distributed and multi-domain technological systems. These studies identified the need to take into account a broader range of issues and the need for some kind of scheme and process for accomplishing that. Some of the recommendations made have been applied by those organisations, but more needs to be done to encourage wider take-up.

The analysis performed then and now during this project has clearly shown that none of the existing schemes covers all life cycle phases and all domains of a service. It is also unrealistic to expect that this can be subject to a single scheme. Due to the wide range of aspects that need to be covered and the difference in the contribution to risk reduction of individual security measures, one can reasonably expect that a combination of assessment techniques will be used. This is also driven by the fact that assessments are needed in all phases of the life cycle of a Trust Service, i.e. they have to be performed at different stages and routinely executed on a periodic basis. The strategic utility of risk assessment and analysis has to be considered in the context of updating, enhancing, relocating, reconfiguring, etc., to assure that the best alternative from a business perspective is also the best from a risk management perspective (the unconsidered risk on the front end may well far outweigh the business perspective upon implementation of a risk-ignorant decision).

None of the existing schemes for assessment covers this broad spectrum. On the other hand there is neither a systematic approach for the combination of existing schemes nor has anybody analysed the deficiencies of existing assessment schemes with respect to different kinds of TTP services. In several EU Member States, as well as elsewhere in the world, regulations for TTP services are currently already issued or in preparation but the basis for the development of these approaches is unclear. The analysis performed has shown that the resulting schemes - even when aimed at the same type of service - are very different in their requirements for individual life cycle phases, service domains and assessment techniques. Comparing those schemes is almost impossible since they all use different combinations of Trust Indicators, address different life cycle phases and cover different service domains. But international recognition of TTP services - a key factor for their use within Electronic Commerce applications - requires a consistent and widely recognised method to compare the level of trust that can be placed in the provision of the service.

It is far beyond the scope of this project to derive a single scheme that can satisfy the need for comparability across various kinds of TTP services. Instead it is the intention of the project to provide a basis in the form of an outline description of the aspects of a service requiring assurance and the methods used to provide that assurance. In the previous chapters the document has described the life cycle Phases and the Service Domains as well as Trust Indicators. We now give an outline of a document that can be used to describe how the Trust Indicators are applied to the security measures selected for the life cycle phases and domains of a service. The purpose of this “Trust Assurance Specification” (TAS) is to give a complete and comprehensive overview of security and assurance features the Service Provider has implemented. It may also be used as baseline within some kind of licensing, service certification or auditing process but in those cases it will usually describe more features than required by the individual processes.

A particular function of the TAS is to define the way in which an overall assessment result is brought about through the various assessment methods which are, in reality, likely to be employed within any one Trust Assurance Plan.

It is recognised that many of the standard means of assessment are defined in such a manner as to be quite self-contained. Thus, although FIPS 140 adopts a number of ITSEC-like stylisms, there is no defined manner in which the results of the FIPS 140 assessment could be taken properly into account in an ITSEC Evaluation (neither on the part of FIPS 140 nor by ITSEC/ITSEM). An Evaluation is, in theory, limited strictly to the scope of the Target of Evaluation as described in the Security Target, the format of which is dictated by the ITSEC documentation. There is no defined capacity to specify how the results of other assessments (even ITSEC ones) can be taken into account. And yet, at least three previous studies (each of which were undertaken by some members of the SEDUCER consortium) have identified clearly the scope for extending the ITSEC to make it more amenable to being applied to distributed systems, telecommunication systems, and as part of a broader Accreditation model.

The purpose of the TAS is, therefore, to define the overall set of assessment methods which will be applied collectively to deliver the Trust Assurance for the Service in question. In particular, the TAS provides the ‘glue’ to marry these different assessment methods together and defines any additional methods and assessment procedures for those areas where there may be a need to assess but no existing method which suits the need.

It is not intended that the TAS be a particularly large document. Mainly, it references other documents describing in more detail the information required by each part of the TAS. There is also no need for a single person or entity to see all the details of all aspects. For example the person or organisation responsible for the assessment of the technical security features of a service does not need to have the detailed information on the financial aspects and vice versa. What they do need is a general understanding of what is covered by the aspects and what the dependencies on other security features are. The TAS is therefore the basis document that should be used by any assurance assessment to gain an overall view of the risks and how they are addressed. If different parties are involved in the overall assessment (which one expects to be the case for most services) the TAS is the common document every assessor should have and should work from.



### 9.1.1 Structure of the Trust Assurance Specification

We suggest the following structure for a Trust Assurance Specification:

#### 9.1.1.1 *Part1: Service Description*

This general description must cover the following points:

- Σ Nature of the service, general purpose of the service;
- Σ The Service Provider, its Customers, other parties involved;
- Σ General security objectives and outline security policy of the service;
- Σ Intended method of use of the service;
- Σ General security features provided by the service;
- Σ Obligations of the user of the service;
- Σ Service provider's general conditions for use, limitations of use of the service;
- Σ Service provider's statement of liability;
- Σ Compliance with standards, laws and regulations, achieved certificates, licenses or accreditations;
- Σ Overview of the security measures and trust assessment methods used (i. e. a summary of the other parts of the Trust Assessment Specification) and a high-level view of their relationships, the Dependency Diagram (see Trust Assurance Planning).

This part therefore provides an overview of the service, how it should be used and the security it provides. Since the Service Description is intended to be handed over to potential customers to give them the information they need to select a service from a functional as well as from an assurance point of view, Part 1 should be held in a form that can be readily distributed.

The Service Provider should determine the level of detail he chooses as appropriate for this summary descriptions. Certificate Practice Statements published by some Providers of certification services are examples that could serve as such a summary part. Our review of Certificate Practice Statements (CPS) for Certification Services has shown that many of the existing CPS's already cover much of the content required for this part of the Trust Assurance Specification and some of them even contain information required for other parts of the TAS.

### 9.1.1.2 Part 2: Technical Security Aspects

This part must address all technical security features used in the provision of the service. It is structured into those technical features that are part of products developed independently by a third party. It also addresses technical security features implemented in hardware or software developed by the Service Provider or by a third party under a contract by the Service Provider. The following information should be provided in this part:

For products:

- Σ Description of IT-products used and the security features of these products;
- Σ Description of the way the IT-products are used to provide the service;
- Σ Description which risks are addressed by the security feature;
- Σ Description of the relevance of the product within the life cycle phases;
- Σ Description of dependencies on other security features;
- Σ Description of the assurance given by the product manufacturer as well as additional own or third party assessments performed.

For own developments:

- Σ Description of the hardware and software developed by the Service Providers or on his behalf;
- Σ Description of the security features of this hardware and software;
- Σ Description of the way this own developments are used to provide the service;
- Σ Description which risks are addressed by the security feature;
- Σ Description of the relevance of the developed hardware or software within the life cycle phases;
- Σ Description of dependencies on other security features;
- Σ Description of the assurance methods applied within the development as well as during operation and maintenance.

Part 2 is intended to serve as a basis for the analysis of technical aspects of the service. In those areas where the Service Provider uses commercial products, they should describe how the security features of those products are used and how these features relate to the risks of the service. The methods used to obtain the necessary assurance that these security features work should be stated. This may range from stating a FIPS 140, ITSEC or CC evaluation, own test and analysis performed, up to a self declaration of the product manufacturer. It may also well be a combination of different assurance methods e. g. using an evaluated product but also performing additional tests because the configuration used differs from that which was evaluated. Arguments should be presented as to how those assessment methods are regarded as sufficient.

Usually within the TAS the descriptions given will be an overview or a summary with references to other documentation (e. g. product descriptions or design documents) that provide more details. Documentation resulting from assessments performed (e.g. ITSEC, CC, FIPS 140-1 or other types of evaluations) will be referenced within a summary of the description of the assessments performed. Anybody who needs access to these details (e.g. since they are needed for other assessment schemes such as an Accreditation) then has a direct link to those results.



### 9.1.1.3 Part 3: Physical Security Aspects

This part addresses all physical security measures. It should contain:

- Σ Description of the physical protection features used for the protection of service critical assets;
- Σ Description of the risks reduced by those security features;
- Σ Description of the relevance within the life cycle phases;
- Σ Description of the dependencies on other security measures;
- Σ Description of assurance methods used to assess the effectiveness of the physical security measures. This includes methods applied in the Pre-Operation phase as well as those used in the Operational and Maintenance phases.

Again, it is expected that the TAS presents just an overview of the aspects mentioned, referencing further documents that contain additional details on the physical protection features or the methods used to assess their effectiveness.

### 9.1.1.4 Part 4: Operational Aspects

This part addresses the Operational Procedures defined by the Service Provider to counter risks identified in the risk assessment. It must provide descriptions of:

- Σ The security critical operational procedures implemented;
- Σ The risks addressed by the procedure;
- Σ The life cycle phases addressed by the procedures;
- Σ The dependencies on other security measures;
- Σ The assurance methods used to assess the effectiveness of the operational measures. This includes assurance methods taken when the service is designed and set up as well as methods taken in the Operational and Maintenance phases.

### 9.1.1.5 Part 5: Personnel Aspects

This part addresses the Procedures and Conditions imposed upon Personnel by the Service Provider to counter risks identified in the risk assessment. It must provide descriptions of:

- Σ The personnel measures implemented to protect the service;
- Σ The risks addressed by the measure;
- Σ The dependencies on other security measures;
- Σ The assurance methods used to assess the effectiveness of the measures.

### 9.1.1.6 Part 6: Maintenance Aspects

This part addresses how the Service Provider manages the risks identified in the risk assessment when performing upgrades and enhancements to the service. It must provide descriptions of:

- Σ The change management policy and procedures;
- Σ How the effectiveness of technical, physical and operational measures is intended to be maintained;

- Σ Re-assessment of the effectiveness of security measures after changes have been performed.

Of special importance is the description of the conditions that require an update of the TAS itself. This is required when any of the following conditions are met:

- Σ The general functionality of the service or the intended purpose has changed in a way where the description of the service (i. e. Part 1 of the TAS) needs to be updated since the modifications to the service influence aspects described at this generic level;
- Σ The security measures (technical, organisational, physical or personnel) have changed, needing the description of those measures in parts 2 to 5 to be updated;
- Σ The risks have changed so significantly that those changes need to be reflected in the TAS;
- Σ The trust assessment methods have changed;
- Σ The liability, legal or regulatory situation has changed;
- Σ Dependencies on or relations with other services have changed.

In any of these cases a decision has to be made not only on the necessary updates to the TAS but also if there is a need to update the risk assessment and to re-apply part of the assessment. Part 6 of the TAS should specify minimum conditions for when this is necessary. Since these conditions are dependent on the type of service, the level of assurance needed, the changes in the overall risk and the specific assessment methods selected, no further guidance can be given at the level of this framework.

#### **9.1.1.7 Part 7: Security critical relations with other services**

This part addresses dependencies the Service may have on other services from other providers, and how the risks identified in the risk assessment are managed. It must provide descriptions of:

- Σ Security-critical relationships to other services and which risks are associated with the use of the service;
- Σ The security assumptions made for those services;
- Σ The assurance provided by those services;
- Σ Requirements for additional assessments with respect to other services.

As an example one can consider an electronic payment service relying on certificates issued by another Service Provider. Another example is the aspect of cross certification, where a Service Provider establishes a chain of trust between his Users and another Service Provider. In this case he not only has to look at technical interoperability but must also either demand a comparable level of trust from the other Service Provider or give his Users a warning about the differences in the level of trust between his certificates and those issued by the other Service Provider.

### 9.1.1.8 Part 8: Liability, Legal and Financial Aspects

This part addresses liability aspects identified in the risk assessment and how these risk are countered plus how the Service complies with incumbent legislation and regulation (in both legal and financial senses). It must provide descriptions of:

- Σ The liability provided to the Users;
- Σ The financial standing and resources available to cover liability cases;
- Σ The financial resources to guarantee ongoing provision of the service;
- Σ The methods used to assess the financial circumstances of the Service Provider;
- Σ The laws and regulations with which the service is compliant together with a statement of how these specific requirements have been identified and how this compliance is confirmed.

### 9.1.1.9 Part 9: Service Termination Aspects

This must be a description of the measures taken to ensure that the interests of the service's Users are protected when the Service Provider decides or is obliged to discontinue the provision of the service. This may describe actions taken by the provider to prepare for a controlled shutdown as well as provisions that enable another provider to take over. The degree of continuity must be clearly described under circumstances of outright termination or in the case of transfer. It is recognised that this may be an issue of intention rather than absolute fact, but the availability of provision for such circumstances will provide confidence to the Users.

## 9.2 Alignment with Licensing and Accreditation

In the previous section we have described the outline structure of the Trust Assessment Specification which a Service Provider can use to describe the safeguards he has implemented to protect his service from defined threats and how he plans to perform the assessment. Licensing or accreditation schemes now specify a minimum set of security measures usually accompanied by a set of required assessment techniques. But a licensing or accreditation scheme should also state which assumptions they make on the provided service give some justification why they require the measures and techniques. So the structure of the TAS given in the previous section can (with slight modifications) also be used to describe the purpose and requirements of a licensing or accreditation scheme. The benefit of harmonising the structure of the description of the scheme with the TAS is obvious: Showing compliance with a given licensing or accreditation scheme is much easier, since the relevant items needed to assess can be easily spotted in the TAS. The following structure is therefore suggested for the description of such schemes:

Part 1 would then contain:

- Σ The objectives of the scheme
- Σ The type(s) of services it can be applied for
- Σ The risks addressed by the scheme
- Σ Obligations of Service Providers and users under this scheme

Part 2: Technical Aspects down to Part 5: Personnel Aspects would have the same structure

- Σ Minimum functional requirements that need to be fulfilled to comply with the scheme
- Σ Mandatory functions or standards
- Σ Minimum assurance requirements
- Σ Mandatory assurance methods or standards
- Σ Mapping of the functional requirements and measures to risks

Part 6: Maintenance Aspects contains

- Σ Minimum security requirements for maintenance
- Σ Requirements for the assessment or re-assessment in the case of changes

Part 7: Security Critical Relations on other Services

- Σ Functional requirements for other services
- Σ Requirements for conformance with standards
- Σ Requirements for licenses, accreditation or certification of other services
- Σ Minimum requirements for contractual relationship

Part 8: Liability, Legal Aspects and Financial Standing

- Σ Minimum liability conditions
- Σ Required conformance with laws and regulations
- Σ Minimum financial backing or insurance

Part 9: Service Termination

- Σ Requirements to prepare for hand over to another provider
- Σ Requirements taken in advance to prepare for the termination of the service

The advantage of having a Trust Assurance Specification and the description of licensing or accreditation schemes following the outline given above is obvious: It would present an easy way to compare the functional and assurance aspects of TTP services as well as licensing or accreditation schemes. Hence, identifying the information needed to check the compliance of a service to a given scheme becomes much easier. Both are goals that need to be achieved when TTP services are to be used on a wide basis within any global trust services infrastructure where one will see a network of TTPs operating in different countries under different legislation and regulations.

## 9.3 Trust Assurance Planning

The culmination of the application of the TFM, of the performance of the risk analysis and the preparation of the TAS comes when the measures identified are put into practice. In other words, when the TAS is applied, the assessments are performed and their results used to establish the required Trust.

### 9.3.1 Applying the Trust Assurance Specification

The TAS will serve as the top level description of the security measures and trust assessment methods used within the service. It is therefore necessary to assess the TAS itself for completeness and consistency. Completeness does not only mean that all identified risks are addressed but also if the requirements of those standards and licensing or accreditation schemes are met, compliance with which has been claimed in part 1 of the TAS. Since details of the security measures as well as the assessment methods may be defined in additional documents, a complete check for compliance cannot normally be performed on the basis of the TAS alone. But at least a general check for completeness, consistency and compliance with cited standards and regulations should be performed immediately when the TAS is developed. A generic approach for this check will include the following steps:

1. Examination of which cells in the Phase / Domain matrix security measures have been defined;
2. Justification for why specific cells are empty (i.e. look for arguments that all relevant risks are addressed within the non-empty cells);
3. Relate the trust assessment methods to the individual security measures and verify that at least one method is defined for each measure;
4. Check the security measures and trust assessment methods for compliance with the requirements of the cited standards, laws, regulations and licensing or accreditation schemes;
5. Check that the TAS describes in sufficient detail under which conditions changes to the service imply changes to the service description, security measures and trust assessment methods;
6. Check that procedures for the update of the TAS itself are defined;

For the individual security measures and assessment methods the TAS will on the one hand serve as the document describing the top level requirements for both security measure and assessment activity and on the other hand describe how they all interrelate and which dependencies exist. When different assessment activities are performed by different teams possessing different specific skills (which one expects to be the case for most services) the TAS gives each team the general overview needed to relate the assessment activity performed by the team to those performed by others. In particular, dependencies and interrelationships between different security measures and different assessment methods should be described in the document, so that each team knows which other relies on their results or which results from other teams they should take into account. This description, the high-level Dependency Diagram, will be included in Part 1 of the TAS and may be put into the public domain to aid description of the trust assurance process.

### 9.3.2 Applying the Trust Assurance Plan

In order to finally realise the benefits of the TFM it is necessary to define the plan which will be implemented to perform the assessments and use the TAS to effect their integration into the final statement of trustworthiness. The initial point for this will be the Dependency Diagram.

The following steps are therefore necessary:

- Σ For each separate assessment identified, its scope must be defined in terms of the selected standards or criteria to be applied (e. g. for a CC or ITSEC Evaluation, a Security Target must be prepared);
- Σ For any assessment for which bespoke criteria are required, these need to be drawn up;
- Σ A Trust Assurance Plan (TAP) needs to be prepared, showing the interdependencies between both the actual assessments themselves (already described in the Dependency Diagram), and the Service Development Plan for the service as a whole (this allows for those assessments which are, e.g. related to the development of service components to be undertaken as those events take place);
- Σ Where the Plan shows assessment results being used in further assessments (and indeed for the final assessment at the TAS level) the necessary ‘glue’ which the TAS provides should be defined and included within the definition of the assessment (if not already accommodated);
- Σ Where third-party participation is required for the assessments, external services must be selected and contracted in accordance with the TAP;
- Σ The TAP should be implemented in close co-ordination with the Service Development Plan.

This high-level dependency chart will serve also as a

The implementation of the TAP will require specialist skills to ensure it is competently implemented, but this should be done in close co-operation with the Project manager responsible for the overall development. The need for these skills to be specialist does not imply that they are therefore automatically available only outside the organisation delivering the service. Most Service Providers should be able to use in-house skills for much of the work, at least for preparatory tasks if not for final assessments.

In the case that Trust Assurance is being put into place after the deployment of the service, i.e. retrospectively, the same basic steps need to be considered, although the relationship with any Service Deployment Plan will clearly be different. In such circumstances the inability to assess development of specific components will not exist, and sufficient evidence to allow retrospective assessment may not exist. Such matters should be considered in the overall risk assessment, and accommodating measures identified. E.g. if it is not possible to monitor the development of a software package this may be counter-balanced by undertaking a more exhaustive assessment of the delivered package.

## 10.

## **BENEFITS OF ADOPTION OF THIS FRAMEWORK**

The benefits of the widespread adoption of this framework can be expressed in the following nine points:

### **10.1 Flexibility**

The TFM is **flexible** in that it addresses all aspects of the service (not just the Technical aspects, as is the tendency) and furthermore it covers the whole of the **operational life-cycle**, thus giving the User the basis of **widespread trust** with regard to the long-term provision of the service, not just an assessment at the start of the service provision.

This means that the TFM is capable of being **adapted** to the wide range of PKI trust Services, and potentially to the broader range of **Added-Value services** which will emerge.

### **10.2 Methodology**

The TFM presents a **structured approach** to the assessment of Trust, based upon widely accepted **principles of risk assessment**, but putting the focus on looking at the issues from the point of view of the User's usage of the service. Furthermore, it provides a clear description of the approach to be taken, through the provision of a **clear methodology**.

This means that the TFM can be **readily understood** by those with a non-technical business focus, yet applied by those with the capability of understanding the technical implications and who are familiar with the range of assurance methods available and are therefore capable of **constructing a coherent Trust Assurance Plan**.

### **10.3 Widespread Service Applicability**

The TFM as described herein presents both a **generic approach** to the assurance of Trust Services and also **specific guidance** for the range of PKI services identified within the present model (see Annex I).

This means that the TFM is **not specific** to any particular type of service yet **provides support** for the development of a Trust Assurance Specification for specific instantiations.

### **10.4 Open model**

The model **neither mandates nor excludes** any particular assurance methods or standards or criteria.

This means that it is **Open** to the inclusion of any appropriate method of assessment or assessment criteria / standard whose inclusion can be justified and for which the appropriate 'glue' can be specified to integrate it into the overall Trust Assurance Specification. It also means that the model can evolve with the emergence of revised standards etc.



## 10.5 Extensibility

The openness of the model means that it can adapt to the changing needs of the Service Provider or User, through the inclusion of additional assurance measures, as changes in risk perception or the nature of the service provision dictate.

Furthermore, the matrix which is a central part of the model is not necessarily confined to the five vertical domains we have identified. If a sixth (or seventh) domain can be identified then it can be added to the matrix. A possible example of such is the issue of the way trust may be embedded into a social system. This could be argued to be a sixth domain, although we have chosen to not explicitly recognise it but to declare that it is embodied in the legal domain in particular, and possibly to some degree in operational and possibly personnel domains. Nevertheless, the principle remains that a new domain could be added. Were this to be done, then the existing or new trust indicators might need to be identified and added to the model.

All of this means that the Trust Framework Model is not a dead-end, one-use, concept, but one which can be applied throughout the life of the service provision / consumption.

## 10.6 Adaptability

The structure of the Trust Assurance Specification means that the model can be **applied commonly** through a range of Trust-related paradigms, in particular: the EC **Directive** on a common framework for electronic signatures, national / industry **regulatory and licensing** schemes, and specific Trust Assurance Specifications.

This means that the model provides a **common back-bone** across these differing paradigms which **eases transition** from one to another, **facilitates the verification** of compliance across them (i.e. does a particular licensing scheme align with the EU Directive; does a particular TAS align with the licensing régime within which it claims to fit?) and acts as a **comparative basis** between them (i.e. is one licensing scheme equivalent to another and to what degree?).

## 10.7 Binding qualities

The TFM provides the “**glue**” to integrate a range of otherwise not explicitly compatible assurance methods.

This means that the TFM is a genuine **basis** upon which **to assess** Trust Services across the range of their domains and extended operational lifecycle.

## 10.8 Comparative Trust

By offering a **common framework**, the TFM provides a common basis for **comparison** of trust between different Trust Service Providers.

This means that the consumer has at their disposal a means by which to **judge** a service according to their requirements for trust and the **demonstrated trustworthiness** of the service.

## 10.9 Guidance

The TFM provides, through its **Application Guide**, advice on its application across a range of Trust Services.

This means that Service Providers have available **guidance** for the development of their TAS and hence a basis for **establishing their trustworthiness**.

## APPENDIX I - APPLYING THE 'UNIVERSAL' RISKS

### 1. EXAMPLES

Some simple examples, since we cannot imagine to completely understand all the factors in actually operating a service, even if many can be assumed.

The following section gives some examples of how the generic user risks can be refined in a first step for some types of TTP services. These refinements are still very generic, because implementation specific details of the service cannot be taken into account. We therefore can not claim that this first step refinement gives a complete picture of all user-related risks in providing the service. The purpose of this exercise is more to provide a starting point for the service specific risk analysis and relate risks to the life cycle phases.

The refinement does not have an extra column for each domain, because without further details on the specifics of the implementation and provision of the service this does not make much sense. But this first refinement already gives an indication, which phases and domains will be of special importance for the service. As an example, we have already argued that for some types of TTP services the termination aspect is of almost no importance while for others the importance of this phase has to be regarded as very high. Also some type of services will probably rely more on operational procedures (e.g. a registration service) than others. The examples will give some hints for the most important domains, although as we already said this may vary depending on the specific implementation and way of operation chosen by the Service Provider. It is therefore for the Service Provider to justify how and in which domain the refined risks have been addressed.

The result is a first approach to a risk profile for some types of primary value TTP services. They are mapped to the phases as far as this can be done without knowing details about how the service is implemented. Since the security measures are deliberately not prescribed by the *SEDUCER* framework, a mapping to the domains is only possible when details about the implementation of the security measures of the service are known. Nevertheless the list of risks can be used as a first checklist to see if the most obvious have been covered.

The following examples cover some important Primary Value services

## 1.1 Example 1: Key Generation Service (Public - Private key pairs)

### 1.1.1 Non timely delivery of the service

This is under normal circumstances no problem provided the user has the ability to select another Service Provider. But even if this is not the case many situations where the generation of a key pair is needed are not time critical.

### 1.1.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user

Refined risks and their potential causes are:

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
Generation of weak key pairs	Weak Product, configuration failures → Pre-Operation Phase Not performing necessary checks → Operational Phase
No guarantee of uniqueness of key pair (at least within the Service Provider's space)	No or incomplete checks for uniqueness → Pre-Operation Phase (existence of technical measures to perform the necessary checks) → Operational Phase (performing the checks)
Weaknesses in the key generation algorithm (e. g. will only use a subset of the available key space)	Weak Product → Pre-Operation Phase

### 1.1.3 Service provider stopping to deliver the service

This is usually not a problem, since the user can immediately switch to another Service Provider without any significant losses (provided there is more than one provider of this type of service).

**1.1.4 Misuse of information**

Misuse of the private key generated on behalf of a user is the highest risk for a key generation service. Refined risks and their potential causes are:

Refined risks	Life Cycle Phases that may need to be considered
Inappropriate protection of the private key in the Service Provider's domain	Weak product, inappropriate access control mechanism → Pre-Operation Phase → Operational Phase → Maintenance Phase
Inappropriate protection of the private key during transfer to the user	Weak product, inappropriate system configuration, inappropriate transfer medium, inappropriate access control to the transfer medium → Pre-Operation Phase → Operational Phase → Maintenance Phase
Inappropriate protection of algorithm, parameters, equipment used for key generation	Weak product, inappropriate access control → Pre-Operation → Operational Phase → Maintenance Phase
Unnecessary copies of key generation parameters or the private key	Weak product, inappropriate system configuration → Pre-Operation Phase → Operational Phase → Maintenance Phase
Failure to delete all key generation parameters immediately after key generation and all but the intended copies of the private key immediately after releasing it to the user	Weak product, inappropriate system configuration → Pre-Operation Phase → Operational Phase

The example of a key generation service shows that two of the general risks are highly critical while the other two can normally be neglected. The example also shows that the user will have severe difficulties to detect a security relevant failure or misuse by the Service Provider and therefore needs assurance that those failures or misuses are highly unlikely to happen.

## 1.2 Example 2: Certification Service

This example derives the generic risk for a registration and certification service for public key certificates. In the example we don't make assumptions for what purpose the certificates are used. The example does also not cover the aspects of a directory service and therefore risks associated with the access and distribution of the certificates issued is not covered.

### 1.2.1 Non timely delivery of the service

As in the first example this is normally not a problem for the issue of certificates, because in most cases this service is not time critical. For specific applications of the certification service this may be a problem but since this application dependent we will not discuss this further.

Timeliness however is a problem when revocation is addressed. Delaying revocation may result in a high risk for the user.

### 1.2.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user

The biggest risk is that information contained in the certificate issued is wrong. As the table shows, most of those risks can be related to the operational phase, where problems in the configuration or administration of the system but especially problems in the registration process where the information to be placed in the certificate is gathered can lead to false information in the certificate.

Refined risks and their potential causes are:

Refined Risks	Potential Causes and Life Cycle Phases addressed
Certificate is issued for another user	Failure during registration or transmission of user information → Operational Phase
User key is modified before the certificate is generated	Failure during registration or transmission of key data → Operational Phase
User information in the certificate is wrong	Failure during registration or transmission of user information → Operational Phase
Algorithm or algorithm parameter information in the certificate is wrong	Failure during registration or transmission of user information → Operational Phase
Usage restrictions (or other information for extensions) in the certificate are wrong	Failure during registration or transmission of user information → Operational Phase
Issue of a certificate without proper user registration	Failure in the registration procedure → Operational Phase

Refined Risks	Potential Causes and Life Cycle Phases addressed
Unwanted revocation of a certificate	Hard- or software failure → Pre-Operation Phase Failure in the revocation procedure Failure during transmission of the certificate id. Failure to authenticate the revocation requestor Failure of operating personnel → Operational Phase
Weak or compromised CA private key	Weak key generation process, inappropriate protection of the CA private key → Pre-Operation Phase → Operational Phase → Maintenance Phase

Those risks either result in the issue of a certificate that can not be used or in the issue of a certificate that can be misused. But with a proper registration procedure the user is able to prove that either the registration authority or the certification authority is responsible for the failure. In this case suitable liability conditions are able to cover the risks of the user provided the Service Provider has an appropriate financial standing. Here we consider the mainly the risk that the Service Provider issues a certificate that is unusable. The case of (accidental or deliberate) issue of a certificate that can be used to act on behalf of the user is considered below.

### 1.2.3 Service Provider stops the service

This is usually not a risk, because the user may select another Service Provider. The only critical aspects would be associated with a directory service, which is not considered here. The only aspect that needs to be considered is the ongoing protection of the private key used by the Service Provider to sign the certificates. So actions have to be taken to ensure that the private key the CA has used is not compromised after the Service Provider has stopped to deliver the certification service.



### 1.2.4 Misuse of information by the Service Provider

Refined risks and potential causes are:

Refined Risks	Potential Causes and Life Cycle Phases addressed
<p>The Service Provider issues a certificate on behalf of the user but replaces the user's key by the key of someone else, eventually changing also other information in the certificate e.g. usage restrictions.</p> <p>This results in the ability of someone else to take over the identity of the user.</p>	<p>Deliberate or accidental action after registration but before generating the certificate</p> <p>Compromise of the CA's private key</p> <p>Improper control of certificate generation process</p> <p>➔ Operational Phase</p> <p>➔ Maintenance Phase</p>
<p>Misuse of user information needing privacy protection</p>	<p>Improper control of access to this information</p> <p>Unnecessarily storing user information</p> <p>Not protecting user information during transmission</p> <p>➔ Operational Phase</p> <p>➔ Maintenance Phase</p>

The first entry is actually the largest risk a user has to face. A proper registration procedure where the registration authority has to prove that the user has applied for this certificate will help to identify who is responsible, but the user may detect the failure only after considerable financial or image loss has occurred. Suitable liability conditions are therefore only one aspect of assurance a user wants to have to cover this case. He should also insist on the implementation of suitable methods preventing such failures.

### 1.3 Example 3: Key Escrow or Key Recovery Service

In contrast to most of the other primary value services considered here there is no well defined and accepted model for the implementation of a key escrow / key recovery service. This results in a wide range of potential implementations of those services starting from implementations mainly based on organisational procedures and strong physical protection up to widely automatic IT-based systems with significantly lower requirements for organisational support and physical security.

In our example we will discuss only key escrow or key recovery services for keys used to protect the confidentiality of information. Key escrow or key recovery services for keys used only for the purpose of authentication or digital signatures are considered to be unnecessary and will therefore not be discussed.

Key escrow or key recovery services may either serve the information owner (which may be an individual user or a company) or a third party which has the right to access the information under well defined circumstances. Since the risks are basically the same regardless whether the service is used by the information owner or a third party, we will discuss both cases at the same time.

#### 1.3.1 Non timely delivery of the service

Timely delivery of keys from the Key Escrow / Key Recovery authority may be critical, because the access to critical information depends on the availability of the keys. The acceptable time delays for access to keys are of course dependent on information recovered and may for this reason vary from fractions of second up to several hours or days. But in any case a provider of a key escrow or key recovery service needs to specify the availability parameters of his service.

Refined risks and their potential causes are:

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
Delay in the delivery of the key	<p>Product failure (product introduces an unexpected delay caused by inadequate hard- or software design)</p> <p>➔ Pre-Operation Phase</p> <p>Operational failure</p> <ul style="list-style-type: none"> <li>- Failure in the hard- or software configuration</li> <li>- Failure in operational procedures</li> <li>- Failure / delay of the communication links</li> <li>- Temporal unavailability of                             <ul style="list-style-type: none"> <li>- equipment</li> <li>- persons</li> <li>- power supply</li> <li>- communication links</li> </ul> </li> </ul> <p>➔ Operational Phase and</p> <p>➔ Maintenance Phase</p>

**1.3.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user**

Reliability is another important aspect of a key escrow / key recovery service. The user of such a service expects that key material is only given to persons authorised for the access to that specific key or information. He also expects that the Service Provider will be able to recover and deliver the keys (i.e. not lose them) and will be able to identify the correct key (i.e. not interchange them).

Refined risks and their potential causes are:

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
Delivery of incorrect key	Product failure → Pre-Operation Phase Operational failure (failure in the key entry procedure, failure in the key recovery procedure, access to wrong key); this may be caused by organisational or personnel failures including failures in the configuration or use of the product → Operational Phase → Maintenance Phase
Delivery of another user's key	Product failure (see list below for operational failures. All those problem may also be caused by failures in the product) → Pre-Operation Phase Operational failure - incorrect key entry / key registration - incorrect processing of the request - incorrect key access mechanism - incorrect recovery procedure → Operational Phase → Maintenance Phase
Delivery of a key to an unauthorised person	Product failure - failure in the authentication mechanism - failure in the access control mechanism - possibility to penetrate the system → Pre-Operation Phase Operational failure - incorrect configuration - incorrect user management - incorrect management of access control - user / administrator failure - insufficient protection of storage media → Operational Phase → Maintenance Phase

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
Loosing the key	Product failure - software failure - hardware failure  → Pre-Operation Phase  Operational failure - incorrect system management - user / administrator failure - insufficient backup procedure - inadequate handling of storage media - loosing material needed to recover keys (e. g. keys used to encrypt the user’s keys)  → Operational Phase  → Maintenance Phase

**1.3.3 Service provider stopping to deliver the service**

This can become very critical because a user of the service may loose complete access to the information encrypted by those keys that need to be recovered. Key escrow / key recovery services therefore need to address the controlled handover or controlled shutdown of the service.

Refined risks and their potential causes are:

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
Service provider loses the ability to perform key recovery / key escrow operation	Equipment storing the key recovery / key escrow information got lost or is destroyed  Software, hardware or configuration failure leads to complete loss of the ability to recover user keys  → Pre-Operation Phase choose adequate equipment design for redundancy  → Operational Phase  → Maintenance Phase
Service provider loses his license	Non compliance with the licensing regulations Non compliance with laws  → Termination Phase
Service provider decides to give up the service	→ Termination Phase
Service provider goes out of business	→ Termination Phase

**1.3.4 Misuse of information**

Misuse of the keys stored on behalf of a user is the highest risk for a key escrow/ key recovery service. The general effects of deliberate misuse of keys are similar to the ones described under “unreliable provision of the service”, although the particular damage may be much higher. Depending on how the service is actually implemented, the Service Provider himself may be able to misuse the keys, he may

need co-operation with other Service Providers (e. g. if split key techniques are used) or he himself may not be able to identify where and how the key has been used, but an unauthorised third party may have this knowledge. So not all of the refined risks described below will apply to all possible implementations of key escrow / key recovery services.

Refined risks and their potential causes are:

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
<p>Recovering a key or plaintext without request by an authorised person</p>	<p>Product failure</p> <ul style="list-style-type: none"> <li>- inadequate control of access to keys</li> <li>- inadequate protection of storage media</li> <li>- possibility to penetrate the system</li> </ul> <p>➔ Pre-Operation Phase</p> <p>Operational failure</p> <ul style="list-style-type: none"> <li>- generating a spoofed request</li> <li>- bypass the control mechanisms for requests</li> <li>- replay of a previous request</li> <li>- bypassing protection mechanisms</li> </ul> <p>➔ Operational Phase</p> <p>➔ Maintenance Phase</p>
<p>Misuse of the information generated by an authorised request</p>	<p>Product failure</p> <ul style="list-style-type: none"> <li>- inadequate protection of replies to requests</li> <li>- possibility to intercept replies to requests</li> </ul> <p>➔ Pre-Operation Phase</p> <p>Operational failure</p> <ul style="list-style-type: none"> <li>- intercepting keys or information generated as replies to valid requests</li> <li>- misconfiguration of the system</li> <li>- failure in the management/administration procedures</li> <li>- insufficient protection of storage media</li> </ul> <p>➔ Operational Phase</p> <p>➔ Maintenance Phase</p>

## 1.4 Example 4: Time Stamping Service

A time stamping service is used whenever there is a requirement to demonstrate that a specific electronic document existed at a specific time and date. A time stamping service can be used for example to demonstrate that a document was digitally signed before the certificate for the associated public key has been revoked.

### 1.4.1 Non timely delivery of the service

Timeliness is a one of the most important aspects of a time stamping service. Users may require a very short reaction time depending on the purpose they use the service for. The provider of a time stamping service is therefore expected to specify some minimum reaction time as a property of his service. Users need trust in this specification.

Refined risks and their potential causes are:

Refined risks	Life Cycle Phases that may need to be considered
Unavailability of the service	Product failure (software or hardware), failure due to inadequate environment (power supply, network connections etc.) → Pre-Operation Phase Failure within the environment (unexpected problems with infrastructure, fire, flooding, earthquake, bombing) Organisational failures Misbehaviour of users → Operational Phase → Maintenance Phase Shutdown of the service or reduced service due to maintenance actions → Maintenance Phase
Non timely delivery	Product failure (software or hardware) Inadequate design (software or hardware) Inadequate environment (network connections too slow) → Pre-Operation Failure in the administration or maintenance procedures, Misbehaviour of users → Operational Phase → Maintenance Phase

**1.4.2 Unreliable delivery of the service or the results of the service may not have the quality that is expected by the user**

Since the purpose of a time stamping service is to enable the user to demonstrate that he was in the possession of a specific electronic document at a specific date and time, there are two aspects he has to rely upon:

1. The time and date attached by the time stamping service is accurate
2. The signature applied by the time stamping service is correct and will be valid for the period of time the user needs it for demonstrating possession of the electronic document.

Especially the last requirement may be hard to fulfil, because it implies that any revocation of the certificate the time stamping service is extremely critical. Such revocation will invalidate any time stamp issued by the service i. e. making the service completely useless.

Refined risks and their potential causes are:

Refined risk	Potential Causes and Life Cycle Phase mainly addressed
Wrong time in the time stamp	Product failure (clock failure, clock not accurate) → Pre-Operation Phase Operational failure (failure in setting or adjusting the clock correctly) → Operational Phase
Invalid signature	Product failure – compromise of the private key – failure in generating the correct signature → Pre-Operation Phase Organisational failure – incorrect configuration of the product/system – inadequate protection of the private key – applying the signature to the wrong data – revocation of the time stamping service certificate → Operational Phase → Maintenance Phase

**1.4.3 Service provider stopping to deliver the service**

This is usually not a problem, since the user can immediately switch to another Service Provider without any significant losses (provided there is more than one provider of this type of service).

**1.4.4 Misuse of information**

Usually the provider of a time stamping service does not need to see any relevant information. He is provided with the hash value of the document that needs to be time stamped and signs it with the time and date attached. In this case there is no risk of misuse of the information by the Service Provider.



## 1.5 Conclusion

From these examples we can see that different requirements for assurance will come up depending on the risks due to failures or misuse in the Service Provider's domain a user faces when he uses the service. Other services will face other risks. In either case the user may face the loss of critical data resulting in potentially large financial or image losses. Not to mention that for such a service the risks resulting from unreliable delivery or misuse are also very high.

What we also see from the examples is the fact that the risks can materialise in different life cycle phases and different service aspects. If we look at the risks listed for a key generation service, it is obvious that there is a high dependency on the quality of the algorithm and product used for key generation. Good physical security and operational procedures will not address the risks of generating weak keys or other weaknesses in the key generation algorithm. Other services (e. g. a registration service) may depend much more on suitable operational procedures and physical protection. As we also have seen it is dependent on the type of the service, if the life cycle phase 'Service Termination' has to be addressed at all. So each type of service has its own 'risk profile' where the risks can be mapped to service life cycle phases in a high level way. Those risk profiles can be taken by a Service Provider as a starting point for his specific detailed risk analysis and definition of appropriate security measures.

A proper risk assessment has to be the starting point for an assurance framework. Within this risk assessment the Service Provider should address two views: the user's view of the risks associated with the use of the service and his own view of risks.

A security plan will then list the security measures implemented by the Service Provider for the different life cycle phases and map them to the identified risks. This framework does not address how such a security plan is developed. The Security Plan should be covered by an Assurance Plan which lists the assurance measures taken to provide the necessary confidence that the measures are sufficient to reduce the risk to an acceptable level.

Within the risk profile we have deliberately differentiated between risks related to the user and risks related to the provider. This is because the provider should be free in the way how he addresses risks only related to himself but should be able to provide evidence that risks related to the user have been covered by suitable measures and that the effectiveness of those measures has been checked. As we have mentioned before, some risks may be covered by liability clauses combined with the evidence that the provider is able to cover financial claims that may arise from those liability clauses.

## APPENDIX II - APPLYING THE ‘UNIVERSAL’ RISKS

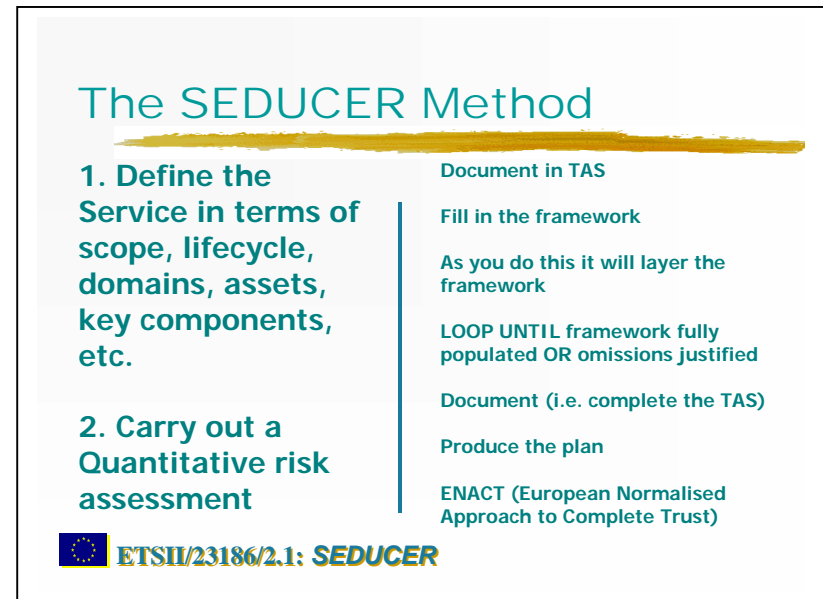
### 1. OVERVIEW

This appendix provides guidance on how to apply the SEDUCER method. The is illustrated in the figure opposite, where the left hand side identifies the objectives and the right hand side identifies the processes that must be followed.

We will first explain the objectives and then go through each process step in turn, elaborating on what is to be done. These activities are supported by a variety of worksheets. To apply the method in practice, complete the worksheets as described in this appendix.

### 2. OBJECTIVES

Essentially, the SEDUCER method is based upon having a clear view of what the service is about and performing a quantitative risk assessment. In defining the service, remember to: (1) scope it, (2) identify the customers, providers and any other key players such as a technology partners, other service providers etc... (3) consider all domains (Technical, Organisational, Physical, Personnel and Legal); (4) consider the whole lifecycle from Start-up to Termination, remembering that the Operation / Maintenance phases are really where it all happens; (5) identify your assets, be they



information, functional or physical and *value* them; (6) identify the key service components. The “Service sPecific User Risks” (SPURs) are combined with the service provider’s own internal requirements, and refined, to compile an overall list of operational concerns. The risk analysis should proceed in the usual way - identifying the threats and vulnerabilities. These are combined with the assets to determine risk, then mitigate that risk to an acceptable level by the application of safeguards.

Remember, risk, in the absence of any safeguard, may be defined as:

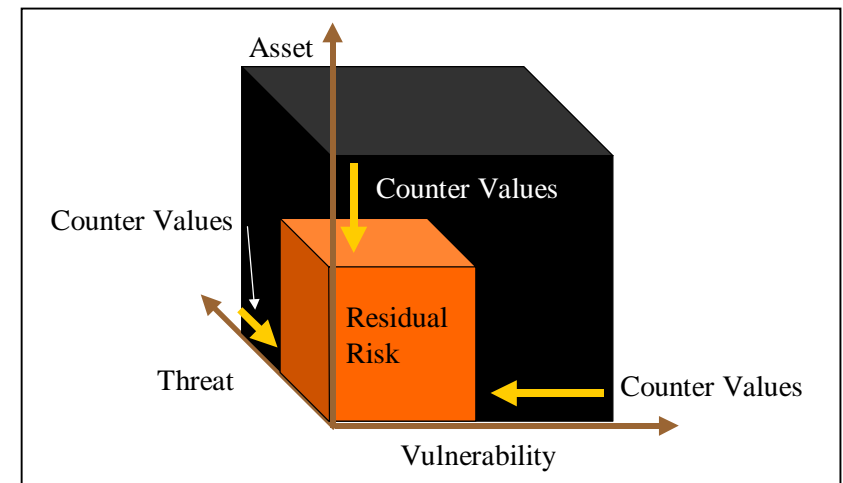
**Risk** is the combination of a **threat** exploiting some **vulnerability** that could cause harm to some **asset**.

The effect of a safeguard is to mitigate (i.e. lessen the effect of) the threat, the vulnerability or even lessen the value of an asset. This leads to the concept of a residual risk:

**Residual Risk Measure** =  $\sum_{\text{all } hjk} (f(\text{Threat Measure } h - \text{CV}) * g(\text{Vulnerability Measure } j - \text{CV}) * h(\text{Asset Measure } k - \text{CV}))$

This is pretty standard, but with SEDUCER, the safeguards include all the trust indicators and assurance measures, and the risk analysis is performed over all domains. Pictorially, we can think of risk as a cube, the residual risk being a much smaller cube (see insert).

In practice, we also need to check that the selected combination of trust indicators and trust assurance methods are having the intended effect. The imminent failure of some trust indicator may be identified through prudent auditing and regular reviews. Corrective action, including the modification, addition or removal of a trust indicator, can then be taken. This approach is akin to the ISO 9000 defect trend analysis and provides an adaptive feedback loop. This management control can be considered as an aspect of Information Security Management. It will also address what needs to be done when other changes are required.



3.

## THE METHOD

In the table below we elaborate on the principal activities necessary to meet the aforementioned objectives. The Worksheets referred to are given in section 4.

Activity	Guidance
Document in TAS	Complete the Risk Assessment Worksheet. This identifies all the information that you need to compile in order to meet the first objective of service definition. Signing off the Worksheet should imply that the requisite information has been reviewed, agreed and documented in the TAS.
Fill in the framework <small>(As you do this it will layer the framework. Loop until the framework is fully populated, or any omissions are justified)</small>	<p>Now carry out your Risk Assessment. Your objective is to determine the risk of failing to meet your customers' need for Trust (and any additional areas of trust required by your organisation – questions 5 and 6 of the Risk Assessment Worksheet) and how to mitigate that risk to a level acceptable to your clients and to your own organisation.</p> <p>Safeguards will include Trust Indicators and Trust Assessment Methods, as well as the traditional Technical, Organisational, Physical, Personnel and Legal measures. Therefore as you go, complete the Trust Framework Matrix (TFM) Worksheets as follows:</p> <ul style="list-style-type: none"> <li>• Once the Risk Assessment Worksheet is complete, start completing the TFM Worksheets 1-6.</li> <li>• On Worksheet 1, for each phase of the service identify the Trust Indicators that you believe will deliver the required level of trust. It is probably best to complete the matrix by Phase (i.e. left to right for each row), rather than by Domain (i.e. top to bottom or each column). In that way you may concentrate on carrying out the Risk Assessment for each phase in turn. Nevertheless, you may exercise your own preference in this matter.</li> <li>• On Worksheet 2, copy across the Trust Indicators that you established for the Technical domain. For each one select the most appropriate Trust Assessment Method. If there is a standard method or set of criteria that helps (e.g. BS 7799, Common Criteria), make a note of it.</li> <li>• Repeat for Worksheets 3-6 for the Organisational, Physical, Personnel and Legal domains.</li> </ul> <p>Continue until you have completed the Risk Analysis and you have fully populated the TFM, or have justified any omissions. Iterate as appropriate</p>
Document in TAS	Now complete the TAS and the first part of the TAS Worksheet.
Produce the plan	Now that the TAS is complete it is appropriate to produce a Trust Assurance Plan to implement the TAS. Where standards have been invoked this plan will identify how they will be met (e.g. ITSEC Certification).
ENACT	The final step is to implement the plan.

Activity	Guidance
	<p>Throughout the lifetime of the service keep a watchful eye on the Trust Indicators that you have chosen. If at anytime that appear to be failing you in delivering the trust that they are intended to give, reach for the TAS Worksheet.</p> <p>(This worksheet assumes a three stage process, in common with many change control systems. If your change control system is different, adapt the TAS worksheet to fit.)</p> <p>First, record the observation or event that suggests that one or more of the trust indicators is failing. Next, suggest what should be done to rectify the situation. Finally, following some appropriate review and approval process, determine what the corrective action should be.</p> <p>The corrective action will either require a change to the TAS or it will not. If it does it may or may not require a reappraisal of the Risk Assessment parameters (i.e. the Risk Assessment Worksheet).</p> <p>It is worth scheduling periodic reviews and audits. Do not assume that whatever you put in place will work. Successful managers monitor what they have put in place and take corrective action when they sense that it is not working.</p> <p>Do not forget to take your customers' views into account. Remember, much of the SEDUCER approach is predicated on the customers' need to trust YOU, the Service Provider. Without customers your service will wither. With customers and well placed trust, your service stands a good chance to grow.</p>

#### 4. WORKSHEETS

There are 8 worksheets. Each follows on a separate page.

<b>SERVICE</b>	Sheet identifier:
----------------	-------------------

<b>Activity</b>	<b>Response</b> <small>(Either provide the response or a reference to a document that contains the response)</small>	<b>Done</b>
1 Describe the service		
2 What are the limits in your organisation's interests in the service? (i.e., what is the scope of the service?)		
3 Who are the key players? (include customers, partners and third parties)		
4 Describe the service lifecycle		
5 What is your customers' need for trust?		
<i>Unreliability of results?</i>		
<i>Disruption of service?</i>		
<i>Total loss of service?</i>		
<i>Loss of Assets/Image?</i>		

<b>Activity</b>	<b>Response</b> <small>(Either provide the response or a reference to a document that contains the response)</small>	<b>Done</b>
6 List any additional areas of trust required by your organisation		
7 What are the primary information, functional and physical assets?		
8 What are the key components of the service? (identify Technical, Organisational, Physical, Personnel and Legal components)		
9 What (and where) are your vulnerabilities?		

***Now proceed to carry out your risk analysis, and complete the TFM worksheets***

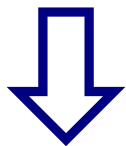
# Risk Analysis Worksheet

Authorised by:	Date:
----------------	-------

<b>SERVICE</b>	Sheet identifier:
----------------	-------------------

Trust Indicators	L-Insurance	✓	✓	✓	✓	✓
	L-Financial Standing		✓			
	C-Financial Background		✓			
	C-Independence		✓			
	C-Overall Image		✓			
	C-Technical Competence					✓
	C-Professional Ethics		✓			✓
	P-Standards Compliance	✓	✓	✓		
	P-Legal Compliance					✓
	P-information Security Management		✓			
	P-Accountability		✓			✓

Move trust indicators into matrix as appropriate



	Technical	Organisational	Physical	Personnel	Legal
<b>Start-up</b>					
<b>Operate</b>					
<b>Maintain</b>					
<b>Terminate</b>					


## TFM Worksheet 1

Authorised by:	Date:
----------------	-------

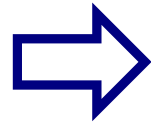
<b>SERVICE</b>	Sheet identifier:
----------------	-------------------



Trust Indicators <b>USE AS A CROSS CHECK</b>	L-Insurance	✓
	L-Financial Standing	
	C-Financial Background	
	C-Independence	
	C-Overall Image	
	C-Technical Competence	
	C-Professional Ethics	
	P-Standards Compliance	✓
	P-Legal Compliance	
	P-information Security Management	
	P-Accountability	

Trust Delivery Methods		Assign the chosen Trust Assessment Method to each Trust Indicator  
<b>A-Testing</b>	<b>A-Certification</b>	
<b>A-Audit</b>	<b>A-Independent Assessment</b>	
<b>A-Self Assessment</b>	<b>A-Independent Accreditation</b>	
<b>A-Self Declaration</b>	<b>A-Independent Testing</b>	

Copy trust indicators from TFM Worksheet 1



	Technical	
<b>Start-up</b>		
<b>Operate</b>		
<b>Maintain</b>		
<b>Terminate</b>		


## *TFM Worksheet 2*

Authorised by:	Date:
----------------	-------

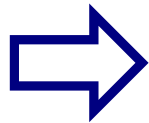
# SERVICE

Sheet identifier:

Trust Indicators USE AS A CROSS CHECK	L-Insurance	✓
	L-Financial Standing	✓
	C-Financial Background	✓
	C-Independence	✓
	C-Overall Image	✓
	C-Technical Competence	
	C-Professional Ethics	✓
	P-Standards Compliance	✓
	P-Legal Compliance	
	P-information Security Management	✓
	P-Accountability	✓

Trust Delivery Methods		Assign the chosen Trust Assessment Method to each Trust Indicator  
A-Testing	A-Certification	
A-Audit	A-Independent Assessment	
A-Self Assessment	A-Independent Accreditation	
A-Self Declaration	A-Independent Testing	

Copy trust indicators from TFM Worksheet 1



	Organisational	
Start-up		
Operate		
Maintain		
Terminate		

## TFM Worksheet 3


Authorised by:

Date:

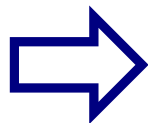
# SERVICE

Sheet identifier:

Trust Indicators USE AS A CROSS CHECK	L-Insurance	✓
	L-Financial Standing	
	C-Financial Background	
	C-Independence	
	C-Overall Image	
	C-Technical Competence	
	C-Professional Ethics	
	P-Standards Compliance	✓
	P-Legal Compliance	
	P-information Security Management	
	P-Accountability	

Trust Delivery Methods		Assign the chosen Trust Assessment Method to each Trust Indicator  
<b>A-Testing</b>	<b>A-Certification</b>	
<b>A-Audit</b>	<b>A-Independent Assessment</b>	
<b>A-Self Assessment</b>	<b>A-Independent Accreditation</b>	
<b>A-Self Declaration</b>	<b>A-Independent Testing</b>	

Copy trust indicators from TFM Worksheet 1



	Physical	
<b>Start-up</b>		
<b>Operate</b>		
<b>Maintain</b>		
<b>Terminate</b>		

## TFM Worksheet 4


Authorised by:

Date:

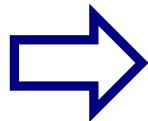
# SERVICE

Sheet identifier:

Trust Indicators USE AS A CROSS CHECK	L-Insurance	✓
	L-Financial Standing	
	C-Financial Background	
	C-Independence	
	C-Overall Image	
	C-Technical Competence	✓
	C-Professional Ethics	✓
	P-Standards Compliance	
	P-Legal Compliance	
	P-information Security Management	
	P-Accountability	✓

Trust Delivery Methods		Assign the chosen Trust Assessment Method to each Trust Indicator  
<b>A-Testing</b>	<b>A-Certification</b>	
<b>A-Audit</b>	<b>A-Independent Assessment</b>	
<b>A-Self Assessment</b>	<b>A-Independent Accreditation</b>	
<b>A-Self Declaration</b>	<b>A-Independent Testing</b>	

Copy trust indicators from TFM Worksheet 1



	Personnel	
<b>Start-up</b>		
<b>Operate</b>		
<b>Maintain</b>		
<b>Terminate</b>		

## TFM Worksheet 5


Authorised by:

Date:

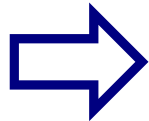
# SERVICE

Sheet identifier:

Trust Indicators USE AS A CROSS CHECK	L-Insurance	✓
	L-Financial Standing	
	C-Financial Background	
	C-Independence	
	C-Overall Image	
	C-Technical Competence	
	C-Professional Ethics	
	P-Standards Compliance	
	P-Legal Compliance	✓
	P-information Security Management	
	P-Accountability	

Trust Delivery Methods		Assign the chosen Trust Assessment Method to each Trust Indicator  
<b>A-Testing</b>	<b>A-Certification</b>	
<b>A-Audit</b>	<b>A-Independent Assessment</b>	
<b>A-Self Assessment</b>	<b>A-Independent Accreditation</b>	
<b>A-Self Declaration</b>	<b>A-Independent Testing</b>	

Copy trust indicators from TFM Worksheet 1



	Legal	
<b>Start-up</b>		
<b>Operate</b>		
<b>Maintain</b>		
<b>Terminate</b>		

## TFM Worksheet 6

Authorised by:

Date:

<b>SERVICE</b>	Sheet identifier:
----------------	-------------------

<b>Trust Assurance Specification Produced</b>	(✓)	Authorised by:	Date:
---	-----	----------------	-------

<b>Trust Challenging Observation or Event</b>	Reported by:
	Date:

<b>Remedial Action Proposed</b>	Proposed by:
	Date:

<b>Remedial Action Taken</b>	Taken by:
	Date:

<b>Trust Review Actions</b>	Authorised by:
	Date:

## *Trust Delivery & Feedback Worksheet*

*END*