EC DG*XIII*/0.7 ETS*II*
Project ***SEDUCER*** (23186)

Document Identification

Title:	**D05: Final Study Report**
Ref.:	**ETS/23186/D05/1.0**
Status:	**1.0**
Date:	**98 12 18**

Approvals

Author/Editor: ..... Date: 1998 12 18
R.G. Wilsher, the Zygma partnership

Quality Review: ..... Date: 1998 12 18
D.F.C. Brewer, Gamma Secure Systems Ltd.

Amendment Record

Status	Issue Date	Comments
1.0	1998 12 18	Final report for the Commission's review and wide dissemination

CONTENTS

1.

DOCUMENT PURPOSE

This document summarises the results of the ETSII SEDUCER project. Its intended readership is all those who have an interest in the development of Trust Services and the way in which the trust they claim can be demonstrated. The report acts as a road map for the project's other deliverables and to the means by which they may be accessed, and where any feedback and response may be directed.

2. EXECUTIVE SUMMARY

The SEDUCER project has established and validated a Trust Framework Model (TFM), supported by a universal structured method (the Trust Assurance Specification - TAS) for describing the measures put in place to establish trustworthiness and a User Guide to support application of the Model and generation of the TAS.

As a framework, SEDUCER has to be applicable to as many types of 'Trusted Services' and in as many contexts as possible. A consequence of this is that it provides alternative means for delivering trust, and thus may be used to demonstrate equivalence between approaches and to determine an appropriate mix of methods. For example, a balance between ITSEC/CC evaluation, BS 7799 assessment, insurance and membership of a professional body, such as the Trust Services Association (now legally established in the UK). The benefits of this approach can be summarised in that it is flexible, addressing all aspects of a service. It is predicated on open standards, wise enough to realise that new standards and assurance techniques will be developed. It provides a common basis for comparing trust, together with a supporting methodology and, where appropriate the missing links (the 'glue' as we call it) to fit together diverse standards, originally conceived as stand-alone specifications. We believe the ability to achieve the integration of intrinsically disparate standards is one of SEDUCER's major strengths.

SEDUCER's results have been validated by a group of experts with wide experience in differing sectors. In the large their response has been significantly in favour of the outcome of our efforts, which seem to fit well with practices being adopted in both the supply and consumer sides of the Trust Services marketplace.

To support its technical outputs the project has made a number of recommendations which adopt a strategy of placing firmly into the public domain the TFM and its related components, proposing parallel measures aimed at both *de facto* and *de jure* standardisation, and supporting actions which the EC DGXIII could implement under its Fifth Framework Programme.

Finally, the project has actually been used by (at least) one of its validators to cross-check their approach to their developing Trust Services, as a result of which their approach was revised and enhanced. Also, the TFM is being applied in a current assignment by one of the consortium partners, and hence we are sure that what we have produced fits well with the approach being taken by commercial providers of trust Services, and fulfils its objectives.

3.

INTRODUCTION & BACKGROUND

This study has set out to fill a gap apparent in previous ETS studies, namely attempting to define what trust is, and moreover, how it could be quantified, measured and in particular, demonstrated. The work undertaken within SEDUCER takes into account the findings of a previous report prepared by the same consortium under an assignment from the British Government's Department of Trade and Industry (the "Market Expectations Study). This study took the form of a European-wide market survey. It asked the questions "What is it about a Trusted Service that a User needs to be able to trust?", and if those 'elements' can be identified, "How could the trust be gauged?"

SEDUCER has built upon the findings of this study, from other work undertaken within the Commission's INFOSEC programme, and elsewhere, and has taken them significantly forward.

demonstration of trustworthiness is one of the most important aspects for the wide acceptance of any service provided by a Trust Service Provider. While the functional requirements of the different types of Trust Services are generally well understood, no complete framework has yet been established which can be used by Trust Service Providers to demonstrate the level of trust or confidence needed by their customers or business partners. Furthermore, trust in technical components is all too often confused with quality assurance and development assurance techniques. Aspects of physical, personnel and procedural security are frequently overlooked, as are the security needs of provider organisations' clients. It is clear that the way trust is provided, as well as the level of trust needed, is dependent on the type of service as well as the value of the assets influenced by the service. Consequently, considering all these factors and requirements, it was unlikely that a single scheme for the provision of trust would satisfy the needs of all types of use and provision of Trust Services, and a flexible approach had to be defined.

4.

OVERVIEW OF FINDINGS & RECOMMENDATIONS

This project has prepared a Trust Framework Model applicable to a multi-domain global environment. The framework embraces the mechanisms and components required to support and enable the combination of internationally-recognised processes for the assessment and seamless recognition of Trust Services, both those providing Trusted PKI Services and those delivering Added-Value services on top of them (e.g. BOLERO, in both its manifestation as a previous EC-funded pilot project and its present status as a commercial service offered by Bolero International Ltd.).

The project produced three major deliverable reports, dealing with "Framework Elements" (Deliverable D02), the "Trust Framework Model" (D03) and the "Recommended Actions" (D04). Deliverable D01 was a revised Project Plan, to establish real target dates after the contract was initiated, and Deliverable D05 is this Final Study Report.

The purpose of the "Framework Elements" report was to establish the basic information and set of ideas required to support the major activity of the project, establishing the Trust Framework Model. This report presented a number of 'information packages', as preparatory work prior to commencing work on the Trust Framework Model.

The "Trust Framework Model" report described a structured approach to the issues of understanding Users' expectations of Trust and for the provision of some form of Assurance that their Trust is well-placed. The Model was scoped to address all aspects of a business and its provision of Trust Services – it was by no means limited only to technical issues. By adopting this approach, the consortium gave cognisance to the fact that businesses will assess their own risks, and that the requirements and solutions for trust may vary according to the nature of the business, the type of trusted service(s) required, and an individual business' own view of its risk.

The Framework Model was supported by a template Trust Assurance Specification document and a User Guide explaining how to apply the model.

The consortium then focused on how the TFM could be taken forward if it proved to have any potential for use (which the consortium had always firmly believed to be the case) and which was confirmed by the validation process.

In Deliverable D04 a strategy for further actions was devised which addressed both the possible actions open to the European Commission (as was the principle intention of the associated work package) but which looked also at actions others might take. The strategy was partitioned into five classes of actions. The first of these was to address, at a broad level, the hosting on suitable web sites of the project's deliverables, so as to achieve world-wide promulgation of the result. The next class considered how the results might be adopted by national and EC bodies for inclusion as the technical trust model for legislative and regulatory frameworks. The next two actions each addressed standardisation, one *de jure* through formal channels, the other *de facto* by following the 'Internet culture' of widespread exposure and public comment and debate. The final strand of the strategy involved identifying actions that the Commission could implement under its Framework Programme V to promote awareness and take-up of the TFM and its associated measures. Once the TFM and recommendations had been prepared, a validation process was undertaken, to gain feedback from as wide a group of respondents as possible. This was two-pronged. Firstly, the TFM was published on the Web, secondly it was specifically sent to a group of selected experts in a range of fields and their opinions sought. As a result of this validation the model and recommendations were revised after consideration of all responses, and final reports delivered to the European Commission at the same time as this Final Study Report. The results of the Validation are given in a subsequent section of this present report (D05).

The project made the most of opportunities to co-operate with other ETS projects, particularly LEGAL and BESTS, to ensure its solutions gained broad support within the programme.

5.

DEVELOPMENT PROCESS

The project addressed all aspects of Trust Services throughout their development, commissioning (installation, integration and trials), commercial operation and close-down. The Trust Framework developed took account not only of technical components (such as might be addressed by schemes such as the Common Criteria, ITSEC/ITSEM) but also the enforcement of security policy in terms of physical, personnel and (operational) procedural measures. The study also considered the means to use and adopt the results of earlier assessments, e.g. when an evaluated technical component supplied 'off the shelf' is incorporated into a service provider's system. To accomplish this effectively and efficiently it was necessary to employ a wide range of mechanisms and to consider carefully the interrelationships and (procedural) interfaces between them. According to the level of demand for self-assessment at various stages of the development of Trust Services, the project also considered the need for a 'multi-tier' framework where differing levels of assurance can be delivered, according to the experience and also the independence of the 'assessor'. The project felt that this might lead to both formal and non-formal assessment practices being developed, ideally with a high degree of commonality. It was felt that the framework should also recognise the potential for market-driven solutions to exist alongside formally licensed services. It was also felt that the development of the framework should benefit from the Market Expectations Study previously carried out by the Consortium .

Accordingly four essential stages were undertaken:

- Σ The first established a pool of reference material from which was identified the key topics which could contribute to the investigations. These topics covered actual commercial requirements, existing and proposed means of assessments, security policy strategies, etc. The topics were extracted and an initial framework produced.

- Σ Next, the project performed a comprehensive analysis of these elements and commercial requirements to produce a much more definitive trust framework. The framework elements were explained and their inclusion justified. It was validated by reference to an external, commercially-focused review. A methodology for application of the framework was also developed.

- Σ In the third stage, recommendations for the development and application of the framework were drafted. These include exploitative actions that could be taken by interested parties such as Ministries of Industry, trade associations, Chambers of Commerce, and the EC itself. These also were validated by reference to external expertise.

- Σ In the fourth and final stage, this report was prepared, describing the work undertaken, the results achieved and identifying any emergent issues.

We started by producing our own definition of Trust, not because we wished to reinvent the wheel but to offer freedom of exploration for the project, as other definitions, conceived in a different context, could be too restrictive.

One of the main points to come out of an earlier study carried out by our Market Expectations Study was that consumer risk can be encapsulated in terms of four concerns:

- Σ Unreliability of results;
- Σ Disruption of service;
- Σ Total loss of service;
- Σ Loss of Assets/Image.

We used these as a principal driver to focus our attention on the Users' concerns, combing these with the service provider's view to establish a complete picture of the trust requirements.

Another output of the Market Expectations Study was the identification of three groups of trust indicators, which have been further analysed and refined in this study. The first group of trust indicators concerns the ability and willingness of a service provider to pay up when things go wrong. Insurance and financial standing are the comfort words. The second group considers the credibility of the organisation, and its people, and the third group considers the policies that the organisation has in place and the means it has to ensure compliance.

Over thirty reference documents were reviewed to identify within them the elements of trust which they convey. These documents covered a wide scope, some specific to TTPs and generally in the field of information security, with a small number from other domains, e.g. safety. The documents reviewed were mapped onto a matrix defining the operational life-cycle and security domains for TTPs. This identified a number of gaps in the coverage of these published works, principally concerning all aspects of physical security in IT systems in general, and also in the operational phase of terminating a service, which has particular relevance to TTP services, where the need for trust in certain aspects may supersede that of the service provision. An Appendix to the report (D02) gave a specimen for each of the major types of document reviewed.

Additionally, the reviews were used to verify and extend a set of initial framework elements developed by the consortium itself, based upon its experience in the TTP domain. These elements were selected according to their contribution to trust, either in a direct fashion or indirectly, as risk-reduction measures. They were related to a number of key aspects which the consortium felt needed to be considered when either developing, operating or using a TTP Service.

In an initial step towards creating the Trust Framework, the "Framework Element" report also considered the matter from the perspective of the prospective User - what would the User be looking for, and which trust elements could provide him or her with confidence with the results of each of those needs?

In addition we identified a range of methods for delivering the trust implied by each of these indicators. On the one hand there are techniques that are applied internally, within an organisation, such as auditing, and techniques that are applied externally, e.g. independent assessment.

The project has put all of these ingredients together to form the framework, taking full account of the various phases of a service (start-up, operation, maintenance and termination) and the domains in which assurance may be required (technical, organisational, physical, people and legal). The framework takes the form of a simple matrix.

We recognised that:

- Σ Only particular trust indicators applied to particular domains;
- Σ There was a choice in selecting trust indicators and trust delivery methods, that might lead to the same overall level of trust;
- Σ Standards, such as ITSEC/Common Criteria and BS 7799 offered particular ways of populating the Trusted Framework Model (TFM).

These realisations allowed us to complete the TFM and deduce the rules for its application. Where there was choice, it seemed sensible to predicate that choice on the output of a risk assessment, where the trust indicators and trust delivery methods are considered as risk mediation safeguards alongside conventional safeguards, such as firewalls, safes and badges.

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

The Model went 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 could 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 such an 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 described a specific document, the 'Trust Assurance Specification', which could act as the 'glue' between potentially disparate Assurance Methods and Results.

Hence, the application of this Model was able to deliver business-focused Trust based upon a methodology which addressed Risks in User-orientated terms, using Assurance Methods which could be as detailed and specific as required, including in the technical domain, and which presented an Assurance based upon a single overall assessment (i.e. through the Trust Assurance Specification).

Moreover, it seemed sensible to give advice on how to apply the TFM, with the assistance of guidelines and worksheets, and on how to document the results. In the latter case, we loosely modelled the document, which we call the Trust Assurance Specification (TAS) on the ITSEC Security Target, as in many ways the purpose is very similar. The difference is that the audience of the TAS is the service provider (although part of it should be made public) and that its coverage is far broader. We also produced a User Guide to support the TFM.

The full explanation of the TFM, the TAS and the User Guide can be found in the project deliverable D03 "Trust Framework Model".

The full Recommendations and justification for them can be found in the project deliverable D04 "Recommended Actions".

6.

VALIDATION OF RESULTS

During the course of the project it was considered that a revised process for the validation would be more effective. Originally intended to be undertaken in two parts, firstly validation of the TFM and then validation of the consortium's recommended actions, it was decided to combine the two. This was justified by the rationale that for those whose expertise lay in the field of assurance methods, they would have an opinion about the measures which might be put in place to promote those methods, and that similarly, those whose expertise lay in the area of EC actions, regulatory and licensing industry schemes could make more relevant comments having gained a comprehensive understanding of the subject being addressed by the recommendations.

Validation was sought by two means, via the WWW and by asking selected experts to provide a response to a validation package. In the case of the Web, the project deliverable D03 was made available as a down-loadable Word file. Secondly, the project prepared an HTTP slide presentation, with supporting narrative text, which described the project's findings and set out a questionnaire – this was viewable on-line and could be copied and used to provide a response. In the case of targeted experts, they were provided with the slideshow as a Powerpoint file as the primary point of reference with the Do3 report as detail for reference if required. The slide show in each case was effectively an enlarged version of that presented at the final Concertation meeting in November (1998).

The validation indicated that the Trust Framework model was one which the vast majority of validators could relate to. Most validators, but by no means all, found that it was coherent and well-structured, and also systematic. The consortium found that in all cases there was something positive to be taken from the validators' comments, whether it was a simple endorsement or a criticism which caused some rethinking of the model, or its coping or perhaps some amendment to the recommendations.

A number of commentators stated that the model was a very good mapping to their own practices with a high degree of fit, or that it would be instrumental in forming their own future approach to the provision of Trust Services. We were particularly encouraged in one instance when we learnt that one reviewer had taken the Trust Framework and had reviewed their own assurance methods, with two significant outcomes: firstly they had found a high degree of coherence with what they had put in place; secondly, the model made them appreciate that they had placed a great deal of emphasis on the technical issues and needed to address aspects of assurance in the other domains which the model addresses.

Responses also suggested that the model had value as a basis for comparison between differing services or for those providers who wished to determine whether they should accept another provider as being suited for a statement of mutual recognition (cross-certification) to be established. Furthermore, the model was seen to be a valuable means by which to determine 'due diligence' when considering the insurance risk when providing cover to, e.g. a Certification Authority.

However, not all validators chose to fully endorse the model. A small number of comments suggested that the model was top-heavy and needed to adopt more of a bottom-up approach. We retain the view that it is necessary to look at the question of trust from the 'outside' and to provide a number of optional and complementary trust assurance mechanisms. To adopt a bottom-up approach would, in our view, tend to over-compensate for risks, rather than to address them until a level of minimal acceptable risk (or perhaps minimum acceptable trust assurance) was reached or could be demonstrated. Furthermore, such an approach could not easily determine the best selection of assurance methods across the range of domains which must be considered. However, we recognise that the model is generic to one extent and that specific instantiations are necessary for discrete types of service in order to address specific risk modes.

Another criticism was that the approach adopted was not cognisant of emerging business models, being too aligned to the 'classical' third-party approach. In response to this we have re-stated within D03 that the scope of the study has been in the realm of public Trust Service. At the same time we believe that the model is equally applicable to 'syndicated' service provision (as we have called it in our own taxonomy of Trust Services), and this is borne out by some of the more positive comments made by certain providers within the validation group.

We also found that a significant number of our validators were not in favour of government regulation in the area of Trust Services. They felt that this stifled innovation and the development of new service offerings. The ability of governments to encourage developments in the retail market was questioned. Some of these comments were also driven by concerns regarding privacy and the access rights of governments. The idea of open publication of SEDUCER's results and the possibility for this to be the basis of its development and adoption was more favourably received.

All of these comments deserve to be further considered as development and application of the model advances, and the consortium would certainly not wish to neglect any of these comments simply because, in considering them, they did not find themselves in complete agreement with them all.

'Hits' on the Web validation copies of the model and recommendations had a huge spread across geographic regions and sectors, with a notable degree of interest from government bodies.

Overall, the project deliverable D03 has been sent to or downloaded by over one hundred individuals, and a similar number have seen the project presentation and attached questionnaire. The results have been viewed by people in Australia, Belgium, Brazil, the Czech Republic, France, Germany, the United Kingdom, Malaysia, the Nederlands, Poland, the United States of America and other countries whose identity cannot be determined with certitude. These cover the financial, services, IT supplier, government and academic sectors.

We found no apparent regional bias within the comments received, commendation and criticism alike coming from all regions.

Undoubtedly, the final outcome of the project has been improved and enriched as a result of the time given by our validators, and we hereby acknowledge the professional contribution they made to SEDUCER, in every case.

7.

OBJECTIVES AND CONFORMANCE

This section addresses the major objectives set for the SEDUCER project and shows how these have been fulfilled. Three major objectives were stated. To deal with each of these in turn, as stated in our original proposal:

Objective one -

> Σ *Bringing together the results of previous work in this sphere, both from tasks which the project partners have undertaken and from other relevant work, in order to identify the desirable elements of a Trust Framework;*

This objective has been fulfilled by the review of a total of 37 reference documents related to the subject of the project, which included:

- Σ Description of various trust assessment methods not necessarily already related to TTP services;
- Σ Certificate Practice Statements from various providers of Certification Services;
- Σ Laws, Regulations, Accreditation and Licensing schemes in place in various countries or industrial sectors;
- Σ Guidelines for TTP services developed on behalf of governments or industrial groups.

From those reference documents we were able to deduce the elements suggested in those documents to establish trust in the TTP service. Despite a number of public presentations and the Public and Expert validations undertaken we have not been advised of any significant omission in this set of references.

Objective two -

> Σ *Establishing a commercially acceptable framework and methodology for the provision of quality assurance (trust) in TTP Services, i.e. a Trust Framework Model focused on commercial applicability, identifying relationships between the elements and the mechanisms needed to implement these elements.*

The model has been shown to be commercially applicable by the majority of validation responses. It identifies the relationships between the generic user risks, specific services, the established trust indicators and the trust assurance methods which are available. At the same time, there has been no hard-and-fast definition of relationships between all the possible trust assurance methods. This is because the determination of the required methods will depend upon the specific type of service, the use to which the User will put it, and the choice of assurance methods which may make it unnecessary to consider certain other methods for the given circumstances.

Objective three -

> Σ *Preparing recommendations which the EC and other parties could implement to deliver and support the Trust Framework Model required to enable the development of TTP Services over the next decade. In doing this consideration will be given to the actual courses of action available to the EC and others, and suggest recommendations that are in keeping with their ability to act.*

The recommendations made are structured and suggest actions which could be adopted solely by the

European Commission, by national bodies, by standardisation bodies and by industry. These recognise the practical limitations of power each party has.

The project team is therefore convinced that the project has achieved the objectives stated in the proposal. The project partners will promote the use of the results of SEDUCER but a fast and widespread adoption needs the support of industry, national regulators and the EC. One of the principle recommendations of the project team is therefore to set up a SEDUCER Users Group serving as a forum for discussion and further development of the Trust Framework Model. This User Group could, if appropriately funded, assist in achieving the long term objective of wide application of the SEDUCER results.

8.

CONCLUSIONS

The SEDUCER project's major objectives have been fulfilled and its results are now widely available for public dissemination. Within our deliverables we have offered a strategically coherent set of recommendations which could take forward the Trust Framework Model in a number of parallel and complementary paths.

The project has arrived at conclusions which are broadly in keeping with commercial attitudes and practices, and has already been put to limited use by one of the validators. It is also being used as the basis for an assignment being undertaken by one of the consortium partners.

We believe therefore that this project has made a positive contribution to the overall understanding of trust in commercial Trust Services and about how that trust can be demonstrated. The forthcoming six months will show whether the interest shown so far is justified and the framework and related concepts have real potential to contribute in the industrial and governmental spheres.

The project's validators have been a diverse group. Some of them have requested that their identity not be disclosed. Since it has at all times been the principle of the consortium that anything which might be a possible of source of inference of attribution of comment should not be divulged, we have chosen not to publish the names of our expert respondees.

Any specific comments or suggestions can be emailed to the SEDUCER Project at SeducerPj@aol.com or sent by conventional mail to: The SEDUCER Project, 1 Bridon Close, East Hanningfield,
Essex CM3 8BA, United Kingdom, tel. +44 12 45 40 15 24.

END