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

Document Identification

Title:	**D04: Recommended Actions**
Ref.:	**ETS/23186/D04/1.0**
Status:	**1.0**
Date:	**98 12 16**

Approvals

Author/Editor: ..... Date: 1998 12 16
R.G. Wilsher, the Zygma partnership

Quality Review: ..... Date: 1998 12 16
H. Kurth, Industrieanlagen-Betriebsgesellschaft mbH

Amendment Record

Status	Issue Date	Comments
1.0	1998 12 16	Final version for the Commission's review and wide dissemination

CONTENTS

1.

DOCUMENT PURPOSE

1.1 Objectives

This report serves to set forth and to justify the recommendations being made at the close of the SEDUCER project. These are intended to be seen by a large audience and to encourage wide uptake of the project's deliverables.

1.2 Scope

The recommendations made in this report address the Trust Framework Model produced by the SEDUCER project, and the supporting concepts, namely the Trust Assurance Specification and the User Guide.

The recommendations themselves are targeted at the European Commission, and at national governments and administrations, at all industry sectors and finally towards user & industry bodies.

2.

EXECUTIVE SUMMARY

This report sets out the recommendations developed by the SEDUCER consortium which are believed appropriate to take forward the Trust Framework Model which has been the central objective of the project

A strategy for further actions has been devised which addressed both the possible actions open to the European Commission (as was the principle intention of the recommendations) but which looks also at actions which others might take. The strategy has been partitioned into five classes of actions. The first of these addresses, 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 considers 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 address 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 involves the description of a number of actions which the Commission could implement under its Framework Programme V to promote awareness and take-up of the TFM and its associated measures.

We believe the SEDUCER framework has a future, as endorsed by the adoption of similar or derived practices amongst our validators. With widespread dissemination and support it has the potential to make a serious contribution towards the development of Trust Services both in Europe and in the wider global market. Early adoption of these actions will speed that situation.

3.

BACKGROUND

Subject of these Recommendations

These recommendations address the results and outputs of the ETSII project SEDUCER. They are intended to enhance promulgation, awareness and application of the derived Trust Framework Model and supporting concepts. The recommendations are intended to be aimed at the European Commission in particular, but also at industry in general.

The Strategy adopted by these Recommendations

The recommendations being put forward fall into five classes:

- Σ 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;
- Σ The adoption of the TFM approach and in particular the TAS as cornerstone elements of emergent regulatory schemes;
- Σ *de jure* standardisation moves, through formal channels;
- Σ *de facto* standardisation by following the 'internet culture' of widespread exposure and public comment and debate, and by adoption of the TFM by commercial TSPs;
- Σ identifying actions which the Commission could implement under its Framework Programme V to promote awareness and take-up of the TFM and its associated measures.

A summary of these measures is given in a schema following the explanation of all phases.

4.

RECOMMENDATIONS FOR PROMOTION OF THE TFM

The recommendations made are presented with the intention of developing a market force and a momentum to take forward the SEDUCER results. The results of validation strongly suggest that there is a place for the framework which has been developed.

Class 1 - World-Wide Promulgation

Our first recommendation is:

> WORLD-WIDE PROMULGATION: The European Commission should publish promptly on the World-Wide Web the results of the SEDUCER project (and indeed of all other recent ETS projects) and should take all steps available to ensure that the availability of this information is widely known, by WWW-based means and by bringing it to the attention of key players in the field, including all Heads of Unit and more senior representatives of the Commission and national representatives within the EU / G8 etc.

The justification for this recommendation is that:

It has frequently been the case that past EC-funded studies of this kind have produced worthwhile results but that their exploitation has been weak. Today the means of exploitation and promulgation is much more readily available than at the start of the INFOSEC programme, and that same means is available to virtually all who would or should have an interest in this project's results.

For the future successful development of Ecommerce there will need to be a network of TTPS across Europe and more widely international, such is the nature of trade, and these will need to have a common basis for trust and assurance. A series of different regulatory and legal environments will not serve this unless there is a way to readily compare the characteristics of these services – the SEDUCER TFM and its TSA can do this.

We therefore believe that the single most important step in promulgating SEDUCER's results is to publish them quickly on the WWW, to encourage as many other appropriate sites to either host the results or to provide hot-links to such sites, to register these sites with the most popular search-engines and to bring to the attention of key players the availability of these results.

The availability of these results as open templates will encourage their evaluation and application within the user and business environments. This in turn will spread awareness and the development of *de facto* standards.

In support of this action the SEDUCER consortium will also be publishing their results directly. Furthermore, we shall be taking steps ourselves to bring the availability of these final results to all those expert validators who contributed to the project, and to other key persons accessible to the project's members, in commerce, industry, government, and other areas such as standardisation bodies. The results will also be presented at least three conferences planned for 1999.

Class 2 - Multi-sector Adoption

This class of recommendations is concerned with the contribution which the SEDUCER Trust Framework Model can make to the development of Trust Service provision within the EU, and in other nations which share its objectives.

Putting the results into the public domain will be a key facilitation for dissemination of SEDUCER's outputs. However, there are a number of additional actions which can be implemented which can encourage the development and take-up of the SEDUCER model. We envisage these actions being in

two distinct areas: actions available to administrations, at both the European and National level

The principal recommendation of this class is:

> ADOPTION AS REQUIREMENTS CATALOGUE FOR ELECTRONIC SIGNATURE DIRECTIVE: The European Commission adopts the structure of the Trust Assurance Specification as the basis of the Requirements Catalogue identified in the Proposal for a Common Framework for Digital Signatures, EC COM(1998) 297.

The justification for this recommendation is as follows:

The need for a Requirements Catalogue is introduced in COM(1998) 297 in Article III. 'AIM AND SCOPE OF THE DIRECTIVE', Paragraph 7, which states that "*Common requirements for certification service providers would support the cross-border recognition of signatures and certificates within the European Community. The requirement catalogue shall be applicable for certification service providers, independent of the accreditation model of the individual Member State*". The structure of the TAS as defined by SEDUCER is a sound basis for the definition of PKI services in general, and therefore of 'certification services' in particular (and perhaps an opportunity to define in greater detail the precise meaning of the phrase).

Early definition of the Requirements Catalogue would facilitate its adoption by those states presently having, or developing licensing and accreditation arrangements for Trusted Services. Equally, the provision of a Catalogue could support the development of industry-based schemes for the provision of such services. Collectively, these measures could provide a sound basis for the mutual recognition of Trust Services, whatever their basis of recognition so long as adoption of the TAS / Requirements Catalogue model was the format on which they were defined.

We offer the further recommendation:

> BASIS OF NATIONAL SCHEMES: The EC should encourage the Member States' representatives for national licensing / regulatory schemes to establish their national schemes based on the SEDUCER structure.

The justification for this recommendation is as follows:

At the time of preparing these recommendations the Directive referred to above has not been decided upon and is stalled awaiting further consideration on January 1999. Despite optimism that it will be approved then, there is no certainty that that shall be so, and hence there will continue to be a lack of homogeneity in the way such services are defined.

Nevertheless, Member States continue to pursue their own interests regarding the provision of Trust Services, and this is leading to a number of different approaches which may or may not be similar in principal but which rarely are in practice. There is no consistent way by which to easily establish any degree of comparison between these schemes and laws, and hence having a common basis which allowed the characteristics of these differing approaches to be compared would be an extremely useful step.

Adopting the SEDUCER model could significantly facilitate this step.

Class-3 - *de jure* Standardisation

The principal recommendation of this class is:

> NEW CEN WORK ITEM: European national standardisation bodies should consider the SEDUCER TFM as the basis of a new Work Item in CEN, and should nominate it for a fast track procedure.

The justification for this recommendation is as follows:

Promotion of the TFM at European (and ultimately International) level would serve two purposes: firstly, it would enhance the exposure of the model, thus supporting the primary goal of promulgation, and secondly it would assist the widespread acceptance of the model as a standard, through the processes involved in formal standardisation. Acceptance of the TFM would establish a significant benchmarking process for comparing trust between differing environments where mutual recognition was a goal. Adopting such a move within Europe would add weight to the requirement of COM(1998) 297 for a Requirements Catalogue, if that catalogue was related to a standardised approach to its creation. A European agreement to further this Work Item would also lend weight to the debate at the ISO level.

The recommendation is for 'fast-tracking' the work item in order to ensure that its development is as swift as possible and therefore able to support development of the preceding recommendations and the general advancement of Trust Services.

In support of this recommendation, we also suggest:

> ADOPTION OF ADDITIONAL ASSESSMENT METHODS AND CRITERIA: The EC, in concert with Member States, should encourage the adoption / support nomination of relevant standards and criteria for assessment methods at European and International level standards bodies.

The justification for this recommendation is as follows:

There are a number of assessment methods which can contribute to the approach described by the TFM, many of which have been referred to in the course of this study. At the same time, not all are widely recognised as international standards. However, if there are suitable standards in existence it would seem parochial to not accept them and to try to develop a 'home-grown' variety. Such an approach is not cost effective by any measure. The existence of a range of internationally recognised assessment methods would be instrumental in establishing a broad catalogue of such standards.

Just as examples, two such subjects come to mind are. Firstly, FIPS 140-2: there is no European equivalent to this standard, and it would be foolhardy to attempt to create one. However, the promotion of an international standard based upon it would provide the industry with a means of evaluating (certain kinds of) crypto-engines. At the other end of the scale, the British Standard 7799 is increasingly generating interest amongst other EU Member States and further afield, and could become the basis of a global standard in Information Security Management.

Class Four - *de facto* Standardisation

De facto standardisation will be primarily facilitated by the availability of SEDUCER's results on the WWW (Recommendation from Class 1). Additionally, the EC could support this through a number of actions which are set out below (Class 5).

Therefore, the single recommendation of this class is:

> SUPPORT TO ADOPTION OF TAS BY SERVICE PROVIDERS: Encourage Service Providers to produce TASs in line with the TFM proforma.

The justification for this recommendation is as follows:

The voluntary adoption of the TAS as a means of describing the assurance measures put in place would enable those Providers which follow this approach to be judged on a fair and comparative basis. The likely spin-off from this is that those who adopt the TAS would be seen to be inherently more trustworthy in their approach towards their services. At the same time, the effect of this would be to enhance the level of service and thereby enhance the competitiveness of European service providers in the global marketplace. This of course underpins one of the major objectives of the EC.

Class Five - Fifth Framework Actions

The EC has recognised within the broad thrust of its Fifth Framework Programme that Trust is a significant factor in the development of Ecommerce (Ref., e.g. the Vienna IST conference). By definition, the ETS programme has sponsored a number of developments which are highly relevant in this area, and we can identify a number of actions which could be taken within FPV which could assist with many of the recommendations made above. Thus, whilst the preceding recommendations have been to some extent statements of objectives, these actions are more the means by which EC action could fulfil them.

Our Recommendations are therefore:

> SUPPORT TO PRACTICAL IMPLEMENTATION TRIALS: The preparation of a work programme which would invite applications from commercial Service Providers with at least minimally-established security plans to receive part-funding for the application of the TFM, by independent parties. Furthermore, there should be established an independent expert monitoring group to oversee these projects and to take into account their results so as to develop a refined and more mature TFM.

The justification for this recommendation is as follows:

Part-funding acts as an incentive to take a step which may otherwise be considered to be too uncertain (because of the absence of a well-established framework already operative) but which ensures that the funding recipient has sufficient reason to undertake the step. The funding could cover part of the additional costs to put into place the Trust Assurance Review; it could also cover the costs of having an independent third party undertake (possibly only parts of) the review. In all cases, there should be a requirement that the funding be conditional upon there being reasonable openness, to enable a separate team of independent experts to assess the progress of the Trust Assurance Review and to evolve the TFM and its components in direct response to the findings of the programme. Such examination should address a range of characteristics of the model, including *inter alia* technical matters, operational factors and also the cost analysis relating to the implementation of the model. Whilst recognising the need to protect the level of technical details concerning the specific assessments, the results of this programme should be an enhanced TFM. It is therefore important that the programme itself is properly planned and structured, not with an *ad hoc* review conducted as an afterthought.

We further recommend:

> DEFINITION OF INTERFACES BETWEEN METHODS: To encourage and support the definition of interfaces between specific assessment methods as suggested by the TFM.

The justification for this recommendation is as follows:

Whilst there is the established need to have the means to use the various assessment methods which this project has identified, there is still little practical experience in applying this concept. A series of short studies might be conducted to identify the way in which the results of one type of assessment method might be integrated into the processes of another. Such analysis would support the preceding recommendation by providing a theoretical analysis which the practical trials could adopt. This could either be wholly supported by the EC or national bodies could be encouraged to fund such activities, with the EC providing the forum for comparison and exchange of findings.

We further recommend:

> APPLICATION OF THE TFM TO FIFTH FRAMEWORK PROGRAMME ELECTRONIC TENDERING: The EC should take a leading stance and put into operation a SEDUCER-Assured infrastructure allowing proposers to submit electronic tenders.

The justification for this recommendation is as follows:

With the degree of focus being placed upon developing the Information Society it is time the EC participated to the extent that it could establish a show-case example of a PKI used for the complete tendering, acceptance and contracting processes supporting FPV. Whilst paper-based services would not be completely eliminated, such a service could be 'marketed' as the EC's preferred means of accepting tenders, handling email and establishing contracts. The implementation of such a scheme would have the effect of bringing electronic signatures directly to a large and widespread audience across the EU, and through the application of the SEDUCER model, and understanding of the issues facing them.

There are no significant barriers to this process, particularly if the initial agreement and terms of use are established in conventional writing.

We further recommend:

> SUPPORT FOR A SEDUCER USER GROUP: The EC should fund a User Group to foster discussion, evaluation and development of the SEDUCER TFM in an open, commercially-focused manner.

The justification for this recommendation is as follows:

Many of the recommendations already made could be effectively implemented and managed by there being an organised focus for them. Their complimentarity could then be efficiently exploited. However, to do this effectively requires resources and time, which could be supported in part or whole by the EC. The objectives of this group would be:

- Promotion of awareness of the SEDUCER Trust Framework Model (TFM) and the Trust Assurance Specification (TAS)
- Ongoing responsibility for and enhancement of the TFM/TAS
- A discussion group for Users and Service Providers adopting the TFM/TAS
- Support to Service Providers wishing to apply the TFM/TAS
- Collection of feedback from practical implementations
- Development of outline TASs for specific trust services
- Liaison with government, industry, user and other bodies at national and international level regarding standardisation and regulation issues

.

We finally recommend:

> WIDER PROMOTION: The EC should ensure that the results of SEDUCER are widely disseminated on an active basis, by positively distributing them to other EC-funded activities, particularly the last tranche of Fourth Framework Programme projects and new Fifth Framework Programme actions, and ensuring that information is available through all of its offices.

The justification for this recommendation is as follows:

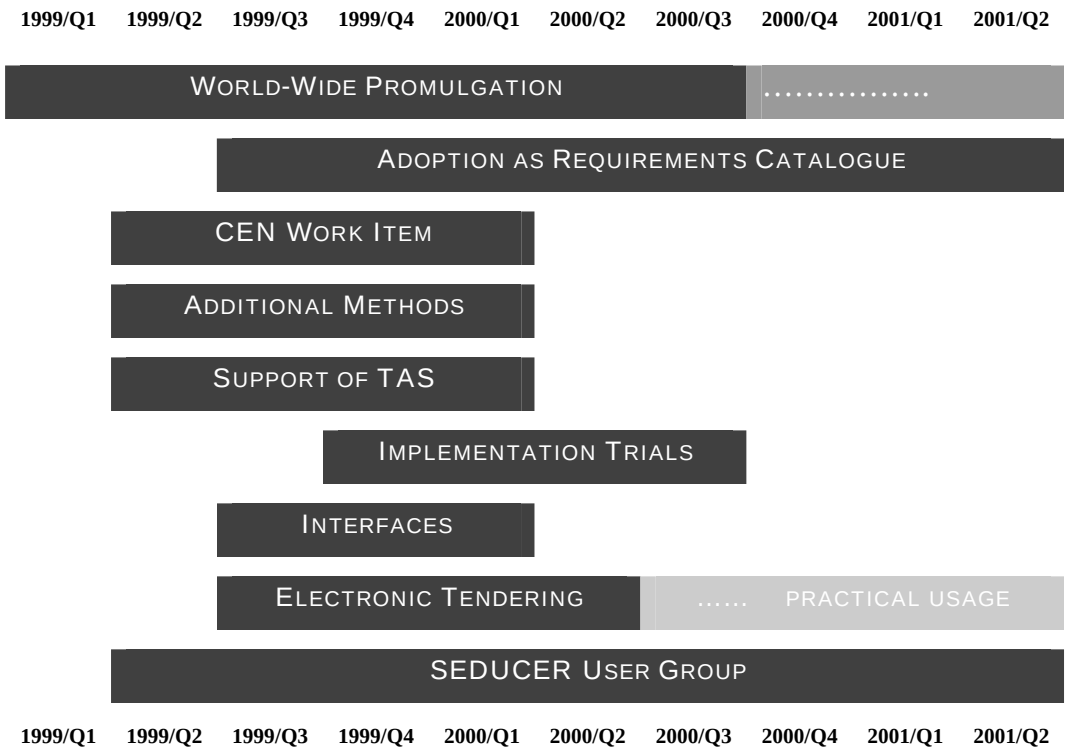
If Trust is to become a significant factor in the development of Ecommerce then the means to

demonstrate trustworthiness should be brought to the attention of all who should have an interest in it. Such parties would be a part of the global community following developments in this field, as supported by previous recommendations. Additionally, the EC could include profiles of SEDUCER in broad actions which promote wider publication and awareness of the issues addressed by the TFM. This could include information packs distributed through their offices in each Member State.

To summarise these recommendations, we would anticipate that none of them would be implemented precisely in the way we have suggested. Two reasons mitigate against this: firstly, there will be details of the development of FPV and the internal organisation of the EC which we cannot be aware of; secondly, the electronic commerce marketplace is dynamic and responsive to developments in a way which can change significantly the environment in which events are taking place. We therefore see these recommendations as pointers rather than absolute plans.

4.1 Timing

There is a degree of linkage between the recommendations we have made, and the implementation of some may mean that others are less significant, or have a different purpose and timespan. Without detail consideration of the impact of these relationships, we suggest the following timeframe for their initial implementation. Although we have shown specific continuation for some actions, we regard these as being important cases. However, we would expect some ongoing activity / interest for all actions.



END