Project Number	AC026
Project Title	Secure Electronic MarketPlace for Europe SEMPER
Deliverable Security Class	Public
CEC Deliverable Number	AC026/SMP/CT1/DS/P/012/b1
Contractual Date of Delivery	Dec. 31st, 1998
Actual date of Delivery	Apr. 11th, 1999
Title of Deliverable	Deliverable D12
	Evaluation of the Enhanced Trial
Contributing Workpackages	WP13
Nature of the Deliverable	Report
Author(s)	A. Weber (FRE)
Editor(s)	A. Weber (FRE)
Keywords	Electronic Commerce, Enhanced Trial, Digital Signatures, Fair Internet Trader (FIT)

SEMPER Consortium:

Evaluation of the Enhanced Trial

Deliverable D12 of ACTS Project AC026

Public Report
Version of 4 June, 2000

SEMPER is part of the European Commission's ACTS Programme (Advanced Communications Technologies and Services). Funding is provided by the partner organisations, the European Union, and the Swiss Federal Department for Education and Science.

The members of the SEMPER consortium are Cryptomathic (DK), Commerzbank (D), CWI Stichting Matematisch Centrum (NL), DigiCash (NL), EUROCOM EXPERTISE (GR), Europay International (B), FOGRA Forschungsgesellschaft Druck (D), France Télécom - CNET (F), GMD - German National Research Center for Information Technology (D), IBM France (F), IBM Corporation Research Division (CH), INTRACOM (GR), KPN Research (NL), Otto-Versand (D), r3 security engineering (CH), SINTEF Telecom and Informatics (N), University of Freiburg (D), University of Dortmund (D), University of Saarland (D). Banksys (B), Banque Générale du Luxembourg (L) and Telekurs (CH) are associated with SEMPER.

Abstract

This documents provides an analysis of the in-depth interviews made on the SEMPER Fair Internet Trader, FIT, an application for secure electronic commerce, developed on the basis of the enhanced security services provided by the SEMPER kernel. This includes the provision of liability limits, as suggested in the SEMPER Electronic Commerce Agreement, SECA. Descriptions of the enhanced security services, of the legal agreement, and of the FIT are provided in the SEMPER Final Report.

For more information on SEMPER visit

<http://www.semper.org>

or contact

Gerard Lacoste	Michael Waidner
IBM La Gaude	IBM Research Division
Centre d'Etudes et Recherches	Zurich Research Laboratory
Le Plan du Bois	Säumerstrasse 4
F-06610 La Gaude, France	CH-8803 Rüschlikon, Switzerland
Phone + 33 92 11 48 07	Phone +41 1 724 8220
Fax +33 93 24 45 45	Fax +41 1 710 3608
Mail lacoste@fr.ibm.com	Mail wmi@zurich.ibm.com

SEMPER Deliverable D12 / 4 June, 2000 / Public

Table of Contents

1. INTRODUCTION 6

2. A SHORT DESCRIPTION OF THE FIT 7

3. FIT SURVEY RESULTS 10

3.1 Survey Design 10

3.2 General Findings on the FIT 10
3.2.1 Benefits of the FIT 10
3.2.2 Suggestions for Improvements of the FIT 12

3.3 Findings on Digitally Signed Business Documents 16
3.3.1 Benefits of Digital Signatures 16
3.3.2 Applicability 20
3.3.3 Values to Be Signed and Willingness to Pay 21

3.4 Findings on the SEMPER Electronic Commerce Agreement 23
3.4.1 Willingness to Sign the SECA Legal Agreement 23
3.4.2 Limits in Case of Compromise 24
3.4.3 Spending Limits 25
3.4.4 General Comments 26

3.5 Overview on Applicability 27
3.5.1 Relative Importance of Key Characteristics 27
3.5.2 Applicability to Types of Trade 27

3.6 Findings on Implementation on Portable, Secure Computers 28
3.6.1 General 28
3.6.2 Willingness to Buy 29
3.6.3 Integration into Phone or PDA 30
3.6.4 Interest in Special Characteristics 31
3.6.5 Applicability 33

4. OUTLOOK 35

5. REFERENCES 36

6. APPENDIX A: TABLE WITH KEY FINDINGS 37

7. APPENDIX B: THE FIT QUESTIONNAIRE 39

1. Introduction

In this document the results of the survey made on the "Fair Internet Trader", FIT, are presented. The FIT is the SEMPER Business Application using the enhanced SEMPER framework code (see Lacoste et al. 2000). A detailed description of the FIT is provided in Chapter 8 of the SEMPER Final Report. A simulation is available at <www.semper.org/simulator/intro.html>. In this document, only a short description of the FIT is provided (Chapter 2). Mainly the survey is presented (Chapter 3). In Chapter 4 an outlook is provided. Conclusions are provided in Chapter 5.

2. A Short Description of the FIT

Our starting points for developing the Fair Internet Trader have been:

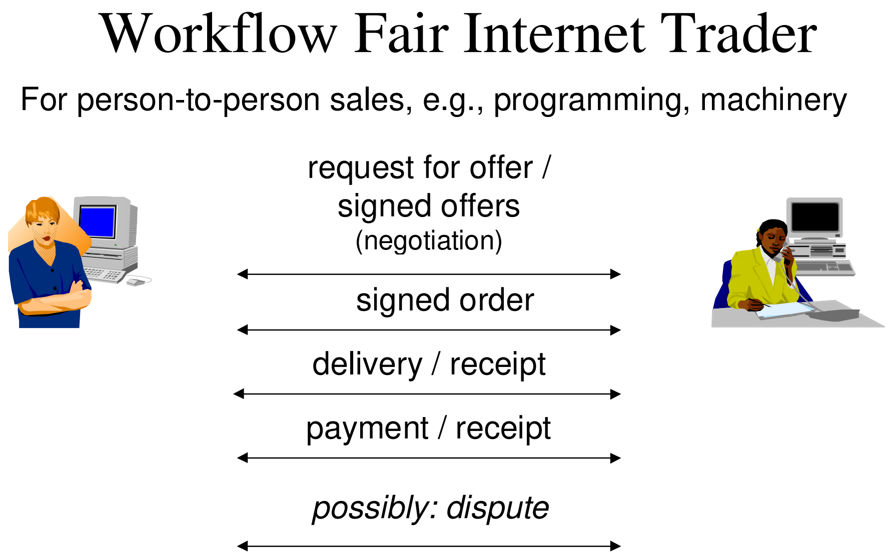
1. Sales on the WWW are dominated by ease-of-use. As there is no infrastructure for secure trade, such as keys deployed with users, it is hard to create benefits out of digitally signing offers, orders, payments, receipts etc. Why should anybody register if a signature can only be used with, initially, only one business partner? Why should anybody agree to be liable for a signature implementation, take the effort of installation and registration, while the same product or service can be bought or sold without it? This issue arose in EU-project SEMPER, both with regard to SET and with regard to signing other business documents. In other words, how can the possible benefits of costs savings through replacing paper documents and increasing legal certainty be earned?
2. During the course of the project small companies and self-employed individuals approached us and requested that they can make their transactions securely. Examples provided were sales of custom-made software and provision of expertise. Both types of sales are typically not conducted through automated WWW-shops.

Signed and encrypted Email as such is not enough for such person-to-person transactions. It does not cover security issues like:

- Match of offer and order
- Completeness of documents
- Commitment in the legal sense to a digital signature
- Integration into payment instruments
- Unambiguous display of characters
- Enforcement of receipts against documents sent on-line

So we defined an easy-to-use tool, allowing everybody to make a transaction in a secure way. We baptised it *Fair Internet Trader,* or *FIT*. It supports person-to-person business scenarios which require human interactions at both ends, from, e.g., occasional private sales of used items, up to high value business sales of equipment or consultancy. The parties involved might have a pre-established relation, or might learn about each other by some yellow pages service, just for a single business transaction of high legal certainty.
A typical example of using the FIT could involve a consultant and his/her customer. The parties negotiate task, delivery schedule and price. The task description becomes part of the contract, which is digitally signed by both parties. All communication can be encrypted. The deliverable will be fairly exchanged for a receipt with a time-stamp (Schunter 2000). The payment can be made with the FIT, also against a receipt. For their information, or in case of a dispute, the parties can review the transaction, and if necessary extract evidence and use it at court.
We used the word “fair” in the name of the application not only for indicating that it uses fair exchange protocols, but also for pointing out to the symmetric design which gives both parties the same power for signing, verifying, payment, and dispute clarification.

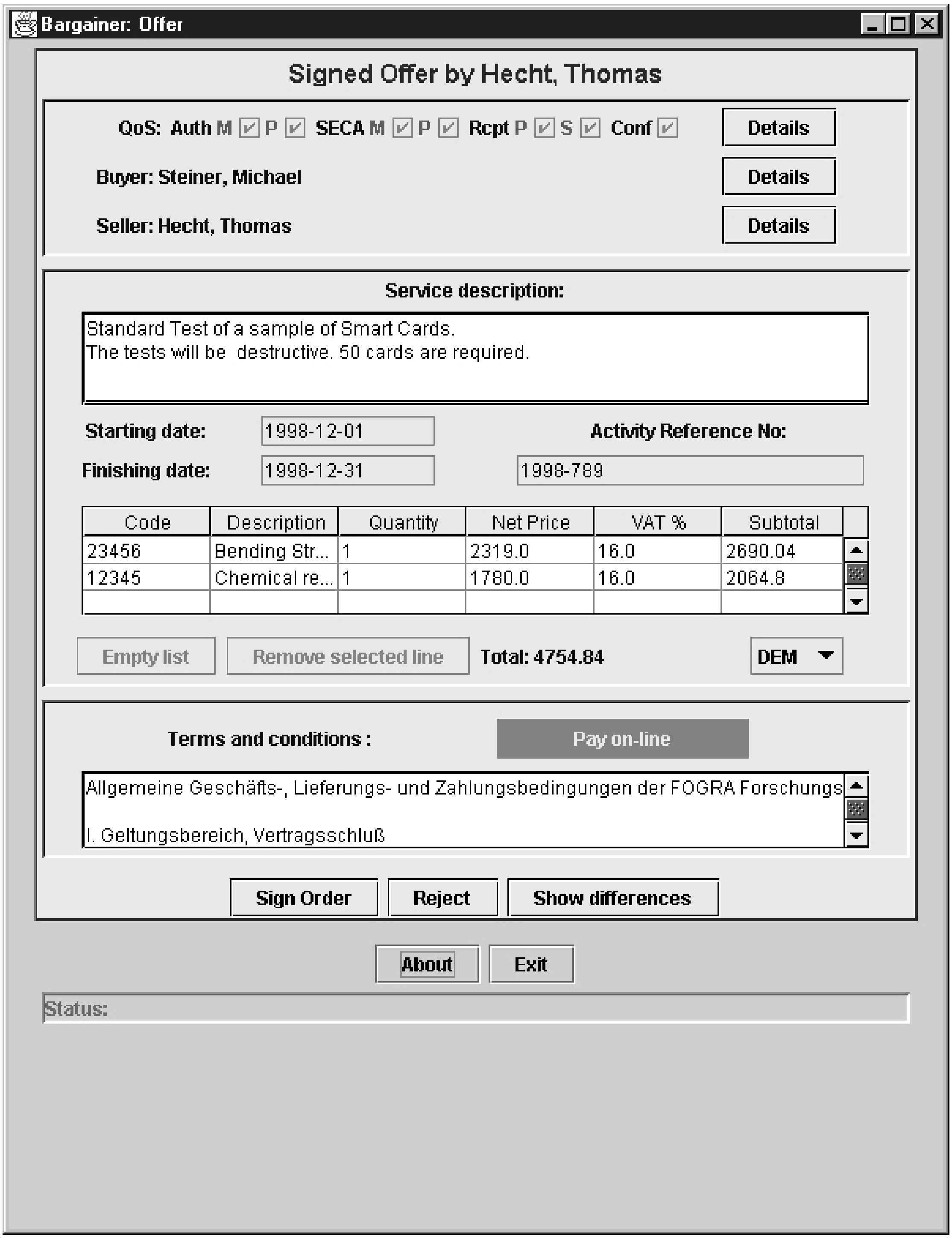
Figure 1



Any FIT interaction follows defined structures, i.e. the FIT guides both parties through the transaction. In a set-up process, players would define whether they want liability limits. Whenever appropriate, they would encrypt their communication. Most of the interactions take place via filling in forms on-screen, and exchanging them over the Internet. The most important options concern out-of-band vs. on-line delivery, out-of-band vs. on-line payment, and in case the latter is select, selection of means of payment. The workflow is triggered by the content of messages exchanged. For having a defined content, we used pre-defined forms. This leads to several advantages:

- Forms are a familiar tool for structuring business processes in the physical world. Thus users know which fields should be on a particular form. As soon as a user knows a form like an “order” it becomes easy to verify the essential fields, like applicable law, reference to terms and conditions, delivery address, signer, amount, etc. An “electronic auditor” can verify that the forms are filled in according to legal or accounting rules, e.g., that an “offer” contains a sender, a date, a description of contents, an amount, a currency, and a signature.
- Forms define fonts and background colours so that there is an unambiguous display.
- Fields can be named and described in several languages, making language support for all business partners easy.
- While automatic copying of data from one form to another (e.g., from “offer” to “order”) as appropriate is default, a party can change data, and the other party can have these changes highlighted. This simplifies negotiation significantly.
- For payment, information like recipient and amount can be taken from the invoice and inserted into a payment instrument. The FIT is designed to work as well with post-payments, like credit cards and e-cheques, as well as with pre-payments, like e-cash.
- Forms with fixed semantics can be imported from and exported to other programs, like accounting, fulfilment or banking programs.

Figure 2: An offer



The abbreviations in the line close to the top of the form with the tick boxes have the following meaning. Quality of Service: Authentication of myself, peer; SEMPER Electronic Commerce Agreement signed by myself, peer; receipts to be provided for payments and statements (deliveries); confidentiality. Ticks mean that during start of the transaction the parties successfully required the characteristic in question to be fulfilled.

3. FIT Survey Results

3.1 Survey Design

The FIT code was installed on Windows NT-machines, with 32 MB RAM and 133 MHz or more, and in most cases demonstrated locally, without an Internet-connection. The respondents were able to play either the role of the buyer or that of the seller. Regarding the SEMPER Electronic Commerce Agreement, SECA, simplified regulations were shown to the respondents (see questionnaire in the Appendix; for the full text of SECA see Baum-Waidner, Zihlmann). The in-depth interviews lasted one to two hours and in most cases were recorded on tape. 21 such interviews have been made by three interviewers in Austria, France, Germany and the United Kingdom between October and July 1999. For obtaining feedback, the FIT was also presented at the IST conference in Sophia-Antipolis, France, Oct. 20, 1998, at the SEMPER-day in Rüschlikon, Switzerland, Nov. 4, 1998, at the Information Society Technology conference in Vienna, Austria, from Nov. 30 to Dec. 2, 1998, at the Internationale Bodenseetagung, St. Gallen, Switzerland March 3, 1999, at the Cebit Fair, Hannover, Germany, March 18-24, 1999, and at the conference Multilateral Security in Communications, 16-17 July 1999 in Stuttgart, Germany. Some of the interviews were made during these conferences. Other interviews took place at meetings between representatives of EU-projects WINDS, Print-It and USINACTS with SEMPER.

All respondents were either experts in related fields, such as public key cryptography, certification services, ergonomics, banking, economics, and law, or representatives of companies buying or selling on the Internet or planning to do so, in particular SMEs. Most respondents had a university degree. The average age was 35 years; six women were among the respondents.

3.2 General Findings on the FIT

It has been aimed at presenting all comments and suggestions in order to give an indication of the relative importance of the arguments.

3.2.1 Benefits of the FIT

Here we present answers to the question “What do you like about the FIT?” (question 1).

Similarities to Traditional Business

The feedback on this general question shows that the FIT was well appreciated. Respondents liked in particular the similarities with traditional business procedures, documents and negotiations.

“I like the similarities with traditional business documents.”
(I like) “the idea that it is a piece of standalone software, which everybody can use with everybody else.”
“Obviously I will sign an offer, an order.”
“Obviously signed orders are needed.”

"I love the idea that private people and small companies can do business over the Internet, without having to invest huge amounts of time and money into a shopping solution. The best part is that I can deliver goods and information on-line, have some kind of proof for that and that I can even at some stage receive some money through the Internet."

The possibility to buy and sell valuable used items easily was appreciated.

"Communication between customer and merchant goes back and forth. Customers raise questions on technical components."
"The possibility to efficiently revise and negotiate a proposal in several rounds is very good. Otherwise he might send an offer ... but I do not want these three screws. Writes another offer. This takes a lot of time. Here it goes fast."
"The transparency of the procedure, that everything goes so nicely step by step. The transparency of the whole process. In normal life this is no longer done in such detail. I think you should not simplify that. It is good as comprehensive as it now is. If it were as usual (on the WWW), things would be clicked and executed."

Evidence

The availability of evidence was appreciated. Respondents said, when asked what the liked:

"Availability of digital signatures."
The transaction "is binding and that is what I do in traditional business anyway."
"The idea that legally valid signatures are valid with the FIT and certificates."
"And when the moment is come, pressing a button is enough for making it legally binding" (the respondent was referring to the simplicity of the Password-entry)
"Auditing, certification. That there is evidence available."
"More security and legal evidence."
"One could use it in real time, call each other and then immediately make it legally binding."

Note: Export and import of documents was available in the prototype, but with different layout of documents. Therefore it was not shown in most demonstrations (see Section 8.2.5 of Hamamtzoglou et al.). Also fairly exchanged receipts were only available with SET, therefore only shown at the SEMPER-day.

Usage of Forms and Checking of Fields

The usage of forms, the checking of content and the display of differences was appreciated.

"Forms are useful. Plain email would not do it."
"I like the automatic checking of content."
"The `show differences` feature is nice. It's quite important to me that such an exchange of forms takes place quickly."
"Good that part is structured, and part not, for entering information."

Easy to Understand and Use

The operation of the FIT did in principle not challenge the users:

"Simple, easy to learn."
"User-friendliness, simplicity and ease of use."
"By and large it can be operated intuitively."
"Easy to use."

Confidentiality

The option of confidentiality was not emphasised in the questionnaire design, as we already knew from past research that confidentiality is an important requirement in many types of business (cf. SEMPER Final Report Chapters 2 and 7). Nevertheless, the issue arose:

"Certainly confidentiality. I do not want that somebody else sees a special offer."
"There are transactions like confidential things, expertise at court, patent applications."

3.2.2 Suggestions for Improvements of the FIT

Here we present answers on question 2 "What do you dislike?"

Interruptions

A frequent suggestion was that interruptions in the process be possible (this was not possible in the prototype due to implementation restrictions). Though some found it a positive aspect to be forced to finalise a transaction quickly, the general impression was that it should be possible to interrupt and continue transactions whenever it is convenient for the players:

"These negotiations - it has to look more like email, you cannot have an application on your PC where you have to wait for the other guy to type in something."
"To be operated more like email."
"It is unusual that one remains connected. Which is positive in the respect that it is like today's situation, when you put the telephone on hold. The customers knows he is still connected. On the other hand, the merchant is forced to finalise the deal, and there is no danger of forgetting an email. It is, however, to the same degree negative to have to remain connected."
"A bit clumsy here and there. For instance, that both have to be present. There should be scope for interruption."
"You cannot interrupt the structure of the negotiations. We both have to there at the same time. I would prefer to be able to say: I want this and that. Which may come to my mind at 10 p.m. Next morning I would expect that something comes back. Later, as soon as I have time, I want to go back in. It must be possible that the communication takes place with interruptions."
"The buyers goes to lunch. Later he will wish to continue."
"For negotiations one should have usage like email. That both are on-line should just be an option."

Negotiation also after Signing

It was requested that negotiations can continue also after a document has been signed as no party will wish to indicate willingness to negotiate by not signing (this was simplified to reduce implementation effort).

Payment Mode

Respondents suggested a number of improvements which would make the FIT better usable for them. The most important suggestion is to be able to pay *after* delivery (whereas in the prototype, if on-line payment was selected, it had to be prior to delivery).

"With on-line payment ahead of delivery is not acceptable to many customers. Neither to merchants, in case of delayed delivery."
"If the seller can later send me a bill, I would order all sorts of things. Then I can place a binding order. "

Improvements of Forms

A question risen by a respondent concerns the important issue of what exactly is going to be signed:

"Is all information shown in the forms? What is hidden behind the (details) buttons?" (leading to the addresses)

Also the tick-boxes, showing whether authentication, liability limits or encryption was selected, were difficult to understand:

"Elaborate on these things here. A bit difficult to understand." (referring to the tick-boxes explained above with Figure 2).
"Certificates should only optionally be visible. The notion "details" is not appropriate. The address should simply be there."

In the prototype code, the players had to define their security requirements initially. Later, the tick-boxes and the abbreviations had to be explained. For products, one should check whether either the abbreviations and tick-boxes need to be changed, hidden or made only available upon request. Or, whether these requirements should rather be selected during a general set-up procedure. Or, whether they should be available during a transaction. For instance, whether encryption should be selectable as soon a party inserts information it regards confidential.

"Settings should be in options, not per transaction."

Respondents requested that more space be provided for descriptions and that more lines for articles should be made available.

"There should be space for more rows. For the customer's article number."
"Too little space in the text fields. With projects, the offer is several pages. Attachments are important."
"Request for offer: not enough space."

Suggestions also concerned that the buyer may have an article number as well. Also it was noticed that several items may be made using the same article number, e.g., when items are packaged differently (it was not possible to use the same article number twice). Also the sequence of items should be identical in all forms, including the invoice.
Respondents requested that attachments can be made at all steps, such as adding a picture of an item to the offer.

"Already with the offer it must be possible to attach, e.g., a picture, when buying a used car."

Respondents remarked that the date frequently needs to be set back or forth, as in business today:

“Date is a key feature in traditional business documents. So it should be set automatically, but it is also true that, with traditional means, the date is set very flexibly. Buyer and seller agree to back-date, e.g., an insurance contract.”
“Starting date and finishing date are not clear.”

Furthermore, it was suggested that the date and place of delivery can be entered:

“Date and means of delivery must be defined.”

It was also suggested that a party can fix that certain fields are not alterable by the partner in subsequent transaction steps:

“I want to be able to influence it. I want a box: Keep these data. Notes which can be taken out. Ticks in fields which have to be fixed.”

It has also been suggested that differences should be shown in red, much like in the Word revision mechanism.
One respondent suggested that the form should provide for an option to enter the seller’s bank account:

“If without on-line payment, then the seller’s bank details must be there.”

It was also requested that the field names (and all messages which stem from the FIT code) should be available in the respondent’s language:

“Field names should be translated.”

Integration into Back-end Systems

Another suggestion was that interaction with existing back-end systems is needed:

“For business-to-business you have to integrate with standard tools, like accounting software or SAP”.
“Integration into accounting and order processing systems, e.g., automatically get a reference number from another system.”
“Interfacing into accounting, with seller’s database, price list.”
“Integration into catalogue.”

The requirement to have integration into a catalogue refers to sales of high value used equipment. The technical information about such equipment may well be put into a catalogue or on the WWW, but prices and conditions will typically be negotiated. The respondent added that this holds for many types of valuable items, also new ones, where the sellers often do not wish to make prices public.

Taxes

Another suggestion is that taxes should be calculated automatically and correctly. Default in the demonstrator was to pay VAT, whereas there are cases in which no VAT needs to be paid, e.g., in private-to-private sales.

“No VAT for private sales. The computation of VAT in trans-border transactions should be correct.”

For instance, basic tax rules should be reflected, such as:

- If both persons are private, no VAT is charged.
- If the seller is from an EU-country, and the buyer is a company from another EU-country, or a party from a non-EU country, no VAT will be charged.
- If both seller and buyer are from the same EU-country, VAT will be charged.

It should be possible to override these pre-set rules manually.

Printouts

Also printouts were requested, in general, and in particular of the invoice:

"As users will check the correct functioning of the FIT software for the first few weeks. Some print functions, which can be used by the user for manual checking would be helpful."
"Printing of the invoice is missing."

Ease of Use

Others requested that it should be easier to operate and understand. The operation would be eased if users could right away start filling in a form, instead of having to go through the selection of security attributes:

"Make it more user-friendly. It should look like an email program. Too many options, e.g., authentication. For normal consumers have a standard set-up, options for experts. People don't want to see messages. The demo is much too difficult to use. For instance, that you get the Tinguin[1] up and you enter what you want to do. Like in Word, there is a document, you can start to type."

The respondent required that as soon the FIT is started, an empty request for offer form is shown.

"Initially, the selection of the role (buyer, seller) should be obvious, not Server/New Bargainer[2] in sub-menus."
"The process of first starting Tinguin and then having to open the pull-down menu applications and then going even into one menu-layer deeper seems to contain some scope for improvements."
"Shortcuts: For repetitive tasks it would be nice for example to be able to save one request for offer (example: 25 pencils for all departments every 5 weeks) and simply start from the file instead of typing the stuff again."
"The user interface which is different to existing Microsoft products and that the users had to learn to operate one more new product. Businesses pay much money for training their staff."
"It looks much more complex than today's shopping applications on the Internet. Why?"
"An icon like an hourglass or a progress bar would be nice to indicate that something is happening in the background."

[1] "Trustworthy Interactive Graphical User Interface", denoting that the SEMPER kernel code has the control of the window, covering fonts, colours etc.
[2] Earlier, the FIT was baptised "Bargainer". The name remained in some menus.

"The terms 'offer' and 'order' sound pretty similar, if possible we should come up with different terms."
"I think it is very difficult for a non-lawyer to distinguish between offer/order and the rest. For example: Is a confirmation, that I am insured, just the result of an offer/order/confirmation process or something different?"
"Have context specific help."
"Does the order of fields reflect the way people think and work when they fill in a request for offer?"
"Keying in passwords so often is boring and at some stage will happen automatically without thinking what is signed. So only sign when really necessary."
"As a user I would like to know in which step I am in."
"After the end of a transaction one should immediately be able to open a new form."

Performance

Also the issue of performance was risen:

"There was a problem with speed."
"Speed would hopefully be better with a real product."
"Low speed."
"What happens if many requests come in?"
"Too slow."

Suggestion on Marketing

Last but not least, a suggestion on the marketing of the FIT was made:

"When defining the potential users of the software we have to be careful not to say that this is something for you and me and everybody, but much more for the PC-literate person with some experience on the Internet."

3.3 Findings on Digitally Signed Business Documents

Several questions were asked on digitally signed documents for three reasons. The first one was to make sure that respondents understood the possibilities of the technology. The second one was to learn whether they would find digitally signed documents useful. The third one was to learn whether the FIT would be applicable for the transactions they had in mind.

3.3.1 Benefits of Digital Signatures

3.3.1.1 Benefits of Signed Offers and Orders

Here we present findings on question 5 on benefits of signed orders and offers.

Would it be cost-effective for you to require digitally signed *orders* from your customers if this costs 0.3 per cent of the transaction value?

The reason why costs were mentioned in this question are that we wanted to be able to identify cases in which there are definite benefits when using digital signatures, and the amount was chosen with in order to show that the costs will be below credit card costs The answers show interest.

"Yes. From a certain amount on, in the computer industry from DM 500 to 1,000."
"Yes. Selling expertise, software or documents. If I personally know somebody I also do business with him over the phone and don't always insist on written documents. In the digital world this might not work that well: How can I identify my peer reliably?"

But also reasons for not requiring digital signatures were mentioned, as long as there are alternatives or as long as the loss is small.

"No. You would not require it if not all of your customers have it. Nobody would turn down an order. We sell software. There is much interaction with the customer."
"Does not make sense. With our printing shop the majority is regular customers from which we accept an order via telephone. Abuse will be limited. However, there will be companies with which these .3 % are justified."

Would it be important for you to require digitally signed *offers* from your suppliers if you had to register yourself for DM 200 / FF 600 / £80 per year?

It was believed that requiring digitally signed offers can well make sense.

"Yes. I outsource software development. It is very important for me that I have the system at a certain date. Otherwise I can't sell to my customers, I may go bankrupt."
"With our suppliers lots of paperwork, which confirms this and that and states that certain standards are met, have to be exchanged. This could be done much faster and with less effort electronically."
"In the area of information technology the suppliers change. Signed offers would be beneficial."
"Offers are something binding, they must be signed."
"All kinds of transactions where I have to insist that they be done correctly: services, tax consultancy. That the declaration is filled-in in time."

Two respondents would require signed offers if the costs were lower.

3.3.1.2 Benefits of Digital Signatures in General

Here we present general comments made on digital signatures, in particular feedback on questions 3 and 4.

Benefits

General Benefits

In general, respondents appreciated the availability of evidence and the replacement of paper:

"If the signature is legally binding, it would eliminate the need to keep separate records – therefore safe time."
"It have to be expensive and critical items."
"For company invoices."
"I am tired of bank statements".
Sign transactions in "on-line banking".
Require digitally signed documents? "Certainly, then it is legally binding."

“Signatures are good because mistakes happen.”

One respondent, however, said that digital signatures do not make sense in transactions done electronically today.

“If something can be done without digital signatures already electronically, there is no need to replace it.”

That respondent was referring to the costs and risks of using digital signatures, such as costs of on-line certificate revocation checks, time-stamps, or costs of secure key handling.

Save Travel Time

One respondent liked the perspective of replacing documents which one has to fetch or sign elsewhere:

“I hate having to walk to the bank, to government offices, to the post-office.”
“The idea of working from wherever you are without having to be physically present to sign something would enable disabled people or people who have to look after their sick relatives or children to take part in the workingplace again.”

Replace Credit Cards

Respondents concluded that digital signatures have the potential to reduce the use of credit cards. They saw that they need not send their card data if they were able to provide a signed order. The statements below were made when discussing private usage, though the considerations are also applicable for transactions made with procurement cards.

“Mail Order: Today the credit card number is sent through the Internet. If tomorrow you could simply sign the document or even sign for instalment payment schemes, this would be a benefit.”
“SEMPER could replace the current business practise of using credit cards for everything.”
“(Would use digital signatures) because of unauthorised use of credit card. For security reasons, because it is no problem to obtain credit card data.”

Of course, as compared to credit cards, no payment guarantee would be provided (unless a letter of credit were given).

Tax Payments

Some suggested that filing tax forms would be very attractive for making users interested in digital signature technology and registration:

“Big English companies already file their VAT electronically. By signing them (and if the Inland Revenue accepts them) quite some paperwork could be saved.”
“Make it available in such a way that it will save time to first time users. If, e.g., we allow to fill TVA[3] forms electronically, this will save time.”
“Tax and legal documents.”

[3] "Taxe sur la Valeur Ajoutée", Value Added Tax

Summarising, we present the feedback on the questions 3 and 4 which were to be ticked:

Do you think digital signatures would be beneficial in certain transactions *already done electronically?*

company use:	yes 14 / no 2
private use:	yes 10 / no 3

Do you think digital signatures would be beneficial to replace *current paper documents?*

company use:	yes 12 / no 4
private use:	yes 9 / no 6

This shows the clear interest to use digital signatures. Note that the interest to have evidence in electronic transactions is slightly higher than to use it in paper transactions.

Issues with Digital Signatures

Some issues arose when discussing digital signature.

Uncertainty Regarding Evidential Value

Some comments show fear of not obtaining usable evidence, e.g., if manipulations can be made, or if the document will not be accepted at court.

"Can somebody manipulate?"
"How will jurisdiction react? (It is important) to have a trace of evidence, which can be used in case of legal disputes, which may happen from time to time."
"(Non-repudiation data) It is claimed that they cannot be manipulated? (Digital signature) If it is secured in a way that no manipulation is possible, definitely. I am doing that with UPS every other day (misunderstanding). (What sort of transaction would you not do electronically today?) Transactions which threaten one's existence: If the customer could cancel, because no written document exists. Work contracts should better be made in ink. I am afraid that something can be inserted digitally."

Trade-off with Privacy

One respondent saw the potential trade-off with privacy:

"Digital signatures would be beneficial for all transactions, in many emails. I would like to know that everything I get is genuine. On the other hand it would be a pity if everything on the Internet has to be signed because I am also concerned about privacy."

Secure Key Handling

The issue of secure key handling rose, in general, and in particular if users will have to have many keys in the future.

"This certificate is for email only. How many certificates do we want? And the more we have, the less secure. There are Verisign certificates which can only be used for signing software. I am not interested in that."

"We need to separate non-repudiation from authentication. You know it is from me, but you cannot go to court. In PGP-newsgroups they sometimes have keys 'not for non-repudiation'."

It was also suggested to have, for signing high value transactions, special signature keys and even a special computer:

"Have a high liability key and a low liability key. If I have to sign something for a million Dollars, then I'll go in a special room where I have a PC which is not on the network. For 10 $ I don't care, maybe I don't even want to be asked for a password, just say 'sign this stuff'."

The network solution would require the usage of a liability limit.

Inter-operability

The issue was risen whether cross-certification and trans-border usage of digital signatures can take place securely. A representative of a British certification authority brought up the issue whether cross-certification can take place because registration will be of very different quality:

"There is no signature law in Britain at all. Therefore different certification authorities have completely different certification procedures. Therefore cross-certification is almost impossible as most of these certification authorities are not very thorough. Apart from that: How do you uniquely identify somebody in a country without IDs? You prove your identity by showing three letters addressed to you."
Another respondent was referring to Thawte: "Why should I trust an unknown company in South Africa?"

Minimum Age

"Digital signatures should only be available for person with the age of 18."

3.3.2 Applicability

We now present results on question 8.

Assume you and your business partners were registered for making digital signatures and had the FIT. Would the FIT be instantly applicable for you?

Yes: 8
No: 6

As many suggestions for improvement have been made, it can be assumed that the feedback would be better if these improvements had been made. Also, some respondents said "no" because they saw that there is a problem of diffusion, as their partners neither have the FIT, nor are registered or have signed the SECA.

"We are facing the chicken-and-egg problem. As long as nobody really accepts digital signatures the benefits of using them are limited and as long as the benefits are limited nobody wants to invest into a digital signature."
"Certification Authorities will have to give away a lot of free certificates, just to get the user base."

Another respondent also mentioned the “chicken-and-egg problem” preventing her from using it. “The system makes sense as soon as a critical mass of people has signed the SECA agreement and uses the software.”

The issue may sometimes be particular difficult to solve should senior management not be willing to use the new technology:

“Our suppliers would not be able to use the new technology. People who are entitled to sign on suppliers’ behalf will be the last ones to pick up on new technology.” (referring to transactions worth millions of Brit. £.)

One respondent compared this diffusion problem to the diffusion of fax machines, thus demonstrating that such problems can be solved over time.
We also asked what the respondents would buy or sell using the FIT (question 9). This is presented below in Appendix A, column 4.

3.3.3 Values to Be Signed and Willingness to Pay

3.3.3.1 Values to Be Signed

We now present findings on question 10. One group of respondents imagines to do transactions with values such as in private consumption or with credit card transactions. This group is thinking of the following values:

Initially DM 100 (in order to get to know the technology)
Above DM 500-1,000
Max. DM 2,000, average DM 120
Max. DM 1,000, average DM 60
Max. DM 4,000, average DM 800
Max. DM 100, average DM 50
below DM 2,000

Others, however, think of doing transactions worth thousands and millions, e.g., when buying a large number of computers or valuable telecommunications equipment (antennas, amplifiers etc.), or when providing valuable expertise.

“Up to DM 200,000.”
“Up to DM 500,000. 25,000 would be small values.”
“Offers for 25 mio. Brit. £, average 100,000 £.”
“For a consumer who buys a food-processor for DM 100, a Visa card is OK. But for companies, where a purchase of equipment can be worth millions, you better use digital signatures to replace the paper (contracts) used today.”
“We are not so much talking only about a purchase worth DM 100, but also about a distributor like Computer 2000 ordering 1,000 computers with HP for 1 Million or more.”
“Transactions worth DM 20'000. Our company would offer the whole range of services. Up from DM 500.”
“In procurement digital signatures will become important. That’s about millions of DMs.”

“Offers for 5 mio. Brit. £ (from insurance companies), average 100. For instance, I would conclude a liability insurance on the Internet, if I could be sure that they guys are really going to pay from the moment on in which I signed.”

In the last quotation it becomes visible that the value of a contract, here an insurance, can be much higher than the face value of the transaction actually made, here equivalent of the fee.

3.3.3.2 Willingness to Pay

Here feedback questions 12 and 13 is presented, which were designed to find willingness to pay.

Pay for the Certification Authority

In the questionnaire, respondents have been prompted with certain figures of what certification services could cost, as a means to make clear that the handling of digital signatures will come with some costs. Given the above findings showing interest to make high value transactions, it would make sense to investigate pricing models for high values. The amounts mentioned are:

Pay for the Certification Authority as a relying party

.2 %, 10 DM
.3%, .10 DM per check, 50 DM for registration
.1 %, 1 DM per check, 100 DM registration
.3 %, not much for a seller
.3%
3 %
DM 40-60 for registration, as with Eurocard
£ 50
DM 100 p.a. (DM 200 too much for private transactions)
Less than DM 200

Comments showed that respondents believe that the seller will have to bear the costs.

“All costs have to be carried by us.” (talking about selling to private customers)
“The seller would have to bear the costs for the signatures. Otherwise I would have to go to a company and also convince them of the idea.”
“If somebody wants to earn money with me, he will have to bear the costs.”
“Prices for CA (certification authority) should depend on transaction volume.”
“As a seller I would not like to bear the costs for both the signature and the payment.”
“On-line checks of certificates are very important.”

Some respondents indicated a willingness to pay for the Certification Authority, also in the role of the signing party:

.2%, DM 99, DM 49 for registration
50 DM annually, 50 DM for registration
250 FF
“I can imagine to pay for a certificate. Don't know how much.”

Comments:

“ (Danish bank group) charged 250 kroner (Euro ~34) for SET. Crazy, only to lower their risk”.
“Percentage payments are fine until I find that I pay more than just a few pounds to the CA. As soon as I pay more than 100 EURO, I would search for ways to re-negotiate my terms and conditions.”
(A representative of a CA:) “Businesses do not understand anything about certification or security. Therefore they are willing to ‘buy’ a certificate if the complete solution is worth the effort and the money. Therefore (we) will issue Class 3 certificates for 50 pounds, not expecting to make any money for some years, but then.”

It was also mentioned that respondents would make a cost-benefit analysis and decide thereafter.

Pay for the FIT

Comments showed that the FIT is compared with other Internet software, which frequently is distributed to private users for free.

“The customer (‘Endkunde’) certainly would not pay for it.”
“For non-commercial users the FIT should be for free.”

But respondents also suggested they would pay more for a FIT which can be integrated into other systems, or if packaged with CA-services.

“Would pay more if integrated into other systems. Would be good if bundled with CA-services.”
“Would pay more if integrated into databases.”

It was also suggested that before paying for the FIT for business use it would be good to collect experience with using it privately.

“Would first gather experiences at the PC.”

Prices respondents mentioned to be willing to pay were:

Brit. £ 50
DM 10
DM 200
DM 500
DM 50-150 as for shareware

3.4 Findings on the SEMPER Electronic Commerce Agreement

3.4.1 Willingness to Sign the SECA Legal Agreement

Overall, the general approach of SECA, providing for legal certainty by signing it with a hand-written signature, knowing that a participating partner has also signed it, was well understood (questions 6 and 7) and most would sign it.

Yes: 16 / no: 1 / don’t know yet: 3
For company use: 5 For private use: 8

Those respondents who expressed that they would sign it as a private user appreciated the liability limits. The somewhat lower number of respondents willing to sign it as a business player may well be due to the fact that it was not clear how liability limits will work for a high value business transaction; see the discussion below.

3.4.2 Limits in Case of Compromise

3.4.2.1 General Liability Limits

The values respondents mentioned are:

For company use: 2,000 DM, 10,000 DM, 10,000 FF, 30,000-50,000 DM[4]
For private use: 500 DM, 1,000 DM, 1,000 DM, 2,000 FF, 100 ECU

Several respondents found it reasonable that the signatory, in case of a compromised key, has to bear some damage, but at the same time appreciated that there is a limit to their possible damage. A respondent suggested a limit of DM 10,000 being a loss the company can bear.

"SECA reminds me of the situation of today's credit card payments: I'm liable as long as I didn't report my card loss. This gives a clear understanding and confidence."
"As a buyer I like to limit my liabilities to prevent getting into deep trouble if somebody steals my keys. When I request a credit card, I sign similar regulations."
"SECA reminds me of the situation of today's credit card payments: I'm liable as long as I didn't report my card loss. This gives a clear understanding and confidence."
"DM 10,000 is a loss our company could bear."

Users compared the situation with the possible losses with certain bank cards. Though these can be higher with some brands of cards, the low liability limit which is associated with credit cards comes to their minds:

"The liability for loss of key should be as limited as with the VISA-card."

A French respondent refers to French regulations regarding orders made by private individuals.

"For consumers, above 5000 FF, you have to have some protection. Certification authorities have to have guarantee or funds."

Several respondents thought of an insurance taking over the risk:

"By simply signing an insurance contract for private liability cover, I am easily signing a contract worth some million EURO."
"Who will bear the damage? An insurance company? I am afraid that the risk will remain with the seller. With a Eurocard I pay DM 40 or 60 for which all damage is covered. The sum ought not to be much higher. DM 50 is appropriate. How good is the insurance? An insurance has to be part in any case. If I'm not protected against manipulations my whole existence could go down the drain. This must be prevented."

[4] Later in the interview the respondent spelt out that he expects an insurance company to pay for any damage.

The latter respondent was thinking about purchases in the range of DM 100,000. Other respondents saw the benefits of having a clear regulation for the case of damage, but were not able to identify an amount which is high enough for the seller, but small enough for the buyer. After some reasoning, one of them arrived at appreciating low limits as banks provide them:

“Limits would give me a secure feeling. The question is, how to select a limit if one wishes to make high value transactions.”
“Difficult to calculate the possible damage. The seller expects a certain amount of liability. But I am also asking myself what is the worst case which can happen? How likely is it?
If I say ‘zero’, the other one will not make business with me. One would have to know in more detail what the standard type of business is to be conducted with SEMPER. For bank transactions, they have their own infrastructure. There are amounts in the range of DM 100, if something goes wrong.”

There was also a respondent who suggested a limit of FF 10,000 for company use, and added “I do not like idea of liability limits for company use” because he found this to be impractical for a company.

3.4.2.2 Liability Limits Towards Pre-selected Partners

Some respondents found the suggestion interesting to have a different limit for pre-selected business partners, and chose higher ones than they chose for a general limit.

For company use: 10,000 DM, 100,000-200,000 DM[5]
For private use: 1,000 DM, 2,000 DM

Others did not find this suggestion sensible:

“Don't like the idea of limits for pre-selected partners.”
“Limits per business partner do not make sense.”

3.4.3 Spending Limits

In the discussions of the subject, some respondents envisaged a *spending limit*, much like employees have it when buying on behalf of their companies. Such a limit could indeed protect the signatory, if signing privately, or her company from very large losses in case of key compromise.

“I don’t think that I would agree to obtain a certificate that would allow me to pay any amount of money. If this certificate is stolen then somebody can sell my house.”
“Signing within authorisation limits would have helped in the case of Barings.” In which case Barings Bank, according to the respondent, was not able to control trading because employees such as Nick Leeson had a limit on paper, which the respondent believed to be not controllable.

[5] Later in the interview the respondent spelt out that he expects an insurance company to pay for any damage.

“You have a limit of what you are allowed to buy without your manager’s approval. And he has a limit and so forth. This scheme can be implemented with a certification scheme. I would buy microcomputer a or software for a microcomputer. 10,000 FF would be reasonable. To begin with this is a very good limit.”

The respondent who would not accept a certificate good for values like his house is the very same person who would find offers of his suppliers useful, being worth several personmonths. So the challenge is: How can one securely make an offer worth several 10,000 Euro, without incurring the risk of losing such amounts of money? Restrictions on the applicability of a signature key should be investigated.
In any case, the conclusion is that spending and liability limits, in general, per type of transaction or business partner, are an issue worth considering when offering digital signature contracts. It is in particular important to give holders the option to avoid very high transactions and possible losses (>50k). Recall that respondents envisage to spend much more than what is typically the case in a credit card transaction. But for such high values they would probably not be willing to sign that they can be held liable even in case of compromise. More results could be obtained when discussing the complete SECA, options for general spending limits, and an insurance solution, in more detail. An insurance solution deserves particular attention as there will probably be no useful evidence in case of damage (i.e. genuine and fake evidence will look alike), and as it will thus be very difficult to tell real fraud from claimed damage.
Another conclusion is that certification authorities could encourage the use of secure hardware with secure user input and output, so that key compromise is unlikely to take place (see Section 3.6).

3.4.4 General Comments

It was also proposed that the purchasing contract itself should be standardised.

“Standard contracts for electronic commerce.”
Another respondent suggested ”eTerms[6], standard contracts.”
“Good idea. You make a substitute for a non-existing global jurisdiction.”
“For consumers regulating the applicable law is important.” (Respondent means the law of the transaction to be signed).

Other suggestions were that the SECA agreement should state which law is applicable, and consider during registration who is allowed to represent a company.

“Missing is: under which country’s law is this applicable?”
“One would have to take into account who is authorised to sign.”

Applicable law is being treated in the full SECA (see Section 14.5.2 of Baum-Waidner, Zihlmann). Authorisation has optionally been treated during the registration, and was visible if the “Details” button was pressed (see Figure 2).

[6] An initiative of the International Chamber of Commerce (cf. International Chamber of Commerce 2000).

3.5 Overview on Applicability

3.5.1 Relative Importance of Key Characteristics

Table 1 Key Characteristics

The solution should	For you as a seller	For you as a buyer
Be similar to traditional business procedures	6.3	8.2
Be easily tailorable to your needs	7.9	7.7
Support different payment schemes	7.3	6.7
Support different encryption schemes and certification authorities	*3.7*	*4,2*
Be available for different operating systems	7.5	7.4
Create records with evidential value	7.3	**9.1**
Allow you to define the liability for digital signatures	6.1	7.6
Allow for integration into existing back office tools	6.5	5.4

Notes:
Not important at all: 0 .... absolutely necessary: 10
Creating records scored best (bolded); support of different encryption schemes and certification authorities scored worse (italics)

These above results show that:

- Records with evidential values are required by both buyers and sellers.
- The similarity to traditional business procedures is appreciated.
- The possibility to configure the FIT according to one's needs is important, in particular for the seller.

It also becomes visible that selections the respondents are used to, such as the selection of means of payment, are more appreciated than new concepts, such as to negotiate encryption, or to select certification authorities. These points have not been presented in much detail, neither in the program nor in the questionnaire, so no conclusions can be drawn out of their low rating.

3.5.2 Applicability to Types of Trade

The types of trade the respondents wish to make with the FIT, as visible from the table in Appendix A, can be grouped as follows.

1. One is consultancy, such as providing expertise or software. Such contracts are typically specific per business partner, negotiations take place, and the deliverable can be sent *on-line*. Values mentioned by the respondents range from a few thousand Euros up to the equivalent of several personmonths. Respondents of this type are no. 2, 6, 7, 16, all working with companies with less than 100 employees (also no. 19, but with 140 employees).

2. Another type of trade will be purchases of hard goods with *out-of-band* delivery. Respondents mentioned computers, printing machinery or telecommunications equipment, possibly to be bought in public procurement. Also such contracts are frequently subject to negotiation. Respondent no. 4, 9, 10, 18 and 20 are examples of this type and mentioned values up millions of Euros. Occasional private sales of hard goods, as mentioned by respondents no. 10 and 21, are of similar nature.
3. A third type of trade for which the FIT is attractive could be the purchase of services, such as from teachers or craftsmen. In this case, delivery would also be *out-of-band*. Respondent no. 14 is an example, buying and providing teaching services. It would be worth interviewing providers of other services, such as craftsmen, which had not been among the respondents.

We also checked whether there is perhaps a group which is unlikely to use it. It was not possible to identify such a group among the respondents. Respondents number 9 and 14 look a bit less convinced than the others, but have strong arguments for the FIT being beneficial somewhere in their company if sufficiently modified (e.g., for procurement) and if their bosses used it. It was also not possible to identify a group which would use it only privately (possibly respondents number 3, 8, 10, 21). They all had strong arguments why such an application would make sense in business for themselves or their partners.

We believe that the FIT can be easily improved in order to match the requirements for the first type of sales. What would be good for all types of sales, but in particular for high value procurement of hard goods, would be the support of sending offers to several parties, and of obtaining several bids. Also an interface into catalogues will be a useful enhancement.

Regarding private use, the number of transactions per user and period of time will probably be small, but, of course, the number of possible users is large. Note that the FIT can be seamlessly integrated into secure, automated WWW-based sales. This could lead to a substantial demand for the services involved, such as certification, time-stamping, fair exchange services, liability limit services, and last but not least payment services.

3.6 Findings on Implementation on Portable, Secure Computers

3.6.1 General

We anticipate that it will be difficult for users to keep their machines secure from malicious code. Once digital signatures will be in wide-spread use, we must anticipate that attacks will be aimed at. Virus scanners and firewalls may not sufficiently protect users, in particular not against Trojan horses which are new, self-deleting or which address only a few victims (see Weber 2000). This is why typically certification authorities request from their customers to keep their computers free of malicious code. So we thought that a valuable transaction should better take place on secure hardware, with a secure viewer. We suggested to the respondents:

One could put the signature function and the screen of the FIT onto a small, handheld computer, to be connected to your normal Internet-computer (via cable or infrared). Possible benefits for you are:

- **Protection against computer or network fraud, e.g., viruses changing your documents. As a protection, your keys would be stored in a tamper-resistant**

chip, and the device would have its own, secure display.

- **Portability, i.e. you could use the FIT for buying and selling with several computers.**

Respondents were shown pictures of pocket calculator-like devices, mobile phones and PDAs (see end of questionnaire).
Some respondents wondered whether there is a threat at all:

"Do not believe that laptops are so insecure that something like secure hardware is needed."
"Microsoft will solve this" referring to the issue of Trojan horses.

Other respondents see that secure hardware with secure displays will protect them from certain risks.

"From a certain amount on this will be interesting."
"With such hardware I would trust into amounts ten times as high." This respondent had mentioned Euro 5,000, so this would be Euro 50,000.

A respondent was saw the risk, but wondered if a secure device would help:

"If I have to sign something for a million Dollars, then I'll go in a special room where I have a PC which is not on the network...
A device just for signing contracts? I don't think I would need that. Why are paper signatures good enough for a multi-million Dollar contract, but our PC is not good enough? Is the security in the (paper) signature, or is it in the whole process? But you will never ever have a system which is 100 % secure. If we talk about million dollar contracts, there might be a backdoor by the guy who made the machine. I would prefer to trust software on my PC where I can see the source code, compile myself, than some device I would get from you. The Crypto AG in Switzerland, they sell crypto devices. They Iranians found out there was a problem, they sent a message to this device and the Americans knew about it. They were controlled by the NSA...
Of course it should be a trusted device, then it should interface to my PC and upload all the data. That could be a good idea. A secure display is extremely important. How do you know what the smartcard signs?"

So that respondent clearly sees a need, as expressed by his suggestion to use a special room, and his emphasis of a secure display. He arrives at the conclusion that a device would be particularly important when his money is concerned. But he also wonders whether it is really achievable to produce a trustworthy device and quotes the case of the Crypto AG:

"The Crypto AG in Switzerland, they sell crypto devices. They Iranians found out there was a problem. They sent a message to this device and the Americans knew about it. They were controlled by the NSA."

3.6.2 Willingness to Buy

Respondents were asked (question 14):

Would you be prepared to buy such a device?

11 said they would be willing to pay for the device, after having been prompted with

costs of Euro 50 for a basic device, 25 for an add-on to existing mobile devices, and an additional 25 each for one of the following characteristics: larger screen, biometrics, or a self-destroying chip. 7 Respondents would use it for business, and 5 for private use, 1 for payment only. Those who want to use it for business use, commented on their willingness to pay:

- 25 for an add-on
- 100 if it includes biometrics and large screen
- 200 for business use
- 500 to 1,000 if it contains important business functions

Comments:

“Regarding secure hardware I as a business man would have to consider: How much time or money will this device save me? Because without it I would have to do the business manually. This amount saved would be the upper limit for me to pay.”

3.6.3 Integration into Phone or PDA

We also inquired whether respondents rather want to have a special device, something like a secure smartcard-reader with user I/O, or rather a multi-functional device, having also phone and organizer functionality (question 16).

What is your opinion about combining
- **a phone or organizer functionality with**
- **FIT and secure email**

in one multi-functional device?

	Agree (1,2)	**Disagree (4,5)**
I believe a mono-functional device would be more secure (FIT + email)	8	5
I find multi-functionality important because I do not wish to carry around another device	9; (4 agreed to both)	4

The comments respondents made are helpful for understanding their feedback. Some expressed an interest in integrating the signature function into a mobile phone or PDA:

(It should work) “via my Palm Pilot or mobile phone. No new device, one should build upon what exists. For the Palm it will be a file.”
“Combination of phone and PDA would be ideal.”

Others, however, were wondering whether such an integration is secure:

“Should be separate. Otherwise I’d have the problem: ‘Give it to me’ and the other one makes a phone call. Then the whole mechanism is in hands in which it should not be. Or it gets left somewhere.”
“I like very much the idea to use a PDA, but it will have the same problem like my PC very soon, I’ll download all kind of shit on it.”

"Palm: gives me the possibility to take addresses and paste them into the form. I am afraid of wrongly attributed texts."
When discussing viruses: "Everything I will get onto the PC I will also get onto the device."
One said, for private use "include other functionality"; for business use "stand-alone device".
Another one: "If integrated, the security would be lower."
One respondent strongly objected any multi-functional devices because she was afraid of the risk of using the device for something less important than signing: "And then the device will be either empty, broken or corrupted at the time when I want to sign."

The feedback on that question explains the surprisingly high number of sceptical respondents, i.e. eight, of which four would appreciate multifunctionality. A consequence is that multifunctional devices open to arbitrary code need to be designed in a way that users have reason to believe that their secure applications will indeed remain secure. Another issue is that users may wish to keep the device under some physical control. A phone is not necessarily controlled that way. Possibly the signing key could be designed to be taken out, attached to traditional key-rings, or put into a traditional wallet, together with other cards.

3.6.4 Interest in Special Characteristics

In question 15, we asked which characteristics are particularly important.

Table 3: Characteristics of Mobile Hardware

	Important	Not important
Mobility	10	2
Self-destroying chip[7]	5	6
Secure display	13	1
View half A4	8	3
Fit into leather wallet	2	7
Fit into shirt pocket	8	3
Compact from like C	2	10
Biometrics	7	3

Comments on mobility:

"Very important: I want to take it with me."
"Mobility very important."
"If I carry that thing always around with me, I would have more confidence that nobody can do mischief with it."
Matchingly, respondents want to store it in some pocket, but it needs not necessarily fit into a leather wallet.[8]

[7] With zeroisation circuitry, see Weber 2000.
[8] The question of whether a very thin device is required was asked because in the surveys made for project CAFE male respondents had suggested that an infrared payment wallet should be so thin that it can be inserted *into* a leather wallet (Furger et al. 1998).

Two comments were made on self-destroying chips:

"I assume that it is being designed that way."
"Not so important."

Comments on biometrics:

"Biometrics is better than a passphrase. Theoretically, a passphrase can be entered by everybody."

Comments on viewing large documents:

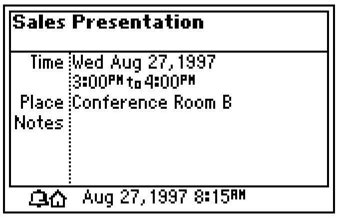
"How will the FIT look on a small hardware device?"
"That the essential points are visible. When I offer an expertise, except of the price, of course, also deadlines and partners are important, and the contents. So if all this fits, I would prefer the smallest."
"It would be sufficient to display text."

One respondent suggested to use a secure device for payment, but a very small one.

"Rolodex, five small buttons, the Rex. Something like that for payments, that would be nice. If it is something I have to carry it has to be very small. If it is in my mobile phone, ok. Some kind of an active card... I'll see here what I have to pay, and it will transmit to the cash register. Should be able to give me the information where I paid what. I would definitely buy a secure device for payments."

The display shown in handout A in the questionnaire was indeed derived from what can be displayed on a Rex (see Figure 3; www.franklin.com/rex)

Figure 3. Information as shown on a Rex device.



The device of type C was said to have a screen with a magnifying lens, as, e.g., manufactured by Kopin. These are available with resolutions from 320x240 pixels up to 1280 x 1024 pixels (see www.kopin.com) On a device of type C, there were two positive remarks:

"Nobody can look over one's shoulder."
"Interesting because nobody sees what you are looking at. With fingerprint good, under a flap so that one does not sign by accident. Also put a PIN-pad under a flap in case the biometrics won't work. Would irisscan be possible? Handling of C is somewhat unusual, but also mobile phones had initially been met with a pitying smile."

The feedback on C was not very enthusiastic. Though there was interest to have a secure display (13 respondents) and view, e.g., half an A4 page (8 respondents), the idea to use a screen with a magnifying lens scored poorly, as only 2 respondents found it important. We believe the reason for the low scoring of the viewer is that using such a device is in contrast to the existing rule for viewing business documents, which is to check them in normal reading distance. A further issue is that an approval of a document during signing will be difficult. When hold the viewer in one's hand, how would one express approval? One would not be able to key in a PIN conveniently. Also a fingerprint reader will be difficult to use, as one might unwillingly touch it. It was suggested to put a flap above it, to be lifted only when signing. As these screens are technically very good, the issue should be investigated in more detail, with an appropriate application being shown on the screen, and real prototypes instead of printouts. Possibly voice recognition could be used for approval, but this is probably also in contrast to today's rules of approval.
One could design an application in the way that selected parts of the document to be signed are clicked on the main computer, and these sections are then securely viewn on the mobile computer. Thus one would not have to check the whole document on the secure screen. This might work with some applications. We found, however, that respondents who are interested in high value transactions mentioned attachments, which in general have been produced by other applications (text editor, CAD program, etc.). Viewing such arbitrary documents securely will not make visualisation easier. As it is most likely very difficult to view them on the "portrait" type of PDA-screens, the usage of "landscape" screens has to be explored.
Note that the terms and conditions, digital signature agreements, certification practice statements etc. could be included by reference, e.g., "standard terms type F" (eTerms, see International Chamber of Commerce 2000).

3.6.5 Applicability

We now describe the findings regarding two groups.

Moderately High Value Business Transactions Group (bolded)

- Engineer, selling expertise (respondent no. 2).
- Computer dealer, discussing sales and purchases of computer. Envisages that larger sellers will buy larger numbers of computers electronically (no. 4).
- Selling expertise, each worth several thousand Euro (no 6).
- Consultant, providing e-commerce related services (no 16).
- Consultant, looking for solution for selling high-value used machinery (no. 18).

This group is both interested in the FIT and in secure hardware. They would pay up to Euro 100 to 1,000 for secure hardware.

High Value Procurement Group
There were three respondents mentioning transactions worth millions of Euros. They thought of procurement with several bids. The FIT has not been presented as a solution supporting that.

- Printer: “In procurement digital signatures will become important. That’s about millions of DMs.” Later: “B to b on-line is not really appropriate. Would prefer to go the traditional way.” Respondent does not see a need for mobility and is sceptical regarding secure hardware: “Everything I will get onto the PC I will also get onto the device.” (no. 9)
- Economist, on the need for signatures: “For a consumer who buys a food-processor for DM 100, a Visa card is OK. But for companies, where a purchase of equipment can be worth millions, you better use digital signatures to replace the paper (contracts) used today.” He mentioned telecommunications equipment as well as consortium agreements such as in EU research projects as attractive cases for being handled digitally. Regarding a secure device, he is thinking about private usage (no. 10).
- Project manager, selling training services: Suppliers would not be able to use the new technology. “People who are entitled to sign on suppliers behalf will be the last ones to pick up on new technology. ... With the training suppliers there is lots of paperwork, which confirms this and that and states that certain standards are met, have to be exchanged.” It would be the respondent’s board who would accept the offers and sign. He sees benefits as much paper needs to be moved in procurement. He requires, for business use, a stand-alone device (no. 14).

How to view and sign these attachment, though mentioned as being possible with the FIT in software, has not been worked out for mobile hardware. So the high value procurement group had little willingness to pay for secure hardware. The issue of high value procurement thus deserves further research.

4. Outlook

The most important feedback and some consequences are:

1. The FIT can be used in order to provide for more security in "manually" conducted business transactions. It should be enhanced for handling several offers and bids and have an interface for integration into databases such as catalogues and accounting programs. Certainly it would be beneficial if other secured business applications could be used with the same security enhancements, as proposed by project SEMPER.
2. Business respondents expressed a certain willingness to pay for the FIT, ranging from very low amounts, up to Euro 100 or 200. It could be higher if the FIT were more powerful or integrated into other solutions for Internet trade.
3. Most respondents would sign SECA as an agreement for globally handling digitally signed documents.
4. Liability limits have been appreciated, but an insurance needs to be integrated which pays in case of claimed compromise, in particular for business transactions in the range of 100,000 Euros or more.
5. Fair exchange would certainly be a beneficial characteristic, securing two-party contracts, acknowledgements of orders, and receipts for payment and deliveries. The interface would have to be worked out (need for approval, actions in case something goes wrong, production of replacement signatures by third parties).
6. There is a group of respondents who is prepared to pay Euro 100 to 1,000 for secure mobile hardware with secure user input and output and use it for transactions of a value up to Euro 10,000 to 100,000.
7. Developing a user interface which allows to develop trust into a device which is at the same time open for code from unknown sources but can also keep secure applications secure is an unmet challenge.
8. Visualisation of normal business documents on mobile devices is another challenge. The usage of screens with magnifying lenses and the development of appropriate approval procedures, as well as the usage of "landscape" screens, should be further investigated.
9. There is a need for strong encryption as respondents mentioned that they wish to trade information such as patents or expertise, and want to keep prices confidential.
10. With the approach of using two computers, a normal PC and a mobile one, it will be difficult to handle confidential business information. The reason is that in this concept the transaction will be on the normal computer in full, thus the confidential information can possibly be eavesdropped. Therefore secure PCs will be beneficial. However, in cases in which the means of user input and output of smaller devices is sufficient, these can be turned into little fortresses with tamper responsiveness and evidence.

5. References

Baum-Waidner, Birgit; Zihlmann, Rita: *Legal Aspects.* In: Lacoste et al. 2000

Furger, Franco; Paul, Gerd; Weber, Arnd: *CAFE Survey Results.* Paper, 1998. Available at <http:/www.iig.uni-freiburg.de/~aweber/>

Hamamtzoglou, Akis; Hecht, Thomas; Papadopoulos, Iannis; Weber, Arnd: *The Fair Internet Trader.* In: Lacoste et al. 2000

International Chamber of Commerce, <http://www.iccwbo.org/home/electronic_commerce/electronic_commerce_project.asp>, 26/05/2000

Lacoste, G.; Pfitzmann, B.; Steiner, M,; Waidner, M. (eds.): *SEMPER Final Report.* LNCS, Springer-Verlag, Berlin 2000

Schunter, M.: *Fair Exchange: A New Paradigm for Electronic Commerce.* In: Lacoste et al. 2000

Weber, A.: *Full Bindingness and Confidentiality. Requirements for Secure Computers, and Design Options.* Proceedings of ECIS 2000, Vienna 2000

6. Appendix A: Table with Key Findings

Notes to the table on the next page:

Values are in Euro. “Y” means “yes”, “N” means “no”. In the column “Sign SECA”, “b” means “business role”, and “p” means “private role”. Some knew which role they would play, but were not sure whether they would sign it. “MP” means “mobile phone”, “PDA” means Personal Digital Assistant or organizer.

Respondents who are particular interested in both the FIT and in secure hardware are bolded.

In Column 4 it is being presented what respondents would use the FIT for. Values in brackets mean that the respondent mentioned such type of trade, but found it difficult to use the FIT as it was for conducting it.

x) At first glance, one would expect that respondents either agree to “I believe a mono-functional device would be more secure” or to “I find multi-functionality important because I do not wish to carry around another device.” But it turned out that several respondents agreed to both statements (see Section 3.6.3).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
No.	Profession	What do you like?	Dislike / Suggestions for Improvements	Use it for	Pay for FIT	Max. values signed	Pay s'th. for CA	Sign SECA	+/- 100 em-ployees	Owns	Buy device	Mono-multi-funct. x)	Self-destr chip	View half A4
1	Engineer	Analogy	Interruption		Y	(limit 500)		Y p	-					
2	**Engineer**	**Digital signatures**	**More intuitive**	**Expertise**	**100**	**500 (limit 5,000)**	**x**	**b**	**-**	**MP PDA**	**Y**	**multi**		
3	Engineer	Simplicity	Inflexible		250	(limit 2,000)	x	p	-				x	
4	**Computer Dealer**	**Negotiation**	**Interruption**	**Computers**	**25-75**	**100,000**	**x**	**Y b**	**-**	**MP PDA**	**Y 500-1000**		**x**	
5	Accountant	Can work at home			Y	2,000	x	N	-		N			
6	**Technical expert**	**Negotiation**	**Interruption**	**Expertise**		**10,000**		**Y b, p**	**-**		**Y 50+50**	**mono**	**x**	**x**
7	Security Consultant	Forms	Standard set-up	Programming	Y	worth MMs	x	Y b, p	-	PDA-phone	for paym.			
8	Lawyer	Ease of use					x		-	MP	Y	mono, multi		x
9	Printer	Evidence		(Procurement)		millions		Y p	+	PDA	N			
10	Economist	Structure, openness	Append files	Procurement, used cars	5	millions	x	Y p	+	MP	Y Δ25	multi		x
11	Economist	Transparency	Speed	WWW-shopping, banking		50,000	x	Y p	+	PDA	Y Δ50	multi	x	
12	MSc (Internet Solution Provider)	Trusted window	Tedious	(Programming)		14,000			-	MP PDA		mono, multi		x
13	BSc (Certification Authority)	Security	Interface like MS-products					Y	-	MP PDA	Y	mono		x
14	Project Manager	Evidence	Less complex	(teaching services)		30 mio.		Y	+			mono (b)		x
15	Expert in ergonomics	Auditor	Help, print-outs	(for replacement of cc)	70		x	Y	-	MP	Y	multi	X	depends
16	**Computer scientist**	**Usability, proofs**	**Less steps**	**Programming**		**30,000**	**x**	**Y**	**-**	**MP PDA**	**Y 200**	**mono, multi**		
17	Retailer	Show differences	Speed, integration	Retail of food	50		x	Y	-		N			
18	**IT consultant**	**Negotiation**	**Interface to catalogue**	**Used machinery**	**Y**	**25,000 - 250,000**			**+**		**Y**			
19	Economist	Easy to use	More space	Consultancy	10	initially 50, poss. mio.	x	Y p	+	PDA	Y 10	mono		
20	Banker	Legal certainty	Easy choice of being seller or buyer	Custom-made goods	50+	3,000	x	Y	-		Y 25-150	mono	x	
21	Economist	Immediate legal certainty	Fields need more space	Car, banking		(limit 5,000)	x	Y	-	MP	Y Δ25	multi		x

7. Appendix B: The FIT Questionnaire

Number:____ Interviewer: Date: FIT:__ Simulation:__

Survey on the Fair Internet Trader (FIT)

A program which enables

- buying and selling over the Internet
- of digital or hard goods
- with digitally signed offers, orders and receipts
- with encryption of all communication
- and has a standard procedure to do this spontanously

Options:
- The seller can request payment after delivery, or when the order is made.
- Payment can be electronic, or out of band.
- The seller can send an invoice right after the order was made, or send the invoice with the delivery.
- The invoice can be electronic, or out of band.

Examples:
- you as a business person buy something, e.g. computers
- you as a business person sell something, e.g. software or music
- you as a private person buy something, e.g. trousers or stocks
- you as a private person sell your work or something second hand.

(show FIT)

1. What do you like about the FIT?

....

....

....

2. What do you dislike?

....

....

....

SECA Legal Agreement - a Proposal for the Usage of Digital Signatures

- You (or your business partners) would have to sign an agreement.
- This agreement would most likely make digitally signed documents acceptable as evidence before court, independent of legislation.
- It would work on a global scale.
- By checking electronic certificates your business partner can verify that you have signed this agreement and vice versa.
- The agreement also regulates what happens if you lose your key, if somebody spots or guesses your password, etc. (compromised key).

SEMPER Electronic Commerce Agreement SECA

Extract - To be signed in person at the certification authority

This agreement is made between the certification authority XYZ and the signatory.

I am liable for my digital signatures (tick at least one):

- ☐ representing company __________
- ☐ as a private user.

You can chose one or two options from the following, or none.

Option: Liability limit for compromised key

If I claim that my secret digital signature key was compromised, I am liable for my digital signatures up to the limit of

for company use:

amount: .... currency: ......

for private use:

amount: .... currency: ......

These amounts will not be revealed to my business partners.
My business partners may request that I provide a message from my certification authority stating that the amount of a transaction is below my liability limit for the compromise of key.

Option: Liability limits for compromised key towards pre-selected business partners

If I claim that my secret digital signature key was compromised, I am liable for my digital signatures towards pre-selected business partners up to the limit of

for company use:

amount: .... currency: ...... towards: ....
amount: .... currency: ...... towards: ....

for private use:

amount: .... currency: ...... towards: ....
amount: .... currency: ...... towards: ....

Place, date: ....
Signature

3. Do you think digital signatures would be beneficial in certain transactions *already done electronically?*

company use: yes ☐ no ☐
private use: yes ☐ no ☐

If so, please give examples: ....

4. Do you think digital signatures would be beneficial to replace *current paper documents?*

company use: yes ☐ no ☐
private use: yes ☐ no ☐

If so, please give examples: ....

5. The certification authority will have certain costs for registering you or your business partners in person, for having a central computer with a hotlist of lost and stolen keys, and for the optional checking whether liability limits are exceeded. Pricing could be flat, e.g., Euro 100 per year for the signer, or the relying party would have to pay a fee per transaction, e.g., 0.3 per cent of the transaction value, at least when checking the central computer.

Would it be cost-effective for you to require digitally signed *orders* from your customers if this costs 0.3 per cent of the transaction value?

Orders	company use	private use (if applicable)
Yes		
No		
Possibly in the future		
Don't know yet		
If the costs were lower		

Would it be important for you to require digitally signed *offers* from your suppliers if you had to register yourself for Euro 100 per year?

Offers	company use	private use
Yes		
No		
Possibly in the future		
Don't know yet		
If the costs were lower		

Comments: ....

6. Would you be prepared to sign the SECA legal agreement for producing binding digital signatures with evidential value?

yes ☐ no ☐ don't know yet ☐

7. If yes, please fill it in right now.

Suggestions for modifications of agreement:

....

8. Assume you and your business partners were registered for making digital signatures and had the FIT. Would the FIT be instantly applicable for you?

yes ☐ no ☐

Comments:
....

9: What would you buy or sell with the FIT (or a FIT improved according to your needs)?

Sell: ....

Buy: ....

10. If you think of the documents *you* would *sign* with the FIT (or an improved FIT), what value would they have?

	Signing on behalf of company			Signing privately		
	Maximum value	Average value	No. of documents per month	Maximum value	Average value	No. of documents per month
Orders						
Offers						
Don't know yet						

Currency: .....

11. Please indicate for each attribute the importance for a trading tool:

Fill it in for your role as a player in: business: ☐ private: ☐

(Agree: 1 ... Disagree: 5)

The solution should	**For you as a seller**					**For you as a buyer**				
	1	2	3	4	5	1	2	3	4	5
be similar to traditional business procedures										
be easily tailorable to your needs										
support different payment schemes										
support different encryption schemes and certification authorities										
be available for different operating systems										
create records with evidencial value										
allow you to define the liability for digital signatures										
allow for integration into existing back office tools										

12. As a *relying* party, e.g., as a commercial seller getting orders, or as a private consumer getting offers, what would you be prepared to pay for the FIT, for signed documents and for checks of databases regarding lost and stolen keys?

	I'd pay as a business relying party	I'd pay as a private relying party
For the FIT-software Purchase price of:		
For the certification services A percentage of transaction value of: An amount per check of database: For the initial registration of myself / my company:		
Don't know yet		

Currency: _____

13. As a *signing* party, what would you be prepared to pay?

	I'd pay as a business signing party	I'd pay as a private signing party
For the FIT-software Purchase price of:		
For the certification services A percentage of transaction value of: An annual fee of: For the initial registration of myself / my company:		
Don't know yet		

Currency: ______

Implementation on Portable, Secure Device

One could put the signature function and the screen of the FIT onto a small, handheld computer, to be connected to your normal Internet-computer (via cable or infrared). Possible benefits for you are:

- Protection against computer or network fraud, e.g. viruses changing your documents. As a protection, your keys would be stored in a tamper-resistant chip, and the device would have its own, secure display.
- Portability, i.e. you could use the FIT for buying and selling with several computers.

(discuss handouts A, B, C, D)

Costs:

- The basic device would cost around Euro 50.

- If you want integration into your mobile phone, organizer, or personal digital assistant (PDA), you would have to pay for today's cost of that device, and an additional Euro 25.

- For certain characteristics, you would have to pay more:

  - for a screen to view half a page (A4) at once
  - for biometric verification, so that only you could use the device (the biometric data would remain in your device)
  - for a self-destroying chip, destroying the keys in case someone tries to break a stolen device in his laboratory

  Each characteristic would cost you roughly Euro 25.

14. Would you be prepared to buy such a device?

	Yes	No	Don't know yet
Business			
Private			

(if you want to use it in both spheres, you would use only one, but with different signature keys)

If "yes" or "don't know yet", continue with 15. If "no", continue with 19.

15. Which of the following characteristics are important for you:

	Would not buy without	Important	Not important	Don't know yet
Mobility (usability of the signature function with several computers)				
Self destroying chip				
Secure display (protection against viruses / fake interfaces)				
Display to view 1/2 A4				
Thin enough to fit into leather wallet				
Thin enough to fit into shirt pockets				
Compact form, like C				
Biometric user verification (protection against eavesdropping of password, loss and theft of device)				

16. What is your opinion about combining

- a phone or organizer functionality
  with
- FIT and secure email

in one multi-functional device?

	Agree 1	2	3	4	Disagree 5
I believe a mono-functional device would be more secure (FIT + email)					
I find multi-functionality important because I do not wish to carry around another device					
I don't care					

17: How much would you be prepared to spend on it?

As a mono-functional device (FIT + email) : .... currency ....

In case of integration into phone or organizer (multi-functional), on top of the normal price an additional: .... currency ....

What do you expect to be included:

Biometrics: ☐
Display to view 1/2 A4: ☐
Self-destroying chip: ☐

18. A few personal details:

I am: ☐ male ☐ female

My age is: ☐ under 18 ☐ 18 - 25 ☐ 26 - 30 ☐ 31- 40 ☐ 41 - 50 ☐ 51 - 60 ☐ over 60

Highest level of education completed:
☐ Secondary School
☐ Examination for entry to higher education
☐ Apprenticeship
☐ University or technical college
☐
☐
☐
☐ Other:

Nationality: __________

I work in branch: __________

Number of employees in my company: __________

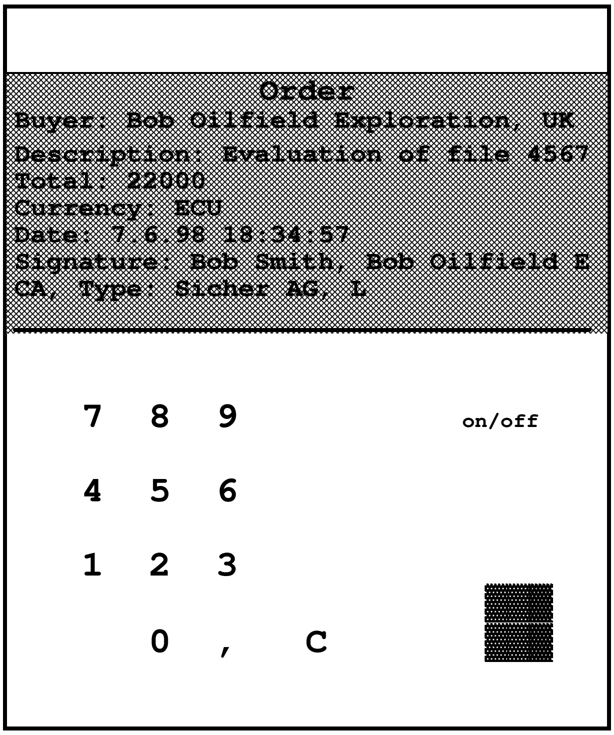
I use a mobile phone: ☐

I use an organizer or PDA: ☐

	Yes	No	Don't know	Planned for next 12 months
My company sells on the Internet, e.g. accepts orders via email, or sells on the WWW				
My company buys on the Internet				
My company uses credit cards for buying or selling on the Internet				
My company uses EDI				
My company does electronic banking				
Other:				

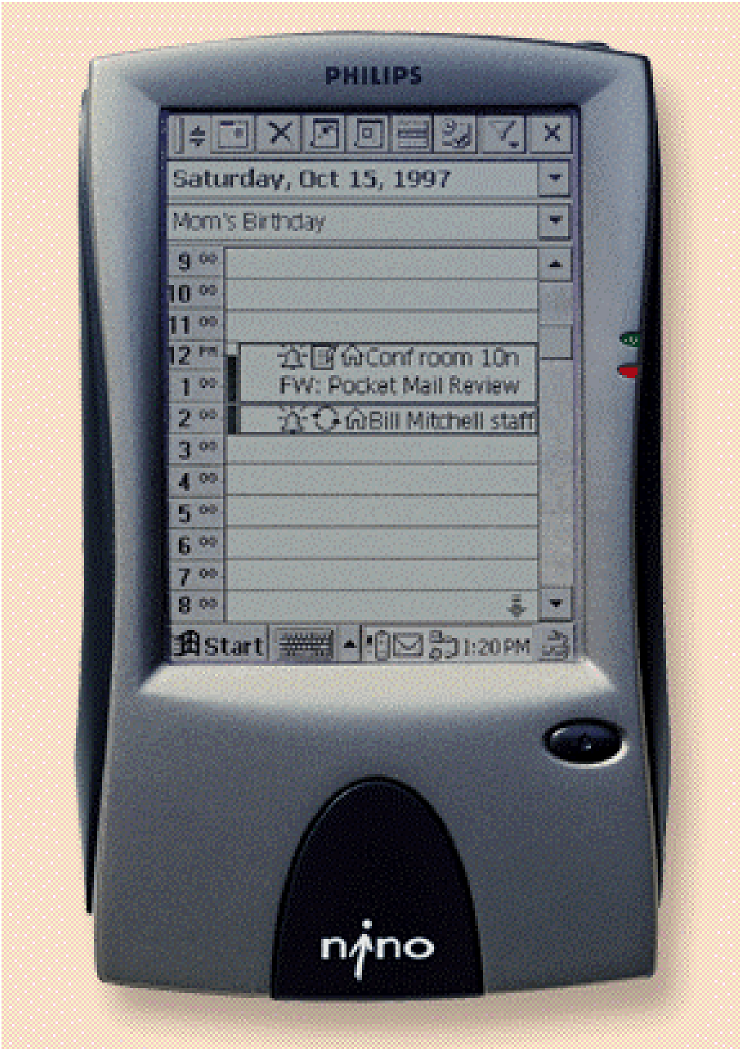
A) Pocket calculator-like

- Display shows only the most important data, such as amounts, recipients, the first words of items descriptions.
- The rest of the information is only on the normal computer screen.
- Could fit into leather wallet.



B) Organizer/PDA-like

- A larger display, showing whole text, around 1/3 an A4-page at once. Through larger documents one would have to scroll.
- Could fit into shirt pockets.



SHOWN ACTUAL SIZE 5.25" L x 3.41" W x .87" D 7.33oz./200g.

C) Compact

- A very small screen with a magnifying lens.
- You would see around 1/2 of an A4-page and could scroll through the rest of the document.
- Could be very compact.

D) Mobile phone

- With a display either like in A or in B.