

# SEMPER Field Trials and User Evaluation

**Dale Whinnett**  
**University of Freiburg, Germany**  
**<dalew@iig.uni-freiburg.de>**

## Outline

- 1. Description of Basic/SME Trials**
- 2. Security Services Tested**
- 3. Buyer Reactions**
- 4. Seller Reactions**
- 5. Initial Reactions to Fair Internet Trader (FIT)**

# Trial Scenarios

## Business contexts

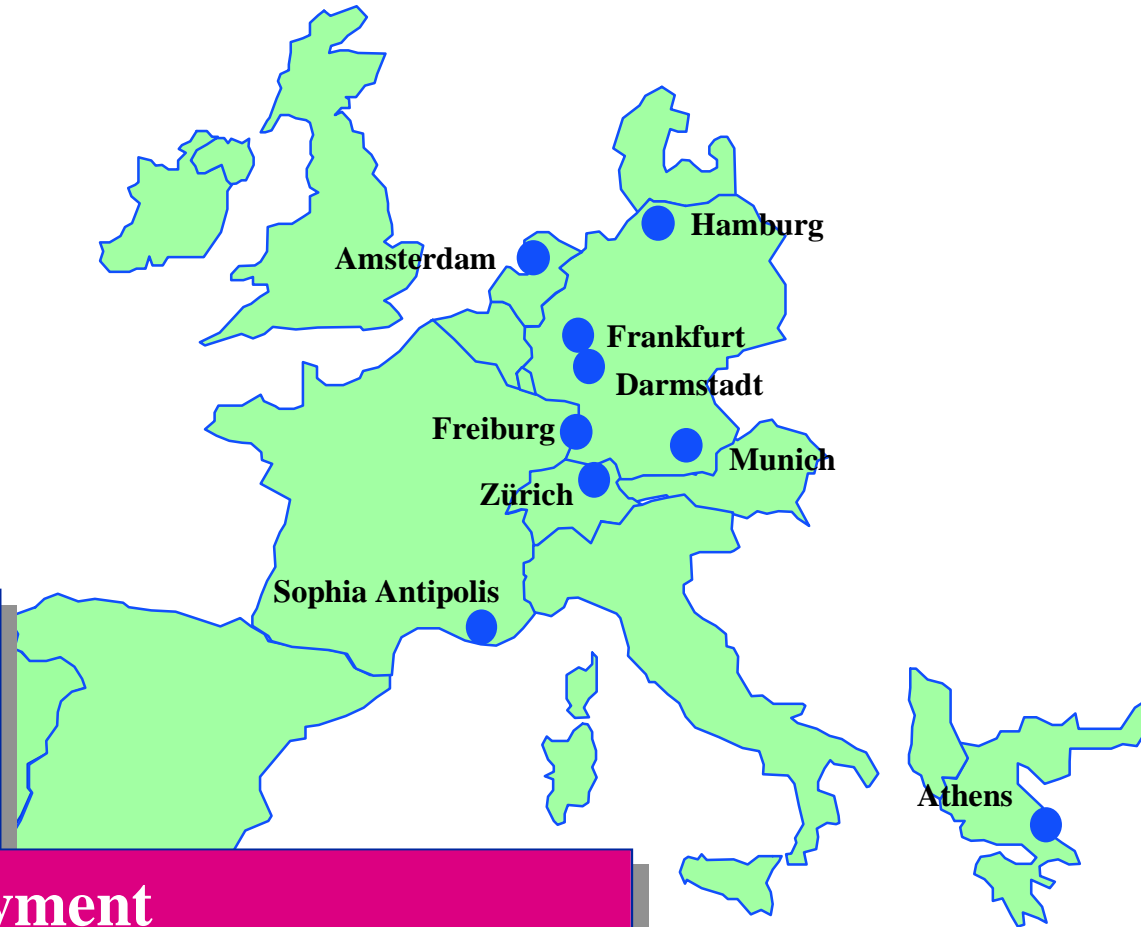
- Mail order
- Tele-training
- Literature Service
- Database access
- Image distribution

## Players

- Registration authorities
- Sellers
- Buyers
- Banks

## Payment

- Credit cards
- stored value
- SET
- Customer accounts



## Decision to make supervised *Basic & SME* Trials

### Problems:

- ◆ computing skills of users, i.e. lack of confidence to install & configure a software prototype
- ◆ user understanding of security technologies, e.g. types of encryption, key lengths, public key infrastructure
- ◆ restricted “real life” opportunities for use
- ◆ necessary to explain SEMPER architecture to enable evaluation

### Solutions:

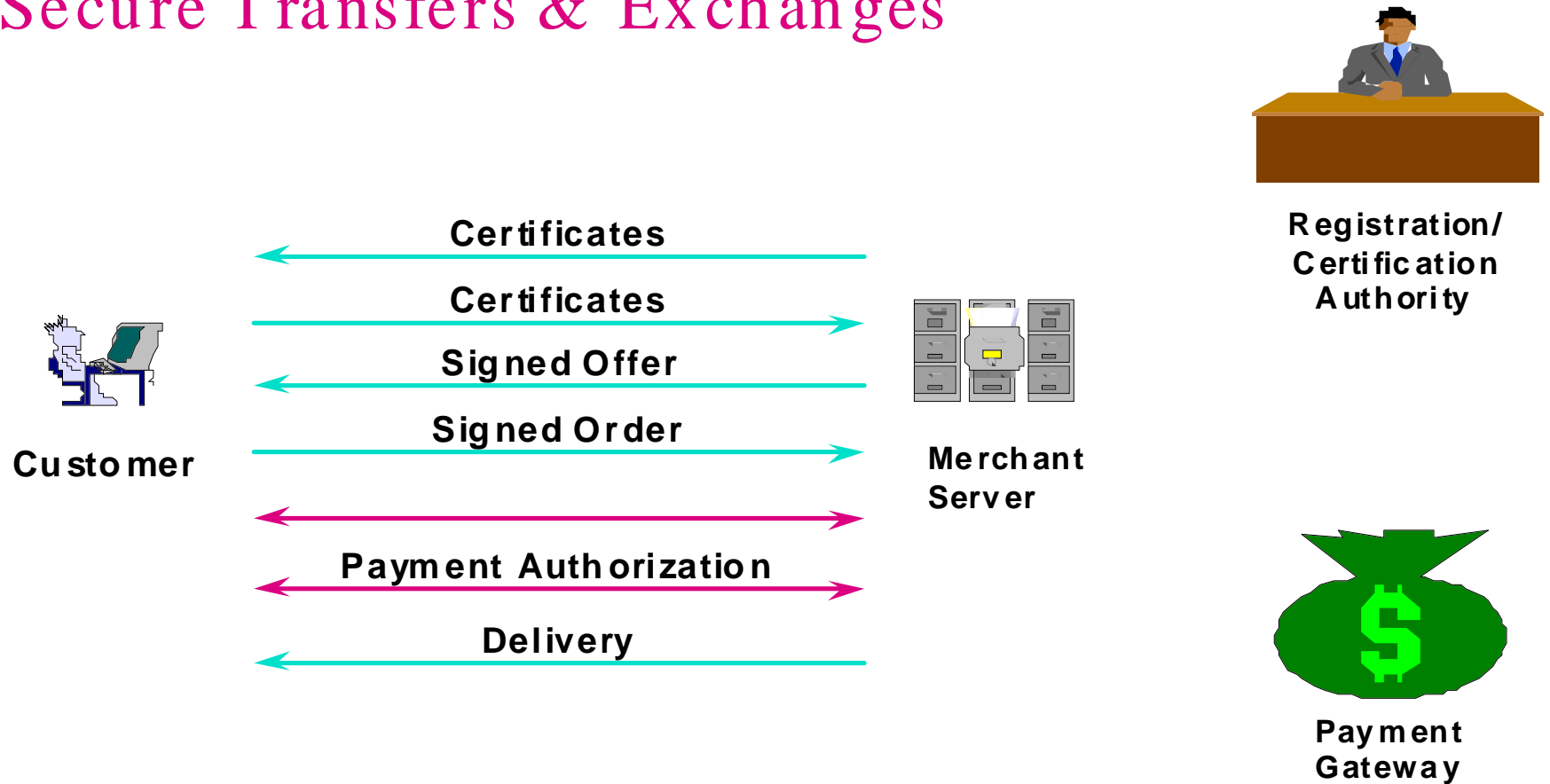
- ◆ supervised interviews with pre-installed software
- ◆ additional information regarding security mechanisms provided by interviewer
- ◆ SME trial sites offered “live” testing of real sites
- ◆ supplementary information used to explain architecture (illustrations, etc.)



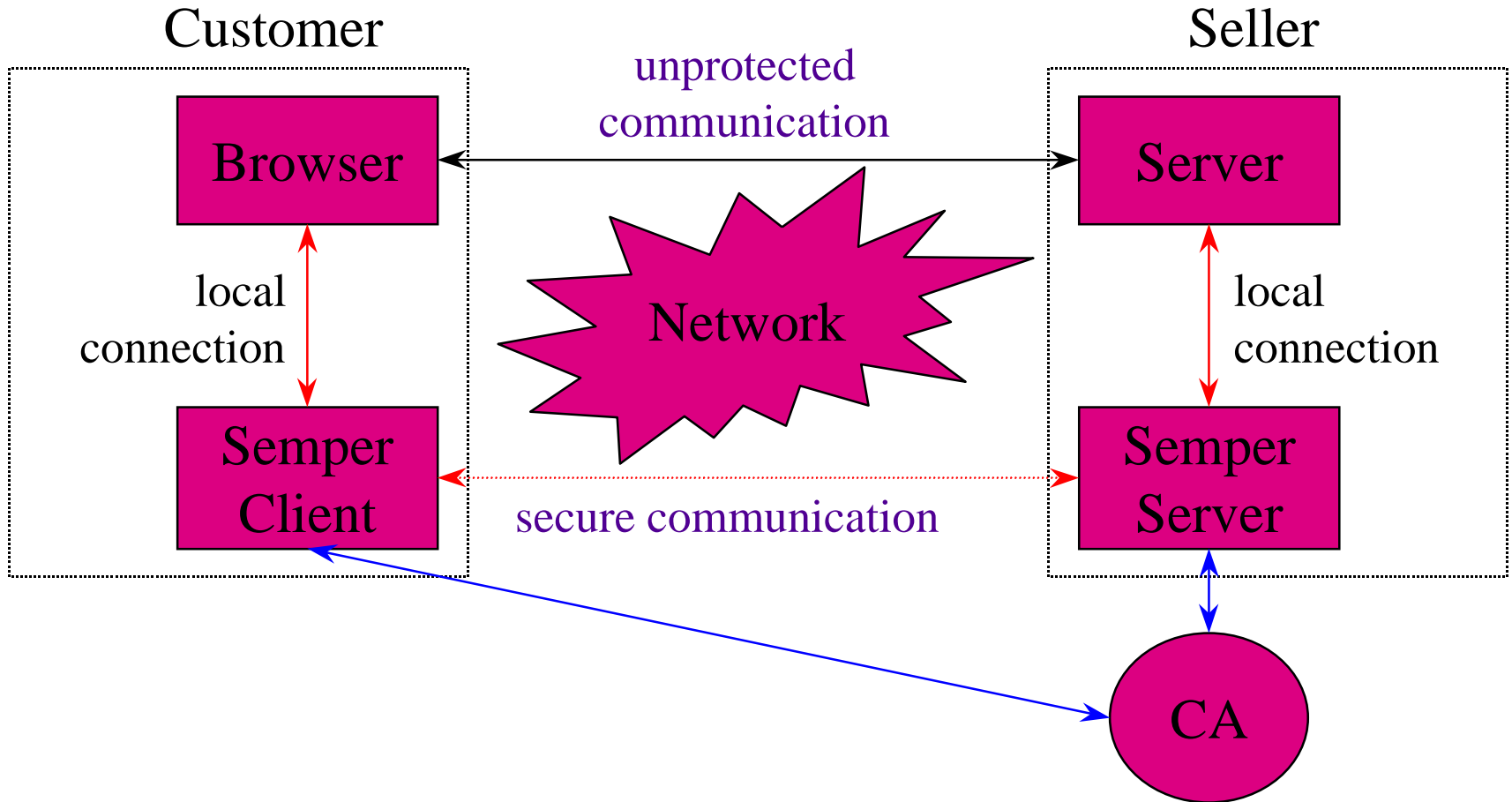
## Trial Participants

- ◆ **80% have used the Internet for more than 2 years**
- ◆ **applications used:**
  - ◆ **WWW**                      **93% daily**
  - ◆ **email**                      **87% daily**
  - ◆ **FTP**                      **57% weekly**
- ◆ **Average duration of trial + interview = 2 hours**
  - ◆ **local software initialised (login, password entry, key generation, registration with CA)**
  - ◆ **creation of 1 or more purses**
  - ◆ **visit SEMPER trial site**
    - ◆ **authentication - customer by merchant, merchant by customer**
    - ◆ **transfer of signed statements - offer/order**
    - ◆ **payment - credit card (SET, SSL), generic purse, stored value with user device**
    - ◆ **online delivery of digital goods - offline delivery of hard goods**

# Secure Transfers & Exchanges

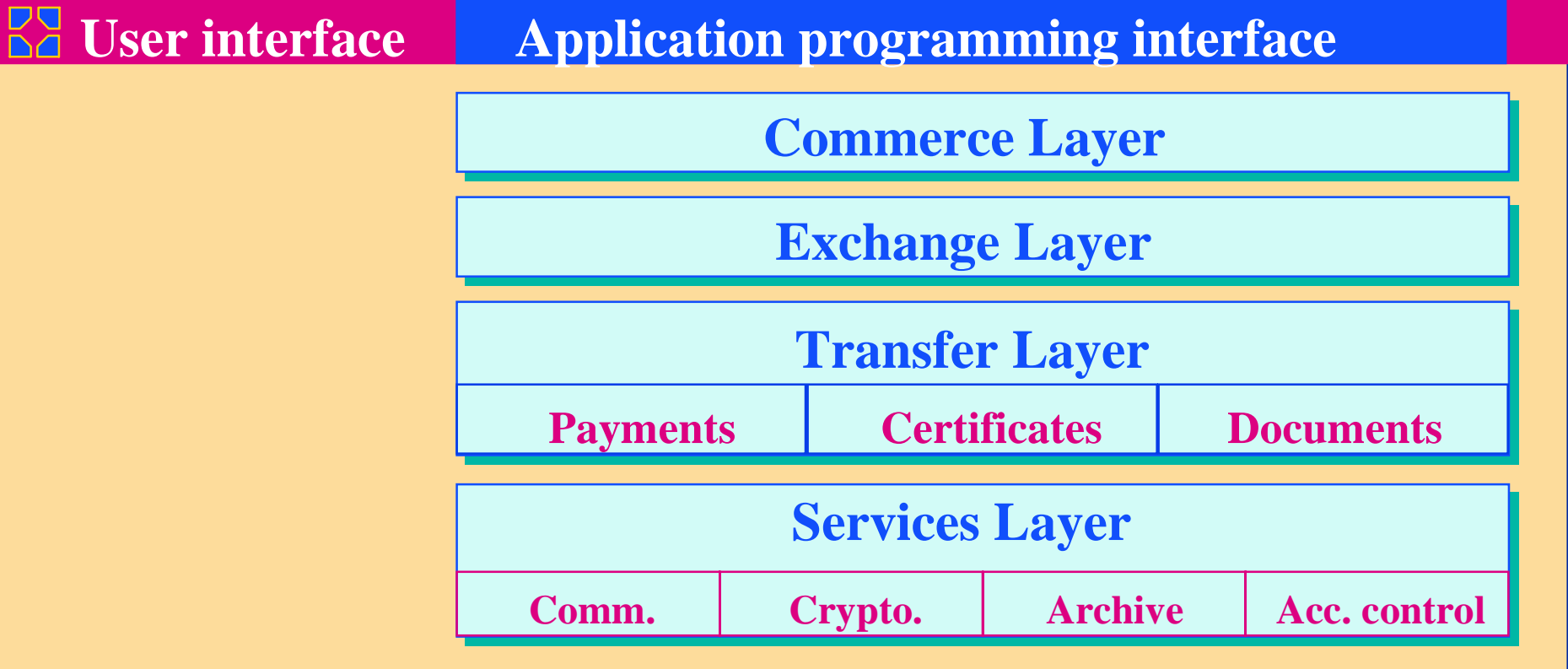


# Participants & Connections



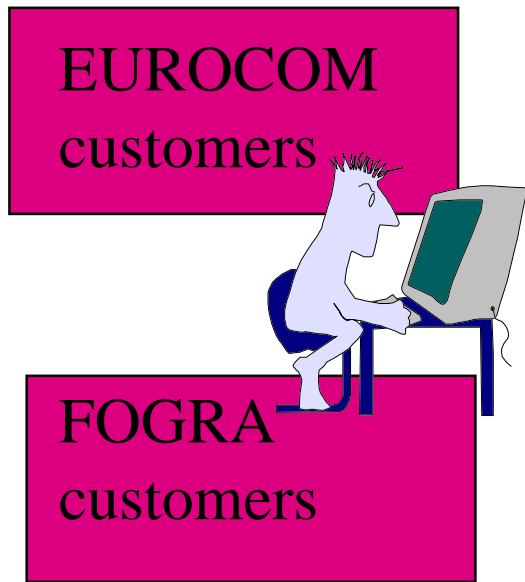
**Browser/server**

**Business applications**

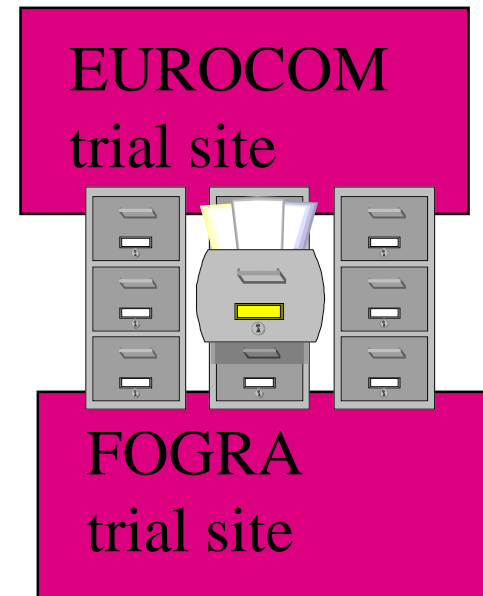


# Phase I Trials

33 Trial Participants



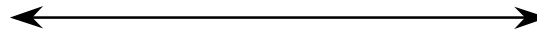
Trial Sites



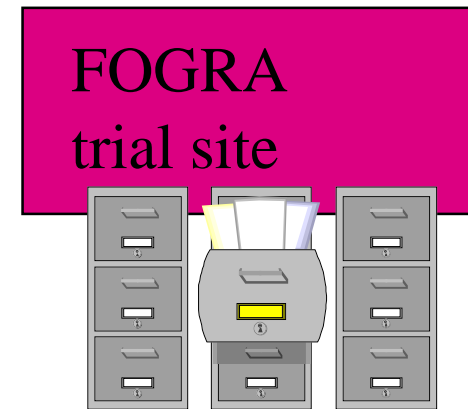
secure ID, signed offer/order, online delivery, generic purse

## Phase II Trials

12 Trial Participants



Trial Site

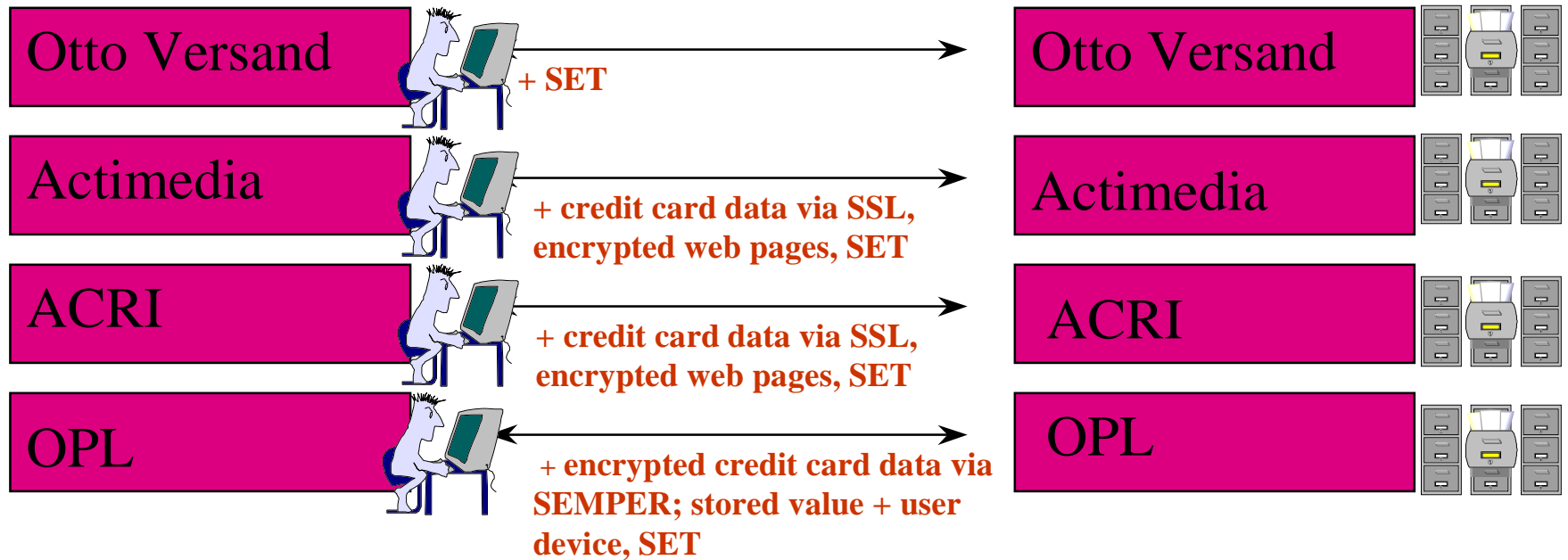


secure ID, signed offer/order, online delivery, generic purse  
*plus* initialisation of software (registration, purse creation)

# Phase III - SMeTrial

16 Trial Participants:  
Customers of

Trial Sites

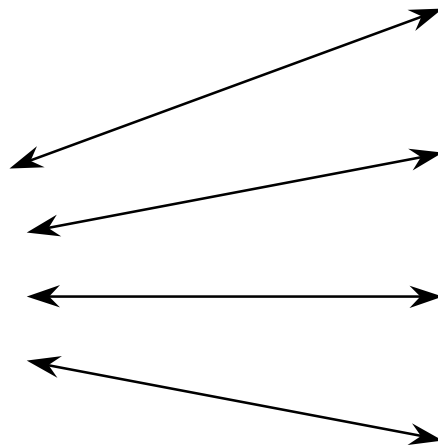
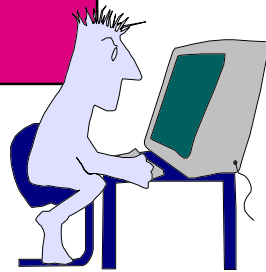


secure ID, signed offer/order, online delivery, generic purse  
*plus* initialisation of software (registration, purse creation)  
*plus* new forms of payment





# Phase III - SMEtrial

10 Trial Participants

invited "testers"  
IIG Freiburg

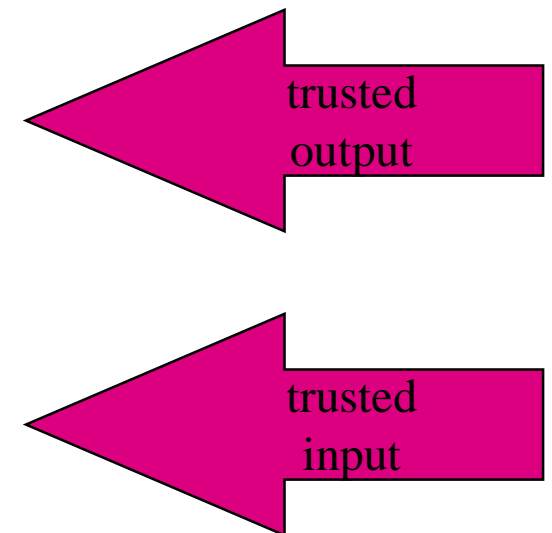


Trial Sites

- Otto Versand 
- Actimedia 
- ACRI 
- OPL 

trial participants tested all SME trial sites and forms  
of payment from one computer

## User Interface in Basic/SME Trials



A central element of Semper is the *Trustworthy INteractive Graphical User Interface*, “**TINGUIN**”.

## Trustworthy User Interface

## Browser Window

**Connected to ACTIMEDIA**

---

**Offer**

**BACH Suites for violin**  
**BEETHOVEN Trios**  
**BEETHOVEN Piano Sonatas**

<b>Price</b>	<b>1150 FF</b>
<b>VAT tax</b>	<b>50 FF</b>
<b>Shipping</b>	<b>70 FF</b>
<b>TOTAL</b>	<b>1270 FF</b>

**Signed May 25, 1998 14:00**

---

**ORDER**    **SIGN**    **PAY**

### Classical Music CD Roms - Platform PC

<input checked="" type="checkbox"/>	<b>BACH Suites for violin</b>	<b>250 FF</b>
<input type="checkbox"/>	<b>BACH Partitas</b>	<b>400 FF</b>
<input checked="" type="checkbox"/>	<b>BEETHOVEN Trios</b>	<b>400 FF</b>
<input checked="" type="checkbox"/>	<b>BEETHOVEN Piano Sonatas</b>	<b>500 FF</b>
<input type="checkbox"/>	<b>BEETHOVEN Sonatas</b>	<b>700 FF</b>
<input type="checkbox"/>	<b>COUPERIN</b>	<b>400 FF</b>

# Trial Participant Reactions

## ◆ valued

- ◆ all security relevant information in one window
- ◆ one “security tool” to manage e-commerce needs
- ◆ clear separation of secure window from insecure browser
- ◆ variety of payment options
- ◆ transaction archive/browser
- ◆ ability to personalise according to individual needs
- ◆ ability to extend with use (e.g. add purses, certificates)

## ◆ criticised

- ◆ no status bar or symbol in TINGUIN to indicate connectivity
- ◆ too many user confirmations required
- ◆ information in transaction browser difficult to understand
- ◆ no digitally signed receipts
- ◆ not enough information about keys & key storage
- ◆ no certificate browser



# User Prerequisites for Electronic Commerce Tool

(questionnaire results)

## ◆ Essential in e-commerce tool

- ◆ secure payment (93%)
- ◆ ease of installation and maintenance (85%)
- ◆ data privacy (81%)
- ◆ ease of use (80%)
- ◆ signed offers/orders (76%)
- ◆ encrypted data transfer (73%)
- ◆ choice of payment options (60%)
- ◆ record-keeping (57%)

## ◆ Essential changes before willing use SEMPER

- ◆ legal acceptance of digitally signed evidence (69%)
- ◆ used by broad range of suppliers (64%)
- ◆ secure key storage (60%)
- ◆ electronic receipts (57%)



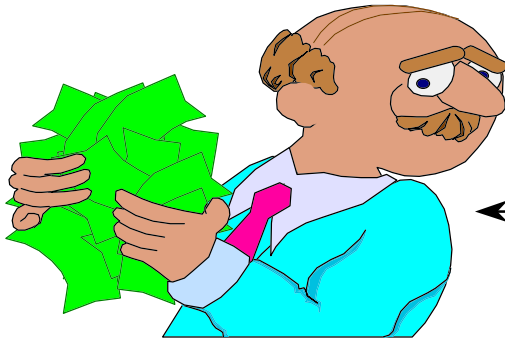
## Services in three trial phases

Trial Characteristics	EU R	FOG	FRE Basic	OTV	ACRI	Acti	OPL	FRE SME
secure identification of business partner	√	√	√	√	√	√	√	√
digitally signed offer	√	√	√	√	√	√	√	√
digitally signed order	√	√	√	√	√	√	√	√
generic purse (test payment system)	√	√	√	√	√	√	√	√
digital goods delivered on-line	√	√	√				√	√
real goods delivered off-line				√			√	√
webpages encrypted / sent via SEMPER					√	√		√
credit card data transmitted via SSL					√	√		√
SET payment protocol				√		√	√	√
encrypted credit card data via SEMPER						√	√	√
stored value - chipcard and user device							√	√
real credit card payment							√	√

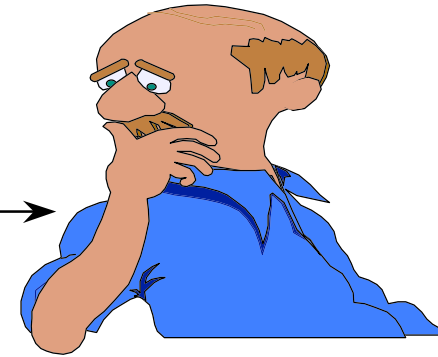
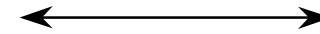
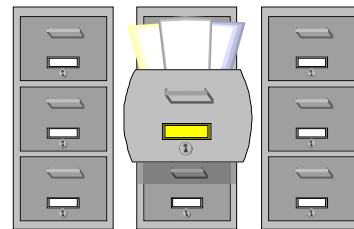
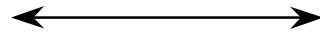
## Seller Reactions

- ◆ **infrastructure (financial/ legal) to support secure electronic commerce not yet in place**
- ◆ **customer base not yet experienced enough for transition**
- ◆ **future prospects for use good, all required the functionality in the SEMPER architecture, it needs to be exploited and refined**
- ◆ **consumer education essential**
- ◆ **businesses need easy way to create business applications, e.g. “module installer”**

# Advanced Trials Fair Internet Trader (FIT)



business partner



business partner

- + negotiation of contract content
- + forms with fields
- + warning of changes
- + negotiation of security settings
- + non-repudiation tokens (signed receipts)
- + dispute handling (import/export)
- + SECA (limiting liability)

# Fair Internet Trader (FIT) - initial reactions

( 9 demonstrations/interviews)

- ◆ **appreciated similarities to traditional business documents**
- ◆ **for businesses signed order is more important than electronic payment**
- ◆ **ability to configure to suit different business processes valued**
- ◆ **want to be able to forward documents to other departments**
- ◆ **means of limiting liability important for private and business use**

---

# SEMPER - The Swiss Knife for Electronic Commerce

“The advantage of SEMPER is that the existing tools are incorporated into one tool that I can use for doing business. Its possible to assign meaningful roles to the various tools. I can say here is a databank, with goods and offers in it, and I can abstract an offer from it, digitally sign it and send it over as a container and that’s much more than just PGP and RSA and emails.”

“It is the only software I’ve seen which organises all the relevant issues in electronic commerce.”