Semper -
The last chapter, or the first?

- Did SEMPER reach its objectives?
  - Where they the right ones?
- Can we eventually take SEMPER to the market?
  - Will it satisfy/appeal to the users?
- What are the most prominent features of SEMPER?
  - The Architecture?
  - TINGUIN?
  - The bargainer (FIT)/SECA?

What has happened since we started?

1. SSL, SET and Java arrived
2. The User is less and less in control
3. Workstations are getting more and more vulnerable
   - SEMPER adapted to SSL, SET and Jav without problems
   - The SEMPER architecture can cope with 2) & 3)
   - Are the any alternatives to SEMPER
     - – even if SEMPER is not the best solution. I think not.

What has *not* happened since we started?

- Still no useful PKI
  - with a few exceptions (e.g. Swisskey)
  - EC still seems to be about mail order and off-line/credit-,debitcard payments
  - The banks are not playing!

Problem: Unless this changes, SEMPER may be considered overkill for EC

- – but appealing for other applications!

- because what is SEMPER?

- A very advanced security approach
  - still looking for the right application
- But, you cannot sell security

  - only secure applications
- SEMPER is not a product
  - It is trying to set a trend
  - It is pre-competitive
  - It may becomse a standard

Who are
the potential customers?

- Vendors
- Banks
- Governments/Public Institutions
- Education!

  Only they will appreciate - if any - the depth and quality of the solutions

- and they will not even have to pay for it!

So what is SEMPER again?

- Its an advanced security solution
  - which must be tamed and trimmed!
- Its an open adaptive architecture
  - which will only survice if adopted by vendors and users
- It focuses at this stage *too much* on security
  - e.g. fingerprints of keys, even in TINGUIN
  - users not interested in key management

    - only security services

In conclusion - on a scale from 1 to 10 ....

I would give SEMPER 8 points

Why not more?

1. Too complex (too slow, too large)
2. At most 1 in 4 will have the intellectual ability to use it
3. Too much can go wrong
4. And too much academic security freaking!

But on the whole a very impressive, sound and innovative approach!

Where are we heading then?

I believe EC in the near future will be characterised by

- Off-line or credit/dibit card payments (still)
- Is build around individual applications provided by a service provider (e.g. BOLERO)

  - in semi-closed systems
- quite likey initiated/required by governments
  - – e.g. the FSTC-"check" pilots in USA
- There is a growing understanding for TUI
- Chipcards arte moving in