

SMART.IS Accompanying Measure Minutes of March 2nd 2001 meeting

Attending organisations :

The following participants attended to the meeting :

- Prime contractors organisations of the Smart.IS Accompanying Measure (Smart.IS AM) :

Olivier Trebucq for Eurosmart, olivier.trebucq@gemplus.com

David Ankri for SIS MARKETING, david.ankri@wanadoo.fr

Stéphane Ménager for CYBER-COMM, stephane.menager@neurocom.com

Bruno DUPONT for EURALIA, bruno.dupont@euralia.com

Patrice Santi for SIS MARKETING, psanti@eap.net

Astrid COUSIN for EUROSMART, astrid.cousin@eurosmart.com

Excused :

Claude MEGGLE for CYBER-COMM, cm@cyber-comm.com

David Stephenson for CYBER-COMM, ds@cyber-comm.com

- EUROSMART members

Thierry Collin for THALES, tcollin@dassault-at.fr

Anastasie Akibodé for PHILIPS SEMICONDUCTORS, anastasie.akibode@philips.com

Stefan Posch for PHILIPS SEMICONDUCTORS, stefan.posch@philips.com

Ian Duthie for ATMEL, iduthie@atmel.com

- FINANCIAL operators

Susanne Bidsell for VISA INTERNATIONAL, bidsells@visa.com

Angel Lozano for SERMEPA, alozano@sermepa.es

- Other experts

Eddie Bleasdale, for NETPROJECT, eddie@netproject.com

MAIN OUTCOMES

1 Approval of the agenda and approval of the previous meeting's decisions

AGENDA

10am	Common welcome
10:30	Reminder of previous meeting (25 January): conclusions and approval of the minutes.
11:30	Relation with e-Europe trailblazers/Smart.IS Web site (working procedures/Company logos)/Budget allocations.
12:30	Discussion

1pm Lunch break

Afternoon will be divided into two working sessions:

Working Group 1 (**definition of a cardholder identification module**) - Chairman: Cyber-Comm

2pm	WG1 action plan: reminder of objectives and deadlines
2:30pm	Interim Report: current status of work. Integration of inputs and contributions of participants.
3:30	Next steps before first draft report
4pm	End of meeting

Working Group 2 (**banking and telecom convergence model**) - Convenor: Cyber-Com

2pm	WG2 action plan: reminder of objectives
2:30pm	Definition of action plan and of contributions of partners.
3:30pm	Next steps
4pm	End of meeting

2 Review of the project status by Olivier Trébucq and David Ankri

- Link with the eEurope initiative

It has been agreed by Smart.IS participants that Smart.IS should be linked to eEurope, but has to remain a different initiative.

A decision should therefore be made during next Steering Committee as regards to which eEurope Trailblazer Smart.IS should contribute. It was suggested that it could also be a Trailblazer in itself.

It has been suggested that a summary and proposal should be sent to each Trailblazer chairman in order to discuss possible collaborations.

- Budget

It has been reminded that a budget has been authorised for written contributions which will be sent by participants, on the basis of 75 Euros per hour, and of 2 men day per month during 6 months for each participant as an average.

Total budget for each working group should be around 50 000 €.

In order to get the authorisation, contributors should send their proposal with the name of the contributor, the number of hours, and details on the contribution.

Contribution proposals should be sent to Patrice Santi (psanti@eap.net)

Olivier Trébuçq will soon confirm the overall budget available and the planning for proposals submissions.

- Review of Working Group 1 status

It has been reminded that the scope of the project has been defined, and that Smart.IS participants have agreed to make a single authentication.

It has been agreed that first draft report should be finished by 4 or 5 June, then a final report should be presented to ETSI on 5/6 July. A coordinator from ETSI should be found for this purpose.

- Review of Working Group 2 status

It has been agreed that this working group is having a problem of management. Cyber-Comm has accepted to be the convenor of this working group, but with the help of a financial or telecom operator. Their involvement is therefore necessary to improve the efficiency of WG2 management.

It has been suggested that Working Group 2 should be linked with Trailblazer 12. Participants therefore encourage Cyber-Comm, which is also convenor of TB12, to make that link, notably in order to facilitate information exchange between the two.

3 Working Group 1 session

The WG1 meeting started with a review on existing standards and systems of interest for NAME.

- Sermepa first presented its contribution on EMV SDA & DDA & on-line 3-DES Authentication methods (slides are available on Smart.IS Web site). Main messages:
 - NAME requires DDA like process.
 - WAP certificate format is different from X509, EMV certificates are not X509 as well. WIM as well.
 - Comparison between these certificate formats shall be done.
 - SERMEPA is already using DDA.
 - It has been suggested by Stéphane Ménager that some elements of the presentation should be included in the NAME report. There is a need however to go deeper in EMV certificate and specifications. Sermepa agreed to provide additional information. Visa will see if it can contribute as well.
- Stéphane Ménager presented the Identrust systems (slides are available on Smart.IS web site). Main messages:

- Identrus LLC was formed in April 1999 to create an International trust infrastructure to facilitate global electronic commerce & provide a root CA for financial institutions.
- 300 financial institutions, mainly oriented BtoB, are members, including: ABN-AMRO, Citibank, IBJ, Barclays, Chase, HSBC, WELLS FARGO, CIBC, Bank of America, etc.
- Use of smart cards for end-users device and OCSP (On line Certificate Status Protocol based on IRTF protocol) responder for real-time certificate validation.

Identrus specifications (as of 31/08/1999):

- Identrus Minimum Operating Requirements (IO-MOR) Identrus & level one participants
 - Identrus PKI & Certificate Profiles (IT-PKI) : Identity certificate for authentication & signature, and utility certificate for SSL, S/MIME)
 - Identrus SmartCard requirements (IT-SCR) : RSA & SHA-1, code PIN (6 Minimum), security evaluation compliant requirements: ITSEC E4+ with SoF High, FIPS 140-2 Level 2
 - Identrus Signing Interface Requirements (IT-SIR): SW requirements Java library & plug-ins for browser, PKCS11, PC/SC or OCF interface with SC. *(TB7 & TB12 should be interested, not an issue for NAME)*
 - Identrus Naming Conventions & Object Identifier Schema (IP-NAMOID)
 - Detailed specifications are confidential, but it has been suggested that Identrust representatives could be invited for next meeting for a presentation and discussion.
 - It has been also suggested that someone from GTA, which are developing a similar system might be invited (by Sermepa).
- A representative from Netproject presented this 3 years project involving users and aiming to achieve secure E-Business (slides available on Smart.IS web site). Main issues presented:
 - A solid test bed is required for NAME
 - Infrastructure for e-business must be vendor neutral
 - Several UK universities are building a secure sign on solution based on public domain products, (open source is mandatory for several governments (German,...)).
 - Proposal define a test bed in order for PKI providers to test their solutions and prove conformance against std.
 - Open source is required, stability (e.g. LINUX). No virus on well configured LINUX systems up to now.

- Participants have identified the standards for which similar overviews should be made:

Banks	Telecom	Internet
7816, EMV, SET, Identrus, GTA?	SIM, WIM, USIM, WTLS	SSL/TLS, X509, PKIX, IETF,

- The working group discussion continued with a review on the report summary, for which contributions are needed. The structure of the report should be as follows:

1 Introduction

- 1.1 Objectives and scope of the report. This paragraph should describe the objectives of Name as a common module for smartcard for authentication of the user based on certificates.
- 1.2 Standard survey (description of current standards used, context around WIM). This paragraph should describe the different standards separated in the three main domains that concern Name (Telecom and mobile, Banks and financial, Internet)
- 1.3 Business requirements. This paragraph should describe the business requirements for Name. Name is a standard describing a set of specifications which can be used in several business applications to provide authentication of the users. Some examples should be given.
- 1.4 PKI background. This paragraph should describe briefly what is a PKI and certificates, how it works, and in more details the use of certificates for authentication.

2 Functional description of NAME

- 2.1 Synopsis. This paragraph should describe how Name can be used in a real environment. This paragraph does not include requirements. It describes some examples of how Name can be used, for a better understanding purpose. Some schemas should be included to have an overview of the different elements involved (Internet, Web Server which need the authentication of an internet end-user, the end-user smartcard which include a Name module, etc.).
- 2.2 Overview on generation, authentication process, revocation... This paragraph should describe the different processes involved in the use of Name. This paragraph does not include requirements. It gives a description of the main processes which are needed to enable the use of Name, but which are not inside the scope of the report (registration of the user, delivery of the certificate, revocation of the certificate, etc.).

3 Specifications

3.1 Certificate format. This paragraph should specify the requirements of a certificate used for Name. Two aspects should be specified, first what have to be in the certificate (DN, key usage etc.), second the different format and the implementation associated (X509, WAPCertificate, EMV Certificate).

3.2 One way authentication API. This paragraph should specify the standard API for Name.

3.3 Authentication verification for the service side. This paragraph should describe the requirements for the server which authenticate a Name certificate (Generation of challenge, checking of the revocation status of the certificates, etc.).

3.4 Options (mutual authentication, URL in the certificate, generation of session key,...)
This paragraph should give elements on the conservative measure taken to be able to implement some future functions in Name.

4 Recommendations for implementation

CONTRIBUTION FROM PARTICIPANTS

Name of person/organisation	Chapter	Suggested due date
Olivier Trébucq	1.1	1st April
CSELT (to be confirmed)	1.1	1st April
Cyber-Comm CSELT / Philips Semiconductor (feasibility to adapt WIM model) Thales Sermepa Visa	1.2	1st April
To be defined	1.3	1st April
Neurocom CSELT Telecom Italia, Cyber- Comm and Ernst & Young will send contributions on PKI system CRL and PKI X509 (certificate format).	1.4	1st April

All contributions should be sent to Stéphane Ménager, with copy to Patrice Santi.

Cyber-comm will have to specify the content and objectives of part 2.

Parts 3 and 4 will be considered after above contributions are sent.

First draft to be delivered on 5th of June for eEurope Stockholm meeting (5-6 of June, 2001)

Document to be sent to ETSI to organize a seminar 4-5th of July or 10-11 of July.

A further meeting is scheduled last week of May.

4 Next meetings

WG1, 2 & 3 & Steering Committee on 24-25 April with Steering Committee.