

SMARTIS-AM WG1 and WG3 joint meeting with ETSI

26 June 2001 - Sophia Antipolis

List of participants

Smart-IS A.M.

David Ankri, SmartIS Marketing, 336 0959 3365, david.ankri@wanadoo.fr
Laurent Cea, laurent.cea@int-system.com
Bruno Dupont, Eurosmart ; 322 506 8820 ; bruno.dupont@euralia.com
JP Fortune, ELVA, Boulogne, jpfortune@elva.fr
Frédéric Halter, Axiometech, 331 4083 1200 ; frederic.halter@axiometech.com
Alain Israël, Thalès e Transactions, 331 3080 2144 ; alain.israel@thales-e-transaction.com
Bernard Joly, ActivCard Europe, Suresnes, 331 4204 8484, bernard.joly@activcard.fr
Norbert Lipszyc, SISGEM, 331 4637 5543, irl@club-internet.fr
Claude Megglé, Cyber-Comm ; cm@smartis.com ; cm@cyber-comm.com
Stéphane Ménager, Neurocom ; stephane.menager@neurocom.com
Jean-Marc Meslin, Oberthur, Puteaux, 33 1 4125 2530, jm.meslin@oberthurcs.com
Patrick Sallé, Schlumberger, salle@montrouge.tt.slb.com
David Stephenson, Cyber-comm, 331 5396 8863, david.stephenson@cyber-comm.com
Patrick Sure, patrick.sure@int-system.com
Olivier Trébucq, GEMPLUS, 331 4648 2032 ; olivier.trebucq@gemplus.com

ETSI

Kristian Bergen, ZebSign AS, +47 9078 6438 ; kristian.bergen@zebsign.no
Andreas Bertsch, SIZ, +49 228 449 5538 ; andreasbertsch@siz.de
Gyorgy Endersz, Telia Research AB, +46 70 593 1272 ; gyorgy.g.endersz@telia.se
Joseba Garia, Ministerio de Trabajo y Asuntos Sociales, +34 91 347 7402 ; jgarcia@mtas.es
Miguel Gendive, Ministerio de Trabajo y Asuntos Sociales, +34 91 347 7389 ;
mgendive@mtas.es
Endre Grotnes, Statskonsult ; endre.grotnes@statskonsult.dep.no
Jane Hill, +44 207 831 0222 ; hill4law@aol.com
Tor Hjalmar Johannessen, tor-hjalmar.johanessen@telenor.com
Konstandinos Kaldis, Unemon Germany, +49 163 337 7033 ; kaldis@unemon.de
Timo Lehtimäki, Telecom Admin Centre, +358 9696 6815 ; timo.lehtimaki@thk.fi
Dave Maxey, BT, +44 1442 296 180 ; dave.maxey@bt.com
Andreas Mitrakas, Globalsign, +322 724 3636 ; andreas.mitrakas@globalsign.net
Ove Bardenfleth Nielsen, Danish Standards Association, +45 3996 6395 ; ob@ds.dk
Harri Pasilainen, ETSI, +336 8769 1257, harri.pasilainen@etsi.fr
Denis Pinkas, Intégris, +331 3966 6641 ; denis.pinkas@bull.net
Istvan Renyi, Communication Authority Hungary, +361 457 7420 ; renyi@hif.hu
Daniela Rocca, Studio Notarile Genghini, + 392 7630 3023 ; daniela.rocca@sng.it
Franco Ruggieri, Kir Dig Consultants, +39 348 443 1016 ; f.ruggieri@flashnet.it
Tuire Saaripun, Population Registry Center, +35 050 344 3107 ;
tuire.saaripun@urk.intermin.fi
Anne Seip, Statskonsult Directorate of Public Management, +47 2245 1219 ;
annikken.seip@statskonsult.dep.no
Vesa Votka, Miotec, +358 40756 8576 ; vesa.votka@miotec.fi

1 – AGENDA

9:00

Presentation by G. Endersz of the work done in ETSI-ESI workshop, and of the standards being developed.

9:30 - 11:30

Joint Meeting WG1 and WG3

Objective : To finalise the agreements of all experts on the content of the NAME document, presented by WG1 and circulated before the meeting

11:30 - 13:00

Plenary session with ETSI-ESI, including CEN participants, and Smart.IS AM

Presentation of the NAME document by C. Megglé

Discussion on the NAME document from a European standards point of view

Resolutions and work plan for next steps

e.g. ETSI - Smart-IS AM seminar in the Fall

Plan for the preparation of a European authentication standard

13:00 - 14:00 lunch

14:00 - 17:00

Parallel sessions of WG1 and WG3

The WG1 session objective would be to complete the work started in the morning.

The WG3 session objective would be to finalise the structure of the white paper to be produced, the work plan, and the links to other initiatives such as, for example, TB4 and TB12.

1 - Presentation of the work done in ETSI-ESI workshop

Gyorgy Endersz presented the work carried on presently by ETSI on the qualified electronic signature (copy of presentation attached).

2 – Discussion on the NAME document

The present draft of the NAME document was circulated to the members of ETSI for review, with the contribution of ELVA which had not been distributed. It was decided to include it in the draft. Smart-IS Marketing will prepare the new version of Smart-IS – NAME V093, by integrating this contribution and the remarks and suggestions made during the meeting. It will distribute it to the participants with the meeting report, attached to this mail.

It was reminded that Name is a document of proposition. Originally it was to be an analysis of what is required by the Telcom operators. Now the application providers are also requesting a common API for authentication to simplify their work.

The restricted choice of PKI for NAME was questioned, as it is expensive to implement. The reason was interoperability so that many certificates remain possible but all with one interface only, whether there is one or more certificate emitting authorities.

The cost of deployment of PKI can be reduced by centralising NAME on one server accessed via a traditional card.

JM Meslin of Oberthur presented their card-based PKI solution. The conclusion accepted by all was that interoperability of certificates stored on a card requires a common format. The format chosen for that is X509. There is a need to define the means of accessing and transporting this certificate and PKCS15 is the basis on which to define this standardised API. A common profile for the certificates has also to be defined.

ACTION: J.M. Meslin will check with Oberthur Card Systems the way to co-ordinate for Smart-IS AM the work on requirements for smart cards and PKI, formats in particular, with other card manufacturers (Gemplus, Schlumberger, G&D, ...).

3 - JOINT meeting ETSI

Claude Megglé presented NAME and mentioned its availability on the SmartIS-AM site.

ETSI has a smart-card work group on card specifications. NAME is aware of their work but both groups work on a different level. ETSI members ask how NAME is related to the TB12 (qualified electronic signature) work ?

NAME is limited to authentication, security requirements come after. SmartIS-AM are working with TB12 to see which common actions will be taken between the 2 groups.

ETSI focuses its work on fully qualified electronic signature: the signer of a document is the person having the power to sign it and the signature is non repudiable.

TB12 will identify the problems linked to a «secure environment », therefore all three groups (ETSI-ESI work group, Smart-IS A.M. WG1 and TB12) will have to work together. Smart-IS AM does not define the security requirements and does not address the user interface, even if it recognises that security requirements are absolutely needed. Its mission is limited to interoperability of the authentication solutions.

Authentication is not a focused area for ETSI. They suggest that Smart-IS AM defines the applications classes for NAME. They also suggest that the IETF standards (Radius and Diameter) and the ISO Norm 10181-1 have to be looked at.

The way to use an authentication certificate is independent of the security requirements. Smart-IS AM are looking at how to store an authentication certificate on a card and how to address it.

The identification and the hash of the certificate are the minimum information needed for ETSI, if there is not enough space to store the whole certificate. FINREAD is working on secure environments and devices. Smart-IS AM WG3 is only addressing multi-channel access for defining a common card holder interface based on authentication functions.

ETSI: Mutual authentication is not needed for secure signatures, it can even be dangerous in non-repudiation environments.

Smart-IS AM: Agreed, it is only an option provided by NAME.

The work of NAME is to look at what is being done elsewhere and address what is missing in it for authentication only. The question is « is there a business model for an authentication token only ? ».

ETSI conclusion: there is no substantial overlap between the activities of the 2 groups today. They propose to follow what Smart-IS AM are doing and to comment on it, but they are not ready to commit to any work nor contribution to it, except by individual contributors. David Ankri concludes that Smart-IS AM would welcome the participation of experts of ETSI in its work. The plan to have a common session in October or before the end of the year is approved. Its purpose will be to exchange views on the final draft documents and to disseminate the results of Smart-IS AM.

4 – Joint WG1 – WG3 meeting

General discussion

After a general discussion on overlap between Smart-IS AM and eEurope Smart Card, David Ankri proposes to merge the tasks to be performed by TB12 on signature and non repudiation with the Smart-IS AM tasks on authentication. An evaluation of the additional funding required by this has to be made and TB12 should see how it could obtain the agreement of the European Commission and the needed funding before a decision is reached on this point.

According to C. Megglé protection profiles are not included in the work of TB3 which creates a major void at the e-Europe level. It should be brought to their attention.

Eurosmart is concerned by the certificate format and it should clarify the position of the smart-card industry in Europe on the subject (e.g. should there be a hash only or the full certificate on a card). Once this position is formalised, the new meeting with ETSI will be useful. It should involve all Eurosmart members.

Several tasks are identified, and contributions on these matters requested:

- The application environment of what needs to be authenticated must be defined in order to define what the real needs for NAME are.
- The links with all related European groups must be identified before any extension to NAME be considered.
- Integrity functions use the same mechanisms as the electronic signature but they do not represent what is called the “advanced signature”.
- NAME will have to refer to protection profiles
- A paragraph on the card interface has to be prepared. What is missing in the present Java cards and PCSC solutions to provide really interoperable cards with X509 certificates. What type of API would allow to identify this certificate on any card.
- Should NAME define the mechanism of verification of the validity of a certificate de la and with which level of detail?

TASKS to be covered until the next meeting

1. Concerning the business model for NAME, B. Joly remarks on the fact that PKI is only a very small percentage of the market and suggests that other algorithms be investigated (e.g. SKI). He will make a contribution on this theme.
2. Claude Megglé will prepare a paragraph on the relationships between authentication and signature, including a scale between the various levels in relation to the environments, and

Stéphane Ménager will define the limits and overlaps between authentication and signature.

3. P. Sallé will explore which groups of CEN work on related subjects so that SmartIS-AM can liaise with them.
4. J.M. Meslin will analyse what is missing at the functional level in the NAME document.
5. Claude Megglé will add to the introduction the various levels of interoperability possible.

WG3 – Presentation by Alain Israël.

The full presentation is attached (it includes minor language corrections as suggested during the meeting).

It is agreed that A. Israël works with the Meta Group to evaluate the cost of this market study and to discuss with Smart-IS AM the best way to conduct it. The funds required will come out of the 75K Euro budget which had been allocated to WG3. He will ask them for a formal proposal and for contributions from Eurosmart experts. Other contributions to this task are welcome. Bernard Joly will send a white paper prepared by Mr Angel of ActivCard as such a contribution. It is hoped that Ingénico and Schlumberger Terminals will also contribute.

Concerning the proposed study, what is the attitude of the card manufacturers concerning the needs for authentication, signature and non-repudiation services. The applications and services should be reclassified. The ergonomics is to be defined in relation to the users, not in relation to security. Segmentation of the market should be based on user demands.

WG2 discussion with D. Stephenson.

It is proposed to merge WG2 and WG3 by extending the business requirements tasks to the banking domain. Contributions from banks and Telco representatives will be requested and co-ordinated by D. Stephenson.

WG4 - dissemination of documents to standards authorities and work groups.

N. Lipszyc, expert from SISGEM, member of CEN and AFNOR groups, is named to organise a wide meeting with ETSI and CEN with the help of Patrick Sallé. All documents produced by Smart-IS AM will be presented to ETSI and all CEN groups working on related domains. The meeting should take place in October.

Next Smart-IS A.M. meeting

On September 6, at Eurosmart in Brussels.