3GPP TSG SA WG3 (Security) meeting #25 **S3-020487**

8-11 October 2002

Munich, Germany

Source:	Stuart Ward, Orange
Title:	Digatal Signatures, Who is doing what?
Document for:	Information
Agenda Item:	**7.7**

Digital Signatures: Who is doing what?

ETSI activities

EP SCP#10 June 25th-27th/2002, Sophia Antipolis (France)

The Work Item on Digital Identity Module (DIM) on the UICC is still being discussed. WI advancement was stopped due to the lack of market requirements from operators and participants from the financial sector. SCP decided to revise the WI with respect to what can be handled by WG2 at next plenary meeting.

Furthermore, a revised version of the WI was approved. The outcome of the WI is now intended to be a white paper that builds the foundation for a Stage 1 specification, which will be the basis for a future work on this topic. The title and scope of the WI changed to “Study of available digital authentication specifications and their suitability for a Digital Identity Module on the UICC".

Scope of work to be undertaken:

The UICC is a security token that in combination with a Public Key Infrastructure (PKI) could be used as a digital identity for the subscriber. To allow the applications on the UICC to make use of the digital identity, e.g. for authentication and electronic signature services, it’s essential that there is one generic and common available mechanism to address and handle PKI on the UICC.

In the Internet environment there is already a specification on how to manage this on the card, i.e., PKCS#15. This specification has been adopted, among others, by WAP Forum to form the basis for the WIM. PKCS#15 is also the basis for ISO 7816-15.

The scope of this Work Item is:

Produce a white paper including

- Definition of requirements (e. g. services and interfaces needed)

- Investigation of existing standards and technologies

In a second step the Work Item could be extended to produce a specification including

- definition of a generic DIM

- definition of the generic framework for supporting and managing the DIM on an UICC (e. g. data-model)

1. Analyze the requirements for DIM on the UICC:
- security services to be supported based on digital signature mechanism (origin authentication, peer-to-peer authentication, data integrity, non-repudiation?)

- requirements for usage in legally binding electronic signatures
- other security services
- interfaces:
.. "card-edge interface" at the level of TS 102 221
.. USAT interface
.. other "internal" interfaces

2. Define a generic DIM to be used by the applications on an UICC
3. Define the necessary framework for supporting and managing the DIM on an UICC
- describe different models for the DIM lifecycle: initialisation, personalisation, usage

Supporting ETSI Member organisations:

To be verified….
G&D, MobileMind, SmartTrust, Setec, BT Group plc

M-COMM

Terms of Reference for Specialist Task Force 221 (EP M-COMM) on European standardization initiative in support of business self-regulation: mobile-signature

1 Reasons for proposing the Specialist Task Force

1.1 Introduction

We are more and more in a society where electronic communications is of primary importance, particularly for business. Communication may use different media and bearer networks: vocal with classical telephone network, or mobiles networks, data with Internet, 3G networks, etc.

New business opportunities appear if a secure environment can be provided, even in case of interactive communications between parties who may not have pre-established relationships. This may happen by creating tools to strengthen productivity, reduce delays and costs, as well as new methods of reaching customers. Networks are being exploited by companies that wish to take advantage of new ways of doing business and new ways of working, such as teleworking and virtual shared environments. Government departments are also using these new networks in their interactions with companies and with citizens. Electronic commerce presents the European Union with an excellent opportunity to advance its economic integration.

However, to make best use of these opportunities, a secure environment is required, and particularly with respect to electronic signature since it is commonly admitted that it is a powerful enabling service for e or m-commerce, and more generally for e-Transactions..

The development and use of signature/authentication products and services is still in its introductory stage. Systems exist which provide authentication for commerce, administration and public services. Agreed industry standards or technical specifications are worked out by different bodies, and particularly in Europe by ETSI & CEN within the EESSI framework. Availability of these standards is of course essential, in order to provide a common level of security which can be recognized as being valid for use at regional level, even less at international level.

In the case of the consumer market, i.e. B2C, C2C, C2A e-commerce, we believe that the mobile will play an important role. In fact, if probably smart card will be used as a signature creation device, it is doubtful that consumers may invest in a specific security tool like for example a specific card reader to be connected or inserted in their PC. More over, security requirements for signature creation or verification systems are such that it would require a very special kind of card-reader, with enough processing power and display capabilities to reach the “what you sign is what you see” paradigm. In this consumer market, we believe that mobiles are the natural solution: they are popular, they have and will have more and more display capabilities, they offer voice communication, and Internet browsing, and their core software tend to be trustable, thanks to standards like ETSI SIM and SIM -Toolkit or 3GPP MEXE. They may be used alone or in conjunction with a PC, and in this case may be considered as a kind of card reader connected to the PC via USB, Bluetooth or Irda. Their security is based on a specific smart-card, which is the SIM/WIM.

In fact, these previous statements are fully supported by what is happening now on these issues: several operators are launching m-signature systems. Examples of such initiatives are m-Sign consortium, supported by Vodafone, T-Mobil, Orange Trust service that will be launched in France after a pilot phase up to June 2002. Radicchio consortium is another example.

Interoperability between entities involved in the mobile signature architecture is the main goal of this proposition.

1.2 Purpose of the proposal:

All the existing M-signature systems share a common service approach, which is rapidly described here:

A negotiation phase takes place between a client and a service provider (SP), may be on a WAP, vocal, NET mode…

The SP needs to send a text to the clients mobile via Short Message/WAP Push

The clients if he agrees to commit to this text enters a confirmation PIN

The mobile computes a signature and sends it back to the SP

For this service to be offered with efficiency and simplicity, it is necessary that a signature proxy is associated on one side with mobiles, and on the other side with SP. This signature proxy could be operated by mobile operators, or other parties. The operation on the SP side should be independent from the mobile terminal characteristics. (no PKI, PKI through SAT, through WAP1.2…)Public key directory, Additional services may be offered by the signature proxy: ie

Signature and user certificate verification

Time stamping

Notarisation

An extension of this service to mobile which are not PKI enabled could also be useful, through signature proxy giving a signature on behalf of the client. Depending on the client's mobile capabilities different levels for QoS have to be defined. The SP could negotiate the minimum level for QoS with the signature proxy, which is aware of the capabilities of the client's mobile phone.

So the main purpose of this proposal is to define a precise architecture, protocols between SP and Sig-Gwy, and general security requirements in order to reach a good level of interoperability.

1.3 Proposed Activities

Tasks to be performed :

1 M-Signature web service definition: review of existing systems and business requirement analysis, and then definition of a general architecture of a mobile-signature service architecture and message flow.. Architecture of the system will be evaluated regarding 3G evolution at network level. A generic model for interoperability will be established.

2 M-Signature web service technical specification: a common protocol between signature proxy and SP has to be defined;

3 Definition of a common set of security requirements: The goal is to define minimum set of security requirements concerning mobile signature systems, in order to define standardized trust levels. This will help interoperability agreements to be established between different m-signatures Operators

4 Precise definition of the mean to get roaming capabilities: related data and protocols.

In order to take into account the priority for obtaining different kind of deliverables, and the degree of maturation of the different concepts which are the base of the work to be done, this work programme is to be organized in two phases:

Phase 1 covers tasks 1 and would be achieved end 2002

Phase 2 covering tasks 2, 3 and 4, beginning of 2003

1.4 Why an STF is the most effective way to achieve this objective

The different meetings of m-Comm WG have enabled a common understanding of the goal and necessary tasks to be achieved for m-signature standardization. The technical and detailed work described above needs a specific task force, with if possible, a participations of specialists involved in the above mentioned ongoing initiatives concerning m-signature. The great commonality between different existing m-signatures pilots (at architecture and service level) is a good sign for the possibility of fulfilling this work program, and defining successfully a common set of requirements and protocols.

2 Consequences if not agreed

Timely standardisation for m-signature system will make it possible to influence early developments of these systems. If the standards are delayed, or no standardisation at all is reached, then de facto standards could dominate the market, with problems of interoperability. This will act as an obstacle to the roll out of m-signature systems, and will certainly slow down the use of electronic signature by consumers, in B2C,C2C or C2A relations, and finally, could jeopardize the implementation of the European Directive on the Electronic Signature, at least for the consumer side.

This will also limit the use of mobiles for signature, and certainly also for sensitive applications like payment or ticketing. And will result finally in a slower development of mobiles value added services, and associated benefits for the operators and service providers involved in these value added services.

In addition, it can be mentioned that competence and experience represented by ETSI members would not become part of the new standards concerning this area of e-commerce.

3 Detailed Description

3.1 Subject title:

Mobile-signature web service definition, protocols, security requirements, and roaming

3.2 Reference TB:

M-COMM

3.3 Other interested TBs (if any):

ETSI activities on Electronic Signatures related to ESI (Electronic Signature Infrastructure): previous SEC/ESI STFs 147, 155, 178 and active STFs 209, 210, 220, which are included in the EESSI programmeare interesting for m-signatures.

SCP & 3GPP SA

3.4 Target date for the start of work:

September 2002

3.5 Duration and target date for the conclusion of the work (TB approval):

The tasks covered are to be performed over a period of 8 months

Resources required

3.6.1 Necessary manpower

Total resources required: 7 man/month (91 kEUR), for drafting deliverables.

Phase 1: 3 mm

Phase 2: 4 mm

3.6.2 Estimated costs, additional to the manpower:

9 kEUR for travels

3.6.3 Qualification required

Two persons (including editors) are required.

The candidates will be experts in security, existing digital signature and public key infrastructure technologies, architectures and standards, security management and the European and global standardisation processes: PKI, WPKI, PKCS.

Qualifying experience in areas related to the subject of the tasks include business models, processes and mobile technologies for Task 1, internet technologies (SOAP, Web Service, XML, HTTP) for Task 2, respectively.

It would be of great interest that experts for the STF have participated to the ongoing projects, pilots or services in the field of mobile signature.

3.7 Scope of Terms of Reference:

Areas to be covered include:

Task 1 : M-Signature web service definition

The objective of this task is to define a general architecture of a mobile signature web service. The first step is to identify the business requirements that will lead the specifications.

The second step is to settle a generic model description in order to clarify the actors and the message flows involved. Roaming and interoperability issues (including issues related to number portability) must be addressed to give appropriate guidance for task 2 & 3Details on this issue, related data and protocols will be addressed in task 4.

A review of current initiatives must be done so that the work should be done in co-ordination with other Bodies in the domain of electronic signature, particularly in Europe; however, liaison with other Organizations outside Europe should also be taken into consideration. An initial list of interested bodies is: M-Sign, Radicchio, GSM Association, WAP Forum.

A security review aimed at describing possible security loopholes, possible improvements, and countermeasures will be performed during this task and will feed into specs of task 2 and 3.

The TR will identify the scope of the TSs to be produced by Tasks 2, 3 and 4 and the areas to be covered that cannot be addressed with the present resources.

Comments to the draft documents must be collected from a wide audience, also including stakeholders outside the ETSI community. Drafts must be made available on the WEB for comments. The comments period should be at least one month.

Deliverable: Technical Reports: Business and Functional Requirements (DTR/M-COMM-003)

Task 2: M-Signature web service technical specification

Once the M-Signature web service is settled, the interface of the methods published by the web service must be specified. The following methods must be considered:

Signature request

Proof of Possession request

Certificate or Certificate URL downloading

Signature validation

Certificate validation

Deliverable: Technical Specification: Web service interface specification (DTS/M-COMM-004)

Task 3: definition of a common set of security requirements

The goal is to define minimum set of security requirements concerning mobile signature systems, in order to define standardized trust levels.

Implementation in the mobile

Implementation in the signature proxy

Dialogue and security indications on the mobile

Position towards daft standards of EESSI would also be an important issue.

Deliverable: Technical Specification: security requirements for m-signature systems
(DTS/M-COMM-005)

Task 4: precise definition of the means to get roaming capabilities

Based on the general architecture of §1, this task will have to address:

Precise model for roaming, taking into account work on number portability in other bodies or capabilities of mobile phone to direct itself to its signature gateway

Definition of related data to be shared between different parties;

Protocol between signature gateway for redirection of the signature messages from the visited signature gateway to the home signature gateway;

Deliverable: Technical Specification: specifications for roaming in m-signature services
(DTS/M-COMM-006)

3.8 Context of the task(s):

Work will be conducted in close relationship with above mentioned ETSI initiatives on signature issues, as well as EESSI.

More over relationship with ongoing associations aiming at promotion of m-signature will help to obtain useful feedbacks of actors in the Market, and will allow to reach a good consensus on issues like protocols SP-Sig Gateway.

3.9 Related activity in other bodies and co-ordination of schedules:

We can mention:

IETF work on certificates and attributes

WAP forum

ISO TC68 SC2

Smart Card Charter Initiative (TB2)

CEN ISSS

Base documents and their availability

ETSI Report - Electronic Signature Standardisation (ETSI/TC-SEC(98)8 - TD 008)

European Electronic Signature Standardization Initiative (EESSI) Final Draft of the EESSI Expert Team Report, June 18, 1999

ETSI deliverables from EESSI phase 2 and 3

CEN/ISSS workshop agreements of phase 2 and 3 of the EESSI programme.

WAP standards

SOAP (specified by World Wide Web Consortium, W3C), XML

Work Item(s) from the ETSI Work Programme (EWP) for which the STF is required

Work Item on mobile signature systems:

(DTR/M-COMM-003, DTS/M-COMM-004, DTS/M-COMM-005, DTS/M-COMM-006)

Expected output(s):

Assuming start in September 2002:

First stable drafts for Phase 1	end-October 2002
End of comment period	end-November 2002
Inclusion of comments	mid December
Publication of Phase 1 deliverables (task 1)	**end-January 2003**
Interim report to EC & EFTA	February 2003
Beginning Phase 2	January 2003
First stable drafts for Phase 2	end-February 2003
End of comment period	end-March 2003
Inclusion of comments	mid-April 2003
Publication of Phase 2 deliverables (task 2,3 & 4)	**End May 2003**
Final report to EC & EFTA	**June 2003**

Radicchio – Trusted Transaction Roaming

Summary

There is currently no global network available that would serve as a common platform enabling content and service providers to reach mobile subscribers in a trusted environment. Individual Mobile Network Operators (MNOs) are implementing and piloting projects, but reaching wireless subscribers with sensitive digital content will remain an expensive and confusing proposition until the major parties involved join to build an interoperable framework for Identity, Security and Privacy Management in mobile networks.

As the leading industry forum for trusted mobile services, Radicchio is seeking to establish a trusted infrastructure for wireless data services that will meet fundamental market requirements by enabling:

- Global interoperabilityReliable identification
- Secure network access
- Secure content access
- Privacy management
- Convenience & benefits (for end users, MNOs and service providers)
- Legal enforcement (EU support)

This Trusted Transaction Roaming Platform will benefit the wireless data services market as a whole and - most importantly - the end users, who will receive a larger variety of services, security, and privacy on an infrastructure that they can really trust.

The operator of such an extensive platform, which would deal with different parties' confidential information, needs to be a neutral entity that is truly trusted and recognized by all the players in the data services market (including financial institutions, MNOs, service & content providers and technology providers). This neutral entity would operate the Global Identity Management on behalf of all GSM MNOs.

Radicchio is now proposing the t^2r (Trusted Transaction Roaming) Project to enable the construction, design, and implementation of a Trusted Platform. The t^2r Project will also lay the foundation for one or many neutral entities to operate such a platform for the benefit of the end users, service providers, MNOs, and various other players in the wireless data services market.

The t^2r Project was presented to the leading Mobile Network Operators at the Carrier Summit held in March 2002 in Bandol, France. Operators present included Hutchinson 3G, MTN, Orange, mm02, Sonera, T-mobile, and Vodafone. The aim of this summit was to reach a consensus on the best way to develop a global framework for trusted mobile and wireless transactions. The feedback was encouraging, and Radicchio believes that this summit has signaled the start of global roaming for secure wireless transactions.

The Trusted Transaction Roaming (t^2r) framework will enable secure identification of all end-users in a wireless network. This allows services outside the home operator network to securely identify end-users as they roam. It also will improve service quality through secure payment and personalization. For example, the trust platform would make it possible for subscribers to safely purchase services (such as train tickets) while traveling internationally. Given the total worldwide market of wireless end-users, such services and payment processes can leverage a common interface and increase revenue. Using the same global identity framework, enterprises and governments could use mobile devices to enhance access control.

Trusted Transaction Roaming makes the mobile device significantly more valuable to the user, defines new revenue streams for the mobile operator and creates a new, managed channel for service providers to extend their services to the nearly one billion global wireless users.

Radicchio has also identified cooperation with international legal and regulatory authorities as an essential step towards ensuring the enforceability of digital contracts signed remotely in wireless networks. Furthermore, it will also seek to make the best possible use of standards written by other organizations to avoid duplicating efforts and to guarantee maximum interoperability.

To ensure that the framework becomes truly global, Radicchio invited the GSM Association and the Liberty Alliance to present at the Operator Summit. Follow-on efforts are planned with other leading industry bodies, such as the European Telecommunication Standardisation Institute (ETSI) and the ICT Standards Board.

Based on the discussions at the Radicchio Operator Summit, the Mobile Network Operators agreed on the following general position:

- Operators recognize the strategic potential of trusted actions based on SIM-card security for current and future services, such as end-user identification, enterprise access control, online payment, etc.

- The operator and services industries need to cooperate to enable the widespread take-up of trusted transaction services.

- The potential of trusted transactions involving third parties (e.g. banks) can only be successful if operators co-operate to extend a common, global interface that enables secure services.

- The operators will encourage the development of the necessary technical, procedural, and legal standards on a global scale to establish an open and reliable standard that can be implemented by technology providers and used by content and financial service providers.

Banking Groups

Moby Forum

The mission of the Mobey Forum is to encourage the use of mobile technology in financial services - such as payment, remote banking and brokerage. It aims to do this by:

- Raising the awareness of mobile financial service implementations
- Facilitating the open provisioning of mobile financial services
- Identifying business considerations and working to obtain the interoperability of the technical and security requirements for the mobile finance industry, in order to promote competition
- Acting as an active liaison between various standardisation fora/forums in both the mobile and financial industries, so as to promote competition.

Founder members are ABN AMRO Bank, Banco Santander Central Hispano, BNP Paribas, Barclays Bank, Deutsche Bank, HSBC Holdings, Nordea, SEB - Skandinaviska Enskilda Banken, UBS, Visa International, Ericsson, Nokia and Siemens.

Security

In terms of the security level, customer authentication is envisaged to be the most important security feature from the perspective of a financial institution. It is the belief of the Mobey Forum that strong authentication is preferred for macro-payments; while for transactions of a smaller amount (e.g., under EUR100) could use a less robust form of authentication.

The level of security will also depend on the type of purchase. For example, some local selfservice or Internet micro-payments require only minimum security, as far as the product or service is not re-sellable. On the other hand, purchasing some low-value re-sellable items may require strong security.

Ease of use and implementation are key: the highest security level includes the use of mobile PKI by the issuing bank, for example with a bank-issued WIM application and certificates in the handset. The user confirms the transactions by a PIN-code, which is checked off-line by the bank-issued card. Using this solution with a strong level of security is still consumer friendly, since the same PIN code is used frequently.

European Committee on Banking Standards (ECBS)

A mobile device is *not* a means of payment but a means of activating, initiating and/or confirming a payment. One could also speak of ‘payment approval and/or initiation’ executed by a mobile device. For example, even if a card is not used physically when paying, it may be a payment transaction using a card system. This perspective allows more flexibility and includes, for example, a mobile device initiating a pre-defined payment instruction. It is also possible that when an electronic bill or a card transaction is presented to the mobile device, the user has only to confirm the presented data. Basically, the mobile device is used to initiate and/or complete a payment transaction.

Taken the GSM as an example, the following is applicable:

- By means of the personalisation associated with the SIM, the **users** may choose the telecommunication operator that provides the best business offer for both, traditional airtime and value-added services such as content and payment functionality.
- The **telecommunication operators** decide which functions may be operational on their network and the device it can connect to.
- The **banks** decide the requirements needed for bank-related functions like m-payments and m-banking.

M-payments may be used for content on the mobile (for example, prepaid airtime) and services delivered on other channels (such as PC via the Internet, ITV and even voice telephone ordering).

If the device is personalised and contains dedicated security features (encryption as well as a trustworthy customer verification method), the mobile device, therefore, becomes the user’s personal transaction terminal or even the user’s personal trusted device.

Summary

Group	Members	Groups
ICTSB (Information, Communication & Telecommunication Standards Board)	ETSI, CEN, CENELEC plus w3c, IETF, ECBS, EU Commission	Coordination of standardisation efforts in ICT area
GSMA	Mobile operators	CTO GroupMobile Commerce Interest Group (MCIG)
European Commission T²r project 5th FP Research & Development ended 2002	Gemplus, Vodafone, Orange/FT, Globalsign, SmartTrust, Radicchio	EU funded research project on t²r; September 1st 2002 until June 2003; 300,000 € in total
European Commission 6th Framework Program R&D 2002 – 2007	European Commission	Work program will have track on mobility and security; new research project layout, integrated projects
European Commission Blueprint Initiative on Mobile Payments	New initiatve driven by EC on mobile payments; started July 2002	Core members selected; First draft for discussion; First meeting: beginning October 2002, Brussels
European Committeee on Banking Standards (ECBS)	Develops and agrees on banking standards;	Working groups on wireless security and mobile payment
Paycircle	Industry organisation lead by HP and Siemens	Standardisation of micro payments
Mobile Payment Forum (MPF)	VISA, MC, Orange etc	
OMA	Ericsson, Vodafone etc.	WAP Forum renamed
PKI Forum	IETF Standard group	
Liberty Alliance Project	Federated Identity by United Airlines and others	Identity network, some intrest in adding mobile idenity at a later stage
ETSI	Mcomm working group	Define technical specifications