USECA

Project Number	AC336
Project Title	**USECA: UMTS Security Architecture**
Title	**Final report**
Document reference	AC095/VOD/WP12/DS/P/FR
Editor	Howker

Abstract	This report provides a summary of the work and results of the USECA project.
Keywords	UMTS; third generation; security

The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

The work described has been supported by the European Commission through the ACTS Programme under Contract AC336.

TABLE OF CONTENTS

Summary

USECA set out to provide a firm architectural foundation for the security measures that would play a critical role in the establishment of UMTS or third-generation (3G) - the generation of mobile communications to follow on from GSM.

It was anticipated that this would be in the context of European standards developed in ETSI, but in the event, the industry set up a new forum to focus solely on the establishment of 3G. The Third Generation Partnership Project - 3GPP - arrived in time for USECA to switch its focus to the new organisation. By taking this opportunity, the project was to play a central role in setting in place a number of critical security components for the worldwide industry standard.

The close association with 3GPP developments had major advantages in allowing the project global influence and visibility. The disadvantage may be seen as a curtailment of scope, for instance concentrating on use of symmetric cryptography for the early releases at the expense of some PKI work. The balance is judged to have been very much in favour of the 3GPP path: real, applicable results contributing to the establishment of third generation versus interesting but possibly premature footnotes in the history of mobile communications.

D11 - Final Technical Report

The consolidated results of the project are given in our Deliverable D11.

Part 1 of that report deals with the technical work. Annex 4, below gives an outline of its contents.

In addition to its *technical* results, the project produced a review of the relevant aspects of the *legal* environment – both European and national legislation - as it affects core processes in a business model involving mobile communications. As this is so comprehensive, it has been treated as a separate document that may be of wider general interest and use in, say, development of regulatory frameworks governing the take-up of electronic commerce. In this form it forms Part 2 of D11.

All USECA public deliverables are to be found in the folder *Deliverables*

Project objectives

The goal of USECA has been that of ensuring the development of industry standards for a UMTS security architecture. To this end it was essential that the project remained flexible in its planning, so that timely inputs could be made to standards bodies.

The main objective of the project was defined as

> *to ensure that a viable and complete UMTS security architecture was developed as a basis for standardisation by ETSI.*

At the outset of the project the mobile telecommunications world was undergoing rapid transformation as GSM technology reached maturity and the plans for the next generation - UMTS - firmed up. Mobile usage and the resultant customer base accelerated worldwide, with corresponding increased expectations of the benefits that 3G and would provide.

The provision of economic security measures and facilities was seen as crucial to the success of 3G. A key event was the establishment of 3GPP as an initiative to co-operate in the production of globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support.

The work of ETSI in the field of security, which was seen as the original focus of USECA, was subsumed under this new organisation, allowing much wider dissemination and influence of the results of the project. The project workplan was adjusted at the end of its first year to take account of this shift in emphasis. The consequence has been that USECA has been able to play a leading role in the generation of the specifications of the 3GPP Release'99 specifications, the foundation of UMTS.

Consequent sub-objectives of the project were defined

- *to provide a focal point for UMTS security work;*
  this was successfully achieved through the project's relationship with 3GPP; ✓
- *to provide a sound and validated technical basis for the definition of UMTS security standards by ETSI;*
  as above, this was successfully achieved, but for the global platform afforded by 3GPP; ✓
- *to build on the work of and collaborate with relevant ACTS projects (in particular with FRAMES) to provide the required security expertise;*
  no appropriate collaborations could be identified; however the project played an active role in the concertation process and its activities;
- *to review the security requirements arising from the set of services defined for UMTS and define a comprehensive set of security features for UMTS;*
  Section 1, below, sets out the requirements in terms of services and features; ✓
  Section 2 examines the legal framework and constraints that need to be observed;
- *to define a comprehensive set of security mechanisms, protocols and procedures (with the exception of encryption algorithms) for UMTS;*
  Section 3 gives the results of this work together with the extension which includes a preliminary investigation into the use of IP-based protocols in the core network; ✓
- *to define a complete functional and physical security architecture for UMTS;*
  Section 4 reviews the developments of the UMTS security architecture; ✓
- *to define a public key infrastructure for UMTS;*
  PKI is reviewed in Section 5; scope was limited by there being no requirement for the initial 3GPP specifications ✓
- *to define the security features and procedures involving the USIM;*
  results of work on USIM security features and facilities are described in Section 7; ✓
- *to validate critical concepts in demonstrators.*
  the demonstration has been given successfully at a number of events and to clients including the Commission; the specification and description are given in Section 8. ✓

Relationship to Programme objectives and Consensus Management activities

ACTS Programme objectives

The development of a security architecture for UMTS was work that clearly met criteria for Community action as specified in the 4th Framework Programme:

> *'...research leading, where the need is felt, to the establishment of uniform rules and standards.'*

Any modern mobile communication system needs to be based on standards, to guarantee multiple vendors for interworking equipment, and to allow roaming between network operators both within and across national borders.

When considering the ACTS programme as a whole, it is clear that the work fell within the potential coverage of two Project Areas, namely 'Area 4 - Mobility in Communications Networks' and 'Area 6 - Quality, Security and Safety of Communication Services and Systems'.

However, among the tasks specifying the scope of the Third Call for ACTS, the work fell into that defined as Task AC606 (Secure information exchanges over broadband systems). Here the requirement was stated for '*trustable communication ... systems that meet the needs of the broadest spectrum of users and service providers*'. An objective of USECA was to ensure that UMTS was one of those systems.

The Task expressed the goal for an '*electronic market*' that should be made secure. In many ways, mobile communications is itself becoming an electronic market, as well as facilitating electronic commerce value-added services. When UMTS users register with network operators, roaming agreements will be negotiated electronically. Payments may be made directly to and from a user's electronic purse. USECA's aim was to provide the underlying security to support an electronic market in mobile communication.

At the outset, the impact of new telecommunication technologies on UMTS was still being assessed. Many of the developments would affect the way in which services were offered, and the corresponding security requirements. USECA would develop to address these issues. New technologies would also allow the development of new security solutions, as AC606 indicated, and USECA would use these as appropriate, in particular taking account of the developments in smart card technology.

Of the three main objectives of AC606, USECA focused on the first. This included the development of '*protocols needed to provide authentication, identification and, where appropriate, anonymity, control of access to information and services, protection of information, accountability and non-repudiation.*' The verification of these protocols, wherever possible with established formal techniques, was one of the goals of the project. All this was to be done in the context of UMTS, but the protocols and methods developed would have clear application to other telecommunication systems.

Enhanced remote control mechanisms of data and services on smart cards, in the context of UMTS, was also an objective of the project.

Of the aspects that AC606 suggested be considered, USECA tackled the following:

- *security and protection of interconnected networks (multi-domain)*: this was especially important in a mobile system, where users could roam between networks; UMTS would involve enhanced automatic roaming, where security considerations had to be taken into account;
- *UMTS air interface*: USECA addressed the impact on the air interface of the security features adopted, as well as identifying specific security issues raised by the choice of the air interface;
- *service and network management*: the management of security, as well as the security of the network management system, would form part of any security architecture.

The key results of USECA are seen to be in the standards domain, which is one of the key results suggested by the task. The aim of the project was to develop the standards by consensus, requiring the effective dissemination of results from the project by whatever means possible. The relationship with the standards process is described elsewhere in this report.

The participation of the project in concertation activities with other ACTS projects continued according to the plans laid out in deliverable D01 Project Linkages.

Participation in Domains/Chains

USECA participated in Domains 4 and 5, and in the Security and Applications Cluster within Domain 5. Participation included the organization of conferences and workshops, and the presentation of project results.

Domain 4 For the 1999 ACT Mobile Summit, a representative sat on the Technical Programme Committee and chaired a session. Other USECA representatives refereed papers, and presented a paper and two posters at the conference. USECA representatives attended the Domain 4 workshop on location-based services held in Brussels. Both Domain meetings were attended and USECA results were presented at a Domain 4 Workshop on next-generation broadband networks.

Domain 5 As agreed previously, USECA reviewed two CAMELEON deliverables from a security perspective. A CAMELEON representative presented the results of their work at a USECA meeting, where there was particular interest in the development of the VHE concept. A presentation on PKI for UMTS was prepared for Security and Applications cluster meeting, but was not given due to a change in the agenda.

Contribution to Guidelines

No inputs to guidelines were made, as the focus was on direct contribution to and influence of external standards

Main achievements of the project

Introduction

The communications industry has been developing a strategic vision of the 3rd generation of digital mobile systems referred to in Europe as the Universal Mobile Telecommunications System (UMTS). This has gained momentum, and the interest within the industry has increased. An indication of this is the formation of the UMTS Forum, an association of telecommunications operators, manufacturers and regulators, to promote the work on UMTS; another indication is the increased activity in the pertinent standards groups.

It is clear that UMTS cannot be operated in a commercially successful way and will not meet with the users' acceptance if reliable and effective security measures are not implemented from the start. A lot of groundbreaking work was done in critical parts of this area in the collaborative research projects ASPeCT (ACTS), MONET (RACE) and '3GS3 - Third Generation Mobile Telecommunications System Security Studies' (UK LINK programme). However, there was still a long way to go to establish a security architecture covering all relevant aspects of security, to ensure that the UMTS security standards would be completed on time, and to enable manufacturers to start product development and to enable operators to plan their UMTS networks. This was partly due to the fact that the specifications of UMTS framework in areas other than security had not progressed sufficiently to enable security for UMTS to be specified in all the necessary detail. Work in these other areas has progressed faster subsequently, and it became imperative to take on the task of resolving the problems in UMTS security which might have hindered the timely introduction of UMTS.

USECA set out to provide a firm architectural foundation for the security measures that would play a critical role in the establishment of UMTS or third-generation or 3G - the generation of mobile communications to follow on from GSM.

The USECA project played a leading role in the development of the security architecture in the first release – Release'99 – of the specifications for third generation mobile communications from the 3GPP organization.

It was anticipated that this would be in the context of European standards developed in ETSI, but in the event, the industry set up a new forum to focus solely on the establishment of 3G. The Third Generation Partnership Project - 3GPP - arrived in time for USECA to switch its focus to the new organisation. By taking this opportunity, the project was to play a central role in setting in place a number of critical security components for the worldwide industry standard.

The close association with 3GPP developments had major advantages in allowing the project global influence and visibility. The disadvantage may be seen as a curtailment of scope, for instance concentrating on use of symmetric cryptography for the early releases at the expense of some PKI work. The balance is judged to have been very much in favour of the 3GPP path: real, applicable results contributing to the establishment of third generation versus interesting but possibly premature footnotes in the history of mobile communications.

1.1 WP2.1 - UMTS security requirements and features

1.1.1. Overview

The work on security requirements and features within USECA provides the basis and reference point for all of the other USECA workpackages. A major effort was essential due to the inadequate state of the existing ETSI UMTS Security Requirements document (ETR 33.20).

Because of the fundamental importance of an agreed documented statement of requirements, considerable effort was expended in attempted corrective action on the ETSI text. However, when this was judged to be an ineffective approach, the project took on the task of producing a completely new document that would provide a more authoritative statement of requirements.

The document that was produced was generated as part of the work of ETSI SMG10, using the results of this workpackage. The resulting document is ETS 33.21, which has since evolved into the 3GPP document 21.133. Other documents. All existing UMTS specifications, along with ITU and associated ACTS UMTS documents were taken into account to produce a list of all known security requirements for third generation.

The resulting list was compared against the 'Security Requirements for UMTS' document to determine the source of each requirement, and which requirements did not have an identifiable owner. This information was submitted to ETSI SMG 10 to ensure that no requirements existed in the specification that had no established basis.

The document provides a view of requirements as currently perceived; it observes that, in general, only known generic threats and requirements can be addressed at this time. The document will need to be maintained as UMTS develops.

1.1.2. Security objectives for UMTS

The document states the general objectives for third generation (UMTS) mobile communications security features as:

a) *to ensure that information generated by or relating to a user is adequately protected against misuse or misappropriation;*

b) *to ensure that the resources and services provided by serving networks and home environments are adequately protected against misuse or misappropriation;*

c) *to ensure that the security features standardised are compatible with world-wide availability (There shall be at least one ciphering algorithm that can be exported on a world-wide basis (in accordance with the Wassenaar agreement));*

d) *to ensure that the security features are adequately standardised to ensure world-wide interoperability and roaming between different serving networks;*

e) *to ensure that the level of protection afforded to users and providers of services is better than that provided in contemporary fixed and mobile networks;*

f) *to ensure that the implementation of 3G security features and mechanisms can be extended and enhanced as required by new threats and services.*

Basic security features employed in second generation (GSM) systems will be retained, or enhanced where necessary. These include:

- subscriber authentication,
- radio interface encryption,
- subscriber identity confidentiality,
- use of removable subscriber module,
- secure application layer channel between subscriber module and home network,
- transparency of security features,
- minimised trust between HE and SN.

In some instances, UMTS will need to be equipped with stronger or more flexible security mechanisms than those which were designed for GSM, due to new or increased threats.

Mechanisms to combat fraud in roaming situations should be included in the UMTS specifications from the start.

Mechanisms for lawful interception under appropriate authorisation should be included in UMTS specifications from the outset.

1.1.3. Security context for UMTS

The document examines the context and actors relating to UMTS security in terms of;

- assumptions about the overall system cover the types of services, service management, access to services, service provision, system architecture, security management, interworking and compatibility, charging and billing, and supplementary services
- roles in UMTS: user domain roles – users, subscribers, other parties; infrastructure domain roles - home environment, serving network, value added service provider; together with off-line sector actors such as regulators
- architecture
- UMTS identities
- UMTS data types and groups: user traffic; signalling data; control data; user-related data

1.1.4. Security threats in UMTS

The document examines the following security threats:

- *threats associated with attacks on the radio interface*
    - Unauthorised access to data
    - Threats to integrity
    - Denial of service attacks
    - Unauthorised access to services
- *threats associated with attacks on other parts of the system*
    - Unauthorised access to data
    - Threats to integrity
    - Denial of service attacks
    - Repudiation
    - Unauthorised access to services
- threats associated with attacks on the terminal and UICC/USIM

1.1.4.1. Analysis of threats and countermeasures

A threat model, on which the selection of security mechanisms is based, was set-up. The emphasis was put on new attacks, that were not possible when GSM was designed, but are now or are perceived to be possible in the near future. Reasons for such additional threats are e.g. that intruders have more computational capacities, new equipment has become available to attackers or the physical security of certain network elements is questioned.

A detailed analysis of the security threats and countermeasures cannot be presented here, due to the sensitivity of the investigations made, but some of the most important items are briefly mentioned.

Some of the most serious attacks analysed were based on the availability of so-called false base stations. A part of this problem is the so-called IMSI catching, which is a threat to the confidentiality of the user identity on the air interface.

Another kind of attack analysed was related to an attacker hijacking services of the user.

One important result of the threat analysis was that some signalling elements were considered to be sensitive and therefore have to be integrity protected. One of these signalling elements is the secure mode command, which determines whether ciphering is enabled or not and the ciphering and integrity algorithm to be used. Another example is the set of MS capabilities transmitted from the MS to the serving network, including authentication mechanism, ciphering algorithm and message authentication function capabilities.

Corresponding contributions on threats and countermeasures were forwarded to 3GPP and formed a major input for the 3GPP technical report TR 21.133.

1.1.4.2. Risk Assessment

The document evaluates the following threats as of major importance:

eavesdropping user traffic; masquerading as a communications participant; passive traffic analysis; masquerading as a user, misuse of user privileges; use of a stolen terminal and UICC/USIM; use of a stolen terminal; manipulation of the identity of the terminal, confidentiality of authentication data in the UICC/USIM.

Threats of medium importance include:

eavesdropping signalling or control data on the wireless or other interfaces; masquerading as another user; manipulation of the terminal or USIM behaviour by masquerading as the originator of applications and/or data; masquerading as a serving network; integrity of data on a terminal or USIM.

The result of the threat analysis categorises the main threats as arising from:

Masquerading as other users to gain unauthorised access to services (i.e. charged to another user's account),

Eavesdropping which may lead to compromise of user data traffic confidentiality, or of call-related information like dialed numbers, location data, etc.

Subscription fraud where subscribers exploit the services with heavy usage without any intention to pay.

What is new is the acknowledgement of threats which exploit more sophisticated, active attacks to achieve the eavesdropping or masquerading (see Annex A of 3GPP 21.133). These include attacks which involve the manipulation of signalling traffic on the radio interface and where the intruder masquerades as a radio base station. Furthermore, attention is now not only focused on radio interface attacks, but also on other parts of the system.

1.1.5. Security Requirements

- Requirements derived from threat analysis
  - Requirements on security of 3GPP services
    - *Requirements on secure service access*
    - *Requirements on secure service provision*
  - Requirements on system integrity
  - Requirements on protection of personal data
    - *Security of user-related transmitted data*
    - *Security of user-related stored data*
  - Requirements on the terminal/USIM
    - *USIM Security*
    - *Terminal Security*
- External requirements
  - Regulator requirements e.g. lawful interception

Annex A of 3GPP21.133 describes threats linked to active attacks on the radio access link, examining capture of user identity, suppression of encryption between target and intruder, compromise of authentication data, and hijacking of services

1.1.6. Results

As USECA contributed significantly to the production of 33.21, the relevant sections are outlined below

Section 4 outlined the general objectives for UMTS security. These were largely taken from 33.20, with the significant change that UMTS security should be “better than” that of existing fixed and mobile networks, rather than “at least as good as”.

Section 5 gave the “context” for UMTS security, that is the constraints within which UMTS security would operate. Section 5.1 detailed the system assumptions that would affect UMTS security, such as the requirement to support high date rate asymmetric services. Section 5.2 detailed the UMTS role model that was used for the development of the security requirements. Section 5.3 detailed the types of information to be protected by UMTS security.

Section 6 contained a list of the threats to UMTS security. These threats were used to develop the requirements. Ideally the threats should all be met by requirements, but this need not be the case. SMG10 may decide, for instance, that a threat is so improbable and require so much work to be met that it is better to be accepted as a risk, rather than to be met. Furthermore some threats cannot be addressed by security mechanisms. (Ideally, a risk assessment should be carried out by SMG10 to decide which threats need to be countered.)

The threats are divided into point of attack (air interface; ME/USIM; all other parts of the system) and then by type of attack (e.g. unauthorised access to data, denial of service, etc.). This method of division was chosen as it was thought to be the most likely way that missing threats would be spotted. As a formal threat model was not applied/used, it was important that some structure was adopted to help ensure that all important threats were captured.

Section 7 was the most important part of 33.21 and contained the requirements for UMTS security. Following the approach adopted in the LINK project, the requirements are classified according to the party that benefits from the requirement, the “owner” of the requirement. There are two types of requirement owner, the user and the “provider”. The term provider encompasses both service provider and network operator. Within each division (user and provider) the requirements are divided by type, e.g. “USIM” and “Provision of UMTS Services to users”.

Annex 1 contained requirements and topics requiring further study before they can be incorporated into section 7 or rejected. Examples of such topics would be end-to-end encryption and non-repudiation.

1.2 WP2.2 - Security Mechanisms

1.2.1. 3G authentication and key agreement mechanism

The UMTS authentication and key agreement (AKA) protocol standardised in [3G TS 33.102, §6.3] was completely developed within the USECA project. This includes all accompanying management functions including the management of the sequence numbers used within the protocol and the specific messages to be exchanged in case of failure conditions (e.g. authentication failure, synchronisation failure). The main steps of its development can be looked up in USECA D06, enhancements can be found in USECA D13.

Its development started from an analysis of the GSM AKA protocol and the assertion that the GSM AKA basically worked fine. The idea therefore was to use the GSM AKA as a basis for the construction of a UMTS AKA and to introduce changes only to fulfil new security requirements. It was also a design goal that changes should be introduced in a way that provides maximum backwards compatibility with GSM and thereby eases interworking and handover between UMTS and GSM systems. This principle also facilitates migration from GSM to UMTS.

A new requirement derived from an analysis of threats to UMTS systems was that in addition to the goals the GSM AKA achieves a UMTS AKA shall provide the user with assurance of key freshness. This means that the user can be sure that the cipher and integrity keys derived by the AKA protocol were not used in a previous protocol run. To provide this additional goal it was decided to use GSM AKA and to combine it with a sequence number based mechanism standardised by ISO [ISO IEC 9798-4].

The AKA mechanism can be subdivided into two phases, the distribution of quintets from the user's HE to the visited serving network (SN) and the authentication and key establishment between the UE and the SN.

The distribution of quintets is only carried out, when an SN needs to authenticate a user for whom it does not have the required security information. The SN sends an *Authentication data request* to the user's HE. In the *Authentication data response* the HE sends an ordered array of *n* quintets. These quintets may be actually generated or they may be pre-calculated and taken from storage. Each quintet is later used by the SN for one authentication and key establishment process between SN and user. It consists of five components: a random number *RAND*, an expected user authentication response *XRES*, a cipher key *CK*, an integrity key *IK* and a network authentication token *AUTN* used to facilitate authentication of the network. The SN stores the received quintets and uses the first one for the actual authentication process with the user.

Sequence number management for the UMTS AKA

The UMTS AKA uses sequence numbers in quintets generated by the HE and checked by the USIM to guarantee the freshness of the derived cipher and integrity keys to the user. For this purpose counters are maintained and have to be kept synchronous in the HE and in the USIM respectively. To facilitate this in a flexible way the following mechanisms, developed within USECA, are specified in 3GPP:

- Re-synchronisation mechanism [3G TS 33.102, §6.3.5]:

  This mechanisms facilitates that the UE can indicate to the SN that authentication failed because of a synchronisation failure and that the SN can demand new quintets from the HE which are based on sequence numbers synchronous to the counter in the USIM.

- Mechanism for the handling of sequence numbers in the USIM [3G TS 33.102, Annex C.2]:

  The designed mechanism permits to accept sequence numbers in the USIM which are received out of sequence up to a certain degree. This is e.g. useful when the user moves between VLRs which do not exchange authentication data and is authenticated based on unused quintets when the UE returns into a location area of a previously visited VLR.

- Mechanism for the generation of sequence numbers [3G TS 33.102, Annex C.1]:

  The designed mechanism allows to use sequence numbers consisting of two parts, one part that is UE specific and one that is common to all users, e.g. based on a clock in the HE giving universal time. With an appropriate choice of specific parameters the scheme allows that sequence numbers can be sent in the clear without compromising the anonymity of the UE while allowing re-synchronisation of the sequence number counter in the HE.

Formal analysis of the UMTS AKA

Formal logic provides a powerful means to analyse security protocols in order to verify their correctness in various respects. In USECA, the authentication and key agreement protocol was analysed using two different methods of formal logic. (Cf. USECA D13 for more detailed information.)

The first method is an enhanced variant of the BAN logic and was used to show that the protocol indeed achieves the required security goals.

The second method uses a technique called Temporal Logic of Actions (TLA). The analysis seeks to prove that the 3GPP mechanism, if correctly implemented, will not "crash" or fall into failure scenarios.

In order to keep the results of these two analyses which were performed as part of the USECA project a 3GPP technical report was created, namely [3G TR 33.902].

1.2.2. User identity and location confidentiality analysis

Four alternatives to provide protection of the user identity were investigated within USECA:

- Essentially using the mechanism specified for GSM;
- using group based symmetric key encryption;
- using two layer temporary identity schemes;
- using public key mechanisms.

Mechanisms according to the two latter bullets were evaluated not to be appropriate for UMTS (cf. USECA D06 for details). Further investigations showed (cf. USECA D11) that the mechanism based on group key symmetric encryption could not provide a higher level of confidentiality protection for the user identity, because it is possible to check for the presence of a user in a cell by other means. Therefore it was recommended not to use this mechanism (cf. USECA D11).

All the USECA recommendations were accepted by 3GPP and as a result a feature essentially using the mechanism specified for GSM was standardised in [3G TS 33.102].

1.2.3. Contribution to ciphering mechanism development

UMTS provides confidentiality protection of user traffic (i.e. for signalling as well as for user data). USECA carried out an analysis of the requirements for confidentiality protection in UMTS and showed principle ways to provide confidentiality of user traffic. The principle ideas were to a large extend adapted and further developed within 3GPP and influenced the content of [3G TS 33.102, sec. 6.6] to a large extend. This includes e.g. the employment of a stream cipher (instead of a block cipher) for encryption, the use of so-called hyperframes for the synchronisation of the keystream generators of the ciphering mechanism employed at both ends (i.e. UE and RNC) to provide for the retrieval of the plaintext information.

1.2.4. Contribution to integrity mechanism development

In USECA threats to UMTS and appropriate countermeasures were analysed. The whole discussion was accepted by 3GPP and forms part of the technical specification [3G TR 33.900]. The analysis provided the basis for the selection of security services and mechanisms for the protection of the UMTS access network, in particular the need for the new feature of integrity protection of signalling messages was derived from this analysis.

USECA analysed several alternatives for the provision of integrity protection for signalling messages in UMTS (cf. USECA D06). Based on the analysis in the subsections below on mechanisms to provide integrity protection of signalling data USECA made contributions to 3GPP. The principle ideas of the contribution were preserved and further developed within 3GPP and can be found in the standard [3G TS 33.102].

1.2.5. References

[3G TS 33.102] 3GPP TS 33.102 version 3.5.0: *3G Security: Security architecture*.

[3G TR 33.900] 3GPP TR 33.900: *Guide to 3G security*.

[3G TR 33.902] 3GPP TR 33.902 version 3.0.0: *Formal Analysis of the 3G Authentication Protocol with Modified Sequence Number Management*.

[ISO IEC 9798-4] ISO IEC 9798-4: *Entity authentication - Part 4: Mechanisms using a cryptographic check function*.

1.3 WP2.3 - The UMTS Security Architecture

The main focus of the work carried out within WP 2.3 was on the integration of the USECA-developed 3GPP mechanism for authentication with the key agreement in the system architecture for the ANSI-41-evolved 3G mobile communications standard currently under development within the TIA TR-45 bodies and groups. The work also covered interoperation and handover issues.

The work was tightly integrated with and built on the work for the security mechanism work package. The security architecture work package took over when mechanisms needed to be integrated in the various network protocols. A major achievement, also due to the appropriate design of security mechanisms, was that the security functionality in 3G was positioned where it had previously been in 2G and hardly any new messages needed to be implemented. This reduced significantly the effort needed in specifying and implementation.

Most integration work was contained in [TS 33.102].

Interoperation mechanisms between UMTS and 2G communications systems (GSM)

The mechanisms for interoperation between GSM and UMTS specify what mechanisms and manipulation of security-related data elements need be executed, in the event of inter-system registration (UMTS subscribers in a GSM network and vice-versa) and inter-system handoff. At the network end, one can have a/ a UTRAN connected to a UMTS core network, b/ a GSM radio network connected to a UMTS core network, and c/ a GSM radio network connected to a GSM core network. At the user end, we consider 1/ a UMTS subscription ME that supports UMTS AKA, 2/ a UMTS subscription in legacy ME that only supports GSM AKA, 3/ a GSM subscription.

The study specifies mechanisms that allow roaming and handoff in all scenarios, without compromising the security of UMTS subscribers connected to a UTRAN.

Authentication and key agreement is performed between the core network and the user subscription module, but for UMTS AKA to be executed, the ME needs to support it as well. When the core network and/or the ME do not support UMTS AKA, it is defined how the GSM AKA parameters are derived from the UMTS AKA.

Ciphering (and integrity) key agreement is part of AKA. During GSM AKA ciphering keys for the GSM radio network are established, during UMTS AKA, ciphering and integrity keys for the UTRAN are established. However, GSM AKA may be executed to provide access to a UTRAN and vice versa. Therefore, it is defined how to derive ciphering and integrity keys for a UTRAN from a CSM ciphering key and vice versa.

These mechanisms were accepted by 3GPP and are included in [TS 33.102].

Interoperation between UMTS and other 3G mobile communications systems

The ANSI-41 second-generation mobile communications systems provide security services similar to GSM, but provided by very different mechanisms. Together with other incompatibilities this prevents inter-system roaming.

When USECA started working on inter-system roaming between 3G mobile systems, the TIA had defined the requirements for the 3G authentication mechanisms and the various working parties had before them three candidate mechanisms for evaluation. Two of them were revolutionary new and used public-key cryptography. The third, LESA, was an evolution of the mechanisms they had in place in the 2G mobile communications systems, used symmetric-key cryptography. The third had a clear lead.

USECA then deployed a dual strategy. On the one hand they subscribed and actively promoted the UMTS AKA as a candidate for authentication and key agreement in TIA; and for if that would not work, develop interoperation mechanisms between LESA and UMTS AKA. After long debate and sharp controversy, TIA favoured the UMTS AKA over LESA, the natural winner, leading to the fact that 3G mobile communications systems now have a common authentication and key agreement mechanism. This is probably the most remarkable outcome of the USECA project.

References

[TS 33.102] 3GPP TS 33.102. 3G Security: Security architecture.

[USECA D08] USECA D08. Intermediate Report on the UMTS Security Architecture.

1.3.1. Enhanced subscriber authentication for ANSI-41 evolved 3G mobile communication networks

History

In August 1999 USECA-partners representing the 3GPP submitted the USECA-developed authentication and key agreement mechanism, already adopted by the 3GPP to the program for Enhanced Subscriber Authentication that was being conducted by the TIA TR-45 community.

The main attraction of the submission was that its adoption by the TIA TR-45 community would facilitate global roaming by establishing a truly global authentication architecture for the 3G mobile systems. Nevertheless, first reactions were rather dismissive as the mechanism appeared to represent a larger deviation from mechanisms that were currently used in the ANSI-41 systems and because it seemed that the 3GPP AKA mechanism would not be able to meet key requirements of the Enhanced Subscriber Authentication program. In October then, we proposed an authentication architecture that included the 3GPP AKA as the component that provides global roaming in combination with procedures that were more evolutions from the existing mechanisms, in order to meet some requirements, esp. the requirement to authenticate using challenges that are broadcasted on the common control channels. This modified proposal, sometimes referred to as AKA+, gained support from the TR-45 subcommittees to which it was presented. This finally led to the adaptation of the AKA+ scheme at the TR-45 plenary in December.

From that moment on, the TR-45 subcommittees are working on the assumption that they will use the AKA+ scheme and are investigating what modifications might be necessary to meet their requirements. This process has been at the time of writing this, and will lead to a joint meeting of the security groups of the 3GPP and the TR-45 community next week.

The AKA+ scheme

The AKA+ scheme consists of a global security architecture for both the 3GPP and the 3GPP2 mobile communications systems. that would consist of:

A common mechanism for authentication and key agreement (AKA), the 3GPP AKA mechanism using quintets, establishing temporary authentication data between the MS and the VLR. This common part assures global roaming and a world market for AuC security functionality. In the ANSI-41 system, this would replace the procedures for SSD sharing and SSD Update and make COUNT Update obsolete (existing 2G ANSI-41 procedures).

A system-specific mechanism for local authentication (LA), using the temporary authentication data established by the 3GPP AKA, available in the MS and the VLR. This feature avoids that the network needs to use a fresh quintet for each network access. In 3GPP1 local authentication is provided by means of the integrity protection on the security mode negotiation on a dedicated control channel. 3GPP2 has a tradition which translates in a strong requirement, that authentication can be done on the common control channel, using a “global challenge,” so we suggest that 3GPP2 adopts a different mechanism that meets their requirements.

Figure 3.1 provides an overview of the AKA+ global authentication architecture.

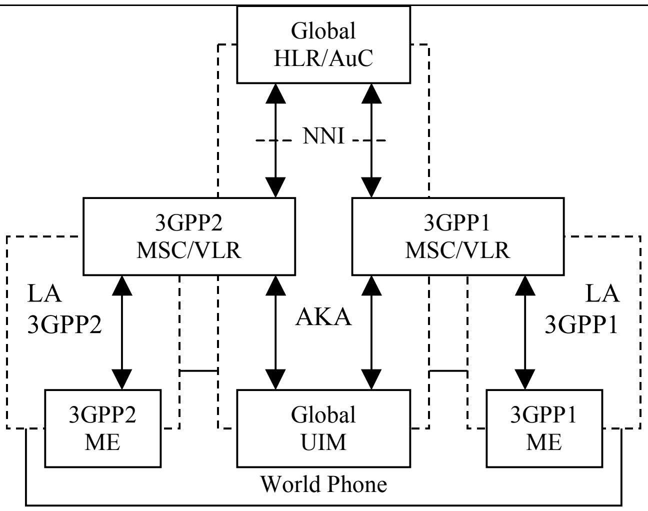


Figure 3.1: The AKA+ global authentication architecture

The AKA+ authentication architecture contains a common security functional entity in the HLR/AuC. This entity only speaks the GSM-evolved quintet-protocol (3GPP AKA). As this is the only protocol on the interface between the HLR/AuC and the MSC/VLR of both systems, no interoperation problem exists. A corresponding common functionality is available in the "Global UIM" in the "world phone". The mechanism uses a dedicated challenge, and may be performed on a dedicated channel or possibly on the common control channel.

The mechanism shall be initiated by the visited serving system at registration and may be initiated at any time when the MS is registered in the visited serving system. It is considered good practice to trigger a cipher and integrity key update at least once a day. It is also foreseen that the MS can indicate to the visited serving network that a new authentication and key establishment is required.

In most cases no synchronization error will occur and the scenario described in 4.3 applies. The scenario with synchronization error is described in 4.4.

Alongside the AKA core, the AKA+ scheme consists of family member specific mechanisms for local authentication (LA) between the MS and the VLR in which the MS is registered. The mechanism can make use of a global challenge broadcasted on a common control channel (4.1) or of a unique challenge sent on a dedicated channel (4.2).

1.3.2. Interoperation and handover between GSM and UMTS

A second important issue to which WP 2.3 has contributed is the specification of interoperation and handover scenarios for GSM subscribers that register in or handover to UMTS network and vice versa. The mechanisms that are currently specified in 33.102 have been largely provided by inputs from the USECA partners working on WP 2.3. The mechanisms describe how what security-related functionality is required to support interoperation and handover scenarios in a hybrid core network and for the many types of mobile stations. The solutions are basic and essentially based on five simple conversion functions, but the overall picture becomes complicated because of the many different combinations.

Authentication and key agreement for UMTS subscribers

Figure 3.6 shows the different scenarios that can occur with UMTS subscribers using either release 99 or pre-release 99 ME in a mixed network architecture.

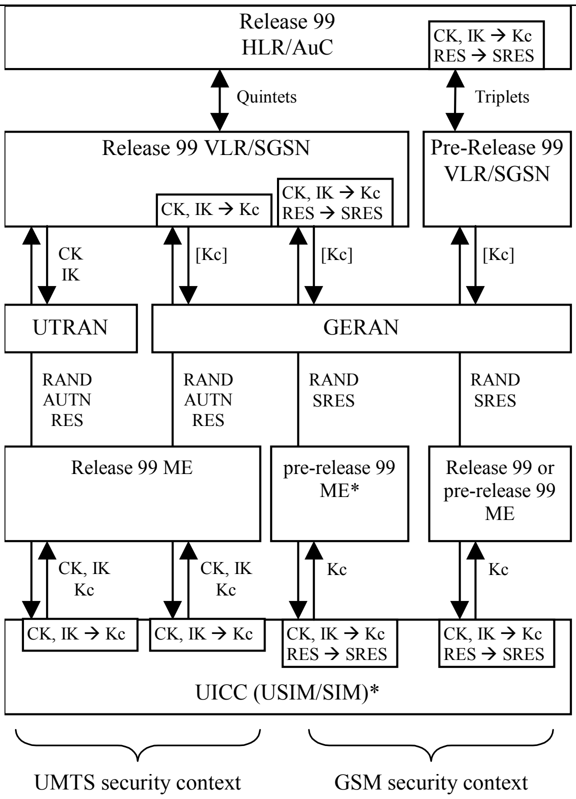


Figure 3.6: Authentication and key agreement for UMTS subscribers

For UMTS subscribers, UMTS authentication and key agreement will be applied when the user is attached to a UTRAN or a GERAN connected to a Release 99 VLR or SGSN and when the user uses Release 99 ME.

In case the user is attached to a GERAN, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys by means of a conversion function (in the VLR or SGSN and in the ME).

In the other cases, i.e., when the user is attached to GERAN that is connected to a pre-release 99 VLR or SGSN or uses pre-release 99 ME, GSM authentication and key agreement is performed. Again, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys by means of a conversion function (within the HLR/AuC and the USIM this time).

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the VLR or SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GERAN and that the GSM parameters RAND and SRES are sent transparently through the GERAN.

In case of a GERAN, ciphering is applied in the GSM BSS for services delivered via the VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS. In case of a UTRAN, ciphering and integrity are always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

The conversion functions are:

a. c1: RAND à RAND[GSM] = RAND;

b. c2: XRES à SRES[GSM] = XRES1 [xor || XRES2 [xor || XRES3 [xor || XRES4]]]

c. c3: (CK, IK) à Kc[GSM] = CK1 xor CK2 xor IK1 xor Complement[IK2]

3.3.3. Authentication and key agreement for GSM subscribers

Figure 3.7 shows the different scenarios that can occur with GSM subscribers using either Release 99 or pre-release 99 ME in a mixed network architecture.

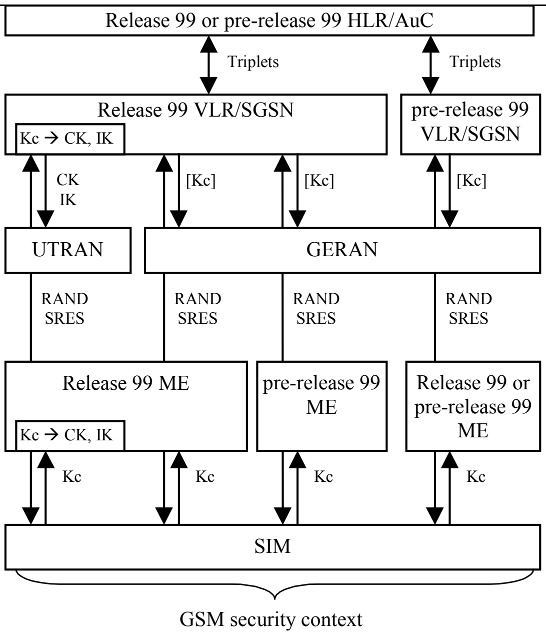


Figure 3.7: Authentication and key agreement for GSM subscribers

For GSM subscribers, GSM authentication and key agreement is always applied, regardless of the access network, and the releases of the mobile equipment and/or the VLR or SGSN.

When in a UTRAN, the UMTS cipher/integrity keys CK and IK are derived from the GSM cipher key Kc by the ME and the VLR or SGSN (implicitly they are Release 99 entities because they support the UTRAN).

The conversion functions are:

d. c4: Kc à CK[UMTS] = Kc || Kc;

e. c5: Kc à IK[UMTS] = Kc || Complement[Kc].

3.3.4. Handover (CS) and intersystem change (PS)

At handover or intersystem change during an ongoing call, with a change from a GERAN to a UTRAN or vice versa, the same conversion functions c3, c4 and c5 are used to derive the proper access link keys. Which functions are used depend on the type of the source and target radio access network and on the security context that has been established. For a full discussion we refer to the relevant papers and TS 33.102.

Along with the keys at handover all necessary information must be transported to the target BSC or RNC to continue ciphering (if applied) and integrity protection. This includes among others values to initialise synchronisation of ciphering and integrity protection, a value to assure the network of the freshness of the message authentication codes provided by the user, the selected ciphering and integrity modes.

1.3.3. Conclusions

The USECA partners active in WP 2.3 have worked with success on the integration of the 3GPP AKA in the network procedures of the ANSI-41 evolved 3G network. This has resulted in the establishment of global roaming.

Further they have contributed to different issues related to the integration of the security mechanisms in the 3GPP network procedures. Special attention has been paid to the specification of the security-related messaging for intersystem roaming (GSM/UMTS), intersystem handover (CS services) and intersystem change (PS services).

1.4 WP2.4 - A Public-Key Infrastructure for UMTS

1.4.1. Application security

Developments such as MExE will use public key cryptography to certify applications and content loaded onto UMTS terminals. In addition, WAP, and related Internet security technologies, will provide public key security for Internet access from UMTS terminals. These application technologies will require support from some form of PKI.

Security objectives on a PKI for WAP and MExE

MExE security is still being defined. The security standards in WAP are at a more advanced stage of development, but work to define a WAP PKI is also at an early stage. An opportunity therefore exists to develop common solutions to satisfy the very similar security problems which exist across both of these technologies.

A common PKI would need to satisfy the following security objectives:

- It must be suitable for both WAP and MExE
- It must be simple and not subject to misunderstanding
- It must have clearly defined relationships between entities
- It must allow “concerned” operators to take control of the “third party” domain, and to limit the power that manufacturers have. Similarly, it must allow “unconcerned” operators the possibility to leave the third party and manufacturer domains open.
- It must allow easy, interoperable provisioning of certificates.
- For WAP, it must not be USIM specific (since WAP is intended to be used in mobile systems which do not have a secure identity module).
- It must be able to be used to secure WAP services such as WTA and interactions between WAP and SIM application toolkit (STK).

A common PKI architecture for WAP and MExE

A common PKI architecture for WAP and MExE could be based on the definition of attribute certificates which are formed by specifying WAP and MExE specific attribute extensions to standard certificate formats. At the most basic level attributes would be required for “Operator”, “Manufacturer” and “Third Party” certificates. In addition “Provisioning” root keys would be used to verify the download of operator and manufacturer root keys or certificates.

Certificates could also contain attributes defining the capabilities of applications verified using the certificate. The definition of these attributes is clearly an important issue. The sub-categories in the MExE security table (Table 3 in the MExE stage 2 specification) could form a basis for the types of capabilities. In addition, WTA and WAP-STK interaction would require their own attributes. Attributes would also be required to delimit capabilities to a fine level of granularity such as is possible when Java fine grain security is available.

Interoperability requirements

Currently, the main requirements for a PKI in WAP have been to support client authentication and WAP gateway authentication. In both of these cases, new infrastructure is required, so a wireless-specific PKI can be deployed relatively easily. Such a PKI can address the constraints imposed by the wireless domain, but can also add enhanced features which are tailored to the service provision model in the wireless domain. While server authentication is also required, the main requirement is currently for authentication to servers which reside in the wireless domain. Since these servers are likely to be wireless specific, then it seems reasonable to assume that a wireless specific PKI could also be quite easily deployed in these systems. The problem comes with Internet server authentication where there needs to be some direct acceptance of an Internet server certificate by a mobile device.

Internet server authentication in WAP would involve storing very large numbers of certificates on the terminal. Although the numbers of certificates could be restricted, this would potentially limit the ability of a client to securely connect to a wide range of servers on the Internet. In the longer term, it would be desirable to offer some form of interoperation between the wireless PKI and the general Internet PKI to support end-to-end Internet server authentication. This may take the form of wireless specific components in Internet servers which will be required if they want to be able to offer services to mobile users. Alternatively, it may require that mobile clients are assisted by WAP gateways and proxies to allow them to handle “standard” Internet server certificates.

For MExE the main requirement seems to be for mobile-specific servers to be able to load MExE applications onto terminals. The general requirement for any Internet server to be able to load MExE applications onto terminals is less clear.

The need for interoperation between the wireless PKI and other PKIs could be facilitated by the adoption of standard certificate formats and certification management protocols. However, standard Internet PKI technology will not be as efficient in the wireless domain, so a trade-off may have to be made between efficiency and interoperation. At one extreme there is an argument which suggests that WAP and MExE do not need a general wireless PKI. As well as for reasons of interoperability, the argument for adopting existing Internet standards is also fuelled by traditional PKI vendors who may not want to invest in new product lines. However, wireless/mobile-specific public key systems have the potential to enhance traditional PKIs. Furthermore, the requirement for products which address and bandwidth and performance constraints imposed by the wireless domain should become clear as services and applications based on WAP and MExE technologies take off. The potential market for wireless Internet services may also mean that Internet service/content providers readily adapt themselves so that they can offer services to wireless users. So it may be the case that the Internet PKI adapts to interwork with the wireless domain rather than the wireless PKI adapting to interwork with the Internet domain.

Another aspect of interoperation is the need for interacting PKI users to be able to use a mutually acceptable suite of cryptographic algorithms. Although general PKIs may allow for the use of different suites of algorithms, in the mobile environment it is desirable that the mobile user does not have to implement a large suite of algorithms in order to be able to interoperate with other PKI users. It is therefore desirable that the number of algorithms that the mobile must support is suitably restricted by profiling the potentially wide range of options given in generic PKI standards.

PKI standards and technologies

Three certificate formats are considered:

- **X.509:** X.509 version 3 is the de facto certificate format used on the Internet. For signature calculation, the certificate is encoded using the ASN.1 distinguished encoding rules (DER) specified in X.208. ASN.1 DER encoding is a tag, length, value encoding system for each element.
- **X9.68:** ANSI X9.68 is a short certificate syntax which attempts to satisfy the needs of mobile, wireless, account based, and high volume transaction systems. It is specifically designed so that the certificates are more compact than X.509 version 3 certificates.
- **SPKI:** A series of draft Internet documents specify a rather different certificate format known as Simple Public Key Certificates. The definition of these certificates does not use ASN.1; instead they use something called S-expressions. Most critically, these certificates do not appear to incorporate any policy identifiers on other mechanisms for inserting policy information.

1.4.2. Provider security

Requirements

The only requirements related to network domain security which are mentioned in the 3GPP security threats and requirements specification, 3G TS 21.133 are that:

- There shall be a secure infrastructure between network operators, designed such that the need for home environment trust in the serving network for security functionality is minimised.
- It shall be possible to secure infrastructure between operators.

In the example protocol in D09 the situation is described that network elements of one network need to transfer sensitive information to nodes of another network. In principle this situation may often be a symmetric one.

In reviewing the requirements we very briefly review what we mean to cover within the scope of public key infrastructures for the purposes of network domain security:

- registration of KACs at a registration authority (RA) (or a CA including RA functionality);
- generation of private/public key pairs for the KACs;
- distribution of the public keys of CAs to the KACs;
- public key certificate generation, storage and distribution to the KACs;

- public key certificate revocation.

Example for a PKI

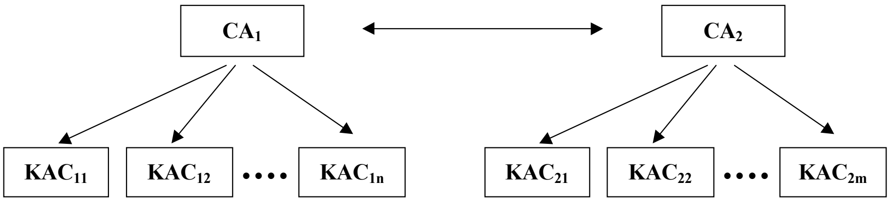
In this section an example for a potential PKI is given for the support of network domain security. As described in the example protocol given in D09, the KACs are the entities in the networks of the different operators that need to exchange public key information to support the layer I protocol.

In this discussion we denote by $Cert_X(Y)$ the certificate on a public key of entity Y issued by entity X.

It would seem that there is a strong case to be made for a PKI if and when individual bilateral relationships between entities are replaced by a smaller number of multilateral agreements. Such a move is likely as the number of mobile network operators increases and can be seen today in the context of the use of roaming brokers in GSM. In the advent of such multilateral agreements, it would seem logical to introduce some kind of PKI to facilitate public key distribution. Indeed, one might envisage a CA being set up as part of each multilateral agreement – this would mean that the operation of the CA could be specified within the multilateral agreement. In practice it seems that CAs would be set up jointly by groups of operators. Of course, one of these operators might actually run the CA, but it would be run under contractual arrangements to which all the operators are party.

Figure A2-2 shows the CA infrastructure in such a scenario. CA_1 issues certificates for *n* networks with key administration centres KAC_{11}, KAC_{12}, ... , KAC_{1n} and CA_2 issues certificates for KAC_{21} to KAC_{2m}.

Trust between different CAs can be established by bilateral agreements. So-called cross-certificates can be used, i.e. CA_1 calculates a certificate $Cert_{CA1}(CA_2)$ of the public certificate verification key of CA_2 and CA_2 calculates a certificate $Cert_{CA2}(CA_1)$ on the public certificate verification key of CA_1. This may be done between a pair of CA operators the first time a network operator of one CA sets up a roaming agreement with a network operator of the other CA.



FigureA2-2: Example CA infrastructure to provide network domain security

If one KAC has to exchange sensitive information with another one and therefore has to carry out the layer I protocol, for each public key needed in the course of the protocol, it always needs to get an authentic copy of the whole certificate chain. Two different cases can be distinguished:

- If the KACs belong to the same CA then the whole certificate chain only consists of one certificate. For instance, KAC_{11} only needs to have $Cert_{CA1}(KAC_{12})$ to verify the public key of KAC_{12}.
- If the KACs belong to different CA then the certificate chain consists of two certificates. For instance, KAC_{11} needs to have authentic copies of $Cert_{CA2}(KAC_{21})$ and $Cert_{CA1}(CA_2)$ to verify the public key of KAC_{21}.

In the example protocol in D09 the certificates on the public keys needed are sent in course of the layer I protocol. It has to be decided whether the whole certificate chain always has to be transmitted, including the cross-certificate. Another possibility would be that the KAC of each network operator stores the cross-certificates of all CAs for a network operator with whom he has a roaming agreement. The KAC may have received these certificates from its trusted CA when the roaming agreement was established. The storage of all these cross-certificates does not seem to be a problem, considering the expected number of network operators in a world-wide UMTS system.

In this description of an example PKI, the issue of revocation has not been discussed. Further study is required into how this might be done. A rather obvious solution would be to use certificate revocation lists (CRLs).

1.4.3. Conclusions

We have continued our investigation into the application of public key cryptography in UMTS by considering the use of PKIs to support selected security features in UMTS. In doing this, D09 has made use of, and elaborated upon, the results presented in USECA D03.

We have discussed the specification of a PKI to support security features in the application security domain. In this area we focused on two important technologies which are currently being standardised for use in UMTS, namely MExE and WAP. As well as elaborating upon the requirements and reporting on the status of the standardisation work, we have reviewed selected certificate formats and described how they might be applied in WAP and MExE. One of the main achievements of the project in this area has been the way it has helped to influence decisions made in the relevant standards bodies. For MExE in particular, USECA provided the following details in the specifications:

- an example signing and verification process
- requirements on the use and management of root public keys/certificates in each of the three domains
- management of certificates held on the SIM

In co-operation with other parties, specifications for the management and control of third party certificates were developed and the specifications of certificate descriptions, using PKCS#15, were developed.

USECA has also investigated the suitability of X.509 and X9.68 certificates for use in WPKI. Some of this work appeared in [D09]. USECA has also investigated the requirements on WPKI from an operator, manufacturer, user and third party perspective, though this work was not actually submitted to the WAP security group. USECA has also investigated possible certificate extensions to be used for WPKI, and proposals for these have been presented at a WPKI ad hoc meeting, hosted by Vodafone and USECA in Newbury on 28-29 October, 1999. In particular, USECA has provided details on extensions to allow operators to authorise and control the use of WTA functions in the client.

The second part of the work focused on specification of a PKI to support security features in the provider domain. After analysing the PKI requirements for this security feature, we have provided an initial specification of an example PKI which may be used to support key management between network nodes that need to establish secure signalling links. Core network signalling security is an important new security feature in UMTS and key management is recognised as a key issue which must be addressed.

1.5 WP2.5 - The USIM

1.5.1. Introduction

The objectives of WP2.5 were the following:

- to ensure viable requirements on the UMTS security architecture are proposed
- to promote beneficial enhancements to smart card specifications
- to increase user confidence in the security and usefulness of the USIM
- to input results to the relevant standardisation bodies

1.5.2. The smart card in UMTS

As with existing GSM networks, where the SIM has proven to be a valuable security device, security in UMTS will be based upon a subscriber-related smart card (*the USIM*) which has to be present in the terminal in order to process any UMTS service. Authentication of the user to the network will be carried out by secret keys and cryptographic algorithms stored on the USIM. Such a key should never leave the card in plain format and thus has to be processed in the USIM.

In contrast to GSM, the serving network will authenticate itself to the USIM by a similar procedure. On the other hand, real-time encryption, for instance speech encoding, cannot take place on the card due to capability limitations. Therefore, at each time a freshly generated session key has to be negotiated between the USIM and the serving network. This key will then be handed over to the terminal.

1.5.3. Specification of the USIM

In [D07] the low-level specification of the USIM was carried out. It was based on the high-level description given in deliverable D04. The USIM will be based on a real SIM smart card for GSM. Although the Release 99 authentication procedure is now focussed on symmetric key systems, we have also implemented a public key system. In particular, USECA has implemented the symmetric 3GPP protocol (SEQ) and the asymmetric ASPeCT protocol (MDH).

The GSM SIM personalisation feature (see GSM 02.22) is implemented for the purpose of terminal authentication. The USIM contains information which is stored in the terminal in order to authenticate the terminal. The USIM includes PIN verification, blocking and unblocking functionality for the purpose of user authentication.

- File system

The USIM files system consists of three 1st level dedicated files: DF_GSM, DF_TELECOM and DF_UMTS.

The elementary file EF_UICCID provides a number uniquely identifying the UICC and the card issuer. The file EF_APP contains information about the applications that are supported by the USIM.

DF_UMTS contains the UMTS authentication application. Elementary files located in the directory DF_UMTS include authentication relevant data that are irrespective of the used protocol. EF_CHV contains the card holder verification and ADM values. The cipher key is stored in EF_CK, the integrity key in EF_IK. EF_IMUI contains the IMSI. EF_SPID stores the service provider ID. The EF_SSD references the security mechanisms that are implemented in the USIM.

The DF_UMTS contains the 2nd level directories DF_SEQ and DF_MDH. DF_MDH includes the application data and keys of the ASPeCT authentication and key agreement protocol. The DF_SEQ contains the 3GPP authentication protocol.

Card commands

The following GSM commands are used by the GSM application as well as by the UMTS application: CHANGE CHV, GET RESPONSE, READ BINARY, SELECT, UNBLOCK CHV, UPDATE BINARY and VERIFY CHV.

The UMTS authentication application includes further commands. As far as possible ISO/IEC commands are used.

- The MANAGE SECURITY ENVIRONMENT command is used to refer to control data elements for a security environment. The data objects will be referenced in the event of a command accessing this object.
- The SECURE READ BINARY function reads a string of bytes from the current EF and encrypts the bytes using a symmetric encryption function and a secret which is referenced by a preceding MANAGE SECURITY ENVIRONMENT command.

3GPP protocol:

- The INTERNAL AUTHENTICATE command initiates the computation of authentication data and the computation and storage of a cipher key and integrity key by the smart card using the challenge data sent from the terminal and a relevant secret key stored in the card.

ASPeCT protocol:

- The GENERATE PUBLIC KEY PAIR command initiates the generation and storing of a temporary Diffie-Hellman public key pair in the USIM. The public key is delivered to the terminal as a random challenge.
- The MUTUAL AUTHENTICATE command allows the authentication of the network by the card, the authentication of the card by the network and the establishment of a session key between the USIM and the network.
- For the verification of a certificate in the smart card the certificate content is delivered to the card in the data field of the VERIFY CERTIFICATE command. The card retrieves a public key from the certificate which can be used for the verification of authentication data in a subsequent MUTUAL AUTHENTICATION command.

1.5.4. Implementation of the USIM

The major ongoing activity in this work package is to implement the USIM. The USECA USIM is a GSM Phase 2+ card with an additional UMTS authentication application. The μ-controller SLE66CX160S is used as the platform for the USECA USIM. The source code of the hardware specific programs like low level cryptographic routines are written in assembler language. The UMTS application is written in C.

1.5.5. Validation

The USIM will be tested with the use of a low level test tool for smart card development. Parallel with the implementation of the routines and functions of the UMTS authentication application test scripts are defined and implemented. The scripts describe test procedures that are interpreted and executed by a script interpreter. The result of each test is logged and will be reviewed by the developer.

1.5.6. Standardisation

Currently, the USIM working group of 3GPP, TSG-T3, is specifying the USIM for UMTS. Since the relevant documents are still not stable, the USECA USIM will certainly differ from the final low-level specification by 3GPP. The USECA USIM will be more compliant to ISO standards than the GSM SIM card. This is in accordance with the intention of 3GPP. Moreover, since the SEQ protocol is in line with the 3GPP-approved document 33.102, the major goal of the demonstration, namely to validate the proposed UMTS security architecture, will be achieved.

Further issues, e.g. integrity protection and ciphering, might become part of the USIM functionality but are beyond the scope of USECA.

1.5.7. Conclusions

The full specification of the USIM as incorporated in the demonstrator is given in [D10]. The specification of the enhanced demonstrator was successfully implemented, showing the correctness of the principles and design.

1.6 WP2.6 - UMTS Terminal Security

The security and protection of actual terminal devices has not been addressed in recent phases of standardisation work. Further work on security of terminal configurations and components is the subject of proposed development work by members of the USECA consortium and others involved in the development of the security standards for the next generation of mobile communications.

The corresponding section of [D11] provides full detail of the work conducted by WP5. As the results have not been adopted by the standards bodies at this time, they are not given at length here.

1.7 WP2.7 - Demonstrations

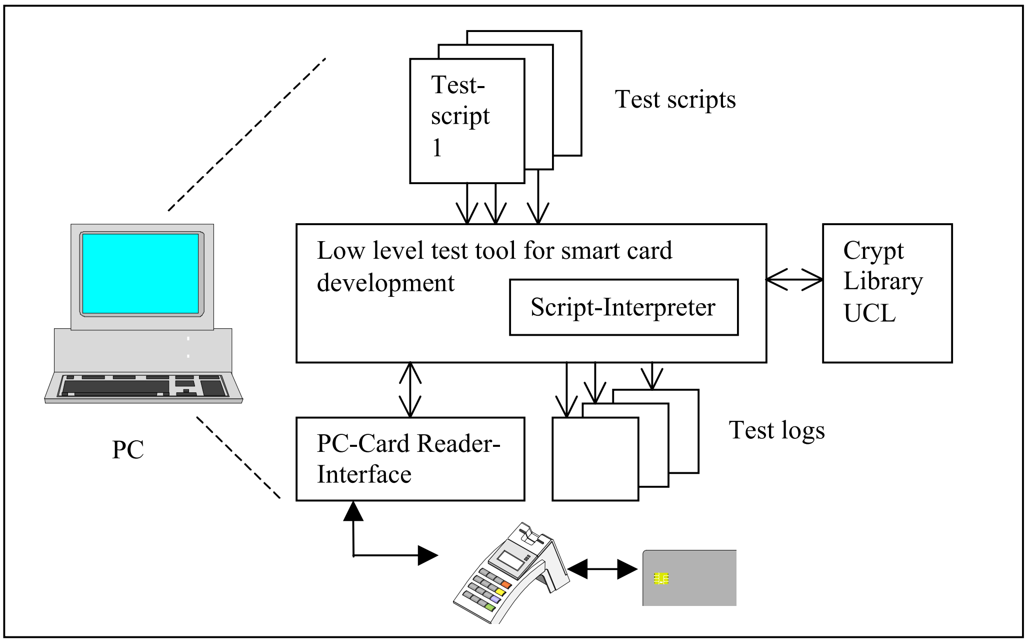
1.7.1. Summary

WP7 implemented a demonstration of the UMTS terminal based on the USIM specification in section 1.6, above. This demonstration system is specified in full in [D10] and [D11].

D11 compares the demonstrator version 1.0 to the 3G specifications release 1999 and explains the differences. Version 1.0 of the demonstrator mainly differs from the 3G specifications in the management of sequence numbers and in the parameters of the authentication command. It also specifies the modifications of the USIM. The goal was to adapt the sequence number management scheme of the USECA USIM to the 3G specifications. For this purpose the authentication procedure (AUTHENTICATE command) was modified and a list for the storage of sequence numbers was implemented.

The modifications of the PC demonstrator SW are specified in [D11]. The parameters and file system as well as the functional behaviour of the instances ‘simulated USIM’, ‘Terminal’ and ‘Network’ are adapted. The management of sequence numbers is implemented according to the 3G scheme.

According to [3GTS31.102] the sequence number consists of two concatenated parts SQN = SEQ | IND. SEQ is the batch number, and IND is the index numbering the authentication vectors within one batch. The USIM keeps track of an ordered list of the highest batch number values it has accepted. In addition, for each batch number SEQ in the list, the USIM stores the highest IND value IND(SEQ) it has accepted associated with that batch number.



1.7.2. Introduction

While version 1.0 of the USECA Demonstrator was implemented and finally finished the specifications of the USIM and the security issues within the 3GPP standardisation group were going on. Since a number of changes were made within 3GPP after the demonstrator V1.0 was finished this version of the demonstrator differs from the current 3G specifications (release 1999). Therefor the USECA group decided to adapt the demonstrator to the current 3G specifications. This chapter covers the enhancements of the USECA Demonstrator from version 1.0 to version 1.1.

First of all the demonstrator version 1.0 is compared to the 3G specifications release 1999 and the differences are examined. Version 1.0 of the demonstrator mainly differs from the 3G specifications in the management of sequence numbers and in the parameters of the authentication command.

Chapters 4 and 5 specify the modifications of the USIM and the PC SW. The goal is to adapt the sequence number management scheme of the USECA USIM and PC SW to the 3G specifications. For this purpose the authentication procedure (AUTHENTICATE command) is modified and a list for the storage of sequence numbers is implemented. The parameters and file system as well as the functional behaviour of the instances ‘simulated USIM’, ‘Terminal’ and ‘Network’ are adapted. The management of sequence numbers is implemented according to the 3G scheme.

According to [3GTS31.102] the sequence number consists of two concatenated parts SQN = SEQ | IND. SEQ is the batch number, and IND is the index numbering the authentication vectors within one batch. The USIM keeps track of an ordered list of the b highest batch number values it has accepted, where b has an arbitrary value chosen by, i.e., the network operator. In addition, for each batch number SEQ in the list, the USIM stores the highest IND value IND(SEQ) it has accepted associated with that batch number.

Comparison and implementation of the USECA demonstrator is proceeded due to the specification [3GTS31.102] which is the main specification for the USIM. This paper was edited in close relation to [3GTS33.102] which specifies the security architecture to be implemented in the USIM and in the network.

1.7.3. Demonstrator V1.0 compared to 3G Specifications

This section includes a comparison of the USECA Demonstrator V1.0 [USE-D07, USE-D10] with the 3G specifications release 1999 [3GTS31.102]. First of all the USECA Demonstrator not only includes the 3G authentication and key agreement protocol but also the asymmetric ASPeCT protocol. Concerning the 3G protocol the USECA Demonstrator V1.0 differs from the 3G specifications in the file system, the smart card commands as well as in the management of sequence numbers.

Section 7 of [D11] specifies the details of

- Parameters
- File System
- Commands
  Authentication
  Enciphering
- Cryptographic Functions
- Management of Sequence Numbers
- Enhancements / Modifications of the USECA USIM
- Enhancements/Modifications of the PC Demonstrator SW
- Generation of sequence numbers in the network
- Modifications of the re-synchronisation procedure

In addition to the functional demonstration, the full step by step animation allowing detailed analysisi of the protocol flows is provided.

1.8 Legal analysis

In addition to the analysis of technical requirements for security in UMTS architecture, WP1 undertook an extensive review of pertinent European legislation, particularly from the perspective of an e-commerce model. The opportunity is taken to reproduce the extended Summary section here. The full version of the report is given as Part 2 of the Final Technical Report [D11].

Introduction

The future mobile telecommunications standard UMTS, due to launch commercially in 2002, is representative of a new generation of e-commerce environments. Creating a unique commercial platform, UMTS will provide mobility, media convergence, and transactional efficiency for a maturing information society with little respect for jurisdictional borders and an increasing appetite for flexible and efficient content provision.

Because the security challenges are vast and unknown, authentication strategies are paramount in ensuring the platform's accountability, reliability, and effectively its commercial viability. Accordingly, the UMTS industry aspires to develop complex security mechanisms drawing upon PKI technology in combination with "brokerage" functionalities supplied by a UMTS network provider. To portray the various legal issues that arise from the diversified design of a UMTS PKI, this report carves out "sliding scale" of tools employing a PKI. The analysis draws on this taxonomy of mechanisms because it jointly synthesizes the latent security features of the broker model.

An Alternative for the Handwritten Signature: authentication may relate to an alternative for the handwritten signature, a concept under which the user's legal or natural personality as well as the user's association with an electronically formatted writing is verified so as to satisfy the requirements for handwritten signatures.

Terminal Equipment Authentication: Device authentication represents a conceptual counterpart to an electronic alternative for the handwritten signature. Rather than substituting for a handwritten signature, the user hardware is authenticated while performing certain on-line activity by virtue of its using a so-called Universal Subscriber Identity Module (USIM).

Online Payment Tokens: Payment tokens are digital payment units for which authentication is based on data sent by the user. As is the case for terminal equipment, this mechanism does not as such purport to be equivalent to a handwritten signature.

Moreover, the distinction between basic tele- and bearer-services (voice telephony, video telephony or high speed data services) and services offering "added value" (examples include data retrieval or more mobile-specific services, such as road transport telematic services providing traffic information and guidance to drivers) is determinative of the way in which existing legislation applies to the UMTS service providers.

The UMTS PKI

Most legislators draw upon the analogy with the handwritten signature to delineate the concept of legal validity of an electronic signature and liability for certification services. Therefore, the UMTS broker model warrants a second, "longer" look, to ascertain whether its comprehensiveness may effectively satisfy the concerns that have dominated regulatory activity.

The UMTS "incontestable charging" scheme is composed of three constituent parties. The first party is a network provider, referred to as the "UMTS broker." Second, the merchants providing content are referred to as "value-added service providers" (VASPs). Third, the party entering into commercial relationships with a VASP is a "user," defined as a human user or an application using a service or network (even where the application may itself be providing a service.

Given a significant degree of volatility in the innovation-dominated telecommunications industry, Community regulation experiences vast challenges. Two directives dealing with electronic signatures and more generally with electronic commerce now strive to address the most urgent matters first.

As to the Directive on electronic signatures (hereinafter: "E-Sig Directive"), guiding concepts during the legislative process were, first, the ubiquitous reliance on an analogy with the "handwritten signature," and second, "legal validity." Accordingly, universal and mandatory validity under Article 5(1), given substantial public visibility, was arguably one of the paramount policy objective to be effectuated under the Directive.

However, the single most important issue for UMTS purposes is whether existing legislation is sufficiently flexible to accommodate the diversification of authentication technology that materializes under the UMTS broker model. The emerging legal issues reverberate in four key topics: technological neutrality, legal validity, the electronic contracts regime under the E-Commerce Directive, and liability for certification service providers (CSPs). The analysis places a particular emphasis on regulatory interaction with ongoing standardization efforts.

The E-Sig Directive—Key Concepts and Provisions

Legal Validity: Article 5 of the E-Sig Directive mandates a two-tiered approach to "validity." Article 5(1) introduces a legal inference, *i.e.*, a "result," namely legal equivalence between a "qualified signature" and a hand-written signature. It thereby creates a legal prerogative of mandatory legal validity that attaches if certain technical requirements are met. Article 5(2) differs from Article 5(1) in that the provision states an operative method by which the Member States must determine substantive questions of legal effect and technological reliability.

Certification Service Providers (CSPs): The Directive provides for a very broad definition. While the definition encompasses a certification authority in a PKI environment, it also includes registration authorities, time stamping service providers, cybernotaries, and electronic archiving service providers as long as there is a link with electronic signatures. It thus embraces a UMTS broker (or an unaffiliated provider).

Technology Neutrality: The drafters recognized that a rapid technological development and the global character of the Internet requires an open approach to technology and services capable of authenticating data electronically.

Technology Neutrality

The UMTS model highlights the fact that in mass-market economies, for which automated electronic agents are crucial, evolving authentication schemes are derived from compound technology concepts and may bear little resemblance with their off-line predecessors, at least in the way they have been extended to inform the legislative process leading to the E-Sig Directive. As a general rule, UMTS providers may design authentication and PKI schemes uninhibited by statutorily mandated specifications and standards. This is true also with respect to Article 5(1) signatures. The Directive does not prescribe the use of the Article 5(1) signature, and formal recognition of certain technological standards does not legally preclude other solutions.

However, given the current state of the art, the technical requirements stipulated in the E-Sig Directive effectively restrict the prerogative' scope of legal equivalence under Article 5(1) to "digital signature" technology supported by a PKI-based certification regime. What is more, the requirements pertaining to Article 5(1) signatures are designed so as to approximate electronic signatures to the distinctive traits of handwritten signatures. Therefore, under the current state of the art, Article 5(1)—the key provision which controls the Directive's main regulatory thrust—is limited to PKI-based digital signatures that substitute for conventional, handwritten, signatures.

With regard to UMTS, a series of concerns should be noted. First, a brief review of the Directive's annexes suggests that it may be cumbersome for UMTS providers to satisfy the requirements mentioned therein. Second, the specific substance of the annexes is yet to be fully matured under the technical standardization process. Third, UMTS in all likelihood will resort to mechanisms that support truly transient relationships. Written communications do therefore not represent a viable solution for the entire range of VAS. However, while less demanding security mechanisms—such as terminal equipment authentication or a payment token scheme—ensure financial and operational flexibility, such mechanisms will likely not qualify for Article 5(1).

Legal Validity

Article 5 of the E-Sig Directive mandates a two-tiered approach to "validity."

The powerful effect of the Article 5(1) signature is derived from two key factors. First, it declares that it shall be valid wherever a handwritten signature enjoys validity. Second, the signature mechanism is specified through legal requirements regarding technical details. In this latter regard, the E-Sig Directive provides for standardization supported by market access and mutual recognition provisions. If a designated Member State body of either private or public nature makes a determination of conformity with the requirements regarding "secure signature-creation-devices," all other Member States must "recognize" that these requirements are satisfied. Moreover, the Commission may identify certain standards with regard to "electronic signature products." Member States must "presume" that electronic signature products that meet those standards are in compliance with the requirements in question.

On the other hand, Article 5(2) essentially states that electronic signatures may not be denied legal effectiveness solely on the grounds that it is in electronic form or that the signature in question is not an Article 5(1) signature. It requires that a substantive disapproval must be involved, such that any objection must be "on the merits" of the particular technology involved. The factors leading to a denial based on the substance or "merits" of any given technology scheme may be grouped in two categories. One category of substantive factors may relate to the reliability or accountability of the technological processes in issue. The second category of substantive factors reflect the technology's interaction with the signature administration and archiving environment.

Since Article 5(1) appears not to support important UMTS mechanisms, Article 5(2) provides for a highly adaptable operative tool under which legal "validity"—if necessary may be asserted. If under national law, "validity" is disputed, denial of legal effect may only be based on an individual and rationally reasoned evaluation of the technology involved.

However, Article 1(2) opens up for the Directive's interaction with national limitations of both regulatory and business nature. The provision reflects the difficulty that affirmative recognition—or affirmative action to remove a writing requirement—will be required in many specific sectors of social life. Article 1(2) thus concedes that Member State may invoke certain concerns if handwritten requirements in sectoral domains of public concern are needed.

The effect of the provision in Article 1(2) in tandem with Article 5(1) is that there is universal "legal validity" for certain PKI-based digital "qualified signatures." However, the circumstances at the national level will often call for affirmative "sectoral" recognition through legislative action after satisfaction of the relevant individual concerns. The effect of Article 5(1) and 1(2) may prove to be diametrically opposed to Article 5(2). Article 1(2) through its sweeping language is predisposed to provide for broader exceptions than Article 5(2) arguably would have permitted under individual evaluations. Thus, Article 5(1) through its making necessary Article 1(2) may cut back into the effectiveness of Article 5(2).

Yet, at least in the context of contract law, the E-Commerce Directive may prove to be helpful. The-Commerce Directive overlaps with Article 1(2) of the E-Sig Directive as far as "handwritten signature" requirements arise implicitly from "writing" requirements for contracts. It states that Member States shall ensure that their legal system allows contracts to be concluded by electronic means, calling for an active evaluation of national law with a view to eliminate requirements which are likely to curb the use of contracts by electronic means. Thereby, it partly restores the effect of Article 5(2) of the E-Sig Directive because it accelerates the use of electronic signatures as a corollary to the facilitated use of electronic documents at large.

A critical evaluation of the rationales on which the E-Sig Directive relies indicates that Article 5(1) derives its prerogative according to a twofold parameter, citing to both "equivalency" with handwritten signatures and "non-repudiation." However, since neither parameter can obscure the fact that electronic certification of a private key relates to a post-signature event, it is more proper to use "maximization of legal probability" as a parameter. Recognition of the "maximization of legal probability" paradigm will permit an inference that other post-signature verification processes may be able to stand the test.

The UMTS model suggests that it may perform well under this parameter. Even where UMTS certificates do not contain a reference to the user's natural or legal personality, the overall UMTS model effectively provides for an equivalent feature through two mechanisms. UMTS combines network authentication of the terminal equipment with a high level of certainty that only a particular user has access to the terminal, at least where biometrics are used. In other words, the broker can trace the use of terminal equipment to a particular user, whereby the broker can identify with legal probability the natural or legal person involved.

The E-Commerce Directive—The "Placing of an Order"

If a given authentication mechanism signature is challenged, it must also be determined whether it satisfies the requirements under national rules on the conclusion of contracts. In referring to the "placing of an order" the attention should be on the unilateral act of the user, rather than on contractual mutuality between the parties involved. Thus, where a user carries out activities online that amount to the "placing of an order," the E-Commerce Directive applies. Second, the provision then particularizes the proper response of the VASP, namely to "acknowledge the receipt of the [user's] order." The subscriber agreement can not by-pass the provision, because contractual derogations are only permitted with respect to business-to-business contracts.

The E-Commerce Directive does not cover documents signed electronically (involving identity authentication under a PKI) if such electronic documents replace individual paper-based communications.

The user "places an order" when sending payment tokens, and the VASP must therefore immediately acknowledge the receipt of the tokens. Moreover, the sending of payment tokens is a measure sufficient to "place and order" (and thus initiate the conclusion of a contract). For UMTS purposes it is important to note that the acknowledgment may take the form of the on-line provision of the service paid for.

Liability for UMTS Certification Service Providers

For the drafters of the E-Sig Directive the liability regime is a necessary tool to support the effect of Article 5(1). The liability regime through its rhetorical context draws on an analogy with handwritten signatures, and, accordingly, the liability regime is drafted predominantly with authentication of natural or legal persons in mind. Because UMTS brokers will not exclusively rely on written representations in an electronic format, the problems regarding applicability of the Directive's Article 6 in the UMTS context are manifold.

First, the objects of certification may be different from what the Directive appears to contemplate, and this result is not altered by current standardization efforts. Mere certification of technical hardware (such as terminal equipment), or software units (that is, UMTS payment tokens), is likely to fall outside the Directive.

Second, where device or payment token authentication spurs legal questions akin to agency law regarding the terminal equipment and software involved, the analysis must look to national law so as to establish whether domestic doctrines embrace such authentication of a natural or legal person through substitutory means. The E-Sig Directive does not aspire to solve this matter.

Third, the Directive's narrow design is also evidenced by its highly contextual language, notably by requiring human traits such as "reason" and "reliance." As this language is patterned upon the qualities of written communications as between two natural persons, it appears to preclude from its scope automated cross-verification through electronic agents not involving written communication. Because UMTS architecture will likely employ automated agents embedded in configured software and hardware its parameters are difficult to bring in line with the reliance scenario. Therefore, the Directive's emphasis on the human quality of "reason" and "reliance" concepts is poorly designed to accommodate UMTS certificates.

Fourth, the UMTS model contemplates a hybrid network, comprising both "open" and "closed" aspects, which partly explains the difficulty in applying the E-Sig Directive. It is safe to conclude that even if it cannot be ruled out that the liability regime may be held to be applicable under its terminology, the regime is framed in a way that more generally renders it very difficult to adapt to the hybrid peculiarities of the UMTS model.

Thus, the liability regime under the E-Sig Directive consistently escapes its potential applicability to the PKI under UMTS. Nevertheless, the significance of the liability question is present from a legal as well as a business perspective. Both viewpoints are directed towards the key advantage of a supranational liability regime, which is that the provision creates a core of normative standards around which national implementation measures will evolve across the internal market. As for self-regulation, little of tangible consequence can be said about these future relationships at the present stage. These assumptions concerning the design of the business model demand further analysis to cover the inevitable technological progress and changes in business strategy, most notably roaming agreements. It is possible, however, to predict that at some point down the road, the network will reach a level of commercial complexity that may require a more stable legal framework than self-regulation. And this prediction becomes a matter of certainty once UMTS expands at a pace that requires flexible agreements.

Conclusions

This report concludes that the analogy is of limited utility for purposes of UMTS and, moreover, that it provokes definitional externalities resulting in legal uncertainty regarding those regulatory areas that do not rely on the analogy. Thus, careful regulatory review of existing legislation to accommodate UMTS authentication mechanisms is warranted to consider regulatory activity in two possible respects.

First, true technology neutrality with regard to Article 5(1) would help spur on-line transactions that lead to contracts with "signatures" generated by conduct (implication), such as by terminal equipment or by sending online payment tokens.

Second, and most importantly, Article 5(1) has acquired a key role in the E-Sig Directive. Other regulatory efforts under the E-Sig Directive are limited to supporting Article 5(1), thereby excluding other mechanisms from their scope. This may give rise to regulatory revision of some specific provisions.

Legal Disputes based on Electronic Data—Admissibility and Related Evidentiary Aspects

As for admissibility and related evidentiary aspects, remaining restrictions appear to be negligible and will not pose a threat to the viability of the UMTS business model. Legislative action at a Community level will strengthen the evidentiary status of electronic data even further.

The report draws on the developments in the United Kingdom, because—at its present state—it represents a good benchmark for the current legal evolution in many jurisdictions.

Generally, it is proper to assume that in most jurisdictions records of electronic data will have to be authenticated by demonstrating a proper working order. The requirements that must be met to satisfy a proper working order standard will be determined on an individual basis. Devices, recordings, and business routines implemented for UMTS billing purposes are likely to be subjected to expert scrutiny only if the mechanisms' reliability is challenged, and to the extent the underlying technology is not widely used, generally known, or has not otherwise been more or less accessible to investigation. Other factors that may have a bearing upon admissibility or the evidentiary weight are: procedures for collecting, verifying data, and entering data into a storage system; any interference with the data and whether this is accounted for in the records; security of the processing and/or storage devices in the period from initially creating the record to successive storage measures, specifically when the latter requires removal from the storage medium; security features of the means of removal; and circumstances of custody until presentation to the court. Once case law has ascertained that the UMTS billing scheme in fact is reliable, a broker involved in a billing dispute will in all probability only have to show that the technology operates properly.

Under the hearsay rule or similar rules evidence has been traditionally discouraged or excluded from civil proceedings on the theory that the adverse party's access to cross-examination is effectively rendered ineffective. As for admissibility of traffic and billing data under rules similar to the hearsay rule it must be established that the mechanical means deployed for UMTS purposes constitute entirely technical operations replacing human effort. Where these findings are in the affirmative, the data should be admissible because the hearsay rule or similar concepts are not properly applicable.

The best evidence rule concerns the "physical" presentation of evidence in a courtroom, or the like. There are significant variations to the best evidence rule, and case law appears to evidence the courts' reluctance to honor the rule's rigid formalism.

As to statutory law, legislators in the United Kingdom clarified any remaining uncertainties by adopting the general principle that evidence shall not be excluded on the ground that it is hearsay. Moreover, the relevant statute has embedded the sweeping rule in broad language so as to embrace records presented in court by means of, *inter alia*, computer disks, videotape, audio tape and computer printouts. The Directives on Electronic Signatures and E-Commerce are designed so as to accelerate these developments in all Member States. The ambiguities that arise from the former Directive's reliance on equivalence of certain electronic signature mechanisms with handwritten signatures are not present with regard to evidentiary questions.

The E-Commerce Directive states a strong rule in this respect. Member States must carry out an evaluation of rules that might prevent, limit, or deter the use of electronic contracts. If this review identifies provisions which prohibit or restrict the use of electronic media, a Member State is under an obligation to repeal or amend the rule in question.

Data Protection Law

As for data protection of electronic data, a distinction between "traffic" or "call" data and written communications remains helpful, because the applicability of different legal regimes is determined along those lines. The general rules concerning personal data protection can be found in national data protection laws. At least in Europe, most Member States have enacted such laws. While national data protection laws are similar in many respects, the level of protection guaranteed in the Member States is not uniform. To remove obstacles to the free movement of data, Directive 95/46/EC aims at harmonizing the national provisions in this field.

Directive 97/66/EC applies the general data protection principles laid down in Directive 95/46/EC to UMTS, striking a balance between individuals' privacy interests and the industry's need to process sufficient data for billing and legal enforcement purposes. However, its definitional design does not properly accommodate advanced technology schemes such as the UMTS "incontestable charging" model, due to its emphasis on circuit switched voice telephony standards. Moreover, Directive 97/66/EC does not extend the relevant provisions to value-added-service providers. Thus, from a UMTS perspective there is a pronounced need for legislative review of the Directive so as to clarify its scope. However, the proposed amendments to Directive 97/66/EC appear to remove these discrepancies to embrace packet switched transmissions, and they expand the scope in respect of value-added-service providers.

With regard to data transfers to UMTS related providers in third countries, the European Commission' decision to approve the "safe harbor" scheme should secure a workable solution for UMTS providers in their setting up a network outside the internal market.

UMTS brokers that wish to ascertain whether their intended US recipient enjoys safe harbor status must refer to a publicly available list maintained by the Department of Commerce. US organizations that are subject to the jurisdiction of either the FTC or the Department of Transportation appear on the list after proper self-certification and a public declaration of adherence to the safe harbor principles. Upon persistent failure to comply with the principles, such data recipients may lose their safe harbor benefits, which will be notified through the list.

The future mobile telecommunications standard UMTS, due to launch commercially in 2002, is representative of a new generation of e-commerce environments. Creating a unique commercial platform, UMTS will provide mobility, media convergence, and transactional efficiency for a maturing information society with little respect for jurisdictional borders and an increasing appetite for flexible and efficient content provision.

Because the security challenges are vast and unknown, authentication strategies are paramount in ensuring the platform's accountability, reliability, and effectively its commercial viability. Accordingly, the UMTS industry aspires to develop complex security mechanisms drawing upon "Public Key Infrastructure" (PKI) technology in combination with "brokerage" functionalities supplied by a UMTS network provider. Legislative activity, on the other hand, is still in its infancy, struggling with a range of definitional issues. Given a significant degree of volatility in the technology-dominated telecommunications industry, Community regulation experiences vast challenges. Two directives dealing with electronic signatures and more generally with electronic commerce now strive to address the most urgent matters first.

As to the Directive on electronic signatures, guiding concepts during the legislative process were, first, the ubiquitous reliance on an analogy with the "handwritten signature," and second, "legal validity." This report assesses how these concepts may control the legal status of a volatile telecommunications market in which commercial decisions are made along the lines of technological sophistication and consumer demand rather than with a view to approximate existing conceptions of off-line authentication tools. Therefore, the report devotes particular attention to the way in which the UMTS business model may deviate from the conception of an electronic signature as an alternative to the handwritten signature.

The overarching question that arises from the analysis is whether the existing legal environment is truly supportive of the development of a mobile e-commerce platform under UMTS. More specifically, the single most important issue is whether existing legislation is sufficiently flexible to accommodate the diversification of authentication technology that materializes under the UMTS Broker model. To illustrate consequential legal issues, the analysis introduces three security mechanisms akin to those likely to be commercially employed during the initial phase.

With regard to the UMTS PKI, the report discusses "technology neutrality," the limitations of mandatory "legal validity" and "equivalence," electronic contracts, and the role and scope of a liability regime for certification service providers (CSPs) under the UMTS business model. It concludes that regulatory activity as regards PKI matters has created a fragmented legal environment, only partly equipped to accommodate the UMTS business model. In particular, the Directive on electronic signatures only marginally supports the evolving e-commerce environment under UMTS. Moreover, the analysis concludes that the UMTS model challenges the legal prerogative attributed to one PKI-based signature mechanism under the directive on electronic signatures. However, the discussed discrepancies are not altogether attributable to the legislative approaches taken. The application of existing law is further complicated by the hybrid design of the brokerage model, involving aspects of both "closed" and "open" environments.

This report's discussion of the PKI is based on the following methodology.

UMTS industry must be empowered to enforce the user's obligation under the subscription contract. To this end, it must also rely on evidence derived from electronic data records. In [D11-2] discusses the question of admissibility and some associated evidentiary aspects of electronic data records. Without aspiring to reach a detailed analysis of the legal status in all Member States, the report identifies general regulatory and judicial developments at the national level, and forecasts the impact that Community legislation will have.

Lastly, pervasive and rigorous requirements of emerging data protection law in EU Member States, the Community level, and internationally, must prompt an analysis of the impact that such legislation has on business environments that rely heavily on electronic data. The establishment and administration of a complex operational platform for commercial transactions, such as the UMTS business model, employing among other things a PKI, must both honor the interests of consumers in preserving privacy, and aspire to design an efficient and reliable data processing, use, and storage system. The aggregation of individual Member State regimes may have a particularly adverse effect on UMTS if existing Community law is not uniformly implemented with respect to the telecommunications industry. The full report discusses how Community law attempts to synthesize these perspectives into a suitable legal environment for the emerging telecommunications industry.

2 Main conclusions reached

Overall project conclusions

The project has successfully completed the planned work, and made many essential contributions to the progress of security aspects of the first specifications of third generation mobile communications - UMTS - mainly through liaison with 3GPP.

The project has enabled the partners to act as a coherent technical focus for the security work leading the specification of 3G mobile globally. The successful individual results are indicated above, but the overall success of the project can be seen in the influence that has been achieved at the worldwide level.

2.1.1. Recommendations

There are number of lessons to be learnt from areas where the project could appear to have fallen short of its original aims; these may be taken as general recommendations for future project activity, and will be taken into account in planned work in this area.

terminal security

it would have been beneficial to have switched emphasis to terminal security issues and requirements that were arising in the WAP and MExE communities; whereas, the project pursued some ongoing equipment-manufacturing-led work in physical security issues that lead to a dead end, at least for the time being
recommendation:
maintain broad outlook on parallel, related activities and allow tactical refocussing

limited PKI results

some self-restraint was imposed by the project through close adherence to immediate priorities of standards processes and timescales, limiting scope for innovation; this is seen as the correct action, overall, the project limiting its work to an analysis of available technology.
recommendation:
maintain a dynamic balance, within the agreed goals of the work, between immediate, next generation requirements and crystal-ball research activity and strategic analysis

inter-project collaboration

this was largely a result of the particular spread of interests at that time (security issues have often been seen as a burden, rather than benefit)
recommendation:
if need be, extend the linkages to projects outside the immediate area, possibly to users of the technology rather than fellow generators.

internal discussion and work on future trends and outlook

this is a more general observation relating to the PKI issue, above; the project could have been more autonomous and concerned with more internally-generated technical goals, but then it would have failed to achieve the global impact ;
the tight working relationship with urgent standardisation work and concentration on its requirements has contributed to the success – the global impact of project results – and weaknesses – limited depth of vision and outlook – of the project
recommendation:
maintain healthy balance of *focus* (narrow) and *vision* (broad); careful management of the relationship with external actions such as the standards processes

3 Inputs to Standards

Please see Annex - 5, below, for complete list of USECA contributions to international standards.

4 Overall impact, exploitation and dissemination of results

The project has had unique impact through its contribution to international standards for security for 3rd Generation mobile telecommunications, not only in European but on world-wide norms.

It was anticipated that liaison with the standards for UMTS security would be in the context of European standards developed in ETSI, however, the industry set up a new organisation concerned solely with the establishment standards for 3G. The Third Generation Partnership Project - 3GPP - arrived in time for USECA to switch its focus to the new forum. By so doing, the project was to play a central role in defining a number of critical security components for the worldwide industry standards.

The list of standards (Section 3 above) demonstrates the extent of the contribution the project has made to the progress of UMTS.

In addition to its technical results, the project has produced a review of relevant aspects of the legal environment - both European and national legislation - as it affects core processes in a business model involving mobile communications. This developed into a very comprehensive report, so it seems fit to treat it as a separate, free-standing document that may be of wider general interest and use in future work on the the development of regulatory frameworks governing the take-up of electronic commerce. It forms Part 2 of the Final Technical Report [D11].

5 Self assessment

Synopsis

The success of the project in its contribution to the development of standards for security for third generation mobile communications (UMTS) exceeded the requirements of the partners and the hopes and expectations of the participants themselves. There is considerable satisfaction in the impact that has been made and in the recognition of this achievement.

Having established a position of some standing in ETSI and 3GPP, members of the project went on to make important contributions to other associated areas concerning standards for security in applications execution and communication environments.

Further, the active liaison work by USECA participants has ensured the global adoption of USECA results. The project contributed a large part of the standards material for this field, and has responded flexibly to the changing requirements and timescales of the body that is now representing the global industry.

The project carried out a very valuable and successful revision and restructuring of the existing input to the standards on security threats and requirements; the resulting document now provides the basis for further work by 3GPP in this field.

An extensive review of existing member state law pertaining to the use of security facilities provides a most useful foundation for further legislative and regulatory development and harmonisation of community law.

The investigation of requirements for security mechanisms was contributed to the requirements work above. Analysis of authentication and key agreement proposals led to the development of the mechanism adopted by 3GPP. The project was also responsible for the mechanisms for synchronization of ciphering in UMTS, mechanisms for interoperation with GSM and proposals for interoperation with ANSI systems.

Following some delays due to priorities within standards body, the project has provided an initial work on the use of public key in the mobile application domain and in the provider and core networks domains – e.g. for support of key management between nodes.

Following work on establishing security and hardware requirements, the project has successfully specified the design and procedure for UMTS USIM which was subsequently prototyped and built into a demonstrator of a UMTS terminal. The requirements work covered the needs of mobile terminal security, the implications of which have been analysed and new facilities proposed in response.

To conclude, the project is by a long way the most significant contributor to the development of 3rd generation security standards. It has amply achieved its original objectives, and is proof of the value of funded collaborative research in this area.

The project achieved a great deal, exceeding initial objectives in terms of influence on and contributions to standards organizations. In view of their perception of the success and usefulness of the USECA work, most of the USECA participants have gone on to collaborate, with new partners, in further advances in security for mobile telecommunications in the Framework 5 IST project SHAMAN.

6 Annexes

A1 - List of deliverables produced

A2 - List of published papers

A3 - List of patents, registered designs or other IPR

A4 - Introduction to deliverable D11 - Final Technical Report

A5 - Contributions to Standards

6.1 A1 – List of deliverables produced

Deliv. Code	WP Code	Deliverable Title	Deliv. Nature	Deliv. Type	Sec. Class
D01	WP1.2	Linkages with other ACTS projects	R	N	R
D12	WP2.3	Overview of UMTS architecture	R	N	L
D02	WP2.1	Security features and requirements for UMTS	R	N	P
D03	WP2.4	Requirements on a PKI for UMTS	R	K	P
D04	WP2.5	Intermediate report on the UMTS USIM	R	N	P
D05	WP2.6	Intermediate report on terminal security for UMTS	R	N	P
D06	WP2.2	Intermediate report on UMTS security mechanisms	R	N	P
D07	WP2.7	The UMTS USIM : Specification of a demonstrator	S	N	I
D08	WP2.3	Intermediate report on UMTS security architecture	R	N	P
D09	WP2.4	Intermediate report on a PKI architecture for UMTS	R	N	P
D10	WP2.7	The UMTS USIM : Implementation of a demonstrator	P	K	P
D11	WP1.2	UMTS security architecture : Final project technical report	R	K	P

6.2 A2 – List of published papers

Authors	Title of paper	Name of journal, conference, etc.	Reference	Date	Ref? (Y/N)
Vinck, Horn & Müller	A viable security architecture for UMTS	ACTS Mobile Summit '99 Sorrento	Proceedings	8/11-JUN-99	Y
Horn, Müller & Vinck	Towards a UMTS security architecture	European Wireless'99 Conference proceedings, Munich	Proceedings pp 495-500	6/8-OCT-99	Y
Horn & Howard	Review of third generation mobile system security architecture	ISSE 2000, Barcelona	Proceedings	26/28-SEP-00	Y
Heckmanns, Horak, Horn, Howard, Müller & Vinck	Design and evaluation of 3G security	IST Mobile Summit 2000, Galway, Ireland	Proceedings pp. 343-348	1/4-OCT-00	Y
Howard	An overview of 3GPP security	IIR Fraud and Security, London	Proceedings	06/09-MAR-00	N
Vinck, Howard & Müller	An introduction to the security features of 3GPP and third generation mobile communications system	IIR Fraud and Security, London	Proceedings	06/09-MAR-00	N
Howard & Horn	An introduction to the security features of 3GPP and third generation mobile communications system	IEEE VTC 2000 Spring, Tokyo	Proceedings	15/19-MAY-00	N
Mitchell	Making serial number based authentication robust against loss of state	ACM Operating Systems Review,	Vol 34 No.3 pp 56-59	July 2000	Y

6.3 A3 – List of patents, registered designs or other IPR

The goal of USECA was to progress the architecture and consequent standards for UMTS security. All intellectual property arising from USECA was targeted at the standards making process, hence the extensive list in the list under Section , above.

6.4 A4 - Introduction to deliverable D11 - Final Technical Report

In addition to its technical results, the project produced a review of the relevant aspects of the legal environment – both European and national legislation - as it affects core processes in a business model involving mobile communications. As this is so comprehensive, it has been treated as a separate document that may be of wider general interest and use in, say, development of regulatory frameworks governing the take-up of electronic commerce. In this form it is Part 2 of D11 – the Final Technical Report.

Part 1 of that report deals with the technical work. The numbered sections give the results of the technical workpackages of the project.

Section 1 Workpackage 2.1 – covers the the work to establish the requirements for 3g security;

the intended update to the existing document [ETSI 33.20] had to be superseded by a complete rework; the results was a new version of ETSI standard.

Section 2 Workpackage 2.2 – deals with the work on security mechanisms for 3G;

the principal results here were the authentication and key agreement (AKA) protocol, which has been adopted worldwide, and a major contribution to user traffic confidentiality and also to integrity protection of signalling data.

Section 3 Workpackage 2.3 – describes the overall security architecture

Section 4 Workpackage 2.4 – provides a survey of the use of public key cryptographic infrastructure (PKI) in UMTS; the work provides a useful foundation for subsequent developments where PKI will be a necessary component although the scope for innovation was limited by the 3GPP's priorities for its early releases.

Section 5 Workpackage 2.5 – documents an approach to terminal security that at the outset appeared to have practical possibilities; in the event this has not been taken up by the industry.

Section 6 Workpackage 2.6 – gives a specification for the Universal Subscriber Identity Module (USIM) that was implemented and demonstrated in WP2.7.

Section 7 Workpackage 2.7 – specifies the demonstrator.

A5 - Inputs to Standards

Notes: (a) Impact Key: 0 = No impact; 1 = Low impact; 2 = Moderate impact; 3 = High impact
(b) all standards here are for future deployment therefor there is no *normal use* at this time
(c) all 3GPPwork will have European impact as ETSI plans to be fully compliant

Stdds Body/ Committee/ Subcommittee	**Date**	*Title of contribution*	**Impact on world standard**	**Impact on European standard**	**Impact on standard in normal use**
TIA/EIA TR45.2 & TR45.5	11Oct99	Questions and answer on the 3GPP authentication and key establishment mechanism	3		
TIA/EIA TR45.2 & TR45.5	11Oct99	Presentation on the 3GPP authentication and key establishment mechanism	3		
TIA/EIA TR45.2 & TR45.5.2	11Oct99	Presentation: Security interoperation between 3GPP and IS-41 systems	3	2	
TIA/EIA TR45.2 & TR 45.3	08Nov99	Brief analysis of network signalling load associated with the 3GPP mechanism	3		
TIA/EIA TR45.2 & TR45.3	08Nov99	Stage 2 descriptions for the 3GPP authentication and key establishment mechanism	3		
TIA/EIA TR45.2 & TR45.3	08Nov99	Stage 2 descriptions for the 3GPP authentication and key establishment mechanism	3		
3GPP TSG SA WG3	11May99	S3-99097: Formal analysis of 3G authentication and key agreement protocol	3	3	
3GPP TSG SA WG3	16Jun99	S3-99170: Results of formal analysis of the 3G authentication protocol with modified sequence number management	3	3	
3GPP TSG SA WG3	16Jun99	S3-99171: Modified sequence number management	3	3	
3GPP TSG SA WG3	16Jun99	S3-99179: Conditions on use of authentication information	3	3	
3GPP TSG SA WG3	16Jun99	S3-99180: Modified re-synchronisation procedure for AKA protocol	3	3	
3GPP TSG SA WG3	16Jun99	S3-99181: Sequence number management scheme protecting against USIM lockout	3	3	
3GPP TSG SA WG3	16Jun99	S3-99183: Formal analysis of the 3G authentication protocol with modified sequence number management	3	3	
3GPP SA 3	16Jun99	S3-99158: Interoperation between UMTS and GSM	3	3	
3GPP SA 3	16Jun99	Conversion functions for interoperation	2	2	
3GPP SA 3	16Jun99	S3-99262: Key selection for signalling	2	2	
3GPP TSG SA WG3	03Aug99	S3-99234: Enhanced window mechanism for sequence number management	1	1	
3GPP TSG SA WG3	03Aug99	S3-99235: Proposed response to LS statement 99231 fromN2 on Super-Charger concept	1	1	
3GPP TSG SA WG3	03Aug99	S3-99236: Response to doc. 99230 “A Possible Problem of the UMTS AKA Mechanism” from T-Mobil/Deutsche Telekom	2	2	
3GPP SA 3	25Aug99	S3-99263: Interoperation between UMTS and GSM	3	3	
3GPP TSG SA WG3	29Sep99	S3-99304: A generalised description of sequence number management options	3	3	

3GPP TSG SA WG3	29Sep99	S3-99322: Brief response to S3-99308 on the window mechanism for sequence number management	1	1	
3GPP TSG SA WG3	29Sep99	S3-99342: Over the air management of window and list sizes	2	2	
3GPP TSG SA WG3	29Sep99	TS 33.102 CR018: Support for window and list mechanisms for sequence number management in authentication scheme	3	3	
3GPP TSG SA WG3	29Sep99	TS 33.102 CR019: A generalised description of sequence number management options	3	3	
3GPP TSG SA WG3	11Oct99	TS 33.102 CRxxx: Modification of text for window and list mechanisms	1	1	
3GPP SA 3	26Oct99	S3-993876The 3GPP AKA as a candidate for ESA	2	2	
SMG4 MExE	12Jan99	4M99-008: Input document on 03.57 security section	1		
SMG4 MExE	12Jan99	4M99-016: Stage 1 security specification	1		
SMG4 MExE	12Jan99	4M99-038: Conclusions of Automatic Execution Workshop	0		
SMG4 MExE	12Jan99	4M99-040: 03.57 security table update	1		
3GPP T2 SWG1/SMG4 MExE	17Feb99	4M99-063: Additions to stage 1 security requirements	1		
3GPP T2 SWG1/SMG4 MExE	17Feb99	4M99-090: E-mail on certification	1		
3GPP T2 SWG1/SMG4 MExE	17Feb99	4M99-091: Network selection	1		
WAP PKI ad hoc	28Oct99	Contirbution on extensions to X.509 for signing of downloaded code	2		
WAP Forum, San Francisco	27Jun99	Contribution on bootstrap/provisioning root certificates	1		
WAP Forum, San Francisco	27Jun99	Contributions on certificate requirements for WAP and MExE	1		
3GPP TSG SA WG3 #1, London	02Feb99	S3-99021: Objectives and principles of 3GPP security	2	2	
3GPP TSG SA WG3 #2, Stockholm	23Mar99	S3-99040: Proposed LS to T3 on integrity on the USIM	1	1	
3GPP TSG SA WG3 #2, Stockholm	23Mar99	S3-99054: Some initial thoughts on end-to-end encryption	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99095: 3GPP Access interface ciphering algorithm requirements	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99098: Comments on authentication and key agreement protocol	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99101: Proposal for radio interface ciphering architecture	2	2	
3GPP TSG SA WG3 #3, Bonn	11May99	S3-99121: Addressing 2G weaknesses	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99162: Proposed CR on key setting	2	2	

3GPP TSG SA WG3 #4, London	16Jun99	S3-99164: Key management for network wide encryption	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99187: Proposed CR on 33.102 on Description of layer on which ciphering takes place	2	2	
3GPP TSG SA WG3 #4, London	16Jun99	S3-99189: Proposed LS to R2 on RLP PDU size	2	2	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99206: Proposed response to “CR to TS 25.301 - Integrity control mechanism”	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99216: Hooks for network-wide encryption	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99217: Location of integrity termination in the network	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99218: Synchronisation mechanisms for network-wide encryption	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99224: Proposed CR to 33.102 on Cipher keys on control and user planes	1	1	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99246: Proposed CR to 33.102 on Cipher key setting	2	2	
3GPP TSG SA WG3 #5, Sophia Antipolis	03Aug99	S3-99248: Proposed CR to 33.105 on Cipher keystream block length	1	1	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99297: Update on MExE security	1	1	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99302: Support for multiple authentication algorithms and keys	2	2	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99303: The use of Zero-Knowledge Identification mechanisms for 3G Terminal Identification	1	1	
3GPP TSG SA WG3 #7, The Hague	26Oct99	S3-99340: Keystream repeat attacks	1	1	
3GPP TSG SA WG3 #6, Sophia Antipolis	29Sep99	S3-99340: Proposed CR 33.102-016 on Network-wide confidentiality	2	2	
3GPP TSG SA WG3 #7, The Hague	26Oct99	S3-99385: Proposed response to LS from R3 on common identification of relocation co-ordination	1	1	
ETSI SMG10 WPC #1/99, Newbury	20Jan99	SMG10-99005: Draft security architecture 33.23 v0.0.2	2	2	
ETSI SMG10 WPC #1/99, Newbury	20Jan99	SMG10-99012: Draft security architecture 33.23 v0.0.3	2	2	
ETSI SMG 10	20Jan99	SMG10-99C013: Mutual authentication and key establishment for UMTS Release 99 based on random challenges and sequence numbers - MAC-based variant	3	3	

3GPP T2, London	15Mar99	T2-99070: Revised CR to 02.57 on security	1	see note, above	
3GPP T2, London	15Mar99	T2-99071: CR to 03.57 on security	1		
3GPP T2, London	15Mar99	T2-99224: CR to 02.57 security	1		
3GPP T2, London	15Mar99	T2-99227: CR to 03.57 Security Sections	1		
3GPP T2, London	15Mar99	T2-99229: Revised CR to 02.57 11.3 Security	1		
3GPP T2, Yokohama	12Apr99	T2-99342: Stage 1 Security section CR	2		
3GPP T2, Yokohama	12Apr99	T2-99430: Stage 1 Security section CR	2		
3GPP T2, Helsinki	06Sep99	T2-99725: LS to WAP Forum on Support of root keys storage on SIM for MExE Release 99	1		
3GPP T2, Helsinki	06Sep99	T2-99727: Draft LS to S3 on MExE security	1		
3GPP T2, Helsinki	06Sep99	T2-99729: LS to WAP EFI	1		
3GPP T2, Helsinki	06Sep99	T2-99730: A brief guide to certificate formats	0		
3GPP T2, Korea	06Oct99	T2-99803: Discussion of pros and cons of storing certificate descriptors on SIM in one CDF or three	1		
3GPP T2, Korea	06Oct99	T2-99806: Proposal for use of same certificate for Administrator and operator roles	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99065: CR to 23.057 to re-organise security section	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99066: CR to 23.057 on APIs (not treated in Tampere) next meeting	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99067: Converged certification requirements for WAP and MExE	0		
3GPP T2 SWG1, Tampere	15Jul99	T2X99068: Provisioning certificates for WAP and MExE	0		
3GPP T2 SWG1, Tampere	15Jul99	T2X99071: CR to 23.057 to re-organise security section II	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99072: CR to 23.057 to re-organise security section III	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99087: revised T2X99071 - CR to 23.057 to re-organise security section II	1		
3GPP T2 SWG1, Tampere	15Jul99	T2X99090: revised T2X99072 - CR to 23.057 to re-organise security section III	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99106: CR to 23.057 on User Preference permissions	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99107: CR to 23.057 on permissions for actions not listed in the security table	0		
3GPP T2 SWG1, Newbury	11Aug99	T2X99109: CR to 23.057 on SIM certificate			
3GPP T2 SWG1, Newbury	11Aug99	T2X99110: Discussion doc on SIM certificate principles	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99111: LS to SMG9/T3 and accompanying CR to 11.11	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99112: LS to SUN on User Preferences	0		

3GPP T2 SWG1, Newbury	11Aug99	T2X99115: LS to SMG9, T3, SMG9 ad hoc on WAP-SAT interaction work item, on indication of terminal MExE capabilities in SAT TERMINAL PROFILE function	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99124: CR to 23.057 on SIM certificate (update of tdoc 109)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99125: LS to SMG9/T3 and accompanying CR to 11.11 (update of tdoc 111)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99126: LS to WAP Forum on SIM card support of MExE	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99129: LS to SMG9, T3, SMG9 ad hoc on WAP-SAT interaction work item, on indication of terminal MExE capabilities in SAT TERMINAL PROFILE function	1		
3GPP T2 SWG1, Newbury	11Aug99	T2X99131: CR to 23.057 on SIM certificate (update of tdoc 124)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99133: LS to SMG9/T3 and accompanying CR to 11.11 (update of tdoc 125)	2		
3GPP T2 SWG1, Newbury	11Aug99	T2X99134: CR to 23.057 on SIM certificate (update of tdoc 131)	2		
3GPP TSG SA WG3	Nov99	S3-99416: CR 33.102-027 clarification of re-authentication during PS connections	1	1	
3GPP TSG SA WG3	Nov99	S3-99420: Evaluation of alternatives for sequence number management	2	2	
3GPP TSG SA WG3	Nov99	S3-99424: Optimising sequence number management	2	2	
3GPP TSG SA WG3	Nov99	S3-99425: Data integrity mandatory for UMTS subscribers only	2	2	
3GPP TSG SA WG3	Nov99	S3-99492: Proposed CR to 33.102 section 6.4.3 on USIM triggered authentication and key setting during PS connections	1	1	
3GPP TSG SA WG3	Dec99	S3-99501: CR to section 6.3 of TS 33.102 (security architecture)("L")	2	2	
3GPP TSG SA WG3	Dec99	S3-99502: CR to Annex C of TS 33.102 ("K")	2	2	
3GPP TSG SA WG3	Dec99	S3-99503: CR to Annex F of TS 33.102 ("M")	2	2	
3GPP TSG SA WG3	Dec99	S3-99504: justification of the proposed changes to section 6.3 and Annex F ("j")	2	2	
3GPP TSG SA WG3	Dec99	S3-99505: Adding BAN analysis of 3G authentication to TR 33.902	1	1	
3GPP TSG SA WG3	Dec99	S3-99523: Discussion on authentication algorithm requirements)	1	1	
3GPP TSG SA WG3	Dec99	S3-99535: SQN management options	2	2	
3GPP TSG SA WG3	Feb00	S3-00127: CR to 33.102: Restructuring of section 6.3	0	0	
3GPP TSG SA WG3	Feb00	S3-00128: CR to 33.102: Update of ciphering specification	2	2	

3GPP TSG SA WG3	Feb00	S3-00129: CR to 33.102: Update of data integrity specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00130: CR to 33.102: Interoperation and intersystem handover/change between UTRAN and GSM BSS	2	2	
3GPP TSG SA WG3	Feb00	S3-00131: CR to 33.102: Local authentication and connection establishment	2	2	
3GPP TSG SA WG3	Feb00	S3-00132: CR to 33.102: User identity confidentiality	2	2	
3GPP TSG SA WG3	Feb00	S3-00133 CR to 25.301: Ciphering and Integrity	2	2	
3GPP TSG SA WG3	Feb00	S3-00134 CR to 33.105: Update of ciphering specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00135 CR to 33.105: Update of data integrity specification	2	2	
3GPP TSG SA WG3	Feb00	S3-00136 Discussion on CRs on ciphering	2	2	
3GPP TSG SA WG3	Feb00	S3-00172: Presentation on USECA	1	1	
3GPP TSG SA WG3	Feb00	S3-00193 CR to 33.102 on Cipher key and integrity key lifetime	2	2	
3GPP TSG SA WG3	Feb00	S3-00194 CR to 33.102 on Cipher key and integrity key setting	2	2	
3GPP TSG SA WG3	Feb00	S3-00195 CR to 33.102 HE control over accepting non-ciphered connections	1	1	
3GPP TSG SA WG3	Feb00	S3-00207 CR078 to 33.102: Conversion functions	2	2	
3GPP TSG SA WG3	Apr00	S3-00222: Initialisation of COUNT-I and COUNT-C	2	2	
3GPP TSG SA WG3	Apr00	S3-00251: Review of TS 24.008	1	1	
3GPP TSG SA WG3	Apr00	S3-00253: CR to 33.102: Authentication and key agreement (editorial)	1	1	
3GPP TSG SA WG3	Apr00	S3-00254: CR to 33.102: Authentication and key agreement (minimal)	1	1	
3GPP TSG SA WG3	Apr00	S3-00255: CR to 33.102: Conversion functions for GSM-UMTS interoperation	2	2	
3GPP TSG SA WG3	Apr00	S3-00256: CR to 33.102: 3G-3G Handover	2	2	
3GPP TSG SA WG3	Apr00	S3-00257: CR to 33.102: 3G-2G and 2G-3G Handover for CS services	2	2	
3GPP TSG SA WG3	Apr00	S3-00258: CR to 33.102: Limitation and reduction of the effective cipher key length by the serving network	2	2	
3GPP TSG SA WG3	Apr00	S3-00259: CR to 33.102: Initialisation of synchronisation for ciphering and integrity protection	2	2	

3GPP TSG SA WG3	Apr00	S3-00268: CR to 33.102: Removal of enhanced user identity confidentiality	2	2	
3GPP TSG SA WG3	Apr00	S3-00269: CR to 33.102: Removal of network domain security	2	2	
3GPP TSG SA WG3	Apr00	S3-00275: 3GPP Security/AKA - Requirements and development (Presentation Slides)	1	1	
3GPP TSG SA WG3	May00	S3-00312 Independence of confidentiality and integrity in MAP Layer III and other layer III issues	2	2	
3GPP TSG SA WG3	May00	S3-00368: Replay protection for core network signalling messages	2	2	
3GPP TSG SA WG3	May00	S3-00378: CR to 33.102: Clarification on terminology in user domain	1	1	
3GPP TSG SA WG3	Aug00	S3-00406: CR to 33.102: Re-transmission of authentication request using the same quintet	2	2	
3GPP TSG SA WG3	Aug00	S3-00444: Core network security protocols	2	2	
3GPP TSG SA WG3	Aug00	S3-00445: Key management for core network security	2	2	
3GPP TSG SA WG3	Aug00	S3-00447: Overview of security mechanisms for access security for IP-based services	1	1	
3GPP TSG SA WG3	Aug00	S3-00467: Review of the integrity protection procedure	1	1	