USECA

Project Number	AC 336
Project Title	**USECA: UMTS Security Architecture**
Deliverable Type	Report
Security Class	Public Usage of the Result

Deliverable Number	D02
Title of Deliverable	**Security Features and Requirements for UMTS**
Nature of the Deliverable	Intermediate deliverable
Document reference	AC336/VOD/W21/DS/P/002/1
Contributing WPs	WP 2.1
Contractual Date of Delivery	August 1998 (Y01M06)
Actual Date of Delivery	23rd September, 1998
Editor	Phil Gosset, Vodafone Ltd

Abstract	This report presents the initial work within WP2.1 of ensuring that a comprehensive and coherent set of security requirements and features are defined for UMTS. A comprehensive review of the legal aspects of UMTS security is also given.
Keywords	ACTS, USECA, UMTS, GSM, IMT-2000, Security Requirements, Security Features, legal aspects of security.

Executive Summary

The main objective of WP2.1 is to produce a comprehensive list of UMTS security requirements and features. These lists of features and requirements can be used as inputs to the other USECA work packages and to validate the requirements and features specifications being produced within ETSI. These lists have been produced and were derived from an examination of ETSI UMTS service requirements specifications and other types of document, ITU recommendations and the output of research projects such as ACTS ASPeCT.

It was hoped that these lists could be compared with the ETSI UMTS report on security principles for UMTS, 33.20, [30]. However, 33.20 was found to be unclear in its specification of what was actually required for UMTS as oppose to what should just be considered. A considerable amount of effort was therefore put into developing a document that contained definite requirements only. This is the UMTS Security Requirements specification, ETR 33.21, [31]. The production of 33.21 should be considered a significant and commendable achievement which has been developed with significant input from USECA WP2.1.

The list of security requirements derived from service requirements specifications and other sources was compared with 33.21 to see what requirements are missing from 33.21 and where 33.21 contains requirements that cannot be justified by service requirements. These two sets of requirements will be used to advance the work of developing 33.21.

A comprehensive review of the legal aspects surrounding UMTS security is also given. The legal aspects of establishing a public key infrastructure (PKI), data protection and encryption are examined in particular.

Table of Contents

1 Introduction

This report provides a summary of the work currently performed as part of the Requirements and Features Work Package of USECA. It also describes how this work will be continued to satisfy the stated objectives of this work package.

An introduction to USECA is given in section4.

The objectives of WP2.1 are given in section 5.

The objectives of this deliverable and the approach taken to fulfil the objectives are given in section 6.

Section 7 contains the results of the comparison between the comprehensive lists of security requirements and features for UMTS with the ETSI UMTS Security Requirements specification.

Section 8 details the future non-legal work that will be performed to complete the objectives of WP2.1.

Sections 9 to 12 cover the legal aspects of the security requirements and features for UMTS.

1.1 Contributors

Phil Gosset Editor	Vodafone Ltd The Courtyard, 2-4 London Road, Newbury, Berkshire RG14 1JX, UK Phone: +44 1635 503035 / Fax: +44 1635 506947 E-mail: Phil.Gosset@vf.vodafone.co.uk
Tim Wright	Vodafone Ltd The Courtyard, 2-4 London Road, Newbury, Berkshire RG14 1JX, UK Phone: +44 1635 506456 / Fax: +44 1635 506947 E-mail: Timothy.Wright@vf.vodafone.co.uk

1.2 Document History

Version	Date	Content / Changes
A	14/08/98	First Draft
B	25/8/98	Second Draft for release within Vodafone. Executive Summary and Introduction written. Section 3 to 7 refined.

2 References

2.1 UMTS Reports and Specifications

[1] UMTS 21.01. Universal Mobile Telecommunications System (UMTS); Requirements for the UMTS Terrestrial Radio Access System (UTRA). Version 3.0.1. October 1997.

[2] UMTS 21.02. Universal Mobile Telecommunications System (UMTS); High level requirements relevant for the definition of the UMTS Terrestrial Radio Access UTRA concept. Version 3.0.0. April 1998.

[3] UMTS 21.06. Universal Mobile Telecommunications System (UMTS); O&M Requirements for the UMTS, Version 3.0.0. April 1998

[4] UMTS 22.01. Universal Mobile Telecommunications System (UMTS); Service aspects; service principles. Version 3.2.1. January 1998.

[5] UMTS 22.05. Universal Mobile Telecommunications System (UMTS); Service and service capabilities. Version 2.0.0. March 1998.

[6] UMTS 22.07. Universal Mobile Telecommunications System (UMTS); Terminal and smart card concepts. Version 2.0.2. March 1998.

[7] UMTS 22.10. Universal Mobile Telecommunications System (UMTS); Service aspects of UMTS Terminals and IC Cards. Version 0.0.4. April 1997.

[8] UMTS 22.15. Universal Mobile Telecommunications System (UMTS); Service aspects: Charging and Billing. Version 1.2.2. December 1997.

[9] UMTS 22.20. Universal Mobile Telecommunications System (UMTS); Service Management. Version 0.0.3 April 1997.

[10] UMTS 22.24. Universal Mobile Telecommunications System (UMTS); Charging and accounting mechanism. Version 2.0.0. March 1998.

[11] UMTS 22.25. Universal Mobile Telecommunications System (UMTS); Quality of service and network performance. Version 2.0.0. December 1997.

[12] UMTS 22.60. Universal Mobile Telecommunications System (UMTS); Mobile multimedia services including mobile Intranet and Internet services. Version 2.0.0. February 1998.

[13] UMTS 22.70. Universal Mobile Telecommunications System (UMTS); Virtual Home Environment. Version 2.0.0. March 1998.

[14] UMTS 22.71. Universal Mobile Telecommunications System (UMTS); Automatic establishment of roaming relations. Version 2.0.0. March 1998.

[15] UMTS 22.75. Universal Mobile Telecommunications System (UMTS); Advanced addressing. Version 2.0.0. March 1998.

[16] UMTS 22.77. Universal Mobile Telecommunications System (UMTS); Service aspects. Version 0.0.3. December 1997.

[17] UMTS 22.80. Universal Mobile Telecommunications System (UMTS); UMTS relationship to other standards. Version 2.0.1. December 1997.

[18] UMTS 23.01. Universal Mobile Telecommunications System (UMTS); General UMTS Architecture. Version 0.2.0, November 1997.

[19] UMTS 23.05. Universal Mobile Telecommunications System (UMTS); Network Principles. Version 0.10.0. September 1997.

[20] UMTS 23.10. Universal Mobile Telecommunications System (UMTS); UMTS Access Stratum – Services and Functions. Version 0.5.0. January 1998.

[21] UMTS 23.20. Universal Mobile Telecommunications System (UMTS); Evolution of the GSM platform towards UMTS. Version 0.3.1. March 1998.

[22] UMTS 23.30. Universal Mobile Telecommunications System (UMTS); Iu Principles. Version 0.1.1. November 1997.

[23] UMTS 23.60. Universal Mobile Telecommunications System (UMTS); Framework of network functions to support multimedia services in UMTS. Version 0.3.0. June 1997.

[24] UMTS 25.01. Universal Mobile Telecommunications System (UMTS); Description of the selected UTRA concept. Version 0.5.6. May 1998.

[25] UMTS 27.00. Universal Mobile Telecommunications System (UMTS); Principles for handling of data services in the UMTS. Version 1.3.1. June 1997.

[26] UMTS 30.01. Universal Mobile Telecommunications System (UMTS); Baseline document – Positions on UMTS agreed by SMG. Version 3.3.0, March 1998.

[27] UMTS 30.04. Universal Mobile Telecommunications System (UMTS); Definition of the limited number of UTRA concepts. Version 3.0.0.

[28] UMTS 30.06. Universal Mobile Telecommunications System (UMTS); UTRA concept evaluation report. Version 3.1.0.

[29] UMTS 30.20. Universal Mobile Telecommunications System (UMTS); Technical characteristics, capabilities and limitations of mobile satellite systems applicable to the UMTS. Version 3.1.0

[30] UMTS 33.20. Universal Mobile Telecommunications System (UMTS); Security Principles. Version 0.5.0. April 1998.

[31] UMTS 33.21. Universal Mobile Telecommunications System (UMTS); Security Requirements. Version 0.1.3. July 1998.

[32] UMTS 33.22. Universal Mobile Telecommunications System (UMTS); Security Features. Version 0.1.0. July 1998.

[33] UMTS 33.23. Universal Mobile Telecommunications System (UMTS); Security Mechanisms. Version 0.1.0. July 1998

ITU-T Recommendations

[34] ITU-R Recommendation M.1078, Security principles for IMT-2000. (1994)

[35] ITU-R Recommendation M.1223, Evaluation of security mechanisms for IMT-2000. (1997)

Informative References

[36] Security principles for the Universal Mobile Telecommunications System (UMTS), ETR 09.01, Version 3.0.0, June 1996

[37] UTRAN Architecture Description, Stage 2 version 0.0.4, Tdoc SMG2 UMTS-ARC 081/98, June 1998.

[38] USECA, UMTS SECurity Architecture, AC336, Technical Annex, Part A, Issue 1 (Year 1), 23rd January, 1998

[39] LINK PCP, 3GS3, Technical Report 1: “Security Features for Third Generation Systems”, February 1996.

3 Abbreviations

Abbreviations and acronyms are usually written in full at their first occurrence in the text and in titles. For abbreviations and acronyms for GSM we refer to [01.04], other abbreviations are listed below:

IP	Internet Protocol (IP)
MAP	Mobile Application Part (GPRS)
UIM	User Identity Module (IMT-2000)
UMTS	Universal Mobile Telecommunication Service
USIM	User Services Identity Module (UMTS)
UTRAN	UMTS Terrestrial Radio Access Network (UMTS)

4 USECA

4.1 Overview

The communications industry is developing a strategic vision of the next generation of digital mobile systems referred to in Europe as the Universal Mobile Telecommunications System (UMTS). While the concept of UMTS has been around for a long time it is only recently that work on UMTS has gained momentum, and interest within the industry has increased. An indication of this was the formation of the UMTS Forum, an association of telecommunications operators, manufacturers and regulators, to promote the work on UMTS; another indication has been the increased activity in the pertinent standards groups.

According to the UMTS Baseline Document [26], the ETSI UMTS Phase 1 standard is to be completed by the end of 1999. Both the completion of the standard by this date and the development and testing of products in the remaining time-span are quite ambitious goals. This is in particular true for UMTS security.

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 ground-breaking work has been 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 is still a long way to go to establish a security architecture covering all relevant aspects of security; to ensure that the ETSI UMTS security standards will be completed on time, to enable manufacturers to start product development and to enable operators to plan their UMTS networks. This is partly due to the fact that the specification of UMTS in areas other than security had not been progressed enough so that security for UMTS could not be specified in all the necessary detail. But recent progress in these other areas has meant that there is a danger that the specification of security may be lagging behind. It is therefore considered of high importance to take on the task of resolving the problems in UMTS security that may hinder the timely introduction of UMTS.

To aid the establishment of the UMTS security architecture, this project USECA, 'UMTS Security Architecture' has been initiated. Its stated main objective is:

- to ensure that a viable and complete UMTS security architecture is developed as a basis for standardisation by ETSI.

To achieve this main objective, it has been separated into the following sub-objectives:

- to provide a focal point for UMTS security work;
- to provide a sound and validated technical basis for the definition of UMTS security standards by ETSI;
- to build on the work of and collaborate with relevant ACTS projects (in particular with FRAMES) to provide the required security expertise;
- to review the security requirements arising from the set of services defined for UMTS and define a comprehensive set of security features for UMTS;
- to define a comprehensive set of security mechanisms, protocols and procedures (with the exception of encryption algorithms) for UMTS;
- to define a complete functional and physical security architecture for UMTS;
- to define a public key infrastructure for UMTS;
- to define the security features and procedures involving the USIM;
- to validate critical concepts in demonstrators.

It should be stated here that, since USECA began, the desire to meet these ambitious UMTS timescales has led to a definition of Phase 1 UMTS that contains a set of requirements that is significantly less than that envisaged by the studies leading up to UMTS . Phase 1 UMTS will largely be based on GSM Phase 2+ release 99, with the fundamental difference being that UMTS will support high bit rate bearer services with the notion of negotiated traffic and QoS characteristics. In particular it shall support bursty and asymmetric traffic in an efficient way. This shall allow UMTS Phase 1 to support interworking with single- and multi-media N-ISDN and IP applications.

Although much current standards work is looking purely at Phase 1 UMTS, USECA will continue to concentrate on the full UMTS Security Architecture.

4.2 Technical Approach

The work on UMTS security in the project has been divided into the following strands:

Security features and requirements: The purpose of this strand is to define a complete and coherent list of UMTS security requirements, and from there to define a suggested list of security features that meet the requirements.

Security mechanisms: Mechanisms to implement the security features will be investigated, and where appropriate, developed and standardised.

Security architecture: A stable UMTS architecture was not available at the time previous projects were active. Therefore, the security mechanisms available from these previous activities could not be integrated into a UMTS security architecture. In addition, there are new concepts that are introduced in UMTS which were not available in GSM and whose impact on security has not yet been studied. Examples of this are macrodiversity and a new air interface. The new air interface, in particular, will be studied from a security point of view. The air interface is expected to have considerable impact on the security mechanism for the provision of confidentiality. This is just one of many examples where the work on security mechanisms and on security architecture are mutually dependent. Therefore, there will have to be close co-operation between the corresponding activities.

Public key infrastructure: If public key based security mechanisms are to be used in UMTS then an appropriate public key infrastructure is required. The infrastructure will consist of a network of Trusted Third Parties. The project will propose a PKI architecture for UMTS.

The USIM: The USIM is a key component of UMTS security. More flexibility regarding the use of security mechanisms will require a new approach to the interface between the USIM and the terminal.

Terminal security: This work will address the issues related to the terminal side of the interface with the USIM, as well as the issue of how to bar stolen or cloned equipment.

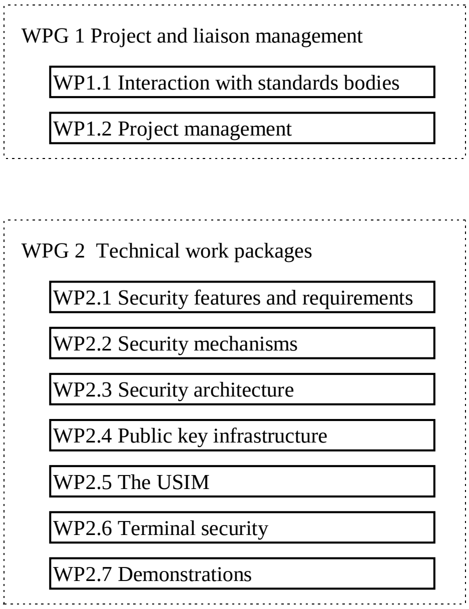
Demonstrations: Critical concepts developed in the USECA project will be validated in a demonstration that focuses on mobile/USIM interaction.

Standardisation: Close collaboration with standardisation bodies is needed. This collaboration will be ensured by the fact that the project partners will also work in the relevant ETSI groups. The most important group is ETSI SMG 10. The project will provide a sound and validated technical basis for the definition of UMTS security standards by ETSI.

Collaboration with other ACTS projects: A number of relevant ACTS projects are working on issues concerning various parts of the UMTS architecture, but do not address security issues. The closest collaboration is expected with the FRAMES project.

4.3 Work breakdown structure

The work of the project is organised in work packages which are grouped into two work package groups, as illustrated in Figure 1



WPG 1 Project and liaison management

- WP1.1 Interaction with standards bodies
- WP1.2 Project management

WPG 2 Technical work packages

- WP2.1 Security features and requirements
- WP2.2 Security mechanisms
- WP2.3 Security architecture
- WP2.4 Public key infrastructure
- WP2.5 The USIM
- WP2.6 Terminal security
- WP2.7 Demonstrations

Figure 1: USECA Work Breakdown Structure

Work package group 1 is concerned with the external relations of the project and with management at the project level and at the work package level. In particular, management has to ensure that the work in work package group 2 is closely co-ordinated among the work packages. In work package group 2, the main technical work is done.

This document falls within the content of WP2.1, Security features and requirements.

5 Work Package 2.1 – Security Requirements and Features

5.1 Introduction

As has been stated above, the definition of the Security Requirements for UMTS by ETSI has been static for some time whilst the Architecture and Services work has advanced. However, whilst ETSI (SMG10) have not been progressing the work, work has been continuing elsewhere in SMG, and in other bodies such as the ITU , such that there is now a number of sources for these requirements. Therefore, before the issues surrounding Security Features and Requirements can be addressed, the existing **requirements** and **features** had to be collected and compiled into a single set of documents. These requirements and features were then checked for aptness and coherency.

In addition to the above, the security implications of proposed UMTS **services** must be considered. The first part of this work is to analyse the service creation environment to see whether any additional security requirements exist. An analysis of the security requirements of any proposed services shall then be performed. This will constitute the majority of the remaining work.

The lists of security features and requirements contained within existing documents and implied by UMTS service requirements specifications has been compared with security requirements and features as defined within ETSI SMG10. This has been done to validate the standards produced by SMG10. This could only be started once an initial draft of the Security Requirements and Features list had been completed.

Another task of this strand is to communicate the full set of requirements *and* any changes that are made to it to all other parts of the projects. In addition, results may be obtained from the other parts of the project that could qualify or potentially conflict with existing requirements and features. These results will be incorporated within the maintained lists of requirements and features.

Another study that will be part of this strand is to look at the requirements imposed by the Satellite component of UMTS. The results of this study will be incorporated into the maintained lists.

There is a further component of the work package related to legal aspects. The proposed security features and services will be examined from a legal point of view and guidelines for the work of USECA, and for UMTS security as a whole, produced.

All relevant results obtained from this work package shall be passed onto ETSI (SMG 10) for consideration.

D02 – Security features and requirements

6.1 *Objectives as originally specified*

The objectives of Deliverable D02 as specified in [38] are:

- To collate and maintain an exhaustive list of security requirements and features
- To collate a list of UMTS services which necessitate additional security requirements
- To study the security implications of the proposed services
- To study the security implications of the satellite component

D02 as specified in [38] is also to contain guidelines from a legal point of view for those developing security features for UMTS. These have been produced as a result of activity A2.1.3.

The list of security requirements and features was to be compiled by comparing existing UMTS relevant specifications and requirements from various sources, such as ETSI, ITU, ACTS etc., against the requirements given in the baseline document, UMTS 33.20 'UMTS Security Principles' [30]. This activity was to generate an exhaustive list of Security Requirements and Features for UMTS.

In parallel, a study was to be made of the relevant UMTS service specifications [22.01, 22.15 etc.], and propose which of the services necessitate additional security requirements, and thus will need provision within the UMTS security architecture.

ETR UMTS 33.20 was then reviewed to see if the features defined therein satisfy the security requirements of the identified UMTS services. If this were found not to be the case, then the type of security features required would be investigated and specified. At the same time, an overall review of ETR UMTS 33.20 was to be made to ensure that the proposed features are still relevant.

The results of this activity would be an exhaustive list of Security Requirements and Features, and a preliminary report listing both the UMTS services with their associated security requirements, and the security features to satisfy these requirements. Indications were to be provided of the UMTS services to which the features should be applied.

6.2 *Production of D02 in practice*

The original plan for D02 and WP2.1 was followed in principle. However, adjustments had to be made because of the poor state of the UMTS Security Principle document, [30].

6.2.1 Production of "Security Requirements Specification"

In the above, it was assumed that the Security Principles document ETR 33.20 [30] would be used as a basis for all of this work. However, on reviewing this document, it was found to be unusable as a baseline document, as it was poorly structured with no clear focus. The document contained security requirements, but also much discursive text, and it was unclear what were requirements and what was discussion and comment.

Before any of the USECA objectives could be met, indeed, before UMTS security as a whole could proceed, a new baseline document had to be created which could be used as a basis for any security work that would be carried out in UMTS. This document was, as far as possible, to contain requirements only, with the minimum of discussion and preamble.

Therefore, an initial task of this work package was to take the lead within SMG10 in generating such a document from the current ETR 33. 20 [30]. This was done by firstly converting discussion in [30] that contained implied requirements into explicit requirements, and removing all other discussion text. Next, the system assumptions and role models were updated and the threats and requirements were re-ordered following the approach adopted in the LINK project [39] for ordering of threats and requirements . The resulting document, ETS 33.21, ‘Security Requirements’ [31], is included as an appendix to this deliverable. An introduction to the document is given in section 7.1.1.

[31]has been well received within SMG10 as a considerable improvement on [30]as a basis for subsequent development of UMTS security, and should be seen as a significant aspect of WP2.1 and a significant contribution by USECA to UMTS security as a whole.

6.2.2 Production of list of security requirements and features

The first task undertaken was the production of the comprehensive Security Requirements List and Security Features List from the ETSI UMTS specifications, and the ITU IMT-2000 specifications. The documents used were the latest available, and are given in the references[1]to [39].

The resulting Requirements list contains security requirements stated explicitly and implicitly within the ETSI UMTS documents and also explicit security requirements stated within ITU documents on security for IMT-2000. The list also contains system requirements that will form the context of UMTS security (such as the requirement for UMTS to support both connection-orientated and connectionless services). A similar list of “system requirements” is given in the “Security context” section of 33.21, [31].

The resulting Features list was forwarded to the editor of UMTS 33.22, 'Security Features' [32].

6.2.3 Comparison of security requirements list and Security Requirements Specification

The lists, once compiled, were to be compared against UMTS 33.20, but as stated above, it was found to unusable for this task.

Therefore, to conduct a useful comparison, it was quickly realised that a stable and useable baseline document should be produced. This realisation led to the majority of the time spent in the early part of this project being concerned with the production of the new Security Requirements document [31]. This new document has yet to be approved by SMG, but as progress has to be made, the latest draft, version 0.1.3, was used as the basis of the rest of the work. 33.21 is expected to be approved at SMG plenary #28.

Once a version of [31] that could be used as the basis of the study was defined, the list of Requirements and Features derived from examination of service specifications was taken and compared with [31]. The list of Requirements was thereby divided into three types:

a) requirements that were on the list and were already in UMTS 33.21 – these are presented in [31] in section 7.2 of this document, which also includes requirements of type (c)

b) requirements that were on the list, but not in 33.21, i.e. security requirements that arise from defined service requirements which have not yet been incorporated into 33.21. These are listed in section 7.3.

c) requirements that were in 33.21 but not present on the list, i.e. requirements generated as part of the production of 33.21 which cannot be justified by service requirements. This does not mean these requirements are superfluous, but this is a possibility which should be examined for each requirement. These requirements are given in section 7.4.

(Following on from D02, these Lists shall be continuously reviewed against both [31]and the Security Features specification, [32], and also against the UMTS Specifications and Requirements. It is hoped that these Lists will either eventually be absorbed into the appropriate Specification, [31]or [32], or, if not required, will be removed from the original source.)

6.2.4 Satellites

Currently, there has been little progress made with the satellite component of UMTS. There is a general guidance document, [29], and some general security principles in 33.20, [30]. This lack of specification has meant that within [31]satellites can only be mentioned within the system assumptions section.

ETSI have stated that for the present, a satellite access interface will not be standardised (the UTRAN is the only new access interface to be standardised). This, along with the fact that "2nd generation" satellites systems (e.g. Iridium, Globalstar) are not yet in operation, mean that one should not be surprised that progress on S-UMTS has been slow.

Once some progress has been made, the proposals will be considered within WP2.1.

6.2.5 Service Security Requirements

D02 as originally specified should have contained a review of the additional unspecified security requirements and features implied by specified UMTS services, and also the security required by the Service Creation Environment that was to have been a significant new aspect to UMTS.

The Service Creation Environment has not been specified to any degree that can be used within USECA. The reduction in the "radicality" of UMTS as compared to GSM casts some doubt on whether the Service Creation Environment will be implemented in the foreseeable future or not. Until it is clear that the Service Creation Environment will form part of UMTS, it will not be examined. This goal of D02 has therefore not been realised.

A formal review of the implicit but unspecified security requirements of UMTS services could not be performed, because of the time required to produced 33.21. However, the "System Assumptions" section of 33.21 was expanded based upon the service set given in 22.01, [4]. The additions were:

- to state that UMTS security must cover a system providing both interactive (such as voice) and "distributive" (i.e. store and forward services, data download) services. GSM security is based on the assumption that most traffic will be voice. That assumption cannot be made with UMTS.
- To extend the interworking requirements of UMTS to cover ATM and IP

7 Results

7.1 UMTS ETS 33.21, 'Security Requirements'

The latest version (1.0.0 at time of writing) of UMTS 33.21, the UMTS Security Requirements Specification ([31]) was a significant part of the D02 work within WP2.1. . At time of writing it had not been approved by SMG10 or by the full SMG plenary. It is to go to SMG#27 (November 1998) for information and to SMG#28 (February 1999) for approval.

As USECA contributed significantly to the production of 33.21, [31],it seems appropriate to introduce the document here. The content of [31] is as follows:

Following on from the usual introductory sections, section 4 outlines the general objectives for UMTS security. These have largely been taken from 33.20, [30], with the significant change that UMTS security should be "better" than that of existing fixed and mobile networks, instead of "at least as good as".

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

Section 6 contains 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 is the most important part of 33.21 and contains the requirements for UMTS security. Following the approach adopted in the LINK project [39], the requirements are divided by 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 contains 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.

7.2 Security requirements from 33.21

The requirements listed in 33.21, [31], are given below. Not including the requirements listed in section 7.3, it should be taken as the list of requirements which appear both in the Requirements and Features lists and in[31]. The heading numbering within 33.21 is used,.

“7 Security requirements

The purpose of this clause is to provide a list of security requirements for UMTS. The security requirements form a natural link between the security threats to the system and the corresponding security features supported by the system to counteract these threats. More precisely, requirements can be derived from threats, and then features may be introduced to satisfy these requirements.

The requirements have been defined with reference to the roles played by the various entities involved in UMTS and the relationships between them, as described in [22.01] and [23.01].

In 7.1 security requirements that benefit users of the UMTS system are listed.

In 7.2 security requirements that benefit providers of the UMTS system are listed.

In 7.3 security requirements that benefit other parties are listed.

7.1 User security requirements

This subclause identifies security requirements that benefit users of the UMTS system. In this respect the requirements are said to be “owned” by users. The requirements are split into the following categories, which are defined in the following subclauses:

- USIM
- User access to UMTS services
- Provision of UMTS services to users
- Lawful interception
- Data protection

7.1.1 USIM

R1a It shall be possible to control access to separate USIMs stored on the same IC card. In particular, access to a specific USIM by unauthorised home environments should be prevented.

R1b It shall be possible to control access to USIMs and other non-UMTS applications stored on the same IC card. In particular, it shall be possible to support multi-functionality whereby two applications on the same IC card interact in a secure manner. For example, interactions between an electronic purse application and a USIM that is paying for telecommunications services using electronic cash.

R1c It shall be possible to control access to the USIM so that it can only be used by the user to whom it was issued or by parties explicitly authorised by the user.

R1d It shall be possible to protect the confidentiality of certain data stored in the USIM, in particular user identity and authentication information.

R1e It shall be possible to detect unauthorised modification of data stored in the USIM, in particular authentication information.

R1f The physical and logical security of the USIM shall not depend on whether it is implemented in a separate IC card or whether it is integrated with the ME.

R1g It shall be possible for the USIM to ensure that the originator of executable code downloaded to the USIM can be authenticated

R1h It shall be possible for the USIM to ensure that executable code downloaded to the USIM has not been subject to unauthorised modification.

7.1.2 User access to UMTS services

R2a It shall be possible for users to be able to authenticate serving networks and home environments before accessing UMTS services.

R2b It shall be not be possible for multi-user calls on one terminal to jeopardise the security of individual calls.

NOTE: Regarding R2a, consideration needs to be given to whom the user needs to authenticate and under what circumstances. This will depend on what data the serving networks and home environments can read from or write to the ME or USIM, or whether the telecommunications services supplied by different providers could effect the charges to the user.

7.1.3 Provision of UMTS services to users

R3a It shall be possible to protect the confidentiality of user and signalling traffic, particularly on radio interfaces.

R3b It shall be possible to detect unauthorised modification of user and signalling traffic, particularly on radio interfaces.

R3c It shall be possible to provide location confidentiality for users particularly on radio interfaces.

R3d It shall not be possible to identify the user(s) associated with a particular communication by eavesdropping on user or signalling traffic.

R3e It shall not be possible to usurp a service already provided to a user.

- R3f It shall be possible for a user to be able to remain anonymous towards the called party or any party to which the call is forwarded.

7.1.5 Lawful interception

R4a It shall be possible to monitor and register every interception and every attempted interception, whether lawful or otherwise, in accordance with the national law. This shall apply to devices and/or via interfaces placed by the serving networks or home environments at the disposal of the national law enforcement agencies according to national law, and intended solely for lawful interception purposes

NOTE: Lawful interception has to be realised according to national legislation and the requirements given in:

- Official Journal of the European Communities, 99/C329/01: Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications [LAWF1].
- ETR 331 Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications - Requirements of the law enforcement agencies. [LAWF2].

7.1.6 Data protection

R5a It shall be possible to detect unauthorised modification of signalling and management data relating to users which is stored or processed by a provider

R5b It shall be possible to protect the confidentiality of signalling and management data relating to users which is stored or processed by a provider

NOTE: Data protection has to be realised according to national legislation implementing directives:

- 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the privacy in the telecommunications sector.
- 95/46/EC of the European Parliament and of the Council of 24 October 1995 n the protection of individuals with regard to the processing of personal data and on the free movement of such data.

7.2 Provider security requirements

This clause identifies security requirements that benefit providers of the UMTS system. In this respect the requirements are said to be "owned" by providers. The term "provider" encompasses both home environments and serving networks, however, home environments and serving networks will be specifically named within the requirements, if appropriate.

The requirements are split into the following categories, which are defined in the following subclauses:

- USIM
- User access to UMTS services
- Provision of UMTS services to users

7.2.1 USIM

R6a A valid USIM shall be required to access UMTS services

R6b It shall be possible to prevent the use of a particular USIM to access UMTS services.

R6c It shall be possible to control access to a USIM. For instance some data may only be accessible by an authorised home environment.

R6d It shall be possible to download executable code to a USIM in a secure way.

R6e It shall not be possible to access data in a USIM that is only intended to be used within the USIM, e.g. authentication keys and algorithms.

R6f If an IC card contains more than one USIM (to access services from different home environments) then different home environments shall only have access to the USIMs of their own users.

R6g If an IC card contains more than one USIM (to access services from different home environments) then security related information (e.g. authentication information) of each USIM shall be protected independently against unauthorised access and modification.

7.2.3 User access to UMTS services

R7a It shall be possible for providers to authenticate users to prevent intruders from obtaining unauthorised access to UMTS services by masquerade.

R7b It shall be possible to authenticate users during service delivery.

R7c It shall be possible for a home environment to authorise the use of services to a user requesting access.

R7d It shall be possible for a home environment to cause an immediate termination of all services provided to a user by that home environment.

R7e It shall be possible to prevent the unauthorised use of radio resources by users (e.g. by misuse of priorities).

NOTE: Regarding R7a, consideration needs to be given to who need to authenticate the user and under what circumstances.

7.2.4 Provision of UMTS services to users

R8a It shall be possible to protect the confidentiality of signalling traffic, particularly on radio interfaces.

R8b It shall be possible to detect unauthorised modification of signalling traffic, particularly on radio interfaces.

R8c It shall be possible for any receiving network to be able to authenticate the origin of user and signalling traffic, particularly on radio interfaces.

R8d It shall be possible to prevent intruders from restricting the availability of services by logical means.

R8e It shall be possible for a provider to verify that a user has been authenticated using a particular authentication mechanism.

R8f It shall be possible to detect and prevent the fraudulent use of services.

NOTE: Regarding R8d, preventing intruders from restricting the availability of services by physical means is outside the scope of this specification.

NOTE: Regarding R8f, alarms will typically need to be raised to alert providers to security related events. Audit logs of security related events will also need to be produced.”

Annex 1: Items for further study

A.1 End-to-end security

1. It shall be possible to inform users about the status of security within the network, and in particular end-to-end security, an indication of security level and state shall be provided to the user.

2. It shall be possible for providers to offer an end-to-end user traffic confidentiality service to users. Access shall be subject to national regulation.

3. It shall be possible to adapt security mechanisms that allow providers to offer end-to-end security under different circumstances.

4. It shall be possible to allow the user to control end-to-end security, security functions shall be selectable and adaptable to the circumstances encountered.

Needs to be discussed further together with other supplementary or end-to-end security services for user traffic. More work is required on the extent of standardisation of end-to-end encryption.

A.2 Encryption in the access network

[Editor: TBA]

A.3 Charging

1. It shall not be possible for unjustified charges to be imposed on users.

2. It shall be possible to protect the confidentiality of charging and billing information.

3. It shall be possible to detect unauthorised modification of charging and billing information.

4. It shall be possible for providers to be able to measure and record chargeable events

and statistics in a secure manner.

5. It shall not be possible for a user to repudiate charges.
6. It shall be possible for a provider to limit charges incurred by users.
7. It shall be possible for a serving networks to limit charges incurred by home environments and other providers.
8. It shall be possible to allow providers to secure charges towards other providers
9. It shall be possible for users to obtain accurate and reliable information about accumulated charges.
10. It shall be possible for users to be able to obtain accurate and reliable information about applicable tariffs used to determine subsequent call charges.
11. It shall be possible for users to pay home environments anonymously.

What level of incontestable charging is required

We should find out if there is a firm requirement for anonymous payment or not. Need to define what anonymous payment actually is. There are two different types: anonymous to network and anonymous to application provider (i.e. part of end to end security)

A.4 Terminal security

1. It shall be possible to control access to the ME so that it can only be used by the owner, or by a party explicitly authorised by the owner.
2. It shall be possible to ensure the privacy and integrity of user-related data stored in the ME.
3. It shall be possible for the ME to ensure that the originator of mobile software can be authenticated.
4. It shall be possible for the ME to ensure that mobile software has not been subject to unauthorised modification.
5. It shall be possible for providers to prevent certain mobile equipment from being used to access UMTS services.
6. It shall be possible to detect and prevent the use of mobile equipment which is not approved but is otherwise acceptable for use.
7. It shall be possible to prevent the use of faulty mobile equipment.
8. It shall be possible to detect, prevent and track the use of stolen mobile equipment.
9. It shall be possible to detect and prevent the use of cloned mobile equipment
10. It shall be possible to deter the theft of MEs.
11. It shall be possible to uniquely identify an ME. This identity shall be unalterable.
12. Any system used to register the status of mobile equipment, for example, an EIR, shall be securely managed.

A.5 Mutual authentication

Should the user authenticate the access network or serving network? If the access network is to be authenticated then this implies integrity protection throughout entire access network? Is it necessary that the user be able to authenticate the network at any time? For packet data authentication at call set up it is meaningless since there is no explicit call set up.

A.6 Non repudiation of user traffic

1. It shall be possible for an originator of user traffic to be able to provide that the information was received by the recipient.
2. It shall be possible for a recipient of user traffic to be able to provide that the information was sent by the originator.

Should non-repudiation be standardised or left at the application level? Non repudiation of the delivery of user traffic should definitely be outside scope of standards, non repudiation of network/service access however may be standardised if incontestable charging is a requirement.

A.7 Provider internal security

1. It shall be possible to protect the confidentiality of management data related to a provider and stored by another provider.
2. It shall be possible to detect unauthorised modification of management data related by a provider and stored by another provider.
3. To allow the home environment to protect information related to persons within his organisation:

- Home environments databases shall be provided with access control
- All forwarding and processing of personal information shall be logged

These requirements may be outside the scope of standards

A.8 Emergency calls

1. It shall be possible for users to make calls to the emergency services using a ME without a USIM being present.

We should discuss whether we want this requirement to remain. It introduces security problems and the service requirement is unclear. Add to this that around 50% of networks do not allow SIM-less calls in GSM.

A.9 Interworking security

1. It shall be possible for user to be offered the same level of protection when the serving UMTS network is interconnected with other non-UMTS networks.
2. It shall be possible to protect provider resources when interconnection with other non-UMTS networks exists.

Some other networks may have their own security architectures. How will the UMTS security architecture interwork with these?

A.10 Management of security

1. It shall be possible to provide a fall-back mode of security in case of network degradation.
2. It shall be possible to inform providers about the status of security within the network
3. It shall be possible that the mechanisms used to manage security features are secure from attack.
4. It shall be possible for a home environment to be able to create, update, retrieve, and delete information related to the security aspects of UMTS in a secure manner.
5. It shall be possible that the mechanisms used to manage network configuration are secure from attack.

What is the status of security? What level of security counts as a “fallback”? Are we talking about the use of a previously used cipher key as can be done for GSM? Much more clarification required.

7.3 Those requirements which appear in Requirements List and not in the Security Requirements document

Ref.	Requirement	Source
A.	UMTS networks should be able to authenticate each other.	UMTS 22.01, Version 3.2.1
B.	The SP shall have control of all aspects of the subscriber and User service profiles.	UMTS 22.01, Version 3.2.1
C.	The UMTS system shall support both connection and connectionless services	UMTS 22.05, Version 2.0.0
D.	It shall be possible to validate the source and integrity of all charging information supplied between entities.	UMTS 22.15, Version 1.2.2
E.	There shall be an authentication procedure between all entities in UMTS that have a commercial relationship.	UMTS 22.15, Version 1.2.2
F.	A multimedia service may involve several parties and connections and therefore flexibility is required in order to add and delete components, resources and parties during a call.	UMTS 22.60, Version 2.0.0
G.	One problem with agents is security, as agents can be used as computer viruses.	UMTS 22.60, Version 2.0.0
H.	The terminal should be able to support activation and deactivation of VHE with appropriate security.	UMTS 22.70, Version 2.0.0
I.	VHE requirements: a) Secure and standardised execution environment for USIM, terminal and network. b) Unique identification of services/software.	UMTS 22.70, Version 2.0.0
J.	Assumes that GSM MAP signalling is secure enough for UMTS	UMTS 22.71, Version 2.0.0
K.	The SP shall be able to resolve the ownership of any USIM to his own or another SP.	UMTS 22.75, Version 2.0.0
L.	Flexibility - Negotiation of bearer service attributes (bearer type, bit rate, delay, BER, up/down link symmetry, protection including none or unequal protection).	UMTS 21.01, Version 3.0.1
M.	UMTS should be able to provide point-to-point and point-to-multipoint (i.e. Broadcast and multicast) communication configurations.	UMTS 27.00, Version 1.3.1
N.	Two general communication modes can be distinguished which may be offered by UMTS data bearer services to teleservices. These are connectionless (CL) and connection orientated (CO) communication.	UMTS 27.00, Version 1.3.1

O.	The ability to support secure Global Cross-standard Roaming should be provided. Security and fraud control must be controlled from the home network wherever you are through the integration and development of MAP, IS41 and INAP signalling protocols.	UMTS 30.01, Version 3.3.0
P.	UMTS should support "Global Multi-Media Mobility" (GMM) Information Society services. Services can be added during a call. Billing must reflect usage and be understandable to the user.	UMTS 30.01, Version 3.3.0
Q.	support of packet data by Internet protocols	UMTS 30.01, Version 3.3.0
R.	automatic establishment of roaming relations	UMTS 30.01, Version 3.3.0
S.	UMTS shall provide for the automatic establishment of roaming relationships between different networks	UMTS 30.01, Version 3.3.0
T.	Handover, for certain services, between UMTS and GSM systems (in both directions) shall be provided.	UMTS 30.01, Version 3.3.0
U.	The requirement in a growing number of countries to be able to locate a Mobile Station in emergency situations makes location services mandatory for UMTS. There are a number of locations mechanism proposed for GSM and UMTS including the use of GPS.	UMTS 30.01, Version 3.3.0
V.	Satellite paths introduce significant delays - signalling must take account of this	UMTS 30.20, Version 3.1.0
W.	IMT-2000 will have an open architecture, based on IN and TMN concepts;	M.1078 (1994)
X.	IMT-2000 will provide a variety of services with a range of bit rates. More than one service may be used simultaneously, and the services and/or their bit rates may vary during communication;	M.1078 (1994)
Y.	An IMT-2000 user has a personal service profile, to which he has direct access. This service profile contains personal data of the IMT-2000 user, and the IMT-2000 user and subscriber have limited ability to modify some of this data. Service profile data include the services subscribed to for the IMT-2000 user by the IMT-2000 subscriber, various subscription options and a range of service parameters	M.1078 (1994)
Z.	The home IMT-2000 service provider role carries responsibility for authentication of the IMT-2000 users and management of user authentication information. The home IMT-2000 service provider may deny the IMT-2000 users/subscribers access to the services under certain circumstances.	M.1078 (1994)
AA.	The home IMT-2000 service providers have roaming agreements with a range of visited IMT-2000 service providers. There will have to be security mechanisms in IMT-2000 such that the home IMT-2000 service provider can openly share information with the visited IMT-2000 service provider, and vice versa.	M.1078 (1994)
BB.	Whatever the category of other network operators, they do not require any call-by-call knowledge of IMT-2000 security related information, and do not	M.1078 (1994)

	participate in the call-by-call IMT-2000 security procedure.	
CC.	IMT-2000 security related information will either: a) Never be passed across these operators' networks, or b) Be protected when passing across them, or c) Be meaningless to them.	M.1078 (1994)
DD.	The IMT-2000 user may wish to have access to his personal IMT-2000 service profile for status information or to modify service parameters. This implies limited real-time interactive access to the service profile data of the home IMT-2000 service provider, and IMT-2000 user authentication is also needed for this feature. Details of this feature are for further study.	M.1078 (1994)
EE.	security features provided for the protection of the IMT-2000 users should be user-friendly and easy to use. They should, as far as possible, be transparent to the users, and should require a minimum of user-interactions on a per call basis;	M.1078 (1994)
FF.	security features provided for the protection of the IMT-2000 users should not significantly increase call set-up times;	M.1078 (1994)
GG.	security features provided for the protection of the IMT-2000 users should work without reduced security during handover and when roaming;	M.1078 (1994)
HH.	it should be possible under controlled circumstances for information over the IMT-2000 bearer channel to be transmitted in the clear. In the event of encryption failure, identified emergency transmissions should be permitted on the clear data channel;	M.1078 (1994)
II.	security features for IMT-2000 should have minimal impact on the user service traffic capacity of the air interface.	M.1078 (1994)
JJ.	it should be very difficult for intruders to obtain IMT-2000 mobile terminal identities and, in particular, terminal authentication information from an IMT-2000 mobile terminal;	M.1078 (1994)
KK.	it should be possible for the IMT-2000 service provider to identify stolen UIMs (they are stolen IMT-2000 mobile terminals if the UIM is integrated in the mobile terminals), and then record and prevent the use of these UIMs (mobile terminals);	M.1078 (1994)
LL.	it should be possible for the IMT-2000 service provider to detect and prevent access to the services by cloned UIMs;	M.1078 (1994)
MM.a	the security mechanisms of IMT-2000 should require the least possible long-distance real-time signalling connections (e.g. in order to avoid international signalling connections at every location update or call when roaming).	M.1078 (1994)
NN.	security keys and possible devices, such as the UIM, distributed to the IMT-2000 users should be easily and securely managed and updated;	M.1078 (1994)
OO.	management of security keys within and between IMT-2000 service providers should be secure;	M.1078 (1994)
PP.	the IMT-2000 service provider should have secure mechanisms to record events associated with IMT-2000 users or subscribers;	M.1078 (1994)
QQ.	it should be very difficult for intruders to impersonate an IMT-2000 service	M.1078 (1994)

	provider in communication with IMT-2000 network operators, and vice versa;	

7.4 Those requirements which appear in the Security Requirements document and not in the Requirements List

No.	33.21 Requirement
R1f	The physical and logical security of the USIM shall not depend on whether it is implemented in a separate IC card or whether it is integrated with the ME.
R3b	It shall be possible to detect unauthorised modification of user and signalling traffic, particularly on radio interfaces. (*only required for M.1078)*
R3c	It shall be possible to provide location confidentiality for users particularly on radio interfaces. (*only required for M.1078)*
R3f	It shall be possible for a user to be able to remain anonymous towards the called party or any party to which the call is forwarded.
R5a	It shall be possible to detect unauthorised modification of signalling and management data relating to users which is stored or processed by a provider (only required for M.1078)
R5b	It shall be possible to protect the confidentiality of signalling and management data relating to users which is stored or processed by a provider (*only required for M.1078)*
R6b	It shall be possible to prevent the use of a particular USIM to access UMTS services. *(but implicitly required by M.1078 requirements on SIM blocking)*
R6e	It shall not be possible to access data in a USIM that is only intended to be used within the USIM, e.g. authentication keys and algorithms.
R6f	If an IC card contains more than one USIM (to access services from different home environments) then different home environments shall only have access to the USIMs of their own users.
R7b	It shall be possible to authenticate users during service delivery.
R7d	It shall be possible for a home environment to cause an immediate termination of all services provided to a user by that home environment.
R8c	It shall be possible for any receiving network to be able to authenticate the origin of user and signalling traffic, particularly on radio interfaces.
R8d	It shall be possible to prevent intruders from restricting the availability of services by logical means.
R8e	It shall be possible for a provider to verify that a user has been authenticated using a particular authentication mechanism.
R8f	It shall be possible to detect and prevent the fraudulent use of services.
A1, 1	It shall be possible to inform users about the status of security within the network, and in particular end-to-end security, an indication of security level and state shall be provided to the user.
A1, 2	It shall be possible for providers to offer an end-to-end user traffic confidentiality service to

	users. Access shall be subject to national regulation.
A1, 3	It shall be possible to adapt security mechanisms that allow providers to offer end-to-end security under different circumstances.
A1, 4	It shall be possible to allow the user to control end-to-end security, security functions shall be selectable and adaptable to the circumstances encountered.
A2	Encryption in the access network - tbd
A3, 1	It shall not be possible for unjustified charges to be imposed on users.
A3, 2	It shall be possible to protect the confidentiality of charging and billing information.
A3, 3	It shall be possible to detect unauthorised modification of charging and billing information.
A3, 4	It shall be possible for providers to be able to measure and record chargeable events and statistics in a secure manner.
A3, 6	It shall be possible for a provider to limit charges incurred by users.
A3, 7	It shall be possible for serving networks to limit charges incurred by home environments and other providers.
A3, 8	It shall be possible to allow providers to secure charges towards other providers
A3, 9	It shall be possible for users to obtain accurate and reliable information about accumulated charges.
A3, 10	It shall be possible for users to be able to obtain accurate and reliable information about applicable tariffs used to determine subsequent call charges.
A3, 11	It shall be possible for users to pay home environments anonymously.
A4, 1	It shall be possible to control access to the ME so that it can only be used by the owner, or by a party explicitly authorised by the owner.
A4, 2	It shall be possible to ensure the privacy and integrity of user-related data stored in the ME.
A4, 3	It shall be possible for the ME to ensure that the originator of mobile software can be authenticated.
A4, 4	It shall be possible for the ME to ensure that mobile software has not been subject to unauthorised modification.
A4, 10	It shall be possible to deter the theft of MEs.
A4, 11	It shall be possible to uniquely identify an ME. This identity shall be unalterable.
A4, 12	Any system used to register the status of mobile equipment, for example, an EIR, shall be securely managed.
A7, 1	It shall be possible to protect the confidentiality of management data related to a provider and stored by another provider.
A7, 2	It shall be possible to detect unauthorised modification of management data related by a provider and stored by another provider.
A7, 3(ii)	To allow the home environment to protect information related to persons within his organisation, all forwarding and processing of personal information shall be logged
A10, 1	It shall be possible to provide a fall-back mode of security in case of network degradation.
A10, 3	It shall be possible that the mechanisms used to manage security features are secure from attack.

A10, 5	It shall be possible that the mechanisms used to manage network configuration are secure from attack.

8 Future Work

Production of the UMTS Security Requirements specification will continue to be part of WP2.1.

The list of requirements that are in the Requirements list but not in 33.21, given in section 7.3of this document, will be input to the process of developing 33.21. Requirements should either be incorporated into 33.21 or, if rejected by SMG10, removed from the source UMTS specification. Also the requirements that exist in 33.21 but not in the Requirements list will be examined to see if these requirements, which cannot be justified by any service requirement, are really required.

There is a constant ongoing activity to examine the ETSI UMTS specifications being developed to see if there are any new documents or new versions of existing documents. These will be used to update both the Requirements List and the Features List, and the lists derived from the comparison of these lists with the Security Requirements specification.

A review of the Satellite component will be made when/if any real progress is made in this area.

9 Legal Issues affecting the security features and requirements for UMTS

The following sections provide an overview of the relevant legislation in Europe affecting the developing UMTS security environment both at Member State level and at EU level.

The overview is divided into three pillars.

Pillar I

The first deals with the use of digital signatures for authentication purposes and the relevant Public Key Infrastructure that governs the use of such signatures[1]. This is important as UMTS foresees the use of public key cryptography to access services, prevent fraud, provide incontestable charging and also facilitate electronic commerce-type applications such as home banking or health service provision. The private key will be stored in a USIM.

Pillar II

UMTS envisages the transfer of not only voice but also data. This data may take the form of user data (e-mails, messages), signalling data (charging and billing) or control data (routing data, network access data). The second pillar examines the Data Protection requirements that effect the transfer of data within a mass user market.

Pillar III

Pillar III looks at the use of cryptography for encryption purposes and examines the relevant laws in Europe that effect this. There are both restrictions on the export and use of cryptography in certain countries. The position on lawful interception is far from clear.

In examining the relevant legal framework in each of these relevant areas, an attempt is made to apply these to the specific UMTS security features and requirements described in the ETSI UMTS (ETR 33.20 and ETS 33.21) documents. However, this report lays only the groundwork for a more in-depth investigation and a forum discussion of the specific problems of UMTS security features and requirements as these arise and develop. The final report will be the product of this continuing and more specific investigation. There is therefore a final section on items for further study as there is in ETS UMTS 33.21.

[1] . The work on PKI will also contribute to D3 as part of WP 2.4, due to be delivered in November.

10 Pillar I - Digital Signatures and PKI

This section is divided into two distinct sub-sections. The first part concerns the legal recognition of digital signatures for authentication purposes in Europe and under the proposed directive. The second part deals with the Public Key Infrastructure as it exists in Germany and Italy and the proposed infrastructures in the UK and Belgium. It also examines the proposed PKI in the Commission draft directive on digital signatures.

Part I - The Legal Recognition of Digital Signatures in Europe

Introduction

UMTS foresees the use of digital signatures, most probably by means of asymmetric cryptography, for security and authentication purposes and possibly for encryption and confidentiality of messages.

Therefore, the recognition of digital signatures and digitally signed electronic documents, and the public key infrastructure necessary to provide the requisite degree of trust when using asymmetric cryptography are important elements of the UMTS framework.

By authentication, we mean:

Data origin authentication

- Integrity of the Contents
- Non-repudiation by the author

There has been some discussion in the forum meetings on whether non-repudiation should be a security feature of UMTS and whether or not it is legally necessary. The definition of 'digital signature' in the German and Italian Laws and the Belgian Bill does not include non-repudiation. Origin authentication and integrity authentication is enough. It is then for the courts to decide whether this is sufficient to guarantee non-repudiation. In practice if the origin and integrity of a message is guaranteed and signed by the unique, uncopiable private key then in practice it will be very difficult for someone signing a document to repudiate the fact that he sent it. This follows as a logical result of the security of the process used and the ability to authenticate both the origin and the integrity of the data. Thus non-repudiation in its own right may not need to be included as a separate feature. As regards non-repudiation of the length of time that someone is on a call in order to ensure incontestable charging, this may require additional attention.

A good authentication tool is:

- Linked to the content of the legal act
- Easy to verify and difficult to forge
- Verifiable as long as the act is of legal importance

The use of public key cryptography with a private key built in to a USIM and the public key certified by a CA satisfies these criteria.

ETSI UMTS Documents

Authentication is required by many of the security features outlined in the ETSI documents. These features are as follows:

Authentication to protect HN and NO resources from fraud

As long as the USIM remains with the rightful owner and the private key cannot be copied or cloned, then a digital signature using the private key that is built into the USIM will protect HN and NO resources. This is directly linked with incontestable charging. If a foreign network is charging the HN as part of a roaming agreement for long distance calls or if the HN is charging the user, then the use of a signature key accompanied with a PIN access should provide adequate evidence for a court that the owner of the public key was indeed the originator of the call.

Authentication to ensure incontestable charging

This is directly linked to the previous paragraph on protection of HN and NO resources.

Non-repudiation of user traffic

This could take the form of preventing (a) repudiation of charge (b) repudiation of user traffic origin in end-to-end communications and (c) repudiation of user traffic receipt. Repudiation of charge is directly linked to the previous two paragraphs. Both (b) and (c) relate to end-to-end communications between users. Non-repudiation of origin can certainly be guaranteed by the use of digital signatures but the non-repudiation of delivery cannot. This poses problems particularly in a distance selling or electronic commerce environment. In common law countries, the rule of contract provides two solutions to when such a contract between distant parties is formed - (a) the 'instantaneous transmission rule' and (b) the 'postal' rule. The first dictates that the contract is formed once the acceptance is received; the second, once the acceptance has been sent. The latter favours consumers as it means the contract is governed by the local jurisdiction. In the Consumer Association's report in September 1997[2], the CA in the UK seems to favour the 'instantaneous transmission rule'. This could operate for Internet based contracts as acceptance is communicated instantaneously, however, acceptance in the form of an e-mail could be more problematic in that (a) the e-mail is transferred through different service providers (b) it may not be read immediately and (c) the sender cannot verify that it has been received. Thus the postal rule would seem to operate more logically in this environment.

In civil law systems[3] the rule is generally that the contract is formed once it has been read or comes to the attention of the distant party. Applying this rule, non-repudiation of delivery of user traffic becomes a very important feature of UMTS and indeed distance selling in general. The offeror would otherwise be able to deny the presence of a contract from the outset. He has to have received it at the very least and furthermore he has to have *seen* it or *have knowledge* of it.

As mentioned above non-repudiation of the user data itself or non-repudiation of origin may not have to be introduced as a separate feature as data origin authentication combined with integrity authentication should suffice to provide for non-repudiation here. Non-repudiation of signalling traffic

See paragraphs 1 and 2.

[2] *Consumer Transactions on the Internet*, September 1997

[3] For example in Belgium see the decision of the Cour de Cassation; Cass, 16 June 1960, Pas. 1960, I, 1960; R.C.J.B. 1962, 303

Integrity of User Traffic

This requirement is from a legal point of view intrinsically entwined with data origin authentication. It is no good verifying the origin of the sender or the recipient if the integrity cannot be guaranteed. If the data can be changed in any way in transit, then, non-repudiation of the contents cannot be achieved.

Integrity of signalling traffic

The same applies here as for user traffic.

Integrity of data stored by network entities

Access to any information stored by network entities should be provided with access control in order to protect the integrity of such data.

Mutual Authentication

One question in the list of items for further study in 33.21 is the need for mutual authentication. Should the user be able to authenticate the access or serving network? If the user will receive downloads to his mobile equipment, then he may want to verify the identity of the network entity sending him the download.

The Legal Recognition of Digital Signatures in Europe

The legal situation in Europe is uncertain. We have two very different laws in Germany and Italy, two draft proposals in Belgium and Denmark and the recent draft directive on digital signatures. This could take up to three years, however, before it is adopted. It is at this stage with the Council and Parliament and the Committees for discussion. The UK DTI has recently adopted a position on PKI.

In the countries where there is no formal recognition of digital signatures, the general principle is one of freedom of contract and means of contract (electronic or otherwise) and a free and open evaluation of evidence. However some laws specifically require contracts in writing and 'hand written signatures' (e.g. for the sale of property). However, this general rule will only apply in closed systems of bilateral contracts and not in open environments such as that envisaged by UMTS.

Overview of National Legislation

Austria

No recognition of digital signatures exists. Some contracts according to the Austrian civil code require a signature in writing. The judge has the discretion as to the probative value of an electronic document but they are unlikely to be classed as 'documentary evidence'.

There have been some developments in the administrative field. A working group has been set up to examine the use of digital signatures here.

Belgium

Article 1341 of the Civil Code still requires a written form with a hand-written signature[4] as evidence for all transactions of monetary value exceeding 15.000 BEF but there are so many exceptions that it can not be considered as the general rule. The most important exceptions are the following:

The provisions of the Civil Code with regard to evidence are of a supplementary nature (droit supplétif):

[4] In the terminology of the Civil Code this is called a "acte sous seing privé" (onderhandse akte).

they only apply when the parties to the transaction do not mention their own evidence rules in the contract[5]. In all disputes between parties evidence is completely free and all means of evidence are accepted. The Civil Code provisions regarding evidence only apply to the evidence of legal transactions and not to the evidence of facts; proof of a fact can be delivered by all means.

If the parties involved do not sign a written document for a transaction of value exceeding 15.000 BEF, each of the parties can use as evidence any document, which originates from the other party to support their side[6].

Neither is a written document with a hand-written signature required when a party can prove that it was impossible for him to establish a written proof of the transaction; 'impossible' in this context also means 'incompatible with the general usage' for the type of transaction involved.[7]

New Bill:

A signature will no longer be restricted to a hand-written signature but can be 'every transformation of data from which proves with certainty the identity of the author and the integrity of the content'. The definition of digital signature in Article 2 of the new Bill prescribes that the signature should be carried out by means of asymmetric cryptography and accompanied by a certificate issued by a Certification Authority. According to Art 3(5) of the proposed law, a digital signature will be given equivalent legal recognition to a hand-written signature (in the sense of Art 1322), if it is accompanied by a certificate from an 'accredited' Certification Authority and issued by a natural person.

Electronic invoices are already being used in social security, administration and by some companies in their VAT returns.

Denmark

In its 1996 report to the Danish Parliament on IT policy, legislation to secure electronic communication was announced as initiative n°6.3 (page 54 of the report). In this document, the proposal is based on the following grounds:

"In order to ensure the secrecy of communication and to make sure that judges can attach the same evidential weight to documents transmitted in electronic format as to when documents are transmitted on paper, the Minister of Research and Communication Technology will introduce a Bill on Digital Signatures and electronic communication (encryption and digital signatures) in the parliamentary session 1996-1997. By introducing such a law, Denmark will place itself in the front when it comes to solving the problems in securing that electronic communication can be used to transfer confidential information and messages with legal effects."

It seems that at present, although work is still going on in this area, the immediate move towards legislation has been abandoned.

It is likely that - among others - the Danish Payment Systems, the Nordic postal services company (former state postal services) and the Danish municipality computer service bureau might apply for a license as a certification authority under any forthcoming legislation.

[5] This is the legal basis of the evidence rules in the interchange agreements which are generally concluded by parties before starting an EDI-project.

[6] This is called "a commencement of a written proof" (commencement de preuve par écrit, art. 1347 C.c.).

[7] Art. 1348 C.c.

Finland

No legislation exists at present. As in many other countries, a real property exception from the principle of freedom of contract exists. The Minister of Justice has planned a Working Group for the use of digital signatures and CAs[8].

France

Identification and authentication of the sender of medical documents for the purposes of reimbursement are currently being carried out by means of an electronic health card.

The legal provisions concerning trusted third parties only apply to key escrow agencies in the strict sense and not to certification authorities in the context of the use of digital signatures for authentication purposes. Consequently a certification authority wishing to provide its services in France only has to notify the SCSSI two months before starting the activities concerned.

Unlike Germany, France does not believe that at present it is already necessary to draft legislation covering digital signatures and CA services with a system of licensing.

Germany

"The concept of the "Willenserklärung" is wide enough to include also a declaration of will given by a mouse click", according to one German legal author[9]. The problem is however that the German civil code (§ 126) requires a written form, the materialising of the expression of the will of a person, identifiable through his hand-written signature. Consequently in all cases where a written form is required, digital signatures can, for the time being, not be used.

A hand-written signature is considered to be an 'Urkunde' which is the strongest evidential instrument in a civil procedure. A digital document with a digital signature will be considered 'factual evidence' by a judge.

Signaturgesetz: Art 3, Multi-Media Law (July 22nd 1997)

The Executive Regulation is contained within the 'Massnahmenkatalog'.

"The application of other digital signature procedures is optional insofar as digital signatures according to this Act are not required by legal provisions." Thus the law is more of a standard which can be made the rule in future legislative provisions.

The provision that the law aims at creating general conditions under which digital signatures are deemed secure does not mean that a German judge will automatically accept a digital signature if the provisions of the Signaturgesetz are respected. On the balance of probabilities it will probably tip the scales in the favour of the signatory which needs then to be disproved by the other party. The explanatory memorandum mentions that the judges will probably accept digital signatures according to the Signaturgesetz as a strong factual element in the context of freedom of means of evidence.

The law[10] defines a "digital signature" as "a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided with a signature key certificate of a certification authority or the authority according to § 3 of this Act".

[8] Certification Authorities

[10] Art 3(2), Signaturgesetz, August 1st, 1997

A "certificate" can 'certify' the assignment of the public key to a natural person - this is called an "identity certificate", but can also contain further information concerning that person. Such a certificate is called an "attribute certificate". The explanatory memorandum specifies as an example of an attribute certificate a certificate mentioning the power to legally represent a third person. Another example would be the fact that an individual was, for example, a medical doctor.

Only digital signatures referring to *natural persons* fall under the scope of the German Signaturgesetz, "because the power to represent a legal person is always linked to a natural person". This doesn't mean however that a digital signature is considered by the German law as an equivalent to a hand-written signature. Such a result would necessitate a modification of the provisions of the Civil Code.

The fact that only digital signatures referring to natural persons are included in the scope of the Signaturgesetz does not mean that a legal person could never use a digital signature but only that such categories of digital signatures are not within the scope of the Signaturgesetz. Thus the use of signatures by network entities in a UMTS environment can not be excluded.

The Signaturgesetz establishes a very detailed legal framework, which is further developed in the Ordinance of 8 October 1997:

German Digital Signature Ordinance[11] - provisions relating to the security and testing of technical components:

S16 provides certain requirements pertaining to the technical components of digital signatures:

Any given key must be such that it is 'nearly certain' that it can occur only once and also that the private key can not be derived from the public key. It must not be possible to duplicate keys.[12]

Use of the private key must be preceded by identification of the holder by PIN, biometrics or otherwise.[13]

The technical components must permit adequate determination, as necessary, of the contents of signed data or of data that is to be signed - so part of a message could be signed but the other part not signed.[14]

The integrity of the certificates must also be protected by access control and that of time-stamping services.[15]

The competent authority shall keep a catalogue of suitable security measures and shall publish this catalogue in the Federal Gazette. The measures shall be taken into account in the design of the technical components. The catalogue shall be prepared in keeping with specifications of the Federal Agency for Security in Information Technology.[16]

S17 deals with the testing of technical components. The tests of digital signatures should comply with the 'Criteria for Assessment of the Security of Information Technology Systems'[17]. For the generation, storage, use or commercial sale of private signature keys, the E4 standard must be complied with. Otherwise the E2 standard applies. The competent authority shall publish in the Federal Gazette an overview of the algorithms and pertinent parameters considered suitable for generation of signature keys.

[11] Signaturverordnung - Sig V, on the basis of s16 of the Digital Signature Act of 22 July 1997 (Federal Law Gazette I.S. 1870, 1872)

[12] S16(1)

[13] S16(2)

[14] S16(3)

[15] S16(4) and (5)

[16] *Bundesamt für Sichereit in der Informationstechnik*

[17] GMBI 1992, S.545

According to S14(4) of the Signaturgesetz, the technical components used have to be tested and confirmed. A copy of the test report and the confirmation by the relevant body must be sent to the competent authority[18].

The overall supervisory authority responsible for the granting of licences to certification authorities, the issuing of certificates for the private keys of the CAs and the monitoring of compliance with the Act, is the "Regulierungsbehörde für Telekommunikation und Post". As of the 1st of January 1998 this body has been operating as the regulatory authority for the German telecommunications sector.

The other provisions of the Signaturgesetz relating to the CA and resulting PKI will be discussed below.

Ireland

No legislation exists here. A report on Ireland in the Information Society was published by the government in May 1997. Recently in June 1998 a framework document on cryptography and digital signatures was released. The document proposes a liberal and essentially unregulated approach to the use of cryptography.
Italy

Article 15 (2) of the March 15, 1997 Law is very broad and gives complete legal recognition to electronic documents:

"*The instruments, data and documents constituted by the public service and by private individuals using computer or telematic methods, contracts stipulated in such form, and their archiving and transmission using computer instruments, shall be valid and effective for all legal purposes*".

According to this article, full legal effect will thus be given to electronic documents and data of public administrations and of private individuals and to the electronic archiving and transmission of these documents and data.

Article 15 (2) contains only a basic principle. It further states: ’*the criteria and methods of application of this paragraph shall be set out, for the public service and for private individuals, in specific regulations*.'

Decree on Criteria and Methods

At its meeting on 5 August 1997, the Italian Council of Ministers approved a draft decree of the President of the Republic setting out "Regulation on the criteria and methods of application of Article 15 (2) of Law 59 of 15 March 1997 on the formation, archiving and transmission of documents by computer and telematic methods."

It was definitively approved by Council of Ministers on 31 October 1997.

Art. 2 of the decree provides that "*computer documents by whomsoever they are drawn up, their storage on a data-processing medium and their transmission by telematic methods shall be valid and effective for all legal purposes if they abide by the terms of this regulation*". According to art. 3, "*the technical rules for the formation, transmission, storage, duplication, reproduction and validation, including time validation, of computer documents shall be laid down by Decree of the President of the Council of Ministers*".

A computer document is defined in Art 1(1)(a) as "*the representation in electronic form of legally relevant acts, facts or data*".

[18] S17(3) Signaturverordnung

Art 4(1) provides that "*the electronic document fulfilling the requirements stated by this regulation shall satisfy the statutory requirement of written form*".

According to Art 5 "*a computer document signed by a digital signature in the sense of Art. 10 has the same evidentiary value as a private instrument - scrittura privata - in the sense of Article 2702 of the Civil Code.*'

The regulation is however not complete and effective since it requires the technical rules to be adopted (Art 3). It also requires technical rules concerning public services (Art 18(3)) and tax regulation (Art 4(2)) to be laid down. These are due to be adopted sometime this summer.[19]

Provisions on digital signatures

A 'digital signature' is defined in Art 1(1)(b) as '*the result of the computerised validation procedure based on a system of paired asymmetric keys, one public and one private, allowing the signatory, by means of the private key, and the recipient by means of the public key, to demonstrate and verify the origin and integrity of a computer document or of a set of computer documents*.'

Unlike the German Signaturgesetz there is no limitation to natural persons. The concept of the digital signature is defined in a purely technical matter. According to the Italian decree a digital signature can be the equivalent of a hand-written signature but it can also replace, for any purpose set out in the legislation, the affixing of seals, embossing, stamps, signs and marks of any kind.

Another interesting item in the Italian decree, and absent in the German Signaturgesetz - is the 'authentication' of a digital signature by a notary of another public official. According to Art. 16 of the decree the authentication of a digital signature consists in 'the attestation by the public official that the digital signature has been attached in his presence by its owner, following the establishment of his personal identity, the validity of the public key and the fact that the signed document reflects the will of the party and is not contrary to the legal order…'

Sweden

An IT Commission was set up 1994. The IT Committee in 1996 published a report on electronic documents which is now under consideration by the government.

UK DTI Consultation Paper

The Department of Trade and Industry (DTI) which is the department in charge of drafting the government policy on the private use of encryption, has prepared a consultation paper with regard to a future regulatory framework in the field of digital signatures and Trusted Third Parties. Legislation is expected sometime in 1999.

For the time it appears useful to keep a short summary of the DTI Consultation Paper included in this report. Trusted Third Parties, as understood by the DTI, will be private bodies offering key escrow and key certification services. They could also provide other related services such as time-stamping, repositories of certificates and other certification related information, arbitration of repudiation claims, and encryption of communications.

Recently in April 1998, the DTI issued a statement on Secure Electronic Commerce[20] which took into account the submissions in response to the original Consultation paper[21] and has now decided that

[19] The author has to validate the status here.
[20] http://www.dti.gov.uk/CII/ana27p.html
[21] March 1997 paper on "Licensing of Trusted Third Parties for the Provision of Encryption Services"

mandatory licensing will not be introduced - only voluntary licensing. **It has been said that a digital signature certified by a licensed Authority will have the same force as a hand-written signature**. Voluntary licensing will also be encouraged for Key Recovery and Key Management agencies.

With respect to the algorithms being considered there is preference for the Digital Signature Standard (DSS) developed by the US government, but it is understood that the RSA algorithm is widely used and therefore will also be accepted. The standards to be followed by TTPs will "be determined by the market". In its statement in April 1998, the DTI announced that the new proposals would not oblige service providers to use any particular type of technology.

Role of the Licensing Authority (DTI)

In general the DTI will be the authority in charge of licensing TTPs. However, it was recognised by them that they would probably not be able to directly exercise overview and supervisory powers, in which case an independent body could be created. One of the possibilities is to implement a similar structure to that of the Data Protection Registrar, which would create an environment of self-regulation with very heavy penalties as a consequence of non-compliance. Apart from its supervisory powers, the DTI will act as a TTP only for its employees in their internal communication. Parallel to the proposal of a TTP infrastructure for the general public is another being developed by the Communications Electronic Security Group (CESG) for communication within governmental entities called "Securing Electronic Mail within HMG". The DTI initiative and the CESG initiative have certain differences, but they are trying to resolve them in order to produce a uniform standard for communication in the public sector and the private sector. The main interest in this uniformity is based on the needs that they, as well as other governmental agencies (e.g. the Inland Revenue), will have to communicate with the general public.

Draft Commission Electronic Signature Directive - 13th May 1998

This proposal on a common framework in the EEA for electronic signatures is now with the Parliament and Council for discussion. It may take a couple of years before the legislative process is completed and the directive can be introduced.

There are five main areas of importance here -

1. Definition of Digital Signatures
2. General Accreditation of Certification Authorities (CAs)
3. Recognition of Foreign Authorities
4. Liability of CAs
5. EU Data Protection Requirements

Definition of Digital Signatures

The definition of digital signature is 'technology neutral'. That is to say, asymmetric cryptography would fall under the definition but not necessarily to the exclusion of other forms of digital signature, current or potential.

A digital signature (Article 2) is a process which indicates the signatory's electronic approval of the content of the data and which is -

- uniquely **link**ed to the signatory
- capable of **identify**ing the signatory
- using a means under **the sole control** of the signatory
- guarantees the **integrity** of the information (i.e. that it has not been changed)

Article 5 of the draft directive establishes the legal effects of electronic signatures based on a *qualified* certificate issued by a CSP that satisfies the requirements laid down in Annex II, they should satisfy the legal requirements of a hand-written signature and be admissible in evidence as such. Electronic signatures should not be denied legal effect solely on the grounds that they are not certified by an accredited certification service provider (CSP). It does not mention what the effect would be of a signature, which is not certified at all. See below under the PKI for more information.

General Accreditation of Certification Authorities (CAs)

Member States may set up voluntary Accreditation Schemes, the details of which should be published in the Member State and the Official Journal of the EU. There should be no fees for obtaining accreditation bar a proportionate administrative cost.

Member States shall ensure that certification service providers meet the following requirements (Article 5) -

a) possess the reliability necessary for offering certification services, in particular be independent of financial or other interest in the underlying transactions

b) employ personnel with the relevant degree of expertise

c) use trustworthy systems, take precautions against forgery of certificates, guarantee confidentiality for the creation of private keys, install a prompt and secure revocation system

d) have sufficient financial resources to cover liability and/or insurance

Part II - The developing PKI in Europe[22]

The Necessity of Having a CA

As a way of introduction it is useful to examine whether or not a certificate is necessary for the utilisation of digital signatures in the first place.

The German law defines a “digital signature” as “a seal affixed to digital data which is generated by a private signature key and establishes the owner of the signature key and the integrity of the data with the help of an associated public key provided *with a signature key certificate of a certification authority or the authority according to s 3 of this Act*”.[23]

Also implicit in the definition of ‘digital signature’ in Art 2 of the Belgian Bill, is a ‘digital signature’ accompanied by a certificate from a CA.

Although the definition of ‘digital signature’ in the Italian decree[24] does not mention the need for a certificate, Art. 8 (1) of the Italian decree does provide that “anyone intending to use a system of asymmetric encryption keys for the purposes set out in Article 2 must obtain an appropriate pair of keys and make one of these keys public by means of the certification procedure carried out by a certifying authority”. These public keys shall be kept for no less than ten years by the CA.

Interestingly, the draft EU directive on a common framework for electronic signatures defines in Article 2 ‘electronic signature’ makes no mention of the need for the public key to be certified.

Article 5 of the draft directive establishes the legal effects of electronic signatures based on a *qualified* certificate issued by a CSP that satisfies the requirements laid down in Annex II - they should satisfy the legal requirements of a hand-written signature and be admissible in evidence as such. Electronic signatures should not be denied legal effect SOLELY on the grounds that they are not certified by an accredited certification service provider (CSP). It does not mention what the effect would be of a signature, which is not certified at all.

A ‘qualified’ certificate is defined in Art 2 as a "digital attestation which links a signature verification device to a person, confirms the identity of that person and meets the requirements laid down in Annex I." Annex I only contains provisions relevant to the content of the certificate so the definition of ‘qualified’ does not mean ‘issued by an accredited CA’. However, to be guaranteed the same status as a hand-written signature, the 'qualified' certificate should also have been issued by a CSP that fulfils the criteria in Annex II relating to standards of acceptable service and reliability.

Licensing/Accreditation

A CA may exist in three legal states.

a) It may be licensed by a government authority. The UK is proposing a system of voluntary licensing. Each licence is granted on an individual basis subject to certain criteria. A class-licensing system may also be introduced. No individual decision is necessary here. Individual licensing *may* have the effect of limiting the number of licensed CAs operating on the market.

b) It may be accredited. An accreditation will be checked by a government authority against certain

[22] The author of this report has also written a report for the COMETS project as part of the ETS II research plan. Much of the work done here for PKI has been derived from that report.

[23] Art 3(2) of the Digital Signature Act - Sig G, August 1, 1997

[24] The Italian Presidential decree which evolves from s15(2) of Law 59 of 15 March 1997.

criteria. This system is more akin to a ‘class-licensing’ system.[25]

c) It may be neither licensed nor accredited but may just exist as a market player providing its own guarantee of reliability.

From a costs point of view, Art 11 of Directive 97/13 dealing with licensing in the telecommunications sector states that the fees to be charged for ‘authorisation’ shall seek only to cover the administrative costs incurred in the issue, management, control and enforcement of the applicable individual licence. The fees for an individual licence shall be proportionate to the work involved and be published in an appropriate and sufficiently detailed manner, so as to be readily accessible. For the management of scarce resources extra fees may be charged to protect the need to ensure optimal use of these resources.

What are the legal effects of each?

Being licensed in the UK or accredited subject to for example the proposed Belgian Bill, subjects the authority to all the incumbent advantages and obligations imposed upon it in by that digital signature law. Thus the CA must comply with all the obligations vis a vis content of certificate, invalidation of certificate, keeping of public register but with that comes the guarantee of security that licensing or accreditation gives to the user of digital signatures. Furthermore, usually only digital signatures accompanied by a ‘qualified’ certificate issued by an accredited CA are given the same legal standing as manual signatures (except for Germany which does not award full legal status to any type of digital signature).

The original DTI Consultation Paper on the licensing of TTPs (published in March 1997) suggested a mandatory licensing for TTPs from the DTI or from a delegated authority. Exclusions to this general rule were proposed - encryption that is used solely in the protection of a business service (e.g. in pay TV systems or in payment systems), or encryption services that are provided only to the employees of the service provider or those in the same group of companies. Restrictions on the number of certificates, the value for which certificates can be used and the overall liability levels of CAs could be contained within the licences although the possibility of allowing some TTPs to operate without restriction is being considered. Licensing was also necessary for the provision of repository and time-stamping services.

However, in its statement in April 1998, taking account the opinions put forward by industry in the responses to the Consultation paper, the DTI reversed its position on mandatory licensing. Thus licensing will be voluntary, however, those organisations providing trust services to the public will be encouraged under the new legislation to obtain a licence and as a result the high standard and the public confidence that this will bring. The DTI states as follows:

We intend that licensed Certification Authorities - conforming to the procedural and technical standards, which such licensing will confer - would be in a position to offer certificates to support electronic signatures reliable enough to be recognised as equivalent to written signatures; an essential ingredient of secure electronic commerce. Licensed Certification Authorities offering secure electronic signature services will, we believe, make a significant contribution to electronic commerce. They will provide trust that the authentication process is reliable (i.e. an owner of an electronic or digital signature certificate is who they say they are) and consumer and business confidence that the signature mechanism employed is robust and secure.

[25] The terminology varies between 'licensing', 'accreditation' and 'authorisation'. It is unclear without clear definitions what is meant by each. In The field of telecommunications services, Directive 97/13 requires 'authorisation' of providers. Art 2 defines 'authorisation' as the umbrella term encapsulating both 'general authorisation' and 'individual licensing'. 'General authorisation' does not require the undertaking concerned to obtain an explicit decision by the national regulatory authority before exercising the rights stemming from the authorisation whilst an 'individual licence' does. Art 3(3) provides that 'member states may issue an individual licence only where the beneficiary is given access to scarce physical and other resources or is subject to particular obligations or enjoys particular rights, in accordance with the provisions of Section III'.

Thus a TTP will be enticed to get a licence in order to ensure the legal validity of the digital signature that it certifies.

The criteria for licensing will take into consideration the following aspects:

a) the technical knowledge of the people working for the TTP,

b) the financial capacity to assume the liability risks of the business, and

c) the extent to which the TTP services are isolated from other business interests.

Under Art 3 of the Belgian Bill, mandatory accreditation will not be expected. However, under Art 3(4) it will be possible to fix by law certain instances where a certificate will be needed from an accredited CA.

A non-accredited CA can not put itself forward as an accredited CA and if it does, the members are punishable by imprisonment and by fines under Art 22, Belgian Bill. Non-accredited CAs are not, however, bound by the law and thus do not have to follow the provisions relative to content, revocation, and electronic register maintenance.

To obtain an accreditation under the proposed Belgian regime, the CA must present itself to the 'Administration' under conditions which will be fixed by the King in the Council of Ministers. These conditions will relate to financial standing, sufficient expertise, independence, professional liability and interoperability.

In Germany, the supervisory authority responsible for the granting of licences to certification authorities, the issue of certificates used by those authorities for the signing of certificates and the monitoring of compliance with the Act, is the "Regulierungsbehörde für Telekommunikation und Post", which functions from the 1st of January 1998 as the regulatory authority for the German telecommunications sector. This body also operates as a certificate issuer and issues certificates to the CAs which it licenses. It also keeps a public record of these certificates and can also revoke these licences. (s4(5))

Licences are mandatory for CAs that wish to operate under the legal framework. Licences will be granted to certification authorities wishing to operate under the legal framework, after examination of their application file which has to include a 'security concept' in accordance with the security requirements of the law and after a check of the implementation of that security concept by a body recognised by the supervisory authority. According to s1(3) of the Signaturverordnung, the supervisory authority has to hear the applicant before rejecting, withdrawing or revoking a licence. After the granting of the licence the supervisory authority will issue the certificates for the signature keys used for affixing signatures to certificates and keep those certificates available for verification and retrieval over publicly available telecommunication links (s 4).

"The application of other digital signature procedures is optional insofar as digital signatures according to this Act are not required by legal provisions." The provision that the law aims at creating general conditions under which digital signatures are deemed secure does not mean that a digital signature will automatically be accepted by a German judge if the provisions of the Signaturgesetz are respected. The explanatory memorandum mentions however that the judges will probably accept digital signatures according to the Signaturgesetz as a strong factual element in a context of freedom of means of evidence.

Under s1 of the German Ordinance, the application for the licence has to be made in writing and the competent authority may request necessary documents such as a current extract from the commercial register or current certificates of good conduct pursuant to s30(5) of the Federal Central Register Act.

The competent authority can charge for the issuance of a licence, rejection of the application, issuance of the certificate and for the regular checks on security a CA must undergo under s15 of the Ordinance.

Art 8(3) of the Italian Law seems to require mandatory accreditation under terms to be laid down in a presidential decree. Under the Italian Law, the certification authorities must be registered in an official public list kept by the AIPA - Autorità per l'Informatica nella Pubblica Amministrazione - and must possess the four requirements listed in Art. 8 (3):

a) if the certification authority is a private person, it has to be a public limited company with a share capital of no less than the share capital necessary to receive the authorisation to operate a bank activity

b) their legal representatives and managerial staff must possess the requirements of trustworthiness incumbent upon persons responsible for the management, direction and auditing of banks

c) the technical staff and the personnel employed on certification work, must fulfil certain conditions regarding competence and experience

d) the computer procedures and related products must be of a quality that is in keeping with internationally recognised standards.

Draft Directive on Electronic Signatures

The draft Directive lays down very broad principles regarding the accreditation/licensing of CAs:

Article 3 lays down the market access principles for Certification Service Providers (CSPs). Mandatory authorisation is not allowed. Voluntary accreditation schemes are allowed for enhanced levels of certificate provision.

Article 5 of the draft directive establishes the legal effects of electronic signatures based on a *qualified* certificate and which also fulfil the criteria on CSPs set out in Annex II - they should satisfy the legal requirements of a hand-written signature and be admissible in evidence as such. Electronic signatures should not be denied legal effect SOLELY on the grounds that they are not certified by an accredited certification service provider (CSP).

A 'qualified' certificate is defined in Art 2 as a 'digital attestation which links a signature verification device to a person, confirms the identity of that person and meets the requirements laid down in Annex I'. Annex I only contains provisions relevant to the content of the certificate so the definition of 'qualified' does not mean 'issued by an accredited CA'.

What happens to the certificates issued by a CA if its licences is subsequently revoked? According to their own CPS, Belsign, if their own certificate is revoked, this does not affect existing certificates - it just prohibits Belsign from issuing further certificates.

Summary

Germany - Voluntary licensing. Preparation of 'security concept'. Application to the Regulierungsbehörde für Telekommunikation und Post and presentation to them of the 'security concept'. Consideration of application. Acceptance of application followed by issuance of a certificate for the public key of the newly licensed CA.

UK - Voluntary Licensing. Same process probably. Except application to the DTI or delegated body for a licence.

Italy - Art 8(3)seems to require that accreditation is mandatory. The details will be laid down in a Presidential decree. However, the four criteria laid out above must be met. More than likely a similar ‘security concept’ will be drafted. Consideration of the application. Acceptance of application and issuance of certificate for the public key of the CA.

Belgium - Voluntary accreditation except for some areas to be prescribed by the law where a certificate issued by an 'accredited' CA will be necessary. Similar procedure is expected for presentation of a CA before the ‘Administration’ which the King will delegate.

Guarantee of Proper Standards

The guarantee for the user stems from the fact that the CA is licensed or accredited by a supervisory authority. The supervisory authority has to guarantee not only that the CA fits the necessary criteria upon application for a licence but it has to guarantee the continued compliance with the laws.

Under s 13, German Law, the competent authority may enter into the production sites of CAs to inspect books, record etc. and failing compliance their licence will be revoked.

S14 requires technical standards to be implemented guaranteeing the secure generation and storage of keys, verification of signed data and its integrity, and protection of the certificate lists. (Presumably these are announced in the Massnahmenkatalog)

S16 of the German Ordinance lays down in general terms the required standards for security of key generation, verification, storage of certificates and time-stamping.

S17 provides for testing of these components and may publish approved algorithms/parameters in the Federal Gazette. Tests should be carried out by the CA and reports sent to the competent authority. The competent authority can employ an expert to verify the results of the test if it thinks this appropriate.

Liability

Here I will be examining the potential liabilities of TTPs in all their potential functions in Germany, Italy, the draft EC directive and under the Belgian and UK regimes and under a model CPS itself.

Unfortunately, the digital signature laws/proposals are fairly quiet on the issue of liability, meaning that the areas of contractual and tortuous liability probably cover sufficiently the existence of a CA.

First a brief explanation of what the liability problem is and the types of solution that can be utilised will be offered, then a look at the laws themselves and a model CPS.

A CA offers a certificate to a recipient so that his public key can be trusted by other users who will then openly communicate and do business with him. An identity certificate guarantees that the recipient is who he says he is. An attribute certificate will guarantee more, for instance the profession or credit worthiness of the individual. Thus it is reasonable for a user to rely on the information as being accurate presuming that he fulfils his side of the bargain e.g. by checking on the public register that the certificate has not been revoked. If as a result the information turns out to be unreliable and the user suffers loss as a result the CA is potentially liable if its certificate held out this information as being accurate verified information. The recipient of the certificate will be primarily liable in that any information on the certificate would have been submitted by him but it may not be possible to sue this person as he may have ‘disappeared’ or he may be bankrupt. Thus the only target for the injured party is to sue the CA.

Other potential liability will stem from failure to carry out the obligations prescribed by law or as part of the common business practice of a TTP. For instance; failure or delay in updating the public register with news of a revoked certificate; incompetence or unreliability of staff; compromise of private key by the Key management centre can all potentially subject the TTP to liability.

The UK DTI paper suggests two formats for liability. The first is to impose a system of strict liability[26] with a cap similar to that already employees in the CREST system of electronic share trading. The second is to allow the market to determine how the liability should be determined.

The Italian decree contains provisions with respect to the liability of the user and of the certification authority. Regarding the liability of the user, the first paragraph of art. 9 states that "everyone who wants to use a system of asymmetric keys or of digital signature must adopt all the organisational and technical measures to avoid damages to others".

Under s10, German Ordinance, the CA is responsible for establishing the reliability of its staff. In particular, it may require certificates of good conduct pursuant to s30 (1) of the Federal central register Act. Under s11 of the same, the CA shall take precautions to protect unauthorised access to private keys, certificate and time-stamp issuance components. Apart from the responsibilities laid out in the Italian[27] and German Laws there is nothing directly said about liability.

In the drafting of the CPS the CA will try and limit its liability in many ways. These methods need to be checked against national tort and contract laws.

They may try to limit liability by:

1) the insertion of exclusion clauses
2) direct financial caps
3) impose obligatory warranties on users
4) oblige certain indemnities from the subscriber

The question does pose itself, however, whether it is reasonable for a relying party to be bound by the terms of the CPS when relying on a certificate? The answer is no the third party will not be bound as they are not privy to the contract of the sale of a certificate. It is even doubtful whether a subscriber (who is privy to the contract) would be bound by such a long and complex document as the CPS. For example the new CPS of Belsign will be succinct and to the point and substantially shorter. The current CPS of Belsign is a 60 page document. Belsign as well as preparing a new CPS are working on a summary of their CPS. This poses the danger that the summary may replace the CPS as the binding document.

Can the third party be bound at all? He will only be bound by what he has notice of - so if minimum information regarding what the 'relying party' should do before relying on the certificate and regarding the liability of the CA were placed in an attachment contained along side the certificate, then it could be possible for the 'relying party' to be bound by this.

Liability under the Draft Directive on Electronic Signatures

CSPs should be governed by national liability rules, however where this may arise in legal uncertainty and hence hamper the Internal Market objective, harmonised liability rules may be preferable.

[26] This type of liability can neither be contested nor waived.
[27] Art 9 of the Italian decree lays down the ten obligations of CA's.

Article 6

As a general rule a CSP is not liable for the accuracy of the information in the certificate if it states so in the certificate. Neither is it liable for information given to it by the subscriber if it can demonstrate that it has taken all reasonably practicable measures to verify that information.

The CSP is liable for non-compliance with this directive. The CSP is liable for making sure that the person certified does indeed hold the private key corresponding to the public key in the certificate. (Art 6(c))

Key generation parties are liable for non-correspondence of their keys.

Loss or theft of CAs Private Key

One of the main sources of potential liability would be as a result of the loss or compromise of a CAs private key. If this happens there is no longer any security or trust in the framework. The CAs certificates can be forged and innocent third parties suffer loss as a result. Could the CA be held strictly liable for such compromise or only if they did not employ all reasonable care in keeping the private key secret? This is why so much security is put in place to protect this key. The key is kept at a secret location in a secure vault under very strict conditions of access. This may indeed be something that should be covered in the insurance contract.

The following section on Operational Controls ties in directly with this section on liability as failure to honour the operational controls laid down will result in incurred liability.

Operational Controls

The Commission may (Art 3(3)) publish in the O.J. ‘reference numbers’ of generally recognised standards for electronic signature products.

The use of electronic signatures in the public sector may be made subject to additional requirements.

Controls under the German Law

Under s12, German ordinance a ‘security concept’ has to be drafted and maintained. This will contain all security measures, an overview of the technical components used and a description of the process of certification. The concept has to be changed as standards are changed. The competent authority shall keep a catalogue of suitable security measures and publish it in the Federal Gazette.

S13, German Ordinance prescribes what documentation the CA should keep for verification by third parties or applicants. It also prescribes what information on the application and issuance of a certificate must be kept on the CAs records: these include a photocopy of the id., documents submitted relevant to third parties, any pseudonyms listed, proof of the required notification of the applicant and third parties, the issued certificates including relevant time, invalidation of certificates, date of hand-over of key pair if CA is generating such. The data must be held for a period of 35 years from the time of issue.

S15 prescribes that the CA should provide for regular checks every 2 years and submit a report to the competent authority and confirmation that it fulfils the provisions of the German Law.

Controls under the Italian Decree

Under the Italian decree, the certification authorities must be registered in an official public list kept by the AIPA - Autorità per l’Informatica nella Pubblica Amministrazione - and must possess the four requirements listed in Art. 8 (3): a) if the certification authority is a private person, it has to be a public limited company with a share capital of no less than the share capital necessary to receive the authorisation to operate a bank activity, b) their legal representatives and managerial staff must possess the requirements of trustworthiness incumbent upon persons responsible for the management, direction and auditing of banks, c) the technical staff and the personnel employed on certification work, must fulfil certain conditions regarding competence and experience, and d) the computer procedures and related products must be of a quality that is in keeping with internationally recognised standards.

The first paragraph of art. 9 states that “everyone who wants to use a system of asymmetric keys or of digital signature must adopt all the organisational and technical measures to avoid damages to others”.

In the second paragraph a detailed list describes the duties of a certification authority: a) identify with certainty the person who applies for the certification; b) release and make public the certificate which has to be issued according to the requirements provided in the decree; c) on request of the applicant and with the consent of the third interested party, specify its agency power or other titles related with the professional activity or with other offices; d) respect the legally required technical rules; e) inform the applicants in a complete and clear way about the certification procedure and about the necessary technical requirements to be admitted to it; f) respect the security provisions of the computer systems and the provisions about the processing of personal data; g) not be depository of private keys; h) revoke or suspend immediately the certificate on request of the applicant or of the represented third person, in case of loss of the key, in case of measures taken by a public authority, in case of knowledge about reasons for the limitation of the capacity of the holder or in case of suspected abuses or falsifications; i) make immediately public the revocation or the suspension of the pair of asymmetric keys; j) immediately inform the AIPA - Autorità per l’Informatica nella Pubblica Amministrazione - and the users giving notice of at least six months of the cessation of activity and about the subsequent take-over of the documentation by another certification authority or of its cancellation.

Controls under the Belsign CPS

A CA is subject to stringent operational controls similar to that of a bank. The controls laid down in the Belsign CPS are as follows:

a) Training of Staff

b) Trustworthiness

c) Financial Responsibility

d) Record Keeping

e) Time Stamping of Certificates

f) Auditing of all events

g) Disaster Recovery methods

h) Data Protection compliance

i) Termination Procedures

Controls under Draft Directive on Electronic Signatures

Annex II - Requirements for certification service providers
Certification service providers must:

(a) demonstrate the reliability necessary for offering certification services;

(b) operate a prompt and secure revocation service;

(c) verify by appropriate means the identity and capacity to act of the person to which a qualified certificate is issued;

(d) employ personnel which possesses the expert knowledge, experience, and qualifications necessary for the offered services, in particular competence at the managerial level, expertise in electronic signature technology and familiarity with proper security procedures; they must also exercise administrative and management procedures and processes that are adequate and which correspond to recognised standards;

(e) use trustworthy systems, and use electronic signature products that ensure protection against modification of the products so that they can not be used to perform functions other than those for which they have been designed; they must also use electronic signature products that ensure the technical and cryptographic security of the certification processes supported by the products;

(f) take measures against forgery of certificates, and, in cases where the certification service provider generates private cryptographic signature keys, guarantee the confidentiality during the process of generating those keys.

(g) maintain sufficient financial resources to operate in conformity with the requirements laid down in this Directive, in particular to bear the risk of liability for damages, for example, by obtaining an appropriate insurance;

(h) record all relevant information concerning a qualified certificate for an appropriate period of time, in particular to provide evidence of certification for the purposes of legal proceedings. Such recording may be done electronically;

(i) not store or copy private cryptographic signature keys of the person to whom the certification service provider offered key management services unless that person explicitly asks for it;

(j) inform consumers before entering into a contractual relationship in writing, using readily understandable language and a durable means of communication, of the precise terms and conditions for the use of the certificate, including any limitations on the liability, the existence of a voluntary accreditation and the procedures for complaints and dispute settlement.

Recognition of certificates abroad

UMTS envisages global coverage. Thus the question poses will the TTP have to establish itself and seek accreditation/licensing in all 15 EU Member States and other third countries or can it establish itself in one country and issue certificates on a European-wide basis?

S 15 of the German Law provides: “Digital signatures capable of being verified by a public signature key certified in another Member State of the European Union or in another State party to the EEA shall be deemed equivalent to digital signatures under this Act insofar as they show the same level of security”. The equivalence is thus established at the level of the digital signatures, not at the level of the certification authorities or of the certificates.

Digital signatures capable of being verified by a public signature key certified in other States - outside the EU or the EEA - are deemed equivalent insofar as relevant supranational or intergovernmental agreements have been concluded and insofar as the digital signatures show the same level of security.

Certificates for public signature keys issued by foreign supreme certification authorities (supervisory authorities), as far as they are recognised in Germany will be confirmed by a digital signature of the German supervisory authority, will be published in the public register kept by the supervisory authority.

Thus for Germany the answer is that as long as the digital signature process is of equivalent security (which presumably includes as well as equivalent security vis a vis technical components, an equivalent security regarding the reliability of the certificate), and an agreement exists German persons and foreign persons can safely communicate and do business with each other electronically, and have the protection of the Signaturgesetz.

If a CA wants to offer certificates directly on the German market, then it has to get accredited by the German authority. It is not clear whether they have to undergo the same process of accreditation, development of a 'security concept' etc. or whether an automatic accreditation can take place with countries in the EU/EEA or with whom multi-national or bilateral agreements have been concluded. The foreign CA will then be kept in the public register by the German authority.

According to Art. 8(4) of the Italian decree, the certification procedures may also be carried out "by a certifying authority operating under a licence or authorisation issued by another Member State of the European Union or the European Economic Area on the basis of equivalent requirements". Thus CAs accredited abroad can directly offer certification services in Italy and foreign certificates by accredited CAs are recognised. However, non-accredited CAs cannot benefit from these allowances in Italy.

Art 17 of the Belgian Bill, recognises certificates coming from any member of the EU or EEA or countries party to relevant conventions with Belgium or the EU which show the same level of security as equivalent to certificates coming from an accredited CA. This provision is equivalent to the German provision. Also foreign certificates from Third countries, as with the German provision, will be recognised if they show the same level of security and there are international mutual recognition agreements put in place with the Belgian government. The 'Administration' will draw up a list of which CAs (foreign or EU/EEA) satisfy the requirement of 'equivalent security'.[28] *Whether this allows direct marketing of certificates to Belgian nationals is less certain, however as certificates issued by foreign supervisory authorities are not mentioned.*

According to the DTI paper, a foreign CA will have to be licensed in the UK to offer services directly to the UK market. This mandatory licensing may now be waived according to the recent position issued by the UK DTI, however, unfortunately the summary of position makes no mention whatsoever of the Internal Market issues concerning certificates.

According to the original DTI paper, foreign certificates will be recognised if issued by a licensed authority abroad and trusted by a UK TTP or by an authority not licensed because no licensing regime exists in that country but still trusted by a UK TTP. It is unsure whether this is still the position taken by the UK DTI.

Article 7 of the European draft directive on Electronic Signatures describes the three ways in which foreign certificates from outside the EU may be recognised. The relevant provisions of Art 7 are as follows:

1. Member States shall ensure that certificates issued by a certification service provider established in a third country are recognised as legally equivalent to certificates issued by a certification service provider established within the European Community:

> (a) if the certification service provider fulfils the requirements laid down in this Directive and has been accredited in the context of a voluntary accreditation scheme established by a Member State of the European Community; or
>
> (b) if a certification service provider established within the European Community, which fulfils the requirements laid down in Annex II, guarantees for the certificate, to the same extent as for its own certificates; or
>
> (c) if the certificate or the certification service provider is recognised under the regime of a bilateral or multilateral agreement between the European Community and third countries or international organisations.

2. The Commission may take measures to facilitate cross-border certification services with third countries and legal recognition of electronic signatures originating in third countries. For this purpose, the Commission may make proposals to achieve the effective implementation of standards and international agreements applicable to certification services, and may, in particular and where necessary, submit proposals to the Council for appropriate mandates for the negotiation of bilateral and multilateral agreements with third countries and international organisations. The Council

[28] Art 17, Belgian Bill

shall decide by qualified majority.

For a digital signature to be given the same recognition as a hand-written signature then it should be a ’qualified’ certificate issued by any CSP satisfying the requirements laid down in Annex II. Thus at the level of legal recognition (and as would be expected in a harmonisation directive), there would be no distinction made between a certificate coming from one EU member state as from another. As regards the use of non-qualified certificates, the principles of the Free Movement of Goods and Services[29] and the Internal Market reign supreme.[30] For foreign[31] certificates, the foreign CA should be accredited by a CA established in the EU. Otherwise, it must get another CSP to vouch for its certificates which would be more burdensome - paragraph (b) does allow for certificates from third countries entrance into the European market by a vouching process. Although the conclusion of agreements with the EU under paragraph (c) would seem the more appropriate way of securing such entrance.

Summary of National Positions

Germany -EU/EEA certificates for EU/EEA keys accepted if equivalent security Foreign certificates for national keys accepted if licensed by the German authority Foreign certificates for foreign keys accepted if international agreement and equivalent security
Italy - EU/EEA certificates for EU/EEA keys accepted EU/EEA certificates for national keys accepted if CA is accredited abroad
Belgium - EU/EEA certificates for EU/EEA keys accepted if equivalent security Foreign certificates for foreign keys accepted if international agreement and equivalent security Foreign or EU/EEA certificates for national keys unsure
UK - unsure at present
EU directive - EU/EEA certificates for EU/EEA keys given full legal status if accredited in any EU MS Foreign certificates for national keys given full legal status if accredited in any EU MS

[29] Does the issue of certificates within the community constitute the issue of goods or the provision of services. It is more likely to be ’services’ and thus would come under Chapter 3, Art 59 of the Treaty of Rome, 1957.

[30] See below in the next section for a brief explanation.

[31] ’Foreign’ meaning issued by a Third Country outside the territory of the EU.

11 Pillar II - Data Protection and UMTS

UMTS will be different from 2nd Generation mobile telephony in that it foresees the transfer by a new air-interface to a mass market of not only VOICE but also many different forms of DATA - 'personal' or otherwise. The possibilities are extensive - we have talked about home-banking and electronic health systems as examples. Such data import varying levels of sensitivity and hence varying levels of required security. Different parts of the network transfer different types of data and as a result have different degrees of responsibility. Some parts of the network merely 'process' the data whilst others 'control' the data. This section on data protection attempts to isolate the various types of data that might be involved in a UMTS environment and also attempts to distinguish between the different parts of the network and how Data Protection laws apply to these. The two European directives on data protection are analysed as the basis of EU law. The new Data Protection Law in the UK is analysed as an example of implementation by a Member State (taken in conjunction with the 1984 Data Protection Act which implements 80% of the Directive already). It will be seen that the Data Protection in the Telecommunications Sector Directive (Directive 97/66), although due for implementation on the same date - October 24th, 1998, has not been implemented by many countries.

Different types of data we are dealing with

The directive applies to all personal data which is defined in Art 2 as 'any information relating to an identified or identifiable natural person ('data subject')'. An identifiable person is one who 'can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. Thus in recital 26 of the Preamble, protection shall not be afforded to data which is rendered anonymous. In the new UK Act, 'personal data' is defined in Art 1(1) as follows:

1(1)…data which relate to a living individual who can be identified -

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual…

The definition of 'personal data' is wide enough to capture any PIN number, private key - even the name of an individual is 'personal data' although it is that data that is the very identification of the individual.

It is useful to note that Directive 97/66 goes further than 95/46 in that it also protects the legitimate interests of subscribers and not just 'users' who are by definition 'natural persons'. Art 2(a) defines 'subscriber' as 'any natural *or legal person* who or which is party to a contract with the provider of publicly available telecommunications services for the supply of such services'.

The new UK Act also elaborates what is meant by 'sensitive personal data":

2. In this Act "sensitive personal data" means personal data consisting of

information as to-

a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

The problem, therefore, is to find out what category each type of data falls into. Is it 'personal data' which receives the protection of the data protection laws; is it 'subscriber data' which receives some protection from Directive 97/66 or is it just 'ordinary' data which receive no protection?[32]

Data Types (as defined in ETR UMTS 33.20)

User data

This type of data comprises all data transmitted on the end-to-end traffic channel by users to other users. This data comprises all types of data generated by a user and includes digital data and voice. This data may or may not be 'personal data', depending on whether it fits the definition. If the data can be linked to an individual, then it is 'personal data' and comes under the terms of the directive. The sending of this data would fit the definition of 'processing' in that Art 2(b) of the directive which defines 'processing' very broadly includes the *disclosure by transmission, the dissemination or otherwise making available* of 'personal data'.

Signalling Data

This type of data consists of the following types of data in a UMTS environment:

Charging Data

- This type of data relates to charges incurred by users whilst using network resources and is normally passed by core network operators to the HN. The owner of the USIM will be the person for whom this charging information is being incurred. Thus the charging data relates to an identified or identifiable individual and will constitute 'personal data'. Unless, provision is made for some form of anonymous payment by means of a pre-paid card, this will be the case.

Billing Data

- This data relates to charges incurred by subscribers for their subscriptions and user charges. Such data is generated by the HN and transferred to subscribers. Subscribers will also send billing data to their users. Any billing data relating to users will constitute 'personal data' unless again anonymous billing is provided for. Subscribers, however, do not come within the terms of 95/46. Data relating to subscribers will be examined under Directive 97/66 below.

[32] However, if this 'ordinary data' is compiled in a 'database' for which there has been 'qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents' then a right exists under the Database Directive 96/9 to prevent the extraction and/or re-utilisation of the whole or of a substantial part of the contents of that database. It is a right which protects the maker of the database whether this is an individual or a legal person and protects the time and investment in compiling such a database rather than the data itself. The Directive was implemented in the UK by the Copyright and Rights in Databases Regulations 1997 which operate as from 1 January 1998. Along with Austria and Germany, these were the only countries that made the required deadline in implementation.

Location Data

- This type of data relates to the location of a user or his mobile equipment. The question is whether if the data relates to the mobile terminal, can it be related to an identified or identifiable individual? Someone else could be using his hand set. If multiple registration is allowed, then it will not be possible to say for sure who is using the terminal unless the data relates to the USIM actually present in the terminal and not the terminal itself.

Dialling Data

- UMTS proposes a person to person dialling system, so a number will relate to a specific user rather than to a terminal and will hence constitute 'personal data'.

Identity Data

- Such identity can be user, subscriber or mobile terminal identity. User identity data will constitute 'personal data' only.

Security Management Data

- Such data includes encryption keys and authentication messages. Such data can be used to identify a user - in fact this is the very objective of the data - and it would hence be 'personal data'. However, such data should always be kept secret and should only ever be processed by the authorised parties. The private key should never be processed in any way unless Key Escrow is introduced in which case LEA's should have access to the keys.

Processors and Controllers of Data

The most important function in the sphere of data protection and the function upon which all the responsibility lies is that of the 'controller' of data. 'Controller' is defined in Art 2 of Directive 95/46 as 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'. Under Recital 47, it is stated that in the sending of a message containing personal data (by e-mail), the controller will be **the person from whom the message originates**, rather than the persons offering the transmission services who are the 'processors' and process the data on behalf of the controller

The 'processor' is simply defined in Art 2(e) as 'a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller'. Thus the processor exercises a purely passive role and acts solely on behalf of the controller.

The definitions in the new UK Act are almost verbatim that of the directive, however, the definition of 'processor' clarifies that it means an entity 'other than an employee of the data controller'.

In a UMTS environment, there are a number of entities; the user, the recipient, the subscriber, the mobile network, the fixed network (local to the user), and the remote or foreign network. This may be an over-simplification of the parties involved.[33] We can further divide the network into Access Network and Core Network, and then further split the Core Network into Serving Network, Home Network and Transit Network.

Depending on what function each one is carrying out at a particular time and the type of data being 'processed' will govern whether that entity will fall within the definition of 'processor' or 'controller'.

The controller of user data according to Recital 47 will be the data subject or the user in the UMTS environment. The processor will then be the network.

[33] This should be discussed at the next forum meeting and elaborated upon in the final report.

The controller of signalling and control data will be the originator of such data, generally the home or serving network. The processor will again be the network. It is possible, therefore, for the network entities to be at the one time the controllers of the control and signalling data and the processors of that data.

The network will for any personal data contained within a message be the 'processor' of that information, however, in the words of Recital 47 the network will normally be considered the controller for 'the processing of ***the additional personal data*** necessary for the operation of the service'.

The following is an outline of what type of data is transferred between the various entities as described in the ETR UMTS documents 33.20 and 33.21. The main question is to whom does the data relate - the user or the subscriber? If it relates to the user who is a natural person, it will be protected by the data protection laws.

Signalling Data

- Serving Network charging the Home Network
- Home Network billing the subscriber
- Serving Network passes Location data to the HN
- Home Network distributes dialling data to users
- The calling user transfers dialling information to the serving network and then on to the appropriate HN
- Generation and sending of User/Subscriber and Terminal ID numbers to Access Network
- Generation of Security Management Data in the form of encryption keys and authentication messages in the Equipment Domain (UE Domain)

Control data

- Routing Data generated by NOs and passed amongst NOs
- Network Resource Management data generated by NOs and passed amongst NOs
- Access Control Management data to terminal equipment, network resources and service profiles in the form of PINs or other authentication information - usually stored by the generator of the information
- Service Profile data passed between user/subscriber and HN

Transfer of Signalling and Control Data to Foreign Networks through Roaming

- Transfer by the Transit Network of user data to other foreign networks
- Receipt of Charging Information from foreign networks

Summary of EU Data Protection Requirements

Directive 95/46/EC of the European parliament and of the Council seeks to reinforce two principles; that of the right of privacy of the individual and the absence of any cross border restrictions of the flow of information between member states (Art 1). Art 8 of the ECHR guarantees the right of privacy of every individual and this directive seeks to reinforce that right.

The scope of the directive is laid down in Art 3. It only applies to the processing of data wholly or partly by automatic means or data which is processed manually but forms part of a filing system.

The two main principles are (1) the imposition of restrictions upon processors and controllers of data (2) the rights of the data subject to be informed about any processing that is going on, to object to this etc.

Art 6 provides that member states shall ensure that data be (1) processed fairly and legally (2) collected for SPECIFIED purposes only (3) not EXCESSIVE for these purposes (4) accurate and up to date (5) kept in a form which permits the identity of the individual only up to when is necessary. Six criteria are laid down in Art 7 for making data processing legitimate. These are (1) if the data subject gives his unambiguous consent (2) under necessity for the performance of a contract (3) under necessity for the performance of a legal obligation for which the controller is subject (4) the vital interests of the data subject (5) public interests (6) the legitimate interests of the controller or third party except where the rights of the data subject override.

The data subject must be informed under Art 10 of at least (1) the identity of the controller (2) the purposes of the processing (3) the recipients of the information, whether the questions are obligatory or voluntary and of his/her rights of access/rectification. Information not collected from the data subject personally under Art 11 must also be notified the data subject. The right of access is provided for under Art 12 where the data subject can have data rectified, erased or blocked if the processing would not comply with this directive, particularly if the data is incomplete or inaccurate. As well as the right to access is the right to object under Art 14 at any time 'on compelling legitimate grounds'. The right to object, in particular, to the processing of data for direct marketing purposes is mentioned. Where a justified objection is established, then the processing instigated by the controller may no longer involve those data.

The directive applies to all personal data which is defined in Art 2 as 'any information relating to an identified or identifiable natural person ('data subject')'. Thus in recital 26 of the Preamble, protection shall not be afforded to data which is rendered anonymous.

Furthermore the directive does not apply to video-surveillance used for criminal law purposes (Recital 16).

Art 28 provides for the setting up in each country of an independent data protection supervisory authority with powers of investigation, intervention which will hear complaints and make decisions. Under Art 18, it is mandatory for the controller to notify the supervisory authority of any processing plans in relation to personal data. These plans must then be published and the supervisory authority will screen the plans to make sure they are compliant with the directive.

There are certain special categories of data, the processing of which must be prohibited by member states unless the data subject gives his consent or it is necessary under employment law or for the defence of a legal claim. These categories are defined in Art 8 and include racial, religious and sexual data.

Art 13 contains some general public interest exceptions and restrictions to the obligations and rights laid down in the directive. These exceptions are related to defence, national security, prevention of crime, important state financial interests and the protection of the data subject or the rights and freedoms of others.

Section VIII of the directive is very interesting from USECA's point of view. The section deals with the security and confidentiality of processing.

Art 17 deals with security:

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

This obligation is paramount and lies upon the shoulders of the controller. Although in a UMTS environment we are usually not dealing with 'special categories' of data as defined in Art 8 (such as data of a racial, sexual or religious nature), the 'nature' of the data should determine the appropriate level of security; the more sensitive or important the data is, the higher the level of security should be. It is, however, unclear what exactly the level of security should be.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures.

Thus a controller - if he does not do the processing himself - and certainly before entering into roaming agreements should demand a security plan and guarantee from the prospective processor.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

- the processor shall act only on instructions from the controller,

- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 23 deals with liability of the controller. It does not mention the processor:

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Chapter IV deals with the transfer of personal data to third countries. The rule is that there must be an adequate level of protection in the third country before data can be transferred. This level of adequacy is assessed in relation to the nature of the data; the purpose and duration of the processing; the general laws and professional rules in that country. Member States may not send data to such countries deemed inadequate in their protection until a remedy can be arrived at.

Art 26 provides some derogations from the general rule:

Transfer is allowed if (a) the data subject gives his unambiguous consent (b) the transfer is necessary for the performance of a contract between the data subject and the controller (c) the transfer is necessary for the performance of a contract between the data between the controller and a third party (d) public interest/defence of legal claims (e) vital interests of data subject (f) the data is for general public consultation.

Without prejudice to the above, transfers are also allowed if specific safeguards are put in place by the controller in the form of contractual clauses with the recipients.

Data Protection Directive in the Telecommunications Sector

In December, 1997, a second data protection directive was promulgated this time regarding the processing of personal data and the protection of privacy, specifically, in the telecommunications sector. It was felt that due to the advances in telecommunications that a second directive was needed. The Council had already in a 1988 Resolution made a call for steps to be taken to protect personal data in the telecommunications sector.

The directive is to be adopted by the member states no later than 24 October 1998, and for the confidentiality and secrecy provisions under Art 5 a two year extension until 24 October 2000 is given.

The directive only applies to public telecommunications networks and therefore excludes purely internal networks.

Art 1 of the directive defines the object and scope of the law. The dual object is one of ensuring the protection of fundamental freedoms in the EU particularly the right of privacy and the free movement of personal data between member states in the telecommunications sector. The directive also extends to subscribers who are legal persons and thus goes further than 95/46.

Art 3 provides that the processing of personal data with regard to all digital services, especially ISDN and public digital mobile networks, come under the directive and where possible subscriber lines connected to analogue exchanges. Cases where this is unreasonable should be notified to the Commission.

The provider under Art 4 should take the appropriate technical and organisational measures to ensure an adequate degree of security, and that the level of security should be proportional to the risk presented. Providers must warn subscribers of potential risks of breaches in the security network.

Confidentiality

Member States shall (Art 4) ensure the confidentiality of communications and in particular prohibit listening, tapping, storage or other kinds of interception or surveillance of communications.

There are exceptions to this. Art 4(2) allows the legally authorised recording of communications for lawful business practice in order to provide evidence of any contract or business communication. Art 14(1) provides a general exception for the interests of public security, defence and the prevention, investigation, prosecution of a criminal offence.

Traffic and Billing Data

This data (as specified in the Annex of the directive) can be processed for the purposes of subscriber billing and interconnection payments Billing data must be erased after the bill has been paid (Art 6(2)). The data can only be used by those persons acting under the authority of the providers. It can also be used for the purposes of marketing the providers own services. Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a PTN must be erased upon termination of the call. Finally this is without prejudice to the possibility of competent authorities being informed with a view to settling disputes, in particular billing or interconnection disputes.

Itemised Billing

Art 7 provides that a subscriber should have the right to receive a non-itemised bill. The right of a subscriber to receive an itemised bill has to be balanced with the right of the user to privacy and adequate alternative modalities of billing/communications should thus be provided.

CLI (Calling and Connected Line Identification)

Art 8 deals with the rights of calling and called subscribers and users to use or reject CLI where this is offered. Where this is offered, the calling user must have the right to eliminate the presentation of CLI on a per-call basis. The subscriber must have the right to prevent the presentation of CLI for incoming calls, reject incoming calls where this CLI has been eliminated if the CLI is presented before the call is established.

This also applies with regard to calls to third countries and originating in third countries.

The exceptions to these rights are laid down in Art 9 as the right to trace nuisance or malicious calls on a temporary basis or on a per-line basis for provision of emergency calls.

Automatic Call Forwarding

Art 10 provides that each subscriber has the right no to have a call automatically forwarded by a third party to his terminal.

Directory Entries

Subscribers have the right to be omitted from directories or may consent to having more personal data than is usual in a directory. Inclusion is the norm, so in order to become ex-directory a charge may be incurred (only to the value of what it costs the operator to exclude the person involved). The legitimate interests of subscribers other than natural persons should also be protected.

Unsolicited Calls

Art 12 prescribes that the use of automated calling systems for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. As regards ordinary unsolicited calls, member states should decide whether these be prohibited unless subscribers give their consent or prohibited to those who state they do not wish to receive them.

Data Protection in the UK - Preparation for the New Law

The EU Data Protection Directive has effect from the 24 October 1998. In the UK a new bill has been proposed which has now received its third reading in the House of Commons. The new Act received Royal Assent on the 16 July. The legislation is not expected to be brought into force before January 1999.

Whilst the Act sets out the overall legal framework, much of the detail will be contained in secondary legislation which is yet to follow. The Act is in essence very close to the current law (the Data Protection Act of 1984) Thus the key elements - the data protection principles; registration; an independent supervisory authority as a watchdog; the right of access of data subjects and their right to have inaccurate data corrected; the duty of the controller to notify the data subject of the identity of the controller and the purposes for which the data is being processed - are all maintained.

There is a three year transition period for controllers to bring processing 'already underway' into compliance with the new law. However, the directive will still have direct effect as of October 24th.

There is a new eighth Principle restricting the transfer of personal data outside the EU. There are to be no restrictions on the free flow of personal data between countries in the EEA (European Economic Area - which includes Liechtenstein, Norway and Iceland as well as the 15 Member States of the EU). Personal data may only be transferred to third countries if those countries ensure an 'adequate level of protection for the rights and freedoms of data subjects'. This restriction can be waived if the data subject consents or it is necessary for the performance of a legal obligation.[34]

[34] Schedule 4, Data Protection Act 1998

12 Pillar III - Encryption Regulation and Lawful Interception

The following section will analyse the various national laws that govern the use and export of cryptography for confidentiality purposes. The EU measures and the US position will also be looked at briefly.

If UMTS is to support an electronic-commerce environment and allow for the privacy of communications in general, free from the danger of unlawful interception, then the use of the key pair for encryption of data will be necessary.[35] In the UMTS ETSI documents, confidentiality of user traffic, signalling traffic and traffic flow should all be guaranteed. Identity confidentiality or anonymity is another feature that will be included. Location confidentiality must also be possible. In order to guarantee the confidentiality of these data, whatever they are, the use of cryptography has to be free. Also if cryptography software will be offered by subscribers to their users by means of downloads to the terminals then the possibility of such downloads taking the form of 'exports', depending on the location of the user, is an issue that could be effected by national 'dual-use goods' export restrictions.

Thus in this section both the use and export of cryptography will be looked at. Furthermore, provisions requiring Key Recovery or Key Escrow in order to provide for lawful interception in certain instances will be looked at:

- National Cryptography Rules including the US
- Cryptography Regulation in the EU
- Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 1995
- EU Dual Use Regulation, 1995
- Proposal for a Council Regulation (EC) setting up a Community Regime for the Control of Exports of Dual-Use Goods and Technology[36]
- Council Resolution on the Lawful Interception of Telecommunications, 1995
- Data Protection in the Telecommunications Sector, December 1997
- OECD Cryptography Policy Guidelines, 1997

National Encryption Regulations

Belgium

Belgium had, since 1994, a very ambiguous legislation with regard to the provision and the use of cryptography. This legislation has been modified by the law of 19 December 1997[37] amending the previous law of 21 March 1991. The provision and the use of cryptography in Belgium is as of the 1 January 1998 regulated by a new Article 109 as follows[38]:

[35] Whether or not signaling traffic can also be encrypted so as to prevent active and passive traffic analysis is unknown to the author at present.

[36] COM(1998)257

[37] Official Gazette (Moniteur Belge) of 30 December 1997.

[38] Official text in Dutch: "*Het gebruik van versleuteling is vrij. De terbeschikkingstelling aan het publiek van versleutelingsdiensten aangewezen door de Koning is onderworpen aan een voorafgaande aangifte aan het Instituut. Deze aangifte moet per aangetekende brief gebeuren uiterlijk vier weken voor de aanvang van de activiteiten*. (Ingevoegd bij art. 79 Wet 19 December 1997, B.S., 30 December 1997)."

"*The use of cryptography is free. The supply to the public of cryptographic services designated by the King is subject to a prior notification of the Institute. This notification has to be done by registered letter at least four weeks before the start of the activities.*"

The explanatory note states that the explicit mention that cryptography use is free was needed to differentiate the former law which wanted to subject encryption to a system of key deposits. The issue of key recovery or escrow is excluded for the time being: "this problem will be reviewed later, having regard to the development of the technology or of potential abuse of encryption by Mafia organisations or terrorists".

France

Very restrictive legislation concerning the use of cryptography exists in France. This legislation is currently in the course of modification. The basic legal provision is Article 28 of the Telecommunications Law n° 90-1170 of 29 December 1990[39] which originally stated that a prior authorisation from the SCSSI (Service Central de la Sécurité des Systèmes d'Information), a public administration belonging to the department of the Prime Minister, was required for the production, offering, exportation or use of cryptographic products and services, unless the products or services could not be used for other objectives than the authentication or the integrity of a message. In this latter case, the product or the service had only to be notified and the SCSSI had one month to deliver its opinion. In all other cases a prior authorisation was required.

The new French Telecommunications Act n°96-659 of 26 July 1996[40] relaxes the position somewhat. The most important changes introduced by Article 17 of this law with regard to the use, provision, import or export of cryptographic products and services (Art 28(I) of the 1990 Telecommunications Act), are:

1. The *use* of cryptographic products and services remains free when the product or the service do not allow the protection of confidentiality, particularly when they are only aimed at authenticating a communication or protecting the integrity of a message;
2. The *use* of cryptographic products or services will no longer be subject to authorisation when they are used for confidentiality purposes provided that this happens in the framework of a licensed TTP service[41];
3. The *provision, importation or exportation* of cryptographic products or services no longer require a prior authorisation from the SCSSI but only a declaration that they can not be used for confidentiality functions[42];

[39] Loi n° 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications, *Journal Officiel de la République Française*, 30 December 1990, 16439.

[40] Loi n° 96-659 du 26 juillet 1996 de réglementation des télécommunications, *Journal Officiel de la République Française*, 27 July 1996, 11384.
See also http://www.telecom.gouv.fr/francais/telecharg/telecharg.htm#texte (text of the Law) or http://www.telecom.gouv.fr/francais/activ/telecom/bfiche454.htm (short explanation).

[41] Art. 17 modifies Art. 28 (I), 1° of the 1990 Telecommunications Act as follows: "L'utilisation d'un moyen ou d'une prestation de cryptologie est
a) libre:
- si le moyen ou la prestation de cryptologie ne permet pas d'assurer des fonctions de confidentialité, notamment lorsqu'il ne peut avoir comme objet que d'authentifier une communication ou d'assurer l'intégrité du message transmis;
- ou si le moyen ou la prestation assure des fonctions de confidentialité et n'utilise que des conventions secrètes gérées selon des procédures et par un organisme agréés (…);
b) soumise à l'autorisation du Premier ministre dans les autres cas."

[42] Art. 17 modifies Art. 28 (I), 2° of the 1990 Telecommunications Act as follows: "La fourniture, l'importation de pays n'appartenant pas à la Communauté européenne et l'exportation tant d'un moyen que d'une prestation de cryptologie/

4. The *provision, import as well as export* of all cryptographic products or services for confidentiality objectives from or to countries outside the European Union require, as before, a prior authorisation from the SCSSI.

Thus the use of cryptography is free if not used for encryption purposes. If used for confidentiality purposes then it is still exempt from authorisation if this happens within a licensed TTP framework.

The provisions of the new article 28(I) are further specified in a draft "Authorisation Decree"[43] from the French government, which has been notified to the European Commission according to Directive 83/189.

The following provisions are important with regard to products and services concerning digital signatures:

Art. 1(a) clarifies the meaning of "products or services not allowing confidentiality functions", giving the following examples:

- "products or services aimed at protecting passwords, personal identification codes or similar authentication data, uses to control the access to data, resources, services or facilities, under the condition that they don't allow the encryption of files other than those containing passwords or identification codes or of any information other than what is necessary for access control;
- products or services aimed at creating or protecting a signature procedure, a cryptographic control value, a message authentication code or similar information aimed at verifying the source of the data, confirming the transmission of the data to the receiver or detecting the alterations or modifications which eventually endanger the integrity of the data, under the condition that they don't allow the encryption of the data themselves or of any information other that what is necessary for the authentication or the integrity control of the data concerned".

Thus encryption to guarantee identity confidentiality would come under the definition for 'products or services not allowing confidentiality functions' and hence would be free from regulation regarding 'use'.

Art. 1 of the draft decree also confirms that the use of the products and services just mentioned is free whereas, according to art. 3 of the draft decree, the provision, import or export of the same products or services require a prior "declaration"[44].

According to art. 5 of the draft decree the declaration has to be addressed to the SCSSI two months before the provision, import of export and the SCSSI has to accept the declaration within those two months provided that 1) the dossier is complete and 2) the product or the service is indeed only subject to declaration.

Two lists of cryptographic products and services will be established by ministerial decree: 1) a list of products and services for which the provision, use, import or export don't require any prior formalities at all, and 2) a list of products and services for which the provision, import or export would normally require a prior authorisation but for which a notification will be sufficient.

a) sont soumises à l'autorisation préalable du Premier ministre lorsqu'ils assurent des fonctions de confidentialité; (…)
b) sont soumises à la déclaration auprès du Premier ministre dans les autres cas."

[43] Décret définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.

[44] Following the remarks of the European Commission in the context of the procedure prescribed by Directive 83/189/EEC, a new chapter has been inserted in the draft decree, introducing for these products and services a simplified regime of notification that would only consist in the transmission of the administrative - and not the technical - part of the file. At the same time, however, the new text of the draft decree specifies that the simplified regime is reserved for cases where "l'impossibilité d'assurer des fonctions de confidentialité ne résulte pas d'un simple dispositif logiciel ou mécanique" (new art. 9bis).

Key escrow agencies

Besides the introduction of some less restrictive rules concerning the use, provision, import and export of cryptographic products and services - Art. 28(I) of the 1990 Telecommunications Act - the Law of 26 July 1996 modifies also the legal provisions for TTPs. The new Art. 28(II) of the 1990 Telecommunications Act provides that:

1. organisations in charge of keeping private cryptographic keys aimed at performing confidentiality functions (key escrow agencies) have to apply for a prior recognition from the Prime minister (the SCSSI);
2. the recognition will specify the products and services which key escrow agencies are allowed to use or provide;
3. key escrow agencies shall transmit the private keys to the judicial or other competent authorities according to the relevant legal provisions (wiretap legislation);
4. key escrow agencies have to exercise their activities on the French national territory.

The provisions of the new article 28(II) are further specified in a draft “TTP Decree”[45] from the French government. This draft decree contains more precise provisions concerning the conditions which have to be fulfilled by key escrow agencies in order to obtain a recognition by the SCSSI:

- only legal persons with a French nationality and effectively exercising their key escrow activities on the French national territory shall be recognised;
- the owner or the majority of the stakeholders, the managers and the board members have to be French nationals but exceptions are possible;
- the recognition needs the prior opinion of the minister of defence, the minister for internal affairs, the minister of industry and the minister of telecommunications;
- the recognition is awarded for a renewable period of four years under the condition that the key escrow agencies respect a folio of responsibilities[46] drafted by the SCSSI.

A recent action plan on "Electronic Commerce"[47], published 7 January 1998, by a task force led by Francis Lorentz, states that the government is "resolutely oriented towards a liberal reading of the law". It also urges a rapid implementation of the new law. It proposes further:

- a strong communication policy to promote the decrees;
- to promote with its (especially European) partners the principles underlying the policy;
- to bring about an agreement with France's most important trading partners on the principles and establishment of TTPs/ key deposits;
- to frequently review the regulatory framework (in particular, the 40-bit limit should be reviewed immediately), conducting a broad consultation on this before the end of 1998;
- a government TTP/deposit service to be established as a role model, while stressing the importance of developing private operators for this function as well;

[45] Décret définissant les conditions dans lesquelles sont agréés les organismes gérant, pour le compte d’autrui, des conventions secrètes de moyens ou de prestations de cryptologie permettant d’assurer des fonctions de confidentialité.
[46] “cahier des charges”
[47] see part III, "Creating Confidence", in particular part III.3 below

- that the decrees should not impose technical architectures for TTPs, but should limit themselves to functional demands.

La sécurité et la confidentialité des échanges

There are a number of interesting points of principle enunciated in this Chapter III.3 in the statement on Electronic commerce. The statement draws attention to the Privacy of Communications Act, 1991[48] and admits the necessity to allow encryption, particularly for commercial entities, whilst protecting the interests of national security.

Parties wishing to use encryption for confidentiality purposes and who do not want to make use of the Key Deposit system (which thus remains voluntary) above 40 bits only will require a prior authorisation. Otherwise, the keys are managed by a third party key deposit[49] which will be an organisation certified by the state and who must exercise its function on the French national territory. Previous restraints as to nationality have been dropped. LEA's will be given access to the keys when authorised by the law, however, no description of when LEA's will be granted authorisation is given. Lawful access can be requisitioned not only in judicial enquiries but also in administrative enquiries.

The statement suggests that the state may have to exercise the function of Key Depository while private operators develop. In such case measures of guaranteed transparency and availability would be put in place.

Germany

The initiative on Electronic Commerce ("Elektronischer Geschäftsverkehr"[50]), dated 29 October 1997, declares: "The federal government does currently not intend to legally regulate the marketing or use of cryptography products". In Germany, therefore, cryptography systems can be freely chosen and used."

The German Federal Parliament, in a 20 June 1996 resolution, found that effective encryption procedures may be freely chosen by participants within the scope of the constitutional right to confidential communication - which may be breached for internal or external security reasons.

UK

The DTI in June 1996 published a paper on regulatory intent for the provision of encryption services. Then in March 1997 a consultation paper was launched on Licensing of Trusted Third Parties for the Provision of Encryption Services for a two month discussion period. The consultation period took longer than anticipated and the resulting policy was published in April 1998.

The position of the UK can thus be summarised as follows:

Key Recovery and Key Management agents are encouraged to seek licensing. A clear distinction is made between CAs and Key Recovery Agents. Licensed service providers that provide encryption services will, therefore, be required to make recovery of keys (or other information protecting the secrecy of the information) possible through suitable storage arrangements to avoid the problems of loss of keys. This suggest more Key escrow than Key Recovery.

In response to these concerns, the Government intends to introduce legislation to enable law enforcement agencies to obtain a warrant for lawful access to information necessary to decrypt the content of communications or stored data (in effect, the encryption key). This does not include cryptographic keys used solely for digital signature purposes. The new powers will apply to those holding such information (whether licensed or not) and to users of encryption products. They will be exercisable only when appropriate authority has been obtained (for example, a judicial warrant for the purpose of a criminal

[49] "tiers de sequestre"
[50] http://www.bmwi.de/infogesellschaft.html

investigation or, in the case of interception of communications, a warrant issued by a Secretary of State) and will be subject to strict controls and safeguards.

United States

Cryptography export used to be controlled by the International Traffic in Arms Regulation (ITAR). At the end of 1996, cryptography export was transferred to the Export Administration Regulations (EAR) of the Department of Commerce. The export policy has since been relaxed. In February 1996, the ITAR rules were amended as regards the personal use of cryptography. Temporary export of products for personal use was exempted from the necessity of having a license. All other export of cryptography of 56 bits or above requires a licence. (Currently and up until Jan 1st, 1999 the export of non-recovery 56 bit encryption is subject to a temporary exemption).

Several attempts have been made in the US, both in Congress and by the public to try and loosen the strict export restrictions on cryptography.

There have been two interesting cases of note in the States - those of Bernstein and Junger challenging the constitutionality of the cryptography laws in the US and specifically the EAR.

In the case of Bernstein, a Northern California district court on December 18, 1996 judged the export regulations to be too restrictive. The district judge, Judge Patel, found the licensing system an unconstitutional prior restraint on free speech, having ruled earlier[51] that cryptography source code was protected by the First Amendment.

Then in August 1996, Junger a law professor and teacher of cryptography again challenged the constitutionality of the EAR regulations. He wanted to publish his class lectures on the Internet. On July 3, 1998 Judge Gwin of the United States District Court of the Northern District of Ohio held that computer programs are not writings protected by the constitution because they are "inherently functional" and granted summary judgement dismissing a suit challenging the regulations that forbid the publication of encryption programs on the Internet or the World Wide Web.

Both cases are on appeal at the moment.

There have also been a number of initiatives in Congress aimed at relaxing the export controls on encryption, the most recent being the E-PRIVACY Act (May 1998) (Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace).

In 1993 the Escrowed Encryption Initiative (EEI) - commonly known as the Clipper Initiative - was announced. This allowed for encryption of messages using an Escrowed Encryption Standard (ESS) which contained a classified, secret algorithm known as Skipjack. It also allowed LEA's to 'tap' these communications by means of a Law Enforcement Access Field (LEAF) that is transmitted along with each encrypted message. The LEAF contains information that can identify the chip used. This allowed LEA's, upon receipt of a warrant for tapping, to decipher the messages by obtaining the two parts of the chip's master key which were deposited with two escrow agencies -the National Institute of Standards and Technology and the Treasury Department's Automated Systems Division.

A follow-up proposal, known as Clipper II, suggested that the escrow agents could be independent bodies chosen by cryptography users.

In May, 1996, a paper was published entitled "Enabling Privacy, Commerce, Security

and Public Safety in the Global Information Infrastructure". Here the U.S. government proposes the establishment of a key management infrastructure (KMI) that incorporates key escrow. Participation in the KMI would be voluntary, and choice of encryption algorithms would be free. A Policy Approving Authority

[51] Decision of April 15, 1996

would certify Certification Authorities (CAs) and establish CA performance criteria to meet LEA needs. Before a public key can be certified, cryptography users should lodge their keys with an escrow agency (either a CA or an independent EA). Self-escrow would be allowed in some instances if for example the 'corporate' CA could guarantee its independence from the rest of the organisation, satisfy certain performance criteria and provide for the handing over of keys to LEA's when necessary.

On March 12, 1997, Key Recovery draft legislation was published. A registered CA may only issue a public key certificate if the user provides a registered KRA with sufficient information to allow timely plaintext recovery by law-enforcement or national security. KRAs - both registered and unregistered - shall disclose recovery information to government agents with a warrant or upon receipt of a written authorisation by the Attorney General. The draft legislation affirms that use of any encryption shall

be lawful except as provided in the Act or other law (which currently means any encryption use is lawful except in furtherance of a crime), and that use of the key recovery infrastructure is voluntary.

Key Recovery in the EU

Since the rise of cryptography use over the past decades, governments are increasingly worried about criminals using cryptography to thwart law enforcement. Many countries are as a result considering laws allowing law-enforcement and national-security capabilities through the regulation of cryptography by providing for lawful access.

If the CA plans to act as a key generator and provide its software to users outside its territory then it will have to consider export restrictions on cryptography.

Since 1995, 30 countries signed up to the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. The Wassenaar Arrangement controls the export of weapons and of dual-use goods, that is, goods that can be used both for a military and for a civil purpose; cryptography is such a good.

The export of cryptography is regulated in the EU by the Dual-Use Regulation, 1995.[52] In general, a license is needed for the export of cryptography hardware and software outside of the EU, with the exception of mass-market and public-domain software.

The dual-use regulation is to be replaced by a new regulation by 1 January 1999, according to the Proposal for a Council Regulation (EC) setting up a Community regime for the control of exports of dual-use goods and technology, COM(1998)257final. According to the proposal, the present regime has not sufficiently stimulated a convergence of national policies and practices; it is complex and "too cumbersome to be useful in practice". The main change for cryptography is that for exporting cryptography products within the EU, export licenses will be replaced by a simple notification. Also, the controls would now also include export through intangible means.

The discussion on Key Recovery in the Communication from the Commission Towards A European Framework for Digital Signatures And Encryption[53] is of interest. Although the Commission does not completely reject the application of a Key Recovery system, the arguments against such a system are given more weight. Art 2(3)(ii) says:

“The acceptance of such a system remains to be seen, but given its implied overheads, can not be regarded as an incentive for electronic commerce. In any case, restrictions imposed by national licensing schemes, particularly those of a mandatory nature, could lead to Internal Market obstacles and reduce the competitiveness of the European Industry.”

[52] The December 1994 EU Council Regulation (EC) No. 3381/94 (amended by Regulation (EC) 837/95 of 10 April 1995) and EU Council Decision No. 94/942/CFSP (last amended by Council Decision 98/232/CFSP), in force since July 1995.

[53] October 1997, COM (97) 503

Council Resolution of 17 January 1995 on the Lawful Interception of Telecommunications

This resolution was adopted in January 1995 but was not published until November 1996. A resolution is what is known as 'soft law' in that it is not legally binding. However, under K 4(3) of the Maastricht Treaty any actions taken by the Council are by unanimous decision unless otherwise stated. Thus the resolution has a great political impetus behind it. The area of competence under which this resolution falls is also the Third Pillar. K1(9) of Maastricht gives the EU competence to act in areas of terrorism, drug trafficking etc., under which the area of lawful interception of communications can come. K(1)(9) states:

For the purposes of achieving the objectives of the Union, in particular the free movement of persons, and without prejudice to the powers of the European Community, Member States shall regard the following areas as matters of common interest:

9. Police co-operation for the purposes of preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime, including if necessary certain aspects of customs so-operation, in connection with the organisation of a Union-wide system for exchanging information within European Police Office (Europol).

Whilst reaffirming the need for individuals to guard their right to privacy, it is acknowledged that in view of technological developments, observing this right comes against specific legal and technical difficulties. It is on the other hand recognised that the legally authorised interception of telecommunications is an important tool for the protection of national interest, in particular national security and the investigation of serious crime.

A list of requirements are laid down in the Annex of the Resolution and these constitute a summary of the needs of law enforcement agencies (LEA's). Article 2 provides that the Minister for Telecommunications should collaborate with the Minister for Justice in the individual member states to ensure that the requirements are implemented satisfactorily.

The most important requirements are as follows:

The entire telecommunications should be transmitted to the LEA and also all call-associated data. The call-associated data constitutes such data as:

- Signalling of access ready status
- Called party number for outgoing connections even if no successful connection was established
- Calling party number for incoming connections even if no connection was successfully established
- All signals emitted by the 'target' even after the call is established to activate features such as call transfer and conference calling
- Beginning, end and duration of connection
- Actual destination and intermediate directory numbers if call has been diverted

LEA's should have access to accurate location data of the 'target'. LEA's should have access to the specific services used by the 'target" (1.6)

LEA's require a real-time, full-time monitoring capability for the interception (2)

If NOs/SPs initiate encoding, compression or encryption of telecommunications traffic, LEA's require the NOs/SPs to provide intercepted communications 'en clair'. (3.3) NB If the target is the one who initiates encryption, what happens?

LEA's require NOs/SPs to implement interceptions urgently (in urgent cases within a few hours or minutes) (9)

Data Protection Directive in the Telecommunications Sector December 1997

Member States shall (Art 4) ensure the confidentiality of communications and in particular prohibit listening, tapping, storage or other kinds of interception or surveillance of communications.

Art 4(2), however, allows the legally authorised recording of communications for lawful business practice in order to provide evidence of any contract or business communication. Art 14(1) provides a general exception for the interests of public security, defence and the prevention, investigation, prosecution of a criminal offence.

OECD Guidelines on Lawful Interception

The OECD[54] Cryptography policy guidelines were issued in March 1997.

National Law cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the

additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for

lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested

and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of

cryptographic methods.

Key management systems could provide a basis for a possible solution which could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access

to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic

key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key

[54] Organisation for Economic Co-operation and Development