EG 201 620 V1.1.1 (1999-01)

ETSI Guide

Intelligent Networks (IN); Security studies for Cordless Terminal Mobility (CTM)

Reference

DEG/NA-061207 (f0000icq.PDF)

Keywords

CTM, security

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide (EG) has been produced by ETSI Technical Committee Network Aspects (NA).

1 Scope

The present document describes the security features that are necessary and sufficient to run CTM in a way that it does no harm to its participants. Recommendations on security are made that fulfil at least the security objectives as stated in the CTM service description and in the documents on IN architecture for the support of CTM. The single network case and the inter-working between different (public, or public and private) networks are considered as well as CTM phase 2 (as far as it is already specified).

As an initial security analysis outlined in annex A shows, CT2 is for security reasons not considered as suitable for CTM, and hence only DECT is assumed as the appropriate radio interface.

The present document is structured in a formal way going from an understanding of the system via a threat analysis to the specification of security mechanisms, as illustrated in the following figure.

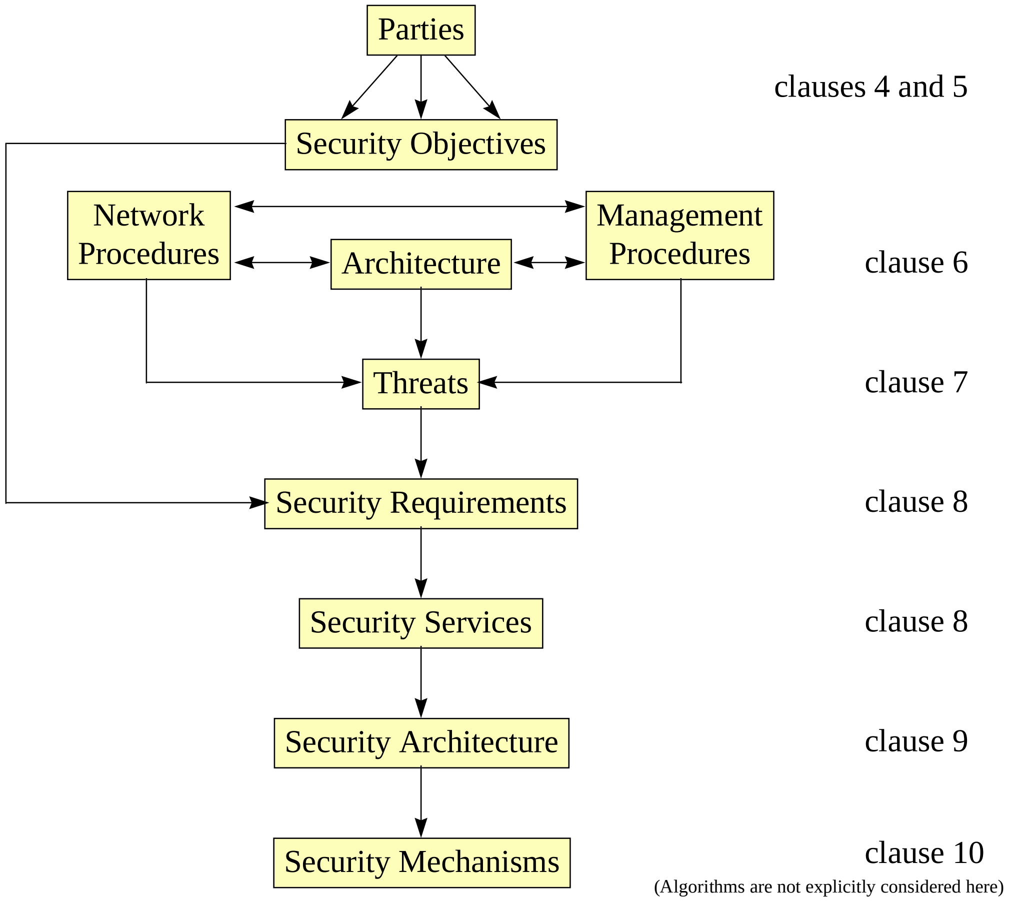


Figure 1: Document structure

The result of the security studies on CTM are the recommendations to be found in clauses 8, 9 and 10. They may be used for further documents guides and standards dealing with CTM security.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] EN 300 175-7: "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features".

[2] ETS 300 331: "Digital Enhanced Cordless Telecommunications (DECT); DECT Authentication Module (DAM)".

[3] ETS 300 444: "Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)".

[4] EG 201 096-1 (V1.1): "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 1: CTM phase 1 for single public network case".

[5] EG 201 096-2 (V1.1): "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 2: CTM interworking between public IN".

[6] EG 201 096-3 (V1.1): "Intelligent Network (IN); Cordless Terminal Mobility (CTM); IN architecture and functionality for the support of CTM; Part 3: CTM interworking between private networks and public IN".

[7] I-ETS 300 131 (1994): "Radio Equipment and Systems (RES); Common air interface specification to be used for the interworking between cordless telephone apparatus in the frequency band 864,1 MHz to 868,1 MHz, including public access services".

[8] EN 301 175 (V1.1): "Cordless Terminal Mobility (CTM); Phase 1; Service description".

[9] EN 301 273: "Cordless Terminal Mobility (CTM); Phase 2; Service description".

[10] ETR 232 (1995): "Security Techniques Advisory Group (STAG); Glossary of security terminology".

[11] ETS 300 391: "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: Specification".

[12] ETR 331: "Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies".

[13] ETR 336 (1997): "Telecommunication Management Network (TMN); Introduction to standardizing security for TMN".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the definitions from ETR 232 apply:

NOTE: "Encryption" is used in the following as synonym for "Ciphering".

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AC	Authentication Code
CAP	CTM Access Profile
CCAF	Call Control Agent Function
CCF	Call Control Function
CS1	Capability Set 1
CS2	Capability Set 2
CT2	Cordless Telephone 2nd generation
CTM	Cordless Terminal Mobility
CUSF	Call Unrelated Service Function
DAM	DECT Authentication Module
DECT	Digital Enhanced Cordless Telecommunication
DSS1	Digital Subscriber Signalling No. 1
DSS1+	Enhanced DSS1
ETSI	European Telecommunications Standards Institute
FP	Fixed Part
FT	Fixed Termination (of DECT)
GAP	Generic Access Profile
HD	Home Domain
IN	Intelligent Network
INAP	Intelligent Network Application Part
ISDN	Integrated Services Digital Network
LE	Local Exchange
PIN	Personal Identification Number
PP	Portable Part
PSTN	Public Switched Telephone Network
PT	Portable Termination (of DECT)
SCF	Service Control Function
SCUAF	Service Control User Agent Function
SCF_{sl}	Service Control Function for service logic
SCF_{mm}	Service Control Function for mobility management
SDF	Service Data Function
SMP	Service Management Point
SSF	Service Switching Function
TMN	Telecommunications Management Network
UAK	User Authentication Key
VD	Visited Domain

4 Security Objectives

The requirements for CTM security and for Management security for CTM are originating from different sources:

- Customers/Subscribers need confidence in the CTM and in the Management for CTM and the services offered, including correct billing.
- The Public Community/Authorities demands security by Directives and Legislation, in order to ensure availability of services, fair competition and privacy protection.
- Network Operators/Service Providers themselves need security to safeguard their operation and business interests, and to meet their obligations to the customers and the public.
- The CTM phase 1 and 2 service descriptions (EN 301 175 and EN 301 273) require security features, in order to protect from fraudulent use, fraudulent access, eavesdropping, and malicious behaviour.

The reason why these interested parties are increasingly aware of security requirements is the fact that there are growing threats and risks caused by changes in the overall regulatory and technological environment.

The purpose of this clause is to describe the aim of the security measures taken in a network for CTM and in a Management for CTM. Focus is on what security will achieve rather than how it is done. These generic security objectives form, together with the system description, a basis for threat analysis and risk assessment.

The listed objectives do not contain general constraints like performance, cost, user friendliness etc.

4.1 Customers' (Subscribers') Objectives

The objectives of customers are not uniform. An enterprise does not always require the same as a private person. The following list gives examples of possible objectives which may have implications on security:

- availability and correct functionality of service subscription and over the air (de-)registration;
- reachability for incoming calls by availability and correct functionality of location registration service;
- availability and correct functionality of outgoing call service;
- no possibility to take unfair advantage of a handheld or a CTM service;
- correct and verifiable billing;
- data integrity;
- data confidentiality/privacy;
- location confidentiality;
- capability to use a service anonymously.

4.2 CTM Service Providers' and Network Providers' Objectives

The goal of network operators and service providers is to make good revenue by operating a CTM system. This means to have large entries of money and a minimum exit of money.

The following list gives examples of possible objectives how to achieve the goal. These objectives may have implications on security:

- availability of network procedures for CTM;
- availability of service, network and element management for CTM;
- correct functionality of network procedures for CTM;
- correct functionality of service, network and element management for CTM;
- correct and verifiable billing, above all no possibility of fraud;
- non-repudiation for all network procedures and for all management activities;
- preservation of reputation (above all preservation of customers' and investors' trust).

4.3 Manufacturers' Objectives

The goal of CTM systems manufacturers is to make good revenue by selling their systems to operators and users, in a large quantity and for a good price.

The following list gives examples of objectives which may have implications on security:

- fulfilling market objectives;
- preservation of reputation.

4.4 Objectives Derived from the CTM Service Descriptions

The CTM phase 1 and 2 service descriptions (EN 301 175 and EN 301 273) require the security features terminal authentication, network authentication and encryption, in order to protect from fraudulent use, fraudulent access, eaves dropping, and malicious behaviour.

The following is an extract of the security objectives and requirements as described in the CTM phase 1 and 2 service descriptions (EN 301 175 and EN 301 273). The security related parts of the two service descriptions are identical. For reference purposes, the statements are numbered by small letters at the end.

Core requirements on security:

- Security mechanisms shall be provided by using terminal authentication, network authentication and encryption, subject to the limitations of the appropriate cordless access standards (a).
- Different service providers may offer different levels of security mechanisms to their subscribers (b).
- Terminal authentication may be invoked in various cases, e.g. when the subscriber requests:
    - access to a service (including some or all of originating/terminating a CTM call, activating or deactivating feature/supplementary service) (c);
    - a change of subscriber related information (including some or all of location handling, registration or erasure of a feature/supplementary service) (d).

Normal procedures, invocation and operation, core requirements:

- Authentication may be invoked by both the user and the network at any time (e).
- Encryption shall be invoked (f).

Exceptional procedures, registration and erasure - core requirements:

- Subscription registration shall be rejected if authentication fails (g).

Exceptional procedures, registration and erasure - optional requirements:

- Termination of access rights shall be rejected if the network authentication fails (h).

Exceptional procedures, invocation and operation - core requirements:

- If authentication fails, the network may withdraw or limit the service to the user (i).
- If encryption fails, then the connection may proceed without encryption (j).

4.5 Main Objectives

The objectives listed above can be summarized to the following main security objectives:

- **confidentiality** of CTM service data, of CTM management data, and of communications using CTM;
- **integrity** of CTM service data, of CTM management data, and of communications using CTM;
- **accountability** for all CTM service invocations and for all CTM management activities; and
- **availability** of all CTM services and of all CTM management functions.

Therefore, threat analysis, risk assessment and security measures will only be based on these objectives.

5 Legislation Issues

The following areas of legislation may have influence on the realization of security.

5.1 Privacy

Privacy legislation is of increasing importance; there are strong restrictions in many countries with regard to storage and visibility of data. Therefore, when offering a CTM service, or when designing data processing functions and defining the kind of data being generated or stored within CTM systems, CTM service providers shall consider the relevant national data protection laws.

The definition of privacy for CTM includes:

- privacy of information: keeping information exchanged between CTM service functions away from third parties;
- limitations on collection, storage and processing of personal data: personal data may only be collected, stored and processed if there is a relationship between the data and the actual provision of CTM services;
- disclosure: the obligation of a network and service providers to keep information concerning customers away from third parties;
- inspection and correction: the right of the customer to inspect and correct information about himself stored by the service and/or network provider.

Privacy legislation will mostly concern the security objectives regarding "data confidentiality" and "data integrity". For CTM special concern in this respect shall be paid to the contents of personal data in the CTM service profile. These data and the access conditions to it for the service provider's personnel, the subscriber and the user himself shall be limited, in accordance with the relevant European guidelines and national laws.

5.2 Security Order

National laws concerning the security order:

- demand proper protection of information and infrastructure to ensure the availability and the integrity of the telecommunication network (including the TMN);
- may restrict the usage of cryptographic methods.

This legislation will mostly concern the security objectives regarding "data confidentiality", "data integrity" and "availability".

5.3 Lawful Interception

Lawful interception means the obligation of the network operator to co-operate and provide information in case of criminal investigations (see e.g. ETR 331).

This legislation will mostly influence the security objectives regarding "data confidentiality".

5.4 Contract

It shall be possible to use information concerning the contract for communication services between two entities in case of a dispute in a court of law.

This legislation will mostly influence the security objectives regarding "accountability" and "data integrity".

6 Architecture

In this clause the mapping of the functional to the physical architecture and the network and management procedures are shortly described. This shall provide the basis for the threat and risk analysis in clauses 7 and 8, and for the placement of the security services and mechanisms described in clauses 9 and 10.

6.1 Functional Architecture

The functional IN architecture for the support of CTM in single networks is described in EG 201 096-1. The functional IN architecture for the support of CTM inter-working is described in EG 201 096-2 and EG 201 096-3.

A mapping of the functional architecture to physical entities for single networks is shown in Figure 2. For multiple networks (see EG 201 096-2 and EG 201 096-3) the same model applies with the understanding that some entities (e.g. those of the Home Domain) may belong to another network.

There are two categories of Service Data Function (SDF) defined: SDFsl and SDFmm.

SDFsl should be understood as a shorthand notation to refer to an SDF which contains CTM user profiles.

SDFmm should be understood as a shorthand notation to refer to an SDF which contains information about roaming users temporarily stored by a Service Control Function (SCF) as the result of location management procedures.

Similarly two categories of SCF, SCFsl and SCFmm, are defined.

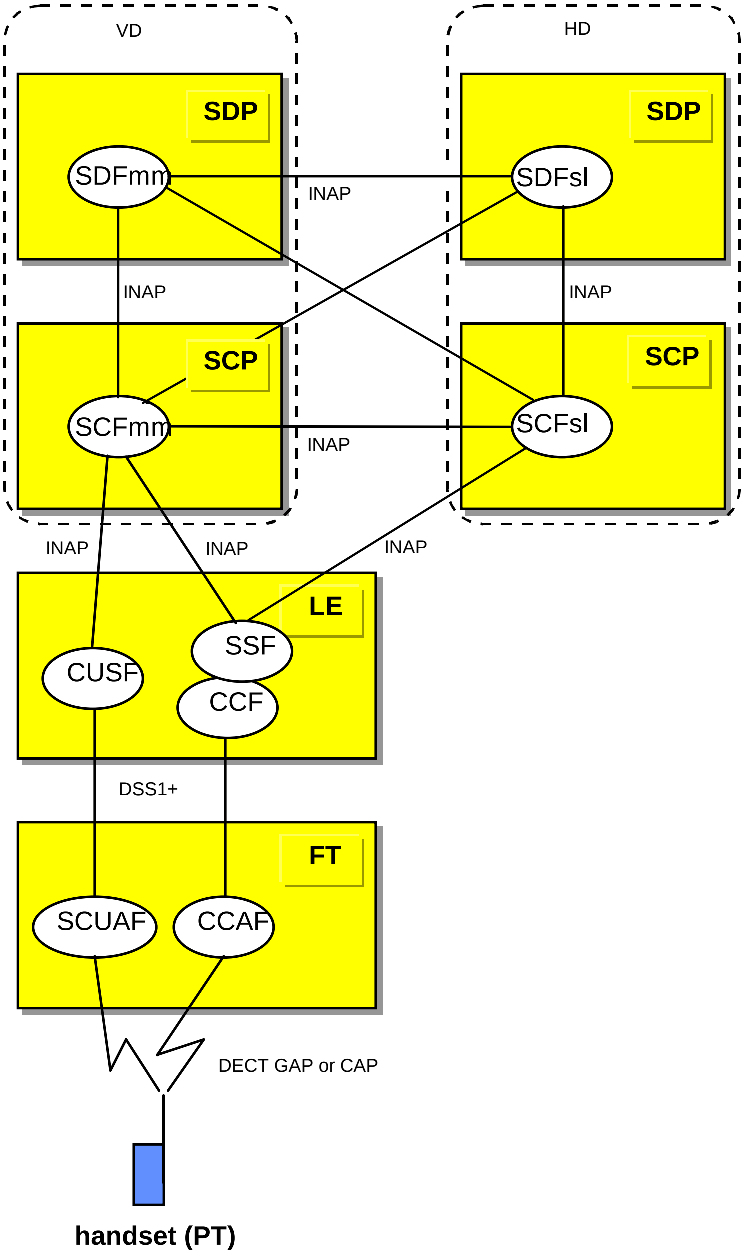
SCFsl should be understood as a shorthand notation to refer to an SCF running a particular service logic.

SCFmm should be understood as a shorthand notation to refer to an SCF running a particular service logic dedicated to location management and mobility authentication.

An SDF may play the role of an SDFsl, an SDFmm or both. Similarly an SCF may play the role of an SCFsl, an SCFmm or both. The introduction of a Visited-Domain (VD), and a Home-Domain (HD) in figure 2 for CTM inter-working requires that the SCF in HD shall act as SCFsl, and in VD the SCF shall act as SCFmm. Similarly for the SDF: in HD the SDF shall act as SDLsl; in VD the SDF shall act as SDFmm.

Home Domain shall be understood to be that entity able to initially create and to permanently modify or destroy the data record of a CTM user.

Visited Domain shall be understood as an entity able to copy and use, but not permanently modify or destroy, the data record of a CTM user.



NOTE 1: The FT shown may be part of an Access Network, a Private Network, a Public Network or a Home DECT System.
NOTE 2: SCUAF and CCAF shall be located in the same physical entity.
NOTE 3: CUSF, CCF and SSF shall be located in the same physical entity.
NOTE 4: The interface between SDLsl and SDFmm is optional.
NOTE 5: Only entities and interfaces relevant for the CTM procedures relating to security are drawn in this figure.

Figure 2: Mapping between functional and physical entities

6.2 Network Procedures

Network procedures are described in EG 201 096-1 to 3. However modifications may be proposed according to the results of the present document for support of security mechanisms.

6.3 Management Procedures

Management procedures will only be considered where necessary in order to guarantee the required level of security.

7 Threat Analysis and Risk Assessment

The threat analysis in the following is done under the assumption that security features are provided according to the descriptions in EG 201 096-1 to 3.

An initial security analysis on the possibilities to use CT2 for CTM led to the conclusion presented in annex A. For security reasons, CT2 has been evaluated as not suitable for CTM. Therefore only DECT is considered as radio interface in the following. Especially, it is assumed that PT authentication and encryption on the air interface can be provided according to the DECT security standard (see EN 300 175-7).

7.1 Threats

In this subclause a description of main threats concerning the network procedure aspects of CTM and the Management aspects is given, in order to evaluate risks. In the context of this concept paper, only intentional non-physical threats are taken into account. The following threats are partly derived from ETR 336. These threats are:

- Masquerade ("spoofing"):

  The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.

- Unauthorized access:

  An entity accesses data in violation to the security policy in force.

- Eavesdropping:

  A breach of confidentiality by unauthorized monitoring of communication.

- Loss or corruption of information:

  The integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.

- Repudiation:

  An entity involved in a communication exchange subsequently denies the fact.

- Forgery:

  An entity fabricates information and claims that such information was received from another entity or sent to another entity.

- Denial of service:

  An entity fails to perform its function or prevents other entities from performing their functions.

These threats counteract the identified main objectives as shown in table 1.

Table 1: Threats to security objectives

Threat \ Objective	Data Confidentiality	Data Integrity	Accountability	Availability
Masquerade	X	X	X	X
Unauthorized access	X (within a system)	X (within a system)	X	X
Eavesdropping	X (on the line)			
Loss or corruption of information		X (on the line)	X	X
Repudiation			X	
Forgery		X	X	
Denial of service				X

7.2 Threats Related to CTM Network Procedures

The threats listed in the following have been found by consideration of the CTM procedures as described in EG 201 096-1 to 3.

7.2.1 General Threats

1) Eavesdropping of CTM-id on IN interfaces or entities:

   On most of the IN interfaces and IN entities used in the differing procedures, it may be possible to eavesdrop a valid CTM-id. This could lead to other persons knowing the location of the CTM user, or to a masquerading threat (see later on threats related to masquerading).

   Resulting threats:

   a) masquerading as a real user;

   b) eavesdropping of personal information.

2) Eavesdropping of CTM-id on the air interface:

   This could lead to other persons knowing the location of the CTM user, or to a masquerading threat (see later on threats related to masquerading).

   Resulting threats:

   a) masquerading as a real user;

   b) eavesdropping of personal information.

3) Getting the CTM-id from a terminal:

   This could lead to other persons knowing the location of the CTM user, or to a masquerading threat (see later on threats related to masquerading).

   Resulting threats:

   a) masquerading as a real user;

   b) eavesdropping of personal information.

4) Denial of service:

   An attacker may wish to make any procedure impossible. This can be done at any interface used during the procedures (e.g. by modification of data) or by manipulating any entity used during the procedures. Normal service for the users and/or service providers is degraded or impossible.

   Resulting threats:

   a) denial of service;

   b) degradation of service.

5) Unauthorized access to data:

   An attacker may wish to get some information stored in the databases (SDF).

   Resulting threats:

   a) denial of service;

   b) masquerading as a real user;

   c) eavesdropping of personal information.

6) Flooding the network:

   A motivation may be revenge or just hacking for fun. Any entities or interfaces can be the target for such an attack method.

   Resulting threats:

   a) denial of service;

   b) degradation of service.

7) Stolen terminals:

   A stolen terminal can be used at least until the real user reports the theft of his terminal if the access to the terminal is not protected by a PIN. The terminal can also be used in order to decipher previously recorded communications from and to the user.

   Resulting threats:

   a) theft of service;

   b) deciphering of previously recorded communications;

   c) the attacker can receive incoming calls intended for the regular subscriber. This is relevant especially for data services.

8) Subscription fraud:

   An attacker can take a subscription and use it extensively with no intention to pay (false address given, no money on his account, etc…).

   Resulting threat:

   a) loss of revenue.

9) Unauthorized access to data in terminals:

An attacker may get some data from a terminal(e. g. CTM-id and authentication data) and use them later on.

Resulting threats:

a) masquerading;

b) deciphering of previously recorded communications.

10) Masquerading as a network entity to an other one:

An attacker may try to masquerade as a network entity towards a network entity in order either to get information, pervert a service, deny a service or re-route some calls.

Resulting threats:

a) masquerading;

b) unauthorized access;

c) eavesdropping;

d) denial of service.

7.2.2 Threats related to Terminal Authentication and Ciphering Procedures

7.2.2.1 Terminal authentication - case 1: DECT couples (RS, KS) previously stored in SDF_{MM}

1) Eavesdropping of CTM-id and KS

on SDF_{MM} - SCF_{MM} interface or on one of these entities itself. It is assumed that the attacker is able to perform the relevant DECT algorithms.

Resulting threats:

a) Masquerading of a user for outgoing CTM calls, resulting in call charged to the regular subscriber.

b) Masquerading of a user for incoming CTM calls, possibly resulting in receipt of information determined for that user.

c) Masquerading as network to the user even if network authentication is required, e.g. in order to perform a subscription de-registration procedure leading to a denial of service to that user.

d) Deriving DCK and eavesdropping the regular subscriber's communication on the air interface by deciphering.

2) Eavesdropping of CTM-id and DCK

on SDF_{MM} - SCF_{MM} interface or on one of these entities itself. It is assumed that the attacker is able to perform the DECT Cipher algorithm.

Resulting threat:

a) Eavesdropping the regular subscriber's communication on the air interface by deciphering. The attacker shall be able to perform the DECT Cipher algorithm in order to decipher. Eavesdropping of the over-the-air communication is possible only for the communication following this authentication procedure, and for further communications as long as the DCK is not changed. In case of access to the SDF_{MM}, several DCKs belonging to a CTM-id may be read and subsequently be used for several eavesdropping attacks of communication over the air interface.

7.2.2.2 Terminal authentication - case 2: DECT triples (RAND, RS, RES) previously stored in SDF_{MM}

1) Eavesdropping of CTM-id and RES

on SDF_{MM} - SCF_{MM} interface, on SCF_{MM} - CUSF interface, on CUSF - SCUAF interface, on one of these entities itself, or on the air interface.

Resulting threat:

a) Masquerading as the regular subscriber. The attacker need not know the DECT algorithms to perform this threat. Masquerading is possible only if the random numbers are not changed for the next authentication attempt. In case of access to the SDF_{MM}, several triples (RAND, RS, RES) belonging to a CTM-id may be read and subsequently be used for several masquerading attacks over the air interface.

2) Eavesdropping of CTM-id and DCK

on SCF_{MM} - SDF_{MM} interface or on one of these entities itself.

Resulting threat:

a) Eavesdropping of the regular subscriber's communication on the air interface. The attacker shall be able to perform the DECT Cipher algorithm in order to decipher. Eavesdropping of the over-the-air communication is possible only for the communication following this authentication procedure, and for further communications as long as the DCK is not changed. In case of access to the SDF_{MM}, several DCKs belonging to a CTM-id may be read and subsequently be used for several eavesdropping attacks of communication over the air interface.

7.2.2.3 Downloading of authentication data

1) Eavesdropping of CTM-id and KS, or eavesdropping of CTM-id and RES, respectively

on SCF_{MM} - SDF_{MM} interface, on SCF_{MM} - SCF_{SL} interface, or on SCF_{SL} - SDF_{SL} interface or on one of these entities itself.

Resulting threats:

a) Masquerading as the regular subscriber. Depending on the use of session keys or triples and on the validity time of these data, the subsequent masquerading or eavesdropping can be performed once only or several times. Depending on the use of session keys or triples, the attacker need or need not know the relevant DECT algorithms to perform the resulting masquerading threat.

b) In case that session keys are used and the KS is eavesdropped, masquerading as network to the user is possible even if network authentication is required, e.g. in order to perform a subscription de-registration procedure leading to a denial of service to that user.

2) Eavesdropping of CTM-id and DCK

on SCF_{MM} - SDF_{MM} interface, on SCF_{MM} - SCF_{SL} interface, on SCF_{SL} - SDF_{SL} interface, or on one of these entities itself.

Resulting threat:

a) Eavesdropping of the regular subscriber's communication on the air interface. This threat is relevant only if the method to transmit triples is used, it is not relevant if the method to transmit session key is used. Depending on the validity time of the DCK, the subsequent eavesdropping of communication on the air interface can be performed once only or several times. The attacker has to be able to perform the DECT Cipher algorithm in order to decipher.

3) Masquerading as SCF_{MM}

in order to get authentication data (CTM-id, and session keys or triples) from the SDF_{SL} on request.

Resulting threats:

a) Masquerading of the regular subscriber if and only if these data are not changed at each request from an SCF_{MM} to an SCF_{SL}/SDF_{SL}.

b) Masquerading of the network if session keys are used, e.g. in order to perform a subscription de-registration procedure leading to a denial of service to that user.

c) Eavesdropping of the regular subscriber's communication on the air interface. This is possible if and only if these data are not changed at each request from an SCF_{MM} to an SCF_{SL}/SDF_{SL}.

7.2.2.4 Ciphering procedure

1) Eavesdropping of CTM-id and related DCK
on SCF_{MM} - SDF_{MM} interface or on SCF_{MM} - CUSF interface or on CUSF - SCUAF interface or on one of these entities itself.

Resulting threat:

a) Eavesdropping of the regular subscriber's communication on the air interface by deciphering.

2) Deletion of Ciphering Request message
on the SCF_{MM} - CUSF interface or on the SCUAF - CUSF interface and (if necessary) modification of the Ciphering Reply and/or Report Ciphering Reply message on the same interfaces.

Resulting threat:

a) Eavesdropping of the regular subscriber's communication on the air interface. This communication is then not ciphered and hence the attacker needs neither know the algorithm nor the relevant key.

3) Deletion of Ciphering Request message

on the air interface, and (if necessary) modification of the according Reply message.

Resulting threat:

a) Eavesdropping of the regular subscriber's communication on the air interface. This communication is then not ciphered and hence the attacker needs neither know the algorithm nor the relevant key.

4) Encryption failure

If encryption fails for whatever reason (on purpose or by system failure), the connection may proceed without protection from eavesdropping - according to the CTM service descriptions (EN 301 175 and EN 301 273).

Resulting threat:

a) Eavesdropping of the regular subscriber's communication on the air interface. This communication is then not ciphered and hence the attacker needs neither know the algorithm nor the relevant key.

7.2.2.5 Location of threats

The following table and the similar tables in the following subclauses detail the different locations where the threats can be performed.

Table 2: Location of threats related to terminal authentication and ciphering procedures

Location Threats	PT	PT - SCUAF	SCUAF	SCUAF -CUSF	CUSF	CUSF - SCF_{MM}	SCF_{MM}	SCF_{MM} - SDF_{MM}	SDF_{MM}	SCF_{MM} - SCF_{SL}	SCF_{SL}	SCF_{SL} - SDF_{SL}	SDF_{SL}
7.3.1.1.1							UA	E	UA				
7.3.1.1.2							UA	E	UA				
7.3.1.2.1		E	UA	E	UA	E	UA	E	UA				
7.3.1.2.2							UA	E	UA				
7.3.1.3.1							UA	E	UA	E	UA	E	UA
7.3.1.3.2							UA	E	UA	E	UA	E	UA
7.3.1.3.3							M			U			
7.3.1.4.1		E	UA	E	UA	E	UA	E	UA				
7.3.1.4.2		E		M		M							
7.3.1.4.3		M, E											
7.3.1.4.4	F	F, E	F	F	F	F							

The following abbreviations are used in this table and in the following tables:

E	=	Eavesdropping
M	=	Manipulation/Modification
UA	=	Unauthorized Access
U	=	Using
F	=	Failure

7.2.3 Threats related to location registration procedures

These threats are covered by the threats related to CTM incoming and outgoing call procedures (see subclauses 7.3.6.1, 7.3.6.2, 7.3.7.1 and 7.3.7.2).

7.2.4 Threats related to Data Deletion Procedures

1) Eavesdropping of old address.

   Resulting threat:

   a) Knowledge of where a PT was.

2) Masquerading network entities to delete data

   In this procedure, a deletion can be done in the following entities: SDF_{MM}, CUSF and SCUAF. This can be done by manipulating these entities or by sending them cancellation request. In the case of a deletion in CUSF or SCUAF, outgoing calls can be performed as a new location registration is done, incoming calls can also be performed as the PT address is in the SDF_{MM}. In the case of a deletion in SDF_{MM}, outgoing calls can be performed as a new location registration is done, however, to perform incoming calls the PT address is to be known by the SDF_{MM}, to do this the location registration suggest procedure is necessary.

   Resulting threat:

   a) Incoming calls to a PT may not happen (in case of deletion in SDF_{MM}) before location registration suggest procedure is performed.

Table 3: Threats related to data deletion procedures

Location Threats	PT	PT/ SCUAF	SCUAF	SCUAF/ CUSF	CUSF	SCUSF/ SCF$_{MM}$	SCF$_{MM}$	SCF$_{MM}$/ SDF$_{MM}$	SDF$_{MM}$	SCF$_{MM}$/ SDF$_{SL}$	SDF$_{SL}$	SCF$_{SL}$/ SDF$_{SL}$	SCF$_{SL}$	SCF$_{SL}$/ SCF$_{MM}$
7.3.3.1 Eavesdropping of old address			UA $*^1$		UA $*^1$	E$*^1$	UA $*^1$	E$*^1$	UA $*^1$		UA $*^2$	E$*^2$	UA $*^2$	
7.3.3.2 Masquerading network entities to delete data			M	M	M	M		M	M					

NOTE $*^1$: The eavesdropping can be done until the cancellation of the information.

NOTE $*^2$: The threat can be done in this entity or at this interface only if this information is present (depending on the different cases described in EG 201 096-1.

7.2.5 Threats related to Subscription Registration Procedures

1) Eavesdropping of data in an over-the-air registration process and subsequent exhaustive search for AC:

Assuming that the attacker knows the DECT algorithms and has attained RAND_F, RS, RES and CTM-id from eavesdropping a subscription process over-the-air, he could find the corresponding AC by exhaustive search and thereby also the UAK. The effort to search for the AC depends on the length of the AC, which is set to a maximum of 8 entered decimal digits in the GAP and the CAP. The attacker could e.g. produce a table with all possible ACs and look for a matching of his calculated RES with the eavesdropped RES. If the random numbers RAND_F and RS are not changed for each subscription registration, the attacker could reuse his table for the data of other subscribers.

Resulting threats:

a) masquerade as the regular subscriber;

b) masquerade as the network towards the real subscriber to eavesdrop his communications;

c) eavesdropping of the user's communications later on.

2) Copying an AC directly from the real subscriber or from the distribution process to him/her, eavesdropping of data in the over-the-air registration process and subsequent calculation of the UAK:

A valid AC can be obtained by an attacker during the distribution (e.g. by phone or mail) of the AC to a real subscriber or by copying it without the knowledge of the real subscriber/user. The attacker can now wait for and eavesdrop on the real user's over-the-air subscription registration and get the RAND_F, RS and CTM-id then. He can then calculate the UAK (knowledge of the DECT algorithms are needed) and enter it together with the CTM-id or simulate an over-the-air registration process to his equipment to load these values.

Resulting threats:

a) masquerade as the regular subscriber;

b) masquerade as the network towards the real subscriber to eavesdrop his communications;

c) eavesdropping of the user's communications later on.

3) Copying an AC directly from the real subscriber or from the distribution process to him/her, masquerade as the network towards him in an over-the-air registration process and subsequently masquerade as network to him ("stolen subscriber"):

An AC can be obtained by an attacker during the distribution (e.g. by phone or mail) of the AC to a real subscriber or by copying it without the knowledge of the real subscriber. The attacker can now masquerade as the network towards the subscriber in an over-the-air subscription registration, using his own RAND_F, RS and CTM-id. He can then calculate the UAK (knowledge of or access to the DECT algorithms are needed) and subsequently masquerade as the network against the subscriber/user. The subscriber now believes (for a while) that he is subscribing to and using the real service provider's network, while technically he can only have services in the faked network. The fraud should be discovered by the subscriber at time of first billing.

Resulting threats:

a) masquerade as network towards the subscriber, which may allow redirecting of calls;

b) masquerade as network towards the subscriber to eavesdrop his communications;

c) masquerade as network towards the subscriber in order to bill him for calls he makes (in the faked network).

4) Masquerading of a user during the over-the-air subscription registration procedure after obtaining the AC illicitly directly from the service provider or from the distribution process to a real subscriber (stealing of identity):

A valid AC can be obtained by an attacker, maybe with assistance of an insider, from the service provider's premises or network (e.g. on the SMP-SCP interface or by unauthorized accesses to network entities or data bases). Alternatively a valid AC can be stolen during the distribution (e.g. by mail) to a real subscriber. The AC can then be inserted in the CTM equipment and used in an over-the-air registration process, instead of the real user doing it. However, the real user may detect the attack quite early since he cannot perform the subscription registration procedure himself (as in threat no. 2).

Resulting threats:

a) masquerade as the regular subscriber (for a while).

5) Masquerading of a user during the over-the-air subscription registration procedure by guessing an AC successfully (stealing of identity).

This threat is relevant if the ACs are very short. However, the real user may detect the attack quite early since he cannot perform the subscription registration procedure himself.

Resulting threats:

a) masquerade as the regular subscriber (for a while).

Table 4: Threats related to Subscription Registration Procedures

Location Threats	PT	PT/ SCUAF	SCUAF	SCUAF/ CUSF	CUSF	SCUSF/ SCF$_{MM}$	SCF$_{MM}$	SCF$_{MM}$/ SDF$_{SL}$	SDF$_{SL}$	SCF$_{MM}$/ SCF$_{SL}$	SCF$_{SL}$	SCF$_{SL}$/ SDF$_{SL}$	SMP	SMP/ SDF$_{SL}$	Others (phone, email)
7.3.4.1		E													
7.3.4.2	M	E							UA		UA*	E*	UA	E	E
7.3.4.3		M							UA		UA*	E*	UA	E	E
7.3.4.4	U	U							UA		UA	E	UA	E	E
7.3.4.5	U	U													

NOTE *: The AC is present in SCF$_{SL}$ and in SCF$_{SL}$/SDF$_{SL}$ interface only during the subscription registration process for calculation of keys and responses.

7.2.6 Threats related to Subscription De-registration Procedures

1) Illegal de-registration by an attacker masquerading as service provider:

The de-registration process over-the-air requires network authentication. Hence only in situations where the attacker has knowledge of the user's UAK, is this possible.

Resulting threat:

a) illegal de-registration leads to denial of service for the user.

2) Subscriber does not allow de-registration by manipulating his terminal:

If the PT is manipulated not to accept the network authentication which should accompany a withdrawal of the PT's access rights, the user can inhibit the de-registration from taking effect in his terminal. Alternatively he can let the PT send back a reject answer to the network's request, which indicates to the network that the re-register procedure has failed.

Resulting threat:

a) the attacker may be able to perform outgoing calls in a visited network, as long as authentication to the home network is not required.

3) Subscriber does not allow de-registration by manipulating the SCF$_{SL}$ - SCF$_{MM}$ interface:

If the subscriber manipulates the data sent for subscription de-registration over the SCF$_{SL}$ - SCF$_{MM}$ interface, he can send to the SCF$_{MM}$ a "Remove Entry (CTM-id)" request. In that case, the home data base will register that the CTM-id has been deleted. However, this CTM-id can still remain in the visited network's database.

Resulting threat:

a) the attacker may be able to perform outgoing calls in a visited network, as long as authentication to the home network is not required.

Table 5: Threats related to Subscription De-registration Procedures

Location Threats	PT	PT/ SCUAF	SCUAF	SCUAF/ CUSF	CUSF	SCUSF/ SCF$_{MM}$	SCF$_{MM}$	SCF$_{MM}$/ SDF$_{SL}$	SDF$_{SL}$	SCF$_{MM}$/ SCF$_{SL}$	SCF$_{SL}$	SCF$_{SL}$/ SDF$_{SL}$	SMP	SMP/ SDF$_{SL}$	Others (phone, email)
7.3.5.1			M		M		M				M				
7.3.5.2	M														
7.3.5.3										M					

7.2.7 Threats related to CTM incoming call procedures

1) Masquerading by using someone's CTM-id:

If authentication is not mandatory for incoming calls, a masquerading attack is possible by knowing only the CTM-id which can be caught easily (see general threats). This attack is possible only if ciphering is not mandatory for the FT and the PT. Nevertheless even in that case the attacker may avoid ciphering by manipulating his PT.

Resulting threats:

a) Incoming long distance calls will be (partly) billed to the regular subscriber in case of charging split. If the attacker gives the CTM number of that CTM subscriber to his friends, they can avoid high phone bills at the cost of the threatened subscriber.

b) The attacker can receive incoming calls intended for the regular subscriber. This is relevant especially for data services.

c) Duplication of CTM-id within inter-network. Both the attacker and the legitimate subscriber may attempt to register at the same time. The network cannot distinguish between a good and bad variant of the same CTM-id.

2) Masquerading by using someone's CTM-id and authentication information:

Even if authentication and/or ciphering is required for incoming calls, a masquerading attack is possible by knowing the CTM-id and the authentication information which can be known by one of the methods described earlier.

Resulting threats:

a) Incoming long distance calls will be (partly) billed to the regular subscriber in case of charging split. If the attacker gives the CTM number of that CTM subscriber to his friends, they can avoid high phone bills at the cost of the threatened subscriber.

b) The attacker can receive incoming calls intended for the regular subscriber. This is relevant especially for data services.

c) Duplication of CTM-id within inter-network. Both the attacker and the legitimate subscriber may attempt to register at the same time. The network cannot distinguish between a good and bad variant of the same CTM-id.

3) Eavesdropping of the communication on the air interface by use of the DCK:

The attacker may have got the DCK by one of the methods described earlier. He needs also be able to perform the DECT cipher algorithm (e.g. using a manipulated portable equipment). Hence, he can decipher the intercepted communication.

4) Eavesdropping of the communication on the air interface by deletion of Ciphering Request message:

on the SCF_{MM} - CUSF interface or on the SCUAF - CUSF interface and (if necessary) modification of the Ciphering Reply and/or Report Ciphering Reply message on the same interfaces, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm nor to know the relevant key (see 7.3.1.4.2).

5) Eavesdropping of the communication on the air interface by deletion of Ciphering Request message:

on the air interface and (if necessary) modification of the according Reply message, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm nor to know the relevant key (see 7.3.1.4.3).

6) Eavesdropping of the communication on the CCF-CCAF interface:

Outside the air interface, where DECT ciphering is not performed, eavesdropping can be done as in any fixed network.

7) Eavesdropping of the start of a communication on the air interface:

This may be possible since call set up may have been successfully performed before the authentication has been completed and the ciphering has started. Hence, some secret data may be eavesdropped.

8) Eavesdropping of roaming number or routing number (e.g. at CCF_o), or of FT address.

This may occur at the LE entities of either the calling or called party.

Resulting threat:

a) this may lead to the knowledge of a CTM user's location.

9) Modification of routing data in order to re-route the communication to another address (which the attacker has access to).

Resulting threat:

a) The attacker may receive (possibly secret) information intended for the regular subscriber. This threat is relevant especially for data services.

10) Deletion of Release message in case of authentication failure

at the SCF_{MM} - SSF_t/CCF_t interface or at one of these entities.

Resulting threat:

a) Since the result of authentication is not forwarded to the relevant CCF, the requested call would be proceeded, i.e. a masquerading threat can be performed.

Table 6: Threats related to incoming call procedures

Location Threats	PT	PT - SCUAF/ CCAF	SCUAF/ CCAF	SCUAF/ CCAF - CUSF/ CCF$_t$/ SSF$_t$	CUSF/ CCF$_t$/ SSF$_t$	CUSF/ CCF$_t$/ SSF$_t$ - SCF$_{MM}$	SCF$_{MM}$	SCF$_{MM}$ - SDF$_{MM}$	SDF$_{MM}$	SCF$_{MM}$ - SCF$_{SL}$	SCF$_{SL}$	SCF$_{SL}$- SDF$_{SL}$	SDF$_{SL}$	SCF$_{SL}$ - CCF$_o$/ SSF$_o$	CCF$_o$/ SSF$_o$	CCF$_o$ - CCF$_t$
7.3.6.1	M	U														
7.3.6.2	M	U														
7.3.6.3		E														
7.3.6.4		E	M	M	M	M										
7.3.6.5		E, M														
7.3.6.6																E
7.3.6.7		E														
7.3.6.8			UA	E	UA	E	UA	E	UA	E	UA	E	UA	E	UA	E
7.3.6.9			M	M	M	M	M	M	M	M	M	M	M	M	M	M
7.3.6.10					M	M	M									

7.2.8 Threats related to CTM outgoing call procedures

1) Masquerading by using someone's CTM-id:

   If authentication is not mandatory for outgoing calls, a masquerading attack is possible by knowing only the CTM-id which can be caught easily (see general threats). This attack is possible only if ciphering is not mandatory for the FT and the PT. Nevertheless even in that case the attacker may avoid ciphering by manipulating his PT.

   Resulting threat:

   a) outgoing calls will be billed to the regular subscriber.

2) Masquerading by using someone's CTM-id and authentication information:

   Even if authentication and/or ciphering is required for outgoing calls, a masquerading attack is possible by knowing the CTM-id and the authentication information which can be known by one of the methods described earlier.

   Resulting threats:

   a) Outgoing calls will be billed to the regular subscriber.

3) Eavesdropping of the communication on the air interface by use of the DCK:

   The attacker may have got the DCK by one of the methods described earlier. He needs also be able to perform the DECT cipher algorithm (e.g. using a manipulated portable equipment). Hence, he can decipher intercepted communication.

4) Eavesdropping of the communication on the air interface by deletion of Ciphering Request message:

   on the SCF$_{MM}$ - CUSF interface or on the SCUAF - CUSF interface and (if necessary) modification of the Ciphering Reply and/or Report Ciphering Reply message on the same interfaces, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm (see 7.3.1.4.2).

5) Eavesdropping of the communication on the air interface by deletion of Ciphering Request message:

   on the air interface and (if necessary) modification of the according Reply message, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm nor to know the relevant key (see 7.3.1.4.3).

6) Eavesdropping of the communication on the CCF-CCAF interface:

   Outside the air interface, here DECT ciphering is not performed, eavesdropping can be done as in any fixed network.

7) Eavesdropping of the start of a communication on the air interface:

This may be possible since call set up may have been successfully performed before the authentication has been completed and the ciphering has started. Especially the called phone number and in case of specific services requiring, e.g. a PIN secret data may be eavesdropped.

8) Eavesdropping of the phone number of the called party:

This may be possible since call set-up may start prior to authentication result and start of ciphering.

Resulting threat:

a) This may lead to the knowledge of a communication partner's identity.

9) Modification of the dialled number in order to direct the communication to another address (which the attacker has access to).

Resulting threat:

a) The attacker may receive (possibly secret) information intended for the CTM subscriber's communication partner. This threat is relevant especially for data services. Here it is not CTM specific.

10) Deletion of Release message in case of authentication failure

at the SCF_{MM} - SSF/CCF interface or at one of these entities.

Resulting threat:

a) Since the result of authentication is not forwarded to the relevant CCF, the requested call would be proceeded, i.e. a masquerading threat can be performed.

11) Masquerading by using someone's CTM-id only, and resulting avoidance of charging for a (probably short) period at the beginning of a communication:

This may be possible since call set up may have been successfully performed before the authentication has been completed. This threat may especially be interesting in order to perform (short) calls to a premium rate service belonging to the attacker or his friends.

Table 7: Threats related to outgoing call procedures

Location Threats	PT	PT - SCUAF/ CCAF	SCUAF/ CCAF	SCUAF/ CCAF - CUSF/ CCF/ SSF	CUSF/ CCF/ SSF	CUSF/ CCF/ SSF - SCF_{MM}	SCF_{MM}	SCF_{MM} - SDF_{MM}	SDF_{MM}	SCF_{MM} - SCF_{SL}	SCF_{SL}	SCF_{SL}- SDF_{SL}	SDF_{SL}	CCF_o - CCF_t
7.3.7.1	M	U												
7.3.7.2	M	U												
7.3.7.3		E												
7.3.7.4		E	M	M	M	M								
7.3.7.5		E, M												
7.3.7.6														E
7.3.7.7		E												
7.3.7.8		E												
7.3.7.9		M	M	M	M	M	M	M	M	M	M	M	M	M
7.3.7.10					M	M	M							
7.3.7.11	M	U												

7.2.9 Threats related to emergency call procedures

1) Misuse of emergency call:

An attacker can send some emergency calls e.g. to the police, without any reasons, e.g. to give false indications. In the case where giving the CTM-id without authentication is sufficient, he can masquerade as somebody else (if he knows his CTM-id). Then the emergency call seems to come from somebody else.
In CTM phase 2, it is not even necessary to have a CTM subscription. Hence, an attacker can just send some false indications when performing an emergency call, without giving any CTM-id. In that case, the misuse of emergency calls is even easier to perform.

NOTE: Emergency calls should be delivered with data identifying the location of the calling party.

Resulting threat:

a) masquerading and giving some false indication during emergency calls.

2) Manipulate data to give an emergency number to somebody:

An attacker can give to a friend an emergency number by manipulating data in the emergency data base. In that case, this new number will be free of charge.

Resulting threat:

a) masquerading as an emergency entity, so that calls to this number are free of charge.

Table 8: Threats related to emergency call procedures

Location Threats	PT	PT/ SCUAF	SCUAF	SCUAF/ CUSF	CUSF	SCUSF/ SCFMM	SCFMM	SCFMM/ SDFMM	SDFMM	SCFMM/ SDFSL	SDFSL	SCFSL/ SDFSL	SCFSL	SCFSL/ SCFMM
7.3.8.1 Misuse of emergency call	U													
7.3.8.2 Manipulate data to give an emergency number to somebody											M			

7.2.10 Threats related to Service Profile

NOTE 1: The procedures considered in the following are not specified as detailed as the preceding ones. Especially, it is not specified if - and how - subscriber authentication shall be performed in order to use or manage these features. However, they are mentioned in the service description documents (EN 301 175 and EN 301 273).

NOTE 2: In CTM phase 2, the CTM user may be given the possibility to interrogate or modify some of the data in the served user's service profile using DTMF signalling procedures. This can be done either with the CTM handset or with an other terminal. In that case the threats mentioned below are easier to perform. However, the service provider may restrict the access to the service profile data.

1) Eavesdropping of transmitted information during Service Profile Transfer.

Resulting threat:

a) Personal data is divulged to unauthorized persons.

2) Manipulation of transmitted information during Service Profile Transfer.

Resulting threat:

a) The service is increased without authorization.

3) Unauthorized access to the service profile of somebody by unauthorized use of Service Profile Interrogation.

Resulting threat:

a) Personal data is divulged to unauthorized persons.

4) Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure.

   Resulting threats:

   a) Modification of the service profile belonging to somebody else, e.g. in order to perform a denial or degradation of service.

   b) Unauthorized modification of, e.g. one's own service profile, e.g. in order to increase the service without authorization.

7.2.11 Threats related to Supplementary Services

NOTE 1: The supplementary services are not specified in the CTM architecture documents. Especially, it is not specified if and how subscriber authentication shall be performed in order to use or manage these features. However, they are mentioned in the service description documents (EN 301 175 and EN 301 273).

NOTE 2: Call Forwarding on Not Reachable is already a CTM phase 1 feature. Call Forwarding Unconditional, Call Forwarding on No Reply, and Call Forwarding on Busy are CTM phase 2 features.

NOTE 3: The Call Forwarding services have in common that they effect charging in a way which may not have been envisaged when the initial call was set up. Charging may be increased substantially or transferred to other parties. Moreover, it could be very interesting for an attacker to get the calls of a CTM user directed to him, in order to receive the information intended for the real CTM user.

1) An unauthorized user may register to a call forwarding service and request registration for the service to another forwarded-to number.

   Resulting threats:

   a) The attacker could make calls by using the number of the attacked CTM subscriber who will then be charged for part of the attacker's communications.

   b) Incoming calls of a CTM subscriber could be re-routed, in order to get all his incoming calls (eavesdropping) and/or to make him loose his incoming calls (denial of service).

2) An unauthorized user may request erasure of the service for someone else.

   Resulting threat:

   a) Loss of call forwarding service for a user.

3) An unauthorized user may interrogate the status of the call forwarding service for someone else.

   Resulting threat:

   a) Information of someone's call forwarding number is divulged.

4) If parallel call forwarding is allowed, an attacker may do several unauthorized call forwarding registrations for another CTM subscriber.

   Resulting threat:

   a) An attacker may make (or sell!) several calls at the same time using the number of the real CTM subscriber who will be charged for these several calls.

The (CTM phase 2) supplementary services Calling/Connected Line Identification Presentation/Restriction (CLIP, COLP, CLIR, COLR) are similar to the corresponding services defined for PSTN and ISDN and are assumed to be subject to the same ability and restrictions as required by laws and rules for personal data integrity protection. When CLIP and COLP are active, only the CTM number shall be presented, and in any case no information of the location of the CTM user. For emergency reasons certain called parties(e.g. police and fire brigade) may nevertheless be allowed to receive the CTM CLIP even if the caller is a CTM user (override CLIR; this overriding is, however, assumed to be managed in a very secure way). Under these assumptions, no threats have been identified with respect to these services.

The (CTM phase 2) supplementary services Incoming Call Screening and Outgoing Call Barring may be used by the user as some extra security features. However:

5) An unauthorized user may manipulate one or both of the two lists specifying the numbers for Incoming Call Screening and Outgoing Call Barring.

   Resulting threats:

   a) denial of service;

   b) making or receiving calls that are not allowed.

No threats have been identified with respect to the CTM phase 2 service Message Waiting Indication.

7.2.12 Threats related to Interaction with ISDN Supplementary Services in CTM Phase 2

Interaction with ISDN supplementary services is described in (EN 301 175 and EN 301 273). No specific threats related to this have been identified.

7.2.13 Threats related to CTM Inter-working between Public Intelligent Networks

The procedures and information flows specified in EG 201 096-2 are very similar to those of EG 201 096-1. The threats identified for the single network case are valid for the inter-networking case as well, and vice versa. They may, however, be more severe in some cases since different network providers may be involved.

Depending on the charging and billing model used for the roaming co-operation between networks, different threats related to economic fraud between operators can be envisaged. In this analysis, only the basic roaming model has been considered.

In addition to the interfaces identified in clause 6.1 of this guide, the following interfaces occur: $\text{SCF}_{\text{SL,visited}}$ - $\text{SCF}_{\text{SL,home}}$ and $\text{SCF}_{\text{SL,visited}}$ - $\text{SDF}_{\text{SL,home}}$.

In the inter-networking case, the procedures can be performed by use of different interfaces, namely the SCF - SCF interface, the SCF - SDF interface, and the SDF - SDF interface.

One additional procedure has been identified in the inter-networking case, namely the terminal authentication in the home network. Dependent of the used interface, there are two possible procedures:

- authentication in $\text{SCF}_{\text{SL home}}$, by use of SEARCH operation;
- authentication in $\text{SDF}_{\text{SL home}}$, by use of BIND operation.

In the first case, the $\text{SCF}_{\text{SL home}}$ has the full control: It generates the random numbers and checks the response (RES); this is the classical approach.

In the second case, the $\text{SCF}_{\text{SL home}}$ has not the full control: The $\text{SCF}_{\text{MM visited}}$ generates the random numbers and the $\text{SCF}_{\text{SL home}}$ checks the response (RES).

1) The DCK may be eavesdropped at some IN interface while transmitted from home network to visited network.

   Resulting threat:

   a) Eavesdropping of a user's communication.

2) If authentication is performed in the home network, the result may be modified at some IN interface during transmission (especially the notification "authentication failed" may be changed to "authentication successful").

   Resulting threat:

   a) Masquerading as chosen user will succeed without valid authentication.

3) Visited network operator claims that more traffic was generated by home network's roaming user(s) than actually took place, by stating more calls, longer calls, calls at higher rates (because of distance, time of day or date, premium rate, etc.)

   Resulting threat:

   a) Home network and its subscribers have to pay too much to the visited network.

4) Home network refuses to pay visited network, claiming (falsely) that the visited network has stated too much traffic for the roaming users. Home network could claim that visited network has not performed authentication as agreed and also claim that the visited network operator has manipulated call data records (as in the previous threat).

   Resulting threat:

   a) Visited network gets too little compensation for the roaming visitors.

7.2.14 Threats related to CTM Inter-working between Private Networks and Public Intelligent Networks

The procedures and information flows specified in EG 201 096-3 are very similar to those of EG 201 096-1. The threats identified for the single network case and the public inter-networking case are valid for the public-private inter-networking case as well. They may, however, be more severe in some cases since both, public and private network providers are involved. If there are roaming agreements, and authentication data are transferred from the public network to a private network, protection levels for these data in the private network have to be adequate.

No new threats for this scenario have been identified.

7.3 Risk Measurement

A potential threat is doing no harm unless there is a corresponding weakness in the system and until the point in time when a weakness is exploited by the intruder. Thus, the threats must be evaluated, i.e. it should be attempted to characterize them according to cost/effort involved (occurrence likelihood) and according to potential benefit/damage that can be done (impact value).

For the risk assessment, the occurrence likelihood of threats is estimated with values from "1" to "3". The meaning of a certain value associated to the occurrence likelihood of a particular threat is explained as follows:

Table 9: Occurrence likelihood

1	for "unlikely"	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat, or the motivation for an attacker is very low.
2	for "possible"	The technical requirements necessary to state this threat are not too high and seem to be solvable without big effort; furthermore, there must be a reasonable motivation for an attacker to perform the threat.
3	for "likely"	There are no sufficient mechanisms installed to counteract this threat, and the motivation for an attacker is quite high.

The impact of a threat is also estimated with values from "1" to "3". The meaning of a certain value associated to the impact is explained as follows:

Table 10: Impact

1	for "low impact"	The concerned party is not harmed very strongly; the possible damage is low.
2	for "medium impact"	The threat addresses the interests of providers/subscribers and cannot be neglected.
3	for "high impact"	A basis of business is threatened and severe damage might occur in this context.

The product of occurrence likelihood and impact value gives the risk which serves as a measurement for the risk that the concerned management function is compromised. The result is classified into the following three categories:

Table 11: Risk

1, 2, 3	for "minor risk"	Minor risks arise, if either no essential assets are concerned, or the respective attack is unlikely. Threats causing minor risks have no primary need for counter measures.
4	for "major risk"	Major risks are represented by threats on relevant assets which are likely to occur, even if their impact is less fatal. Major risks should be handled seriously and should be minimized as soon as possible.
6, 9	for "critical risk"	Critical risks arise, when the primary interests of the providers/subscribers are threatened and when a potential attacker's effort to harm these interests is not high. Critical risks shall be minimized with highest priority.

NOTE: The values 5, 7, and 8 cannot occur.

7.4 Risk Assessment for the CTM Network Procedures

General remark:

- All threats with risk 6 or 9 (critical risks) require countermeasures. Also threats with risk 4 (major risks) shall be minimized as soon as possible. The according security requirements are stated in clause 8.

Table 12: Risk assessment for general threats

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.0.1 a)	2	1-3	2-6	The impact depends on the use of authentication before to perform outgoing calls, incoming calls, location registration, etc. (see note 3).
7.3.0.1 b)	2	1	2	Kind of information eavesdropped (mainly location of the user) not very important (see note 3).
7.3.0.2 a)	2	1-3	2-6	The impact depends on the use of authentication before to perform outgoing calls, incoming calls, location registration, etc.
7.3.0.2 b)	2	1	2	Kind of information eavesdropped (mainly location of the user) not very important
7.3.0.3 a)	2	1-3	2-6	The impact depends on the use of authentication before to perform outgoing calls, incoming calls, location registration, etc.
7.3.0.3 b)	2	1	2	Kind of information eavesdropped (mainly location of the user) not very important
7.3.0.4 a)	1-3	1-3	1-9	The impact could be very strong. The likelihood depends on the implementation (see note 1).
7.3.0.4 b)	1-3	1-2	1-6	The impact of a degradation of service is less important than the denial of service (see note 1).
7.3.0.5 a)	1	3	3	Impact important since denial of service. However it is unlikely to use data (probably got with the help of one employee) for a denial of service which would be easily detected (see note 3).
7.3.0.5 b)	2	1-3	2-6	The data (probably got with the help of one employee) are more interesting to use to perform a masquerading attack. The impact depends of the nature of the data got (see note 3).
7.3.0.5 c)	2	1-2	2-4	The impact depends of the nature of the data got (see note 3).

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.0.6 a)	1-2	3	3-6	Unlikely, but strong impact (see note 2).
7.3.0.6 b)	1-2	2	2-4	
7.3.0.7 a)	3	2	6	Very likely, but the possible fraud should be restricted to only one account, so impact 2 (see note 3).
7.3.0.7 b)	1	2	2	Requires a sophisticated device (see note 3).
7.3.0.7 c)	2	2	4	Easy to perform. Impact depends on incoming data (see note 3).
7.3.0.8 a)	3	2-3	6-9	Very likely. Impact depends on the subscription process. If parallel call forwarding is allowed, the impact increases (see note 3).
7.3.0.9 a)	2	2	4	Manipulation of terminal to get useful data should not be very easy. Fraud limited to one account.
7.3.0.9 b)	1	2	2	Requires a sophisticated device.
7.3.0.10 a)	1	3	3	
7.3.0.10 b)	1	2	2	
7.3.0.10 c)	1	2	2	
7.3.0.10 d)	1	3	3	

NOTE 1: In the case of CTM inter-working between public, or between public and private Intelligent Networks, a rogue operator may have more interest in degrading or destroying the service.

NOTE 2: In the case of CTM inter-working between public, or between public and private Intelligent Networks, a rogue operator may have more interest in degrading or destroying the service. Moreover, an attacker for fun can use the inter-networking interfaces to try to disturb and maybe flood the network.

NOTE 3: In the case of CTM inter-working between public, or between public and private Intelligent Networks, a network operator does not have the full control. Use of stolen terminal, extensive use of a fake subscription, unauthorized access to data related to its subscriber, or eavesdropping of CTM-ids may occur as in the single network case but it will be much more difficult for the network operator to notice it and then to take the adequate countermeasures.

Table 13: Risk assessment for threats related to terminal authentication and ciphering procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.1.1.1 a)	2	2	4	Likelihood 2, because the economic motive is high! Requires modified handsets though.
7.3.1.1.1 b)	2	1	2	Comes automatically with above, though less impact with incoming calls.
7.3.1.1.1 c)	1	1	1	Farfetched, complicated attack; small overall impact.
7.3.1.1.1 d)	1	2	2	Requires running of DECT algorithms, probably also modified CTM handset + actual intercept of target.
7.3.1.1.2 a)	1	2	2	Requires running of DECT cipher algorithm, probably also modified CTM handset + actual intercept of target.
7.3.1.2.1 a)	2	2	4	Economic motives, short exploit, but can be repeated (both in time and over user base). Ciphering may protect against unauthorized use however. Requires modified handsets though.
7.3.1.2.2 a)	1	2	2	Requires running of DECT cipher algorithm, probably also modified CTM handset + actual intercept of target (see note 2).

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.1.3.1 a)	2	2	4	Economic motives, short exploit, but can be repeated (both in time and over user base). Ciphering may protect against unauthorized use however (if RES is used). Full fraud potential (if KS is used). Requires modified handsets though (see note 3).
7.3.1.3.1 b)	1	1	1	Extremely complicated attack, weak motives (see note 3).
7.3.1.3.2 a)	1	2	2	Requires running of DECT cipher algorithm, probably also modified CTM handset + actual intercept of target (see note 3).
7.3.1.3.3 a)	2-3	2	4-6	Economic motives, short exploit, but can be repeated (both in time and over user base). Full fraud potential (if KS is used). Requires modified handsets (see note 4).
7.3.1.3.3 b)	1-2	1	1-2	Extremely complicated attack, weak motives (see note 4).
7.3.1.3.3 c)	1-2	2	2-4	This threat is not relevant if the authentication data (session keys or triples) are changed each time (see note 4).
7.3.1.4.1 a)	1	2	2	Requires running of DECT cipher algorithm, probably also modified CTM handset + actual intercept of target (see note 2).
7.3.1.4.2 a)	1	2	2	Complicated method, timing sensitive, requires also that calls are allowed to proceed un-enciphered, both in FP and PP.
7.3.1.4.3 a)	1	2	2	Complicate/impossible to interfere selectively on the air interface? Requires also that calls are allowed to proceed un-enciphered, both in FP and PP.
7.3.1.4.4 a)	1	1	1	Impossible to exploit effectively, timing between incident and target communication not predictable.

NOTE 1: In the case of CTM inter-working between public, or between public and private Intelligent Networks, a rogue network operator can easily get the CTM-id, authentication data and DCK of any user coming into his network. Hence, he can perform more easily eavesdropping of communication or masquerading as this user.

NOTE 2: In the case of CTM inter-working between public, or between public and private Intelligent Networks, the home network gives the DCK to the visited network in order to perform the ciphering. It is easier for an attacker to get this DCK at the interface between the two networks. However, to perform a threat with this DCK, many other manipulation are necessary, hence, no changes in likelihood.

NOTE 3: In the case of CTM inter-working between public, or between public and private Intelligent Networks, there are two possibilities:

- authentication in the home network. This threat is not relevant.
- Authentication in the visited network. In that case, the threat is easier to perform as there may be less control at the interface between the two networks. However, many other manipulations are necessary to perform this threat. Hence, no change in the risk has been identified.

NOTE 4: In the case of CTM inter-working between public, or between public and private Intelligent Networks, there are two possibilities:

- authentication in the home network. This threat is not relevant.
- authentication in the visited network. In that case, threat easier to perform as there may be less control at the interface between the two networks. Hence, the occurrence likelihood depends on the protection of the inter-working.

Table 14: Risk assessment for threats related to location registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
These threats are covered by the threats related to CTM incoming and outgoing call procedures (see 7.3.6.1, 7.3.6.2, 7.3.7.1 and 7.3.7.2).				

Table 15: Risk assessment for threats related to data deletion procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.3.1	1	1	1	This is a quite complicated threat to get information of minor value.
7.3.3.2	1	1	1	This is a quite complicated threat resulting only in a short time denial of service for a single user.
NOTE: These assessments are also valid for CTM inter-working between public and between public and private networks. Likelihood and impact are low in any case.				

Table 16: Risk assessment for threats related to subscription registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.4.1.a)	1-2	2-3	2-6	Size of AC is critical, shall not be too short for likelihood 1. If calculations can be exploited several times (via table look-up), due to same authentication data used, impact will be 3, otherwise 2. Modified handsets needed.
7.3.4.1 b)	1	2	2	Attack as above, followed up with network masquerade. Difficult + weak motive.
7.3.4.1.c)	1	2	2	Attack as above, followed up with eavesdropping at subsequent calls. Difficult + weak motive.
7.3.4.2.a)	1-2	2	2-4	Again requires running of DECT algorithms with intercepted authentication data, but now with AC intercepted in distribution process. Likelihood depends on security of AC distribution process to users.
7.3.4.2 b)	1	2	2	As 7.3.4.1.b)
7.3.4.2.c)	1	2	2	As 7.3.4.1.c)
7.3.4.3. a)	1	2	2	Intercepting an AC, masquerading as network to same user and performing subscription registration to him means very low likelihood for this attack..
7.3.4.3 b)	1	2	2	Attack as above.
7.3.4.3.c)	1	1	1	Attack as above.
7.3.4.4 a)	1-2	1	1-2	"Stealing" an AC, masquerading as this user to network while performing subscription registration has high motive, but the real user will eventually complain. Likelihood depends on security of AC distribution process to users.
7.3.4.5.a)	1	1	1	Economic motives, higher likelihood if AC is too short!
NOTE: This procedure is assumed to be done in the home network. Hence, CTM inter-working between public and between public and private networks is not relevant here.				

Table 17: Risk assessment for threats related to subscription de-registration procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.5.1	1	1	1	Weak motives (see note 1).
7.3.5.2	1	1	1	Weak motives (see note 2).
7.3.5.3	1-2	2	2-4	Difficult to perform, but the impact can be serious since the attacker manipulates SCF_{SL}-SCF_{MM} interface. The fraud can go on for a while (see note 3).
NOTE 1: For the first threat, there may be a small difference in case of CTM inter-working between public and between public and private networks: A visited service provider may illegally use its information (CTM-id and session key) to perform this procedure without request from the home network. However, when the user claims this denial of service to his provider, he will be able to detect the attacker. Furthermore, the motive is weak in any case. Hence the risk is still 1. NOTE 2: For the second threat, there is no difference in case of CTM inter-working between public and between public and private networks. NOTE 3: For the third threat, there may be a small difference in case of CTM inter-working between public and between public and private networks The subscriber may collaborate with the visited provider in order to avoid de-registration. If the home service provider cannot prove this, the likelihood would be higher, namely 2. Hence the risk is 4 (major risk!) in the inter-working case.				

Table 18: Risk assessment for threats related to CTM incoming call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.6.1 a)	2	2	4	Easy to perform if neither authentication nor ciphering. Important impact regarding charging (only in case of charging split).
7.3.6.1 b)	2	2	4	Easy to perform if neither authentication nor ciphering. Importance of impact depends on incoming data.
7.3.6.1 c)	2	3	6	Denial of service to legitimate CTM-id. For duplicate CTM-id possible confusion in distributed network.
7.3.6.2 a)	1	2	2	Same impact as above but more difficult to perform as authentication and/or ciphering is required.
7.3.6.2 b)	1	2	2	Same impact as above but more difficult to perform as authentication and/or ciphering is required.
7.3.6.2 c)	1	3	3	As for 7.3.6.1 c).
7.3.6.3	1	2	2	See 7.3.1.4.1
7.3.6.4	1	2	2	See 7.3.1.4.2
7.3.6.5	1	2	2	See 7.3.1.4.3
7.3.6.6	2	2	4	Easy to perform (no ciphering in the fixed network).
7.3.6.7	2	1	2	Useful only (for the attacker) for the start of communication (depending on the delay for ciphering).
7.3.6.8	1	1	1	
7.3.6.9	1	2	2	Complicated. Useful (for the attacker) depending on the target.
7.3.6.10	1	2	2	Complicated.

Table 19: Risk Assessment for threats related to CTM outgoing call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.7.1	3	3	9	Easy to perform if neither authentication nor ciphering. Important impact regarding charging.
7.3.7.2	1	3	3	Same impact as above but more difficult to perform as authentication and ciphering is required.
7.3.7.3	1	2	2	See 7.3.1.4.1
7.3.7.4	1	2	2	See 7.3.1.4.2
7.3.7.5	1	2	2	See 7.3.1.4.3
7.3.7.6	2	2	4	Easy to perform (no ciphering in the fixed network).
7.3.7.7	2	1	2	Useful only (for the attacker) for the start of communication (depending on the delay for ciphering).
7.3.7.8	2	1	2	
7.3.7.9	1	2	2	Complicated. Useful (for the attacker) depending on the target.
7.3.7.10	1	2	2	Complicated.
7.3.7.11	3	1-3	3-9	Depending on the length of the period the user is allowed to start and continue a call without authentication.

Table 20: Risk Assessment for threats related to emergency call procedures

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.8.1	2-3	1	2-3	Likelihood 2 for CTM phase 1, and likelihood 3 for CTM phase 2.
7.3.8.2	1	3	3	Likelihood depends on the access security to the emergency data base (insider threat).

Table 21: Risk assessment for threats related to service profile

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.9.1 a)	1	1	1	
7.3.9.2 a)	1	2	2	
7.3.9.3 a)	1	1	1	The likelihood is higher if no authentication is required.
7.3.9.4 a)	1-2	1-2	1-4	The likelihood is higher if no authentication is required. The impact depends on the content of the service profile.
7.3.9.4 b)	1-2	1-2	1-4	The likelihood depends on the access control mechanisms. The impact depends on the content of the service profile.
NOTE: In case of CTM inter-working between public or public and private intelligent network, it is easier to perform threats related to the service profile, especially rogue network operator. Occurrence likelihood depends on the content of the service profile.				

Table 22: Risk assessment for threats related to supplementary services

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.10.1 a)	1-3	2	2-6	The likelihood depends on authentication requirement.
7.3.10.1 b)	1-3	2	2-6	"
7.3.10.2 a)	1-3	2	2-6	"
7.3.10.3 a)	1-2	1	1-2	"
7.3.10.4 a)	1-3	3	3-9	"
7.3.10.5 a)	1-3	2	2-6	The likelihood depends on the procedure to specify the lists (especially authentication).
7.3.10.5 b)	1-2	2	2-4	"

Table 23: Risk assessment for threats related to interaction with ISDN supplementary services, inter-working between public networks and inter-working between public and private networks

Threat	Occurrence Likelihood	Impact	Risk	Comment
7.3.12.1 a)	1	2	2	See 7.3.1.3.2 a).
7.3.12.2 a)	1	2	2	
7.3.12.3 a)	2	2	4	To be considered in case of two public networks and in case of private and public network. Very interesting and easy to do for the attacker, but the risk depends on the relation between operators and on agreements regarding billing.
7.3.12.4 a)	1	1	1	Difficult to do, as the home network has to prove that it is right. Low impact, as it is difficult to do it many times.

7.5 Consolidated Risk Assessment

The following table gives the identified **critical risks**, i.e. the risks with potential value 6 or 9.

Table 24: Threats with critical risk

Risk	Reference	Threat description
9	7.3.7.1	Masquerading by using someone's CTM-id to perform outgoing calls to be billed to the regular subscriber if authentication is not required.
6-9	7.3.0.8 a)	Subscription fraud in order to intensively use CTM services with no intention to pay.
3-9	7.3.7.11	Masquerading by using someone’s CTM-id only, and resulting avoidance of charging for a (probably short) period at the beginning of a communication:
3-9	7.3.10.4	Several unauthorized call forwarding registrations for another CTM subscriber to make (or sell!) several calls at the same time using the number of the real CTM subscriber who will be charged for these several calls.
1-9	7.3.0.4 a)	Denial of service.
6	7.3.0.7 a)	Stolen terminals used for calls.
6	7.3.6.1 c)	Duplication of CTM-id leading to denial of service to the legitimate user.
4-6	7.3.1.3.3 a)	Masquerading as SCF_{MM} to get authentication data, leading to masquerading as the regular subscriber.
3-6	7.3.0.6 a	Flooding, leading to denial of service.
2-6	7.3.0.1 a)	Eavesdropping of CTM-id on IN interfaces or entities to masquerade as the regular subscriber.
2-6	7.3.0.2 a)	Eavesdropping of CTM-id on the air interface to masquerade as the regular subscriber.
2-6	7.3.0.3 a)	Getting the CTM-id from a terminal to masquerade as the regular subscriber.
2-6	7.3.0.5 b)	Unauthorized access to databases (SDFs) to masquerade as the regular subscriber.
2-6	7.3.4.1 a)	Eavesdropping of data in an over-the-air registration process and subsequent exhaustive search for AC to masquerade as the regular subscriber.
2-6	7.3.10.1 a)	An unauthorized user may register to a call forwarding service and request registration for the service to another forwarded-to number, to make calls by using the number of the attacked CTM subscriber who will then be charged for part of the attacker’s communications.
2-6	7.3.10.1 b)	An unauthorized user may register to a call forwarding service and request registration for the service to another forwarded-to number to re-route incoming calls of a CTM subscriber in order to get all his incoming calls (eavesdropping) and/or to make him loose his incoming calls (denial of service).

Risk	Reference	Threat description
2-6	7.3.10.2 a)	An unauthorized user may request erasure of the call forwarding of someone else.
2-6	7.3.10.5 a)	An unauthorized user may manipulate one or both of the two lists specifying the numbers for Incoming Call Screening and Outgoing Call Barring to deny outgoing or incoming calls for the user.
1-6	7.3.0.4.b)	Degradation of service.

The following table gives the identified major risks, i.e. the risks with potential value 4.

Table 25: Threats with major risk

Risk	Reference	Threat description
4	7.3.0.7 c)	Stolen terminals used to get regular user's incoming calls.
4	7.3.0.9 a)	Unauthorized access to CTM-id and KS in terminal to masquerade as the regular subscriber.
4	7.3.1.1.1 a)	Eavesdropping of CTM-id and KS on SDF_{MM} - SCF_{MM} or on one of these entities itself to masquerade as a user for outgoing CTM calls, resulting in call charged to the regular subscriber.
4	7.3.1.2.1 a)	Eavesdropping of CTM-id and RES on SDF_{MM} - SCF_{MM} or SCF_{MM} - CUSF or CUSF - SCUAF, or one of these entities itself, or on the air interface, to masquerade as the regular subscriber.
4	7.3.1.3.1 a)	Eavesdropping of CTM-id and KS, or eavesdropping of CTM-id and RES, respectively, during downloading of authentication data on SCF_{MM} - SDF_{MM} or SCF_{MM} - SCF_{SL} or SCF_{SL} - SDF_{SL} or on one of these entities itself to masquerade as the regular subscriber.
4	7.3.6.1 a)	Masquerading by using someone’s CTM-id to receive incoming long distance calls (partly) billed to the regular subscriber.
4	7.3.6.1 b)	Masquerading by using someone’s CTM-id to receive incoming calls intended for the regular subscriber.
4	7.3.6.6	Eavesdropping of the communication on CCF-CCAF for incoming calls.
4	7.3.7.6	Eavesdropping of the communication on CCF-CCAF for outgoing calls.
4	7.3.12.3	Visited network operator claims that more traffic was generated by home network's roaming user(s) than actually took place.
2-4	7.3.0.5 c)	Unauthorized access to data to eavesdrop personal information.
2-4	7.3.0.6 b)	Flooding, leading to degradation of service.
2-4	7.3.1.3.3 c)	Masquerading as SCF_{MM} to get authentication data, leading to eavesdropping of the regular subscriber's communication on the air interface.
2-4	7.3.4.2.a)	Copying an AC directly from the real subscriber or from the distribution process to him/her, eavesdropping of data in the over-the-air registration process, and subsequent calculation of the UAK to masquerade as the regular subscriber.
2-4	7.3.5.3	A subscriber does not allow de-registration by manipulating the SCF_{SL} - SCF_{MM} interface (relevant for inter-network case; possible collaboration of subscriber and visited operator). The attacker may then be able to perform outgoing calls in the visited network, as long as authentication to the home network is not required.
2-4	7.3.10.5 b)	An unauthorized user may manipulate one or both of the two lists specifying the numbers for Incoming Call Screening and Outgoing Call Barring to make or receive calls that are not allowed.
1-4	7.3.9.4 a)	Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure to deny or degrade the service of the regular user.
1-4	7.3.9.4 b)	Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure to increase its own service without authorization.

NOTE: Threats with minor risk are considered further only in annex B.

7.6 Conclusion

As a result of the previous risk assessment, we can conclude that the following five types of threats are relevant for CTM and have to be carefully considered:

- **Masquerading as a real subscriber in order to make calls without paying for them:**
  The more often the attacker can perform this threat, the worse it is. To perform this threat, the attacker can manipulate the call forwarding service. For other attacks, the CTM-id of the real subscriber is needed. If authentication or ciphering is mandatory, authentication data or ciphering key are needed by the attacker. Several attacks can lead to getting these information:

  - in the distribution process procedure;
  - eavesdropping all of them during their transfer (over the air or in the network);
  - eavesdropping part of them during their transfer and guessing the rest of them by calculation;
  - masquerading as a network entity;
  - stealing a terminal and manipulating it;
  - having unauthorized access to data in the network or in a terminal.

- **Eavesdropping of communications:**
  An attacker can perform this threat:

  - in the parts of the CTM network where encryption is not performed;
  - by masquerading as the real subscriber and getting his incoming calls. To do this, the CTM-id is needed (see above for how to get the CTM-id), but the easiest way is to steal the targeted terminal. An other way is to manipulate the service profile or supplementary services like call forwarding.

- **Denial of service and degradation of service:**
  This is possible against a service provider or a real subscriber.

  - It can be performed at any entity or interface.
  - One way to perform this threat is to have unauthorized access and manipulate the service profile or supplementary services like call forwarding, incoming call screening, outgoing call barring.
  - Unauthorized generation of traffic on any of the CTM interfaces could lead to congestion in the network (flooding).
  - Registering on a masqueraded CTM-id, leading to denial of service to the legitimate user.

- **Billing fraud:**
  Several kinds of billing fraud are possible:

  - subscription fraud leading to no payment of bills;
  - one network overcharges another network for roaming traffic;
  - inhibit de-registration procedure in a visited network by manipulation of network entities, leading to no payment of calls.

- **Other threats:**
  Several kinds of other threats are possible:

  - unauthorized manipulation of incoming call screening or outgoing call barring, to make or receive calls that are not allowed (fraud of user against subscriber, e.g. his employer);
  - unauthorized access to data, to eavesdrop personal information;
  - misuse of emergency calls via CTM can degrade or disturb the emergency call service.

8 Security Requirements and Security Services

In the following, possible security requirements and security services to counter the critical and major risks are described. The tables at the end of this clause show the mapping of the identified threats to their countermeasures.

The general requirement is that countermeasures have to be taken against all threats evaluated with risk 4 or higher. These countermeasures can not all be described at the same level of abstractness:

- some of them can be described as security services, placed at specified locations within CTM networks. The according security mechanisms will be specified in the next clause;
- some of them can be described as specific requirements on the use and specification of security mechanisms;
- some of them are more of a general nature giving guidelines for a security policy.

The security requirements and security services which will be defined in this clause are the following:

➨ **Authentication:**

- A1 = Authentication of the PT by the FT;
- A2 = Authentication of the FT by the PT;
- A3 = Authentication of the user for call forwarding services;
- A4 = Authentication of the user for incoming call screening and outgoing call barring services;
- A5 = Authentication of the user for service profile modification;
- A6 = CTM entity authentication;
- A7 = User authentication.

➨ **Access Control:**

- C1 = Access control to services;
- C2 = Access control to data;
- C3 = Access control to data in terminal;
- C4 = Access control to software;
- C5 = Access control to hardware.

➨ **Confidentiality:**

- E1 = Confidentiality of user communication on the air-interface;
- E2 = Confidentiality of signalling on the air interface;
- E3 = Confidentiality of signalling between IN entities;
- E4 = Confidentiality of signalling between FT and LE;
- E5 = Confidentiality of communication between FT and LE.

➨ **Integrity:**

- I1 = Signalling data integrity.

➨ **General Security Policy:**

- P1 = Bill limitations;
- P2 = Secure billing administration;
- P3 = Subscriber and terminal management;
- P4 = Hotline;
- P5 = Security related reports to the user;
- P6 = Secure dialogue between operators;
- P7 = Contractual agreements between operators;
- P8 = Contractual agreements between service providers and subscribers;
- P9 = Security related reports to the service providers;
- P10 = Secure subscription process.

8.1 Authentication

Authentication is a property by which the correct identity of an entity or party is established with a required assurance. Authentication is possible for several purposes and between several entities.

8.1.1 A1 = Authentication of the PT by the FT

Authentication of the PT can be provided for all outgoing and incoming calls and for location registration.

8.1.2 A2 = Authentication of the FT by the PT

Authentication of the FT by the PT allows assurance that the access point to the network is correct and therefore protects against spoof FTs.

NOTE: It has been assumed already for the threats analysis, that this security service is applied for over the air subscription registration and for subscription de-registration.

8.1.3 A3 = Authentication of the user for call forwarding services

In establishing Supplementary Services (SS) the CTM user may perform the registration and invocation of the service directly or through an agent. The SS user with authority to define and modify the service is referred to as the authorized user. The SS user whose service is modified by the actions of the authorized user is known as the affected user. Authentication can be applied to either of these parties to ensure that the call access rights of the affected user (whose calls may be forwarded) are maintained (see also C1 and C2).

For the call forwarding supplementary services, authentication of the SS-authorized user protects against invalid forwarding being applied to, or withdrawn from, the affected user (see also C1 and C2).

8.1.4 A4 = Authentication of the user for incoming call screening and outgoing call barring services

Authentication can be applied to either the authorized user or to the affected user to ensure that the call access rights of the affected user (whose calls may be filtered or barred) are maintained (see also C1 and C2).

8.1.5 A5 = Authentication of the user for service profile modification

Authentication prior to service profile modification reinforces the access rights (see also C2).

8.1.6 A6 = CTM entity authentication

Authentication of CTM entities to each other provides trust between the entities on a link by link basis. Entity authentication can be provided for each communicating pair of physical and IN entities: i.e. between FT and LE, between LE and any SCP, SCF and SDF, and between VD and HD.

8.1.7 A7 = User authentication

User authentication protects the terminal against misuse.

8.2 Access Control

Access control is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. Access control can be used to protect physical entities, software, data and the use of services.

8.2.1 C1 = Access Control to Services

Prior to accessing CTM services, an access control mechanism can check that the user has the access rights to use this service.

Access control to the CTM service or to certain service functions can be seen as a combined process with identification and authentication of the involved parties, and subsequent authorization to use specified resources.

8.2.2 C2 = Access control to data

Users, subscribers and the service provider's staff can access different part of the overall database. It is important to preserve the rights of access to each part of the database. An access control mechanism may include authentication and can restrict access to parts of a database.

The access to service data can be restricted to the following subjects with different access rights:

- CTM user;
- CTM subscriber;
- CTM service provider.

The service providers have to restrict access to personal data in accordance to national (data protection) laws. After termination of a subscription, the data may be deleted unless and only as long as they are required to deal with complaints, to recover charges or for legal obligations.

The CTM service provider is responsible that only authorized personnel have access to the data.

There may be a specific access control to the service profile data since some of these data may be changed on-line. The information stored in the service profile can be subdivided into fixed information and variable information from the CTM user's point of view. The fixed information is typically fixed at subscription time and can be changed only by the CTM service provider, possibly on request of the user. The variable information can be changed by the CTM user, by using CTM service profile management functions. Authentication data may need specific consideration.

8.2.3 C3 = Access control to data in terminal

A strong physical protection may be used for implementing the access control to the sensitive information stored in the terminal (e.g. keys, PIN). The use of the terminal may be controlled by authentication of the user (see also A7).

8.2.4 C4 = Access control to software

The access to computers' operating software can be controlled. This is particularly important with respect to insertion of viruses. Authentication of personnel and access control in the service provider's systems may be provided.

8.2.5 C5 = Access control to hardware

Hardware can be protected against unauthorized actions either from the CTM staff or intruders. Authentication of personnel and access control in the service provider's environment may be provided.

8.3 Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. It may be used to protect personal communications and data, and signalling data.

8.3.1 E1 = Confidentiality of user communication on the air-interface

Encryption on the air-interface using the DECT mechanisms for outgoing and incoming calls, and for subscription registration procedure can provide confidentiality to the user communication and to DECT signalling.

8.3.2 E2 = Confidentiality of signalling on the air interface

The signalling can be protected on the air interface. Possible solutions include the use of encryption.

8.3.3 E3 = Confidentiality of signalling between IN entities

Security and other sensitive data such as session keys, triplets, call-forwarding number, and personal data can be protected by a number of mechanisms. Encryption is one such mechanism.

8.3.4 E4 = Confidentiality of signalling between FT and LE

The signalling interface between FT and LE (i.e. the SCUAF-CUSF interface) may be protected. This may be done by physical protection or by cryptographic methods. Especially, the CTM-id and the DCK may need to be protected.

8.3.5 E5 = Confidentiality of communication between FT and LE

The communication interface between FT and LE (i.e. the CCAF-CCF interface) can be protected. This link may not be within a fixed network and therefore may be open to interception. This may be protected using either physical protection or encryption.

8.4 Integrity

Integrity mechanisms ensure the prevention of unauthorized modification of information.

8.4.1 I1 = Signalling Data Integrity

Data integrity mechanisms can be provided in the CTM network for data transfers including: specified call forwarding number, call record data, billing records.

8.5 General Security Policy

A general security policy needs to be implemented to counter the identified threats. The following security requirements should be included within this policy.

8.5.1 P1 = Bill limitations

It can be necessary to protect users from bills of unexpected amounts. Further it may be necessary to protect users from misuse of their accounts, and to protect operators from misuse of services.

Different methods, or combinations of methods, are possible to realize this requirement:

- Absolute bill limitation:

  When a subscriber opens an account, there can be an option to set a credit limit on the account. The total amount of the current bill of the subscriber may be checked at call set-up. A policy can be implemented about the acceptance or not of the call in case of exceeding bill limit. This can limit damage if abuse take place.

- Bill limitation with respect to time:

  Another possible measure would be to limit the bill with respect to time. Thus, the credit limit may be on a day-by-day basis, on a weekly basis, or provide an overall limit That means, if e.g. a limit per week is agreed and this limit is exceeded (at call set-up or during a call), the user access would be blocked for the rest of the week.

- Origin and Destination limits:

  Another security measure may be for certain accounts (for new or less trustworthy subscribers) to limit the destinations of calls. The limit may be within a given area, within the country, or even only to a specified destination address. Likewise, a limit may be put on the callers location for outgoing calls.

8.5.2 P2 = Secure billing administration

The billing administration may have to consider security very carefully. Billing data and related personal data can be stored, processed, and transmitted in such a way that user privacy and data integrity are guaranteed. Itemised bills may be a means for the CTM subscriber to check the correctness of the billing. Thus, the billing administration can send to the user an explained bill with the called numbers and split in different part like regional calls, national calls, international calls. However, to avoid conflicts with privacy requirements, the subscriber can also have the possibility to get only summarized bills.

8.5.3 P3 = Subscriber and terminal management

Limiting the access to services by means of subscription restriction or equipment restriction can reduce otherwise unacceptable risks. This can be achieved in a number of ways such as by the use of black lists to identify rogue subscribers or rogue equipment. Service may be denied to subscribers or equipment that appears on such a black list.

A white list gives unrestricted access to subscribers and equipment (within any limits set by their service profile). Intermediate variants of these lists may be maintained to track potential bad debt or potential fraud.

8.5.4 P4 = Hotline

A Hotline can be provided by the operator in order to answer users' questions like " My service does not work", "I have received too high a bill". This service may be useful for security reasons in case of theft or loss of terminal or in case of unexpected behaviour of the service of a subscriber where specific procedures should be implemented. In case of theft or loss of terminal, this procedure can be:

- location of the stolen or lost terminal in order to find it;
- block incoming and outgoing calls;
- put the CTM number on a black list;
- no charging for the subscriber of calls performed after the report of the theft;
- de-registration of the terminal after location.

8.5.5 P5 = Security related reports to the user

Recording and presentation of information about actions performed by users in the system (event reporting) may often function as a supporting security service. (Users' knowledge of this fact may in turn work as a deterrent factor). Announcements must be carefully designed to enlighten users and third parties of the different states of their connection or relation with the operator/service provider. There can be a facility to inform CTM users about actions that affect their privacy and security or the charging. This information can be given on-line by announcements, special dial tones, or short messages.

For example, the following information can be given to the users:

- "BILL LIMITATION EXCEEDED".

8.5.6 P6 = Secure dialogue between operators

Secure dialogues can consist of a mutual authentication procedure, a confidentiality service and a data integrity service on the communication link. It can be provided by:

- mutual authentication;
- link encryption;
- link data integrity;
- non-repudiation;
- key management to support this.

8.5.7 P7 = Contractual agreements between operators

Contractual agreements relating to security issues can be included in the roaming agreement between two operators.

When agreeing upon a roaming agreement two operators may define some security conditions. Those conditions can be:

- frequency of exchange of blacklists;
- liability of a visited network if it does not take the appropriate measures to stop a fraud;
- level of security audit guaranteed;
- follow the rules concerning the use of data an other network can get access to;
- co-operation in case of fraud;
- integrity of file transfer;
- minimum frequency of authentication to be performed for visiting CTM users;
- in case of dispute, one network operator should be able to provide the other network with every information related to billing.

8.5.8 P8 = Contractual agreements between service providers and subscribers

Contractual agreements relating to security issues shall be included in the conditions for the subscription. Security conditions to be agreed and signed by the subscriber could be:

- to follow the rules (as declared by the CTM service provider and adjoined to the subscription contract) regarding secure handling of his PIN if used to protect terminal;
- to report to the service provider immediately loss of terminal which might lead to fraud or misuse;
- to accept limitations of service with regard to agreed levels of credit control/bill limitation;
- to accept limitations of service which the service provider later on may find necessary to introduce to protect the service as such against misuse or fraud.

8.5.9 P9 = Security related reports to the Service Provider

Recording and reporting the use of security services will allow the service provider to conduct security audits in order to detect actual threats against the CTM system. Such audits may be used to investigate unauthorized use of a CTM terminal or unauthorized change of profile or abnormal patterns or misbehaviour or abuses.

The following data may be audited:

- use of the authentication mechanism (date, time, CTM-id, location, number dialled, success or failure of the attempt);

- attempted access to the service profile (date, time, CTM-id, name of the object, type of access attempt, success or failure of the attempt);

- actions by CTM service providers staff (date, time, CTM-id, type of action).

In practice the audit will be restricted to specific sets of users.

Access to audit data should only be permitted to authorized persons (see also C2, C4 and C5).

Dependent on the evaluation of audit data (on-line or off-line) some actions have to be carried out in order to enforce the security policy. These actions may include: alarms to the security administrator, or blocking of the subscription.

8.5.10 P10 = Secure subscription process

A secure subscription process can restrict subscription fraud. A security policy may be applied to new subscribers in order to be to be confident in the ability and motivation of a subscriber to pay any bills. This may be achieved by authenticated or verified delivery of proofs of identity.

It may be possible for subscriptions to be made available on a pre-paid (contract less) basis. It can be possible to inhibit service when the pre-payment is exceeded.

The operator may restrict the number of subscriptions per subscriber.

8.6 Threats and counteracting security measures

As a first step in the process of selecting relevant and suitable security services for CTM, the following choices were made.

- A1 = Authentication of the PT by the FT (at location registration);
- A2 = Authentication of the FT by the PT (for subscription registration and subscription de-registration);
- A3 = Authentication of the user for call forwarding services;
- C1 - C5 = Access control to services, to service data in databases, to data in terminals, and to the service provider's software and hardware, respectively;
- E1 = Confidentiality of user communication on the air-interface;
- P1 = Bill limitations;
- P2 = Secure billing administration;
- P9 = Security related reports to the service providers;
- P10 = Secure subscription process.

These measures are a natural start for one, or several, of the following reasons:

1) These countermeasures will cover all threats with potential risk 9, as shown in table 26, and in addition many other threats, as shown in table 27.

2) They can easily be implemented following the decision to only treat DECT as radio interface.

3) They belong to a set of security policy decisions that are of such a generic nature that they can be expected to be inherently present in a public network service like CTM.

Table 26: Threats with potential risk 9 covered by initial selection of countermeasures

Reference	Threat description	Security Requirements and Services
7.3.7.1	Masquerading by using someone's CTM-id to perform outgoing calls to be billed to the regular subscriber if authentication is not required.	A1, E1 Authentication is assumed to take place at least at each location registration, optionally also at other times. Calls are assumed to be enciphered with the last stored DCK, thus providing an implicit authentication.
7.3.0.8 a)	Subscription fraud in order to intensively use CTM services with no intention to pay.	P1, P9, P10
7.3.7.11	Masquerading by using someone's CTM-id only, and resulting avoidance of charging for a (probably short) period at the beginning of a communication.	E1 Ciphering is assumed to be active already at call set-up.
7.3.10.4	Several unauthorized call forwarding registrations for another CTM subscriber to make (or sell!) several calls at the same time using the number of the real CTM subscriber who will be charged for these several calls.	A3, P1, P9
7.3.0.4 a)	Denial of service.	C1, C2, C3, C4, C5, P9

Table 27: Threats with potential risk less than 9 covered by the initial selection of countermeasures

	Threat description	Security requirements and services
7.3.6.1 c)	Duplication of CTM-id leading to denial of service to the legitimate user.	A1 Authentication is assumed to take place at least at each location registration).
7.3.0.1 a)	Eavesdropping of CTM-id on IN interfaces or entities to masquerade as the regular subscriber.	A1
7.3.0.2 a)	Eavesdropping of CTM-id on the air interface to masquerade as the regular subscriber.	A1
7.3.0.3 a)	Getting the CTM-id from a terminal to masquerade as the regular subscriber.	A1
7.3.0.5 b)	Unauthorized access to databases (SDFs) to masquerade as the regular subscriber.	C2
7.3.10.1 a)	An unauthorized user may register to a call forwarding service and request registration for the service to another forwarded-to number, to make calls by using the number of the attacked CTM subscriber who will then be charged for part of the attacker's communications.	A3
7.3.10.1 b)	An unauthorized user may register to a call forwarding service and request registration for the service to another forwarded-to number to re-route incoming calls of a CTM subscriber in order to get all his incoming calls (eavesdropping) and/or to make him loose his incoming calls (denial of service).	A3
7.3.10.2 a)	An unauthorized user may request erasure of the call forwarding of someone else.	A3
7.3.0.4 b)	Degradation of service.	C1, C2, C3, C4, C5, P9
7.3.0.9 a)	Unauthorized access to CTM-id and KS in terminal to masquerade as the regular subscriber.	C3
7.3.6.1 a)	Masquerading by using someone's CTM-id to receive incoming long distance calls (partly) billed to the regular subscriber.	A1, E1

	Threat description	Security requirements and services
7.3.6.1 b)	Masquerading by using someone's CTM-id to receive incoming calls intended for the regular subscriber.	A1, E1
7.3.0.6 b)	Flooding, leading to degradation of service.	C1, C2, C4, C5, P9
7.3.9.4 b)	Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure to increase own service without authorization.	C1, C2

Assuming that the security requirements and security services are implemented as stated above, the remaining threats with major risk can be counteracted as shown in table 28.

Table 28: Remaining threats and counteracting security requirements/services

Reference	Threat description	Additional security requirements and security services	Security require-ments and security services already chosen
7.3.0.7 a)	Stolen terminals used for calls.	A7, P3, P4, P8	
7.3.1.3.3 a)	Masquerading as SCF$_{MM}$ to get authentication data, leading to masquerading as the regular subscriber.	A6	P1, P9
7.3.0.6 a)	Flooding, leading to denial of service.	A6, supported by P3	P9
7.3.4.1 a)	Eavesdropping of data in an over-the-air registration process and subsequent exhaustive search for AC to masquerade as the regular subscriber.	Change of random numbers for the subscription registration process, AC of maximum length	
7.3.10.5 a)	An unauthorized user may manipulate one or both of the two lists specifying the numbers for Incoming Call Screening and Outgoing Call Barring to deny outgoing or incoming calls for the user.	A4, supported by A6, P4	C1, C2, supported by C4, C5
7.3.0.7 c)	Stolen terminals used to get regular user's incoming calls.	A7, P3, P4, P8	
7.3.1.1.1 a)	Eavesdropping of CTM-id and KS on SDF$_{MM}$ - SCF$_{MM}$ or on one of these entities itself to masquerade as a user for outgoing CTM calls, resulting in call charged to the regular subscriber.	E3, supported by Change of authentication data for each authentication	supported by C2, C5, C4
7.3.1.2.1 a)	Eavesdropping of CTM-id and RES on SDF$_{MM}$ - SCF$_{MM}$ or SCF$_{MM}$ - CUSF or CUSF - SCUAF, or one of these entities itself, or on the air interface, to masquerade as the regular subscriber.	E2, E3, E4 OR Change of authentication data for each authentication	supported by C2, C5, C4
7.3.1.3.1 a)	Eavesdropping of CTM-id and KS, or eavesdropping of CTM-id and RES, respectively, during downloading of authentication data on SCF$_{MM}$ - SDF$_{MM}$ or SCF$_{MM}$ - SCF$_{SL}$ or SCF$_{SL}$ - SDF$_{SL}$ or on one of these entities itself to masquerade as the regular subscriber.	E3, supported by Change of authentication data for each authentication	supported by C2, C5, C4

Reference	Threat description	Additional security requirements and security services	Security require-ments and security services already chosen
7.3.1.3.3 a)	Masquerading as SCF_{MM} in order to get authentication data (CTM-id, and session keys or triples) from the SDF_{SL} on request to masquerade as the regular subscriber (only if these data are not changed at each request from an SCF_{MM} to an $SCF_{SL}/SDF_{SL})$.	A6, supported by P6, P7 OR Change of authentication data for each authentication	
7.3.5.3	Subscriber does not allow de-registration by manipulating the SCFSL - SCFMM interface (relevant for inter-network case; possible collaboration of subscriber and visited operator). The attacker may then be able to perform outgoing calls in the visited network, as long as authentication to the home network is not required.	I1, P7, supported by E3	P9
7.3.6.6	Eavesdropping of the communication on CCF-CCAF for incoming calls.	E5	
7.3.7.6	Eavesdropping of the communication on CCF-CCAF for outgoing calls.	E5	
7.3.12.3	Visited network operator claims that more traffic was generated by home network's roaming user(s) than actually took place.	P7, supported by P3	supported by P2
7.3.0.5 c)	Unauthorized access to data to eavesdrop personal information.	A6, A7, P8	C2, C3
7.3.1.3.3 c)	Masquerading as SCF_{MM} to get authentication data, leading to eavesdropping of the regular subscriber's communication on the air interface.	A6, supported by E3	
7.3.4.2.a)	Copying an AC directly from the real subscriber or from the distribution process to him/her, eavesdropping of data in the over-the-air registration process, and subsequent calculation of the UAK to masquerade as the regular subscriber.	Secure over-the-air subscription registration, secure distribution process of key data	C2, C3
7.3.10.5 b)	An unauthorized user may manipulate one or both of the two lists specifying the numbers for Incoming Call Screening and Outgoing Call Barring to make or receive calls that are not allowed.	A4, supported by P5	C1, C2, supported by P9, C4, C5
7.3.9.4 a)	Unauthorized access to, or unauthorized use of, the Service Profile Modification procedure to deny or degrade the service of the regular user.	A5, supported by P5	C1, C2, supported by P9, C4, C5

9 Resulting Security Architecture

The architecture for provision of CTM security, taking into account the threat analysis of clause 7, and the provision of security services and security requirements as discussed in the subclauses above, can be divided into four parts:

- radio access part;
- service data access part;
- network part;
- policy part.

The radio access part of the security for CTM is by means of DECT technology handsets and the over-the-air protocol defined for DECT. However, a number of implementation recommendations will need to be respected, they are detailed in clause 10.

To protect the user access to invoking and modifying the data for some supplementary services authentication is needed, also in the situation when the access is made from non-CTM terminals.

The network part of the security for CTM relies mainly on a dedicated IN security architecture, generic for all services which rely on the functionality and thus the security of IN. CS2 security mechanisms, where they exist, but also other supporting mechanisms (e.g. for key management) to counter the threats and satisfy the security requirements will have to be exploited. However, as the generic IN security solution should encompass also the requirements from other IN services and their needs (user's, subscriber's, service provider's, network operator's, regulatory, data protection, …), a detailed description of a generic IN security architecture is out of scope for the present document. The present document will give the requirements as derived from the CTM security studies, for use in subsequent work on IN security architectures.

Apart from the generic security architecture, which in principle is independent of CTM and other services, some CTM specific protection is needed also on the network level.

The policy part of the security for CTM again can be considered to be of a general nature for mobile or mobility oriented services and thus the recommendations given here will be common for many similar services. However, it should be noted that implementations may heavily depend on kind of service provider (big or small, public or private, incumbent or new, etc.).

9.1 Radio access part

The radio access part of the CTM security architecture shall be composed of DECT security services as defined by EN 300 175-7. They shall provide the following:

- A1 = Authentication of the PT by the FT, at least for each location update;
- A2 = Authentication of the FT by the PT, in connection with subscription registration and de-registration over-the-air;

NOTE: A2 was incorporated as a required security service for the over-air registration process already in the service descriptions for CTM. See core requirements for CTM, subclause 4.4 in the present document.

- A7 = User authentication (local PIN given to PT or similar);
- E1 = Confidentiality of user communication on the air interface;
- E2 = Confidentiality of signalling on the air interface;
- C3 = Access control to data in terminal.

9.2 Service data access part

For access to and modification of some service data, the following services are required:

- A3, A4, and A5, where the means of access to the specific service/data is via the CTM/DECT radio interface, shall be provided by A1 and A7 in combination (see 8.7.1).
- A3, A4, and A5, where the means of access to the specific service/data is via some other interface or network, shall be provided by its own authentication mechanism.
- C1 = Access control to services.

9.3 Network part

The network part of the CTM security architecture shall provide the following:

- A6 = CTM entity authentication, i.e. authentication of any other entity by an IN entity used for CTM services;
- C2, C4, C5 = Access control to service providers' CTM data, software and hardware;
- I1 = Signalling data integrity;
- E3 = Confidentiality of signalling between IN entities;
- E4 = Confidentiality of signalling between FT and LE;
- E5 = Confidentiality of communication between FT and LE.

NOTE: E4 and E5 are really for protecting network connections to CTM specific entities and do not belong to the so called generic IN security architecture.

9.4 Policy part

The policy part of the CTM security architecture shall provide the following:

- P1 = Bill limitations;
- P2 = Secure billing administration;
- P3 = Subscriber and terminal management;
- P4 = Hotline;
- P5 = Security related reports to the user;
- P6 = Secure dialogue between operators;
- P7 = Contractual agreements between operators;
- P8 = Contractual agreements between service providers and subscribers;
- P9 = Security related reports to the service providers;
- P10 = Secure subscription process.

9.5 Concluding remarks

The recommended CTM security architecture is thus defined by the security services specified in subclauses 9.1 to 9.4 above. They are summarized in figure 3 for illustrative purposes.

The services in subclause 9.1 can be implemented by mechanisms already present in DECT specifications. Their use and size of some parameters is, however, critical for the CTM security. This is detailed in clause 10.

NOTE: Clause A.3 to A.5, when using a non-DECT terminal, will naturally be implemented by one and the same authentication mechanism.

Also note that the security requirements on an IN security architecture evidently can be attained by a few well selected security mechanisms, see further in clause 10.

It should be noted that the security services E4 and E5, for protecting against eavesdropping on the user communication and signalling between FT and LE, are CTM specific and can not be considered part of a generic IN security architecture. They might however well draw upon, co-operate with and co-exist with the generic IN security mechanisms.

E4 and E5 are furthermore considered to be administratively and technically expensive and difficult to implement and should better be considered as an optional part of the CTM security architecture. Also the risks connected with use of the fixed network can be regarded as not specific for CTM. See further clause 10.

The proposed CTM security architecture covers all threats analysed in the present document that have been evaluated at level 4 or higher.

Furthermore it covers also 54 out of the 63 threats evaluated at lower risk levels. The threats not countered for are mostly of the nature that IN or other interfaces are manipulated in such a way that messages are blocked which leads to inhibited actions. To counter this kind of threat, the integrity of the protocol should be assured. This should include identification of out of sequence messages, timely acknowledgement of messages, and integrity checks of data element sequence and content within messages.

Misuse of the emergency call facility can not be protected in an effective way in CTM - very much as is the case in other (mobile) access networks to emergency call centres. This can not be considered to be a CTM specific problem. Only by not allowing these calls to be made without authentication can the problem be solved.

Finding economically viable ways to counter also these remaining threats are of course encouraged as they will contribute to overall CTM security, but they are not considered as being an integral part of the minimum requirements for a generic CTM security architecture.

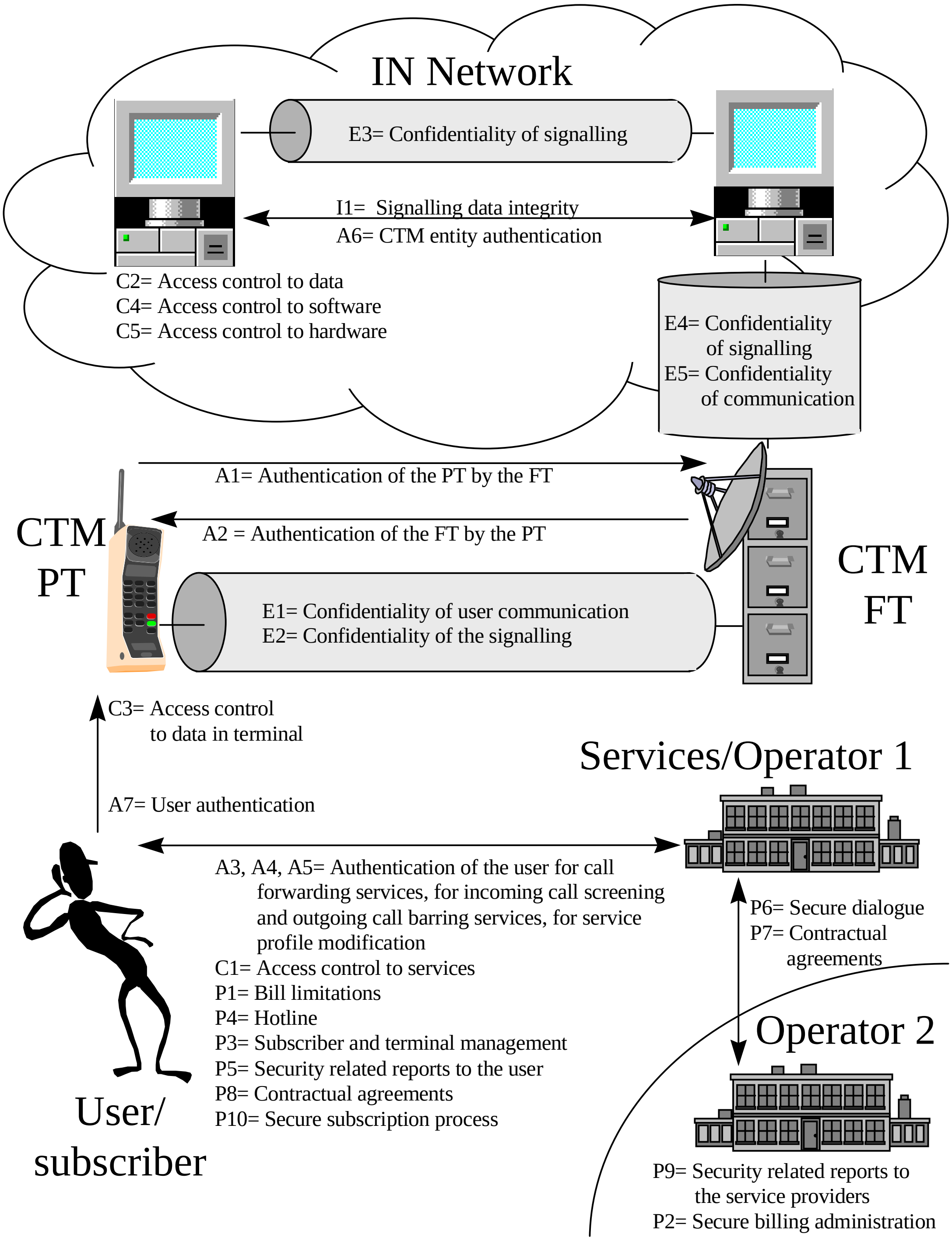

IN Network
E3= Confidentiality of signalling
I1= Signalling data integrity
A6= CTM entity authentication
C2= Access control to data
C4= Access control to software
C5= Access control to hardware
E4= Confidentiality of signalling
E5= Confidentiality of communication
A1= Authentication of the PT by the FT
A2 = Authentication of the FT by the PT
CTM PT
CTM FT
E1= Confidentiality of user communication
E2= Confidentiality of the signalling
C3= Access control to data in terminal
A7= User authentication
Services/Operator 1
A3, A4, A5= Authentication of the user for call forwarding services, for incoming call screening and outgoing call barring services, for service profile modification
C1= Access control to services
P1= Bill limitations
P4= Hotline
P3= Subscriber and terminal management
P5= Security related reports to the user
P8= Contractual agreements
P10= Secure subscription process
P6= Secure dialogue
P7= Contractual agreements
Operator 2
User/ subscriber
P9= Security related reports to the service providers
P2= Secure billing administration

Figure 3: CTM Security Architecture

10 Security Mechanisms

10.1 Radio Access Part

The radio interface shall be protected by means of the DECT security mechanisms as defined by EN 300 175-7. This shall provide the following security services described in clause 8: A1, A2, A7, E1, E2, and C3.

In addition, some requirements on the implementation of the subscription registration are made in this subclause.

A1 = Authentication of the PT by the FT

- For authentication of the PT, the DECT procedures specified in EN 300 175-7 shall be used.
- Authentication of the PT shall be performed **at each location registration**. For outgoing and incoming CTM calls, PT authentication is then implicitly provided since encryption by use of a DCK is performed (see E1).

NOTE: It is not necessary to perform PT authentication in connection with call set-up (whether in parallel or not). However, if nevertheless authentication is performed in parallel with call set-up, the old DCK should still be used for encryption of the new call while the new DCK is kept for subsequent call(s). DECT allows to store several encryption keys for one identity, where the FT decides which one to be used.

- In addition, authentication shall be invoked at other times, in order to frequently change the DCK. Authentication may e.g. be performed at each or some incoming and outgoing calls; or a lifetime for the DCK may be specified and a new authentication may be performed when this lifetime is over.
- Authentication data (at least RAND-F) shall be changed for each authentication.
- In the inter-network case, authentication should be performed in the visited network.

A2 = Authentication of the FT by the PT

- Authentication of the FT by the PT is mandatory for over-the-air subscription registration and for subscription de-registration, by use of the mechanism specified in EN 300 175-7. For outgoing and incoming CTM calls, FT authentication is implicitly provided if encryption by use of a DCK is performed. For that reason (besides the confidentiality requirement), encryption shall be mandatory for all incoming and outgoing CTM calls (see E.1).

A7 = User authentication

- A PIN shall be used to protect the terminal against misuse. This PIN shall be checked in the terminal (as in GSM) whenever the terminal is switched on.

NOTE: It is not recommended to use the UPI (User Personal Identification) as specified in EN 300 175-7, for the following reasons: According to EN 300 175-7, it had to be entered into the terminal at each authentication which is not acceptable from a user point of view. Furthermore, there is no mechanism specified to modify the UPI value which would be desirable for security reasons and for reason of user friendliness.

E1 = Confidentiality of user communication on the air interface

- The confidentiality service shall be provided by encryption as specified in EN 300 175-7 for DECT.
- Encryption shall be mandatory for **all** incoming and outgoing CTM calls, encryption shall be already active at call set-up.
- The DCK, derived from the UAK/KS at an earlier PT authentication (e.g. at location registration) shall be used.

E2 = Confidentiality of signalling on the air interface

- Confidentiality shall be provided by encryption as specified in EN 300 175-7 for DECT, for all signalling with the exception of the beginning of the over-the-air subscription registration procedure and any initial location registration procedure at a new FT.

NOTE: For the over-the-air subscription registration procedure, encryption can be invoked before the CTM-id is transmitted to the PT by use of the DCK derived from the AC.

C3 = Access control to data in terminal

- A strong physical protection is required for implementing the access control to the sensitive information stored in the terminal. It shall not be possible at all to read secret data such as keys and PINs. The use of the terminal and the access to user related data shall be controlled by authentication of the user (PIN, see A7).

Requirements on the implementation of the subscription registration

- For security reasons, it is important to change the random numbers used for the over-the-air subscription registration process for each new subscription registration.

- The AC to be entered by the user shall consist of 8 decimal digits.

NOTE: The GAP ETS 300 444 requires 32 bits for the AC within the system, however, it allows ACs of smaller sizes as user input which are then automatically padded with leading "1"s. The maximum possible AC size for the user input is 8 decimal digits.

- The over-the-air key registration shall only be allowed during a pre-defined time window and at the home domain.

- The AC (and other key data if used e.g. for A3, A4, A5) shall be transmitted to the CTM subscriber in a secure way, e.g. by registered letters.

- The use of a DAM as specified in ETS 300 331 could avoid the threats related to the over-the-air subscription registration.

10.2 Service Data Access Part

10.2.1 Authentication of the user for supplementary services (A3, A4, A5)

Prior to gain access to the three following supplementary services, call forwarding, incoming call screening and outgoing call barring, authentication of the user is required. The same authentication procedure shall be used for the three services.

When the user performs these requests from is own CTM terminal, the authentication of his terminal (A1) is sufficient.

When the user performs these requests from another terminal, a specific authentication is needed. In that case it is recommended to use an authentication ensuring a good level of security such as the strong authentication defined for UPT in ETS 300 391.

When the user performs these requests from a terminal unable to offer a strong authentication mechanism, a weak authentication (PINs) may be used.

10.2.2 Access control to services (C1)

Only authorized personnel shall get access to the users service profile (especially to the call forwarded to number and the lists for screening of incoming calls and barring of outgoing calls).

10.3 Network part

The network part consists of two inter-working sub-parts: The IN part, and CTM specific extensions to the IN part.

10.3.1 Mechanisms

10.3.1.1 Intelligent Network part

The network part shall provide the following services by use of INAP-CS2/CS1 mechanisms:

- A6 = IN entity authentication;
- E3 = confidentiality of signalling between IN entities;
- I1 = signalling data integrity;
- C2 = access control to data.

NOTE: A6 in this case refers to those entities of CTM that reside in the IN part.

The INAP-CS2/CS1 security models are based upon the X.500 directory services model and this in turn uses a public key security model captured in X.509. Current X.509 provisions are unlikely to be adequate to provide signalling confidentiality for real time communications (E3).

10.3.1.2 CTM specific extensions to IN part

Some of the CTM network part falls outside the scope of the IN security model. This in particular refers to the following services:

- A6 = CTM entity authentication;
- E4 = confidentiality of signalling between FT and LE;
- E5 = confidentiality of communication between FT and LE;

NOTE 1: A6 in this case refers to those entities of CTM outside the scope of IN.

It is recommended that the CTM security model draws upon the IN security model (INAP-CS1/CS2). However current X.509 provisions are unlikely to be adequate to provide signalling or traffic confidentiality for real time communications (E4, E5). Provision of a cryptographic means of security for E4 and E5 may be prohibitive in cost, or in management overhead, using existing INAP-CS1/CS2 techniques. It is suggested therefore that E4 and E5 can be provided by non-cryptographic means, e.g. by physical protection. Such protection may be afforded by extension of the automatic fault monitoring facilities provided on most exchange lines. These facilities may be able to detect changes in the characteristics of lines that may indicate tampering and to raise security alarms to the user or to the service provider (P5 and P9).

NOTE 2: The intention of CTM security is to provide mechanisms that allow security equivalent to that of the fixed network. However the security of the fixed network is largely undefined and conformance to the preceding statement cannot be proven in most cases.

10.3.2 Recommendations

The present document shall provide no additional specification of IN security mechanisms. However a harmonized model for all IN services (therefore including CTM) is recommended as future work. The following recommendations are made as the basis for future work:

- provision of a single authentication mechanism between CTM entities (A6) (This covers both IN entities and those CTM entities used to communicate with IN entities);
- provision of a confidentiality mechanism bound to A6 that provides confidentiality of information exchange between IN entities and IN access entities (E3, E4);
- provision of an integrity mechanism bound to A6 that provides integrity checking on the content of information exchanges between CTM entities (I1);
- provision of an access control mechanism bound to A6 and supplementary information to restrict access to data stored by an IN or CTM entity (C2).

In addition due care in specifying a mechanism in future work should take due care to address the items in subclauses 10.3.2.1 and 10.3.2.2.

10.3.2.1 Key management

The CTM security architecture involves the participation of at least two key management domains:

- CTM key management part is provided by each CTM service provider. This shall extend the key management of DECT to transport key material for each of A1 and A2.
- IN security key management is provided by network operators in support of A6. Where network operators inter-operate to provide support for CTM services the key management services of each network operator will require to co-operate. Where A6 is used in the wider CTM network some co-operation between domains may be required.

10.3.2.2 Secure transport for IN signalling (ROSE)

The underlying IN communications protocol of IN is based upon ROSE (Remote Operations Service) with ISO/OSI lower layers. There is no assumption of security provision from the lower layers of the IN protocol. It may therefore be considered as a design option to provide some security within the ROSE operations. A number of such options are proposed for further study:

- private IN (convert actual IN operation to a bit string only);
- secure source IN (as per private IN with addition of A6 for authentication of source);
- secure content IN (as per secure source IN with addition of I1 integrity checking of data);
- secure IN (as per secure content IN with addition of E3 for encryption).

Annex A (informative): Use of CT2 for CTM

This informative annex gives background information on CT2 security and a comparison between CT2 and DECT as regards CTM security.

A.1 Portable Part (PP) authentication

CT2 authentication is described in I-ETS 300 131, normative annex B "Telepoint operation" and is stated to be used by all Telepoint operators and in world-wide roaming, according to UK F1.

Terminal (CPP) authentication should be supported and used in call set-up for Telepoint.

(The protocols also describe the use of an additional CPP authentication using an alternative algorithm. This feature is said to be for possible future use and then possibly mandatory, according to informative annex E in I-ETS 300 131).

The terminal authentication works as follows. CT2 handset has an embedded key of 64 bits. The random challenge, RAND, from Telepoint fixed side is 32 bits. A function, F, for calculating the response of 32 bits from key and RAND is common to all Telepoint systems (using UKF1) and should be incorporated in all handsets.

There is no session key hierarchy in CT2 as there is in DECT.

Terminal authentication takes place for all outgoing and incoming calls in the Telepoint environment and is to be completed before calls are through connected.

The service provider may derive the user key from the CT2 handset identification information (see below), using a proprietary function f.

A.2 Fixed Part (FP) authentication

Fixed side (CFP) authentication is not mentioned in CT2, and is not used in Telepoint, see the "minimum handset configuration" as described in annex B.

A.3 Identities and associated parameters

The CT2 handset contains an identity information comprised of 6 parameters:

MIC	(manufacturer identity code);
HIC	(handset identity code);
OPSIC	(home service identification code);
TCOS	(Telepoint class of service);
TRD	(Telepoint registration data);
ZAP	(zap field).

In addition, a Link Identification Code, LID, which identifies the link to the home service provider, shall be present in the handset.

Furthermore, the KEY for authentication is stored in the handset.

The first two parts are inserted in the handsets by the manufacturer.

The following four parts are related to the Telepoint service account and the service provider. All six parameters are transmitted in clear over-air at different occasions of link initiation, handshaking and call set-up. The values of the parameters, with exception of OPSIC, can not be displayed or otherwise obtained from the handset by the user.

The identity parameters are used by the service provider to uniquely identify the subscriber and to calculate the authentication key using the proprietary function f.

A.4 Registration

Most of the identities used for authentication shall be programmed in to the handset by the user at registration. These are LID, OPSIC, TCOS, TRD and KEY. These data are to be entered to the handset via a standardized procedure.

On-air registration procedure:

This is described in an informative annex F in I-ETS 300 131.

The user enables the on-air registration at the CFP ant then activates the registration sequence from the CPP. The user is requested to enter a four digit PIN from keyboard, which is transported to the fixed side over-air.

There is no over-the-air key setting in CT2 as there is in DECT. The authentication key in CT2 is entered manually and completely off air.

A.5 On-air (de)-registration acknowledgement

On completion of a registration or de-registration process the CFP will transmit an information element for acknowledgement. A de-registration acknowledgement from the network will cause the CPP registration field to be nulled.

A.6 ZAP facility

Each CT2 handset has a ZAP field, associated with the Telepoint registration, which is intended to allow the operator to temporarily or permanently bar that handset. In the authentication response the service provider may thus increase the value of the ZAP field, and by checking the present value of it he may effectively decide to keep that handset out of service. The ZAP field shall be provided by all CT2 handsets, the use of the ZAP field information is however proprietary to service providers.

A.7 Ciphering

There is no ciphering in CT2.

A.8 Comparison of CT2 and DECT regarding security for CTM

The use of CT2 and DECT in the following table is based on CTM features described in EG 201 096-1.

Table A.1: Comparison of CT2 and DECT regarding security for CTM

Features	DECT for CTM, status	CT2 for CTM, status
Handset authentication	⇨ optional for all outgoing and incoming calls ⇨ authentication can be done in parallel ⇨ can be invoked at any time	⇨ for all outgoing and incoming calls in the Telepoint environment and is to be completed before call set up <u>Resulting differences:</u> ➔ CT2 has equal or less vulnerabilities than DECT, depending on how authentication is used in DECT
Network authentication	⇨ performed at subscription registration and de-registration ⇨ can be invoked at any time	⇨ does not exist in CT2 <u>Resulting differences:</u> ➔ masquerading of network towards the subscriber at over-air de-registration and in the ZAP procedure implies increased threats to CT2
Key setting	⇨ short key (AC) entered in the handset by the user before registration, expanded during subscription registration over-air	⇨ full key entered in the handset by the user at registration <u>Resulting differences:</u> ➔ CT2 key setting is safe from attacks over-air, the manual procedure seems more secure than DECT over-air key setting. The distribution process for keys shall be secure in both cases
Identification setting	⇨ identification entered in the handset by the network during over-air subscription registration	⇨ identification entered in the handset by the user before registration and confirmed over-air <u>Resulting differences:</u> ➔ threats during subscription registration are different, but arise in both cases
Registration over-air procedure	⇨ CTM-id and key given by the network during over-air subscription registration	⇨ The user activates the on-air registration at the CFP and the registration sequence from the CPP. The user is requested to enter a four digit PIN from keyboard, which is transported to the fixed side over-air <u>Resulting differences:</u> ➔ no network authentication in CT2, risk of false network
Ciphering	⇨ shall be invoked for all calls ⇨ ciphering optional during subscription registration (?), location registration	⇨ does not exist <u>Resulting differences:</u> ➔ eavesdropping of communication over the air for all CT2 incoming and outgoing calls is possible ➔ no ciphering during CT2 call set-up and location registration; personal data like dialled numbers and geographical positions may thus be compromised, tracking is possible ➔ no ciphering leads to higher requirements on use of authentication
Session key hierarchy	⇨ yes, use of session key, KS	⇨ no, only a direct challenge-response with user key <u>Resulting differences:</u> ➔ no choice of using KS implies transport of either subscriber secret key or (RAND, RES) between networks

A.9 Conclusions

Terminal authentication for DECT and CT2 is similar. Depending on CTM service provider routines, terminal authentication can be used to the extent considered necessary. In DECT it can be used for all call set ups, however, if ciphering is mandatory, authentication is not really necessary.

The CT2 absence of network authentication makes it vulnerable for false network attacks, e.g. for de-registration and for manipulation of and control over a targeted subscriber's calls.

The use of session keys in DECT offers better possibilities in the roaming situation. CT2 shall either use transport of subscriber key, which may prove too vulnerable, or use transport of pairs of authentication parameters (RAND, RES), which increases signalling traffic and may induce delays.

The registration of subscribers in CT2, using a manual procedure for entering identity and key, is more cumbersome than the DECT over-air registration, but both can be conceived to be made secure. The evaluation of risks for the DECT over-air procedure indicates that the AC shall be set to maximum size. CT2 may prove to be the more secure standard for key setting, given the distribution process is made secure. However, if the DECT over-air procedure is not found to be sufficiently secure, it will always be possible to use other DECT procedures, including manual key setting and use of DAM (if supported by handset and service provider!).

The CT2 absence of network authentication and of ciphering (especially) constitutes, however, major drawbacks for CT2 as compared to DECT based CTM. From a security point of view, CT2 can never attain the same level of confidence, neither for users nor for service providers.

The CT2 air interface standard is therefore, for security reasons, not recommended as a basis for CTM.

Annex B (informative): Threats with minor risk and countermeasures

This informative annex identifies the security services described in clause 8 that cover the threats with minor risk (level 1, 2 or 3).

We can conclude from the following table that most of these threats are covered by the security requirements and services. The two main remaining threats are:

- Misuse of emergency calls:

  As described in subclause 9.5, this threat is not unique to CTM and should be addressed by authentication and management actions.

- Manipulation of signalling data:

  As described in subclause 9.5, this threat can be addressed by means of protocol integrity checks. Table B.1 identifies where such a countermeasure may be employed.

Table B.1: Threats with potential risk less than 4 covered by the selection of countermeasures

Threat number and Risk	Threat description	Security requirements and services
7.3.0.1 b) **2**	Eavesdropping of CTM-id on IN interfaces or entities: On most of the IN interfaces and IN entities used in the differing procedures, it may be possible to eavesdrop a valid CTM-id. This could lead to other persons knowing the location of the CTM user, or to a masquerading threat (see later on threats related to masquerading). Resulting threat: eavesdropping of personal information.	E3, E4
7.3.0.2 b) **2**	Eavesdropping of CTM-id on the air interface: This could lead to other persons knowing the location of the CTM user, or to a masquerading threat (see later on threats related to masquerading). Resulting threat: eavesdropping of personal information.	E2
7.3.0.3 b) **2**	Getting the CTM-id from a terminal This could lead to other persons knowing the location of the CTM user, or to a masquerading threat (see later on threats related to masquerading). Resulting threat: eavesdropping of personal information.	A7, C3
7.3.0.5 a) **3**	Unauthorized access to data: An attacker may wish to get some information stored in the databases (SDF). Resulting threat: denial of service.	C2
7.3.0.7 b) **2**	Stolen terminals: A stolen terminal can be used at least until the real user reports the theft of his terminal if the access to the terminal is not protected by a PIN. The terminal can also be used in order to decipher previously recorded communications from and to the user. Resulting threat: deciphering of previously recorded communications.	A7, P3, P4

Threat number and Risk	Threat description	Security requirements and services
7.3.0.9 b) **2**	Unauthorized access to data in terminals: An attacker may get some data from a terminal(e. g. CTM-id and authentication data) and use them later on. Resulting threats: deciphering of previously recorded communications.	C3
7.3.0.10 a) **3**	Masquerading as a network entity to an other one. An attacker may try to masquerade as a network entity towards a network entity in order either to get information, pervert a service, deny a service or re-route some calls. Resulting threat: masquerading.	A6
7.3.0.10 b) **2**	Same as 7.3.0.10 a) Resulting threat: unauthorized access.	A6
7.3.0.10 c) **2**	Same as 7.3.0.10 a) Resulting threat: eavesdropping.	A6
7.3.0.10 d) **3**	Same as 7.3.0.10 a) Resulting threat: denial of service.	A6
7.3.1.1.1 b) **2**	Eavesdropping of CTM-id and KS on SDF_{MM} - SCF_{MM} interface or on one of these entities itself. It is assumed that the attacker is able to perform the relevant DECT algorithms. Resulting threat: Masquerading of a user for incoming CTM calls, possibly resulting in receipt of information determined for that user.	E3, C2 OR Change of authentication data for each authentication
7.3.1.1.1 c) **1**	Same as 7.3.1.1.1 b) Resulting threat: Masquerading as network to the user even if network authentication is required, e.g. in order to perform a subscription de-registration procedure leading to a denial of service to that user.	E3, C2 OR Change of authentication data for each authentication
7.3.1.1.1 d) **2**	Same as 7.3.1.1.1 b) Resulting threat: Deriving DCK and eavesdropping the regular subscriber's communication on the air interface by deciphering.	E3, C2 OR Change of authentication data for each authentication
7.3.1.1.2 a) **2**	Eavesdropping of CTM-id and DCK on SDF_{MM} - SCF_{MM} interface or on one of these entities itself. It is assumed that the attacker is able to perform the DECT Cipher algorithm. Resulting threat: Eavesdropping the regular subscriber's communication on the air interface by deciphering. The attacker must be able to perform the DECT Cipher algorithm in order to decipher. Eavesdropping of the over-the-air communication is possible only for the communication following this authentication procedure, and for further communications as long as the DCK is not changed. In case of access to the SDF_{MM}, several DCKs belonging to a CTM-id may be read and subsequently be used for several eavesdropping attacks of communication over the air interface.	E3, C2, supported by Change of authentication data for each authentication

Threat number and Risk	Threat description	Security requirements and services
7.3.1.2.2 a) **2**	Eavesdropping of CTM-id and DCK on SCF_{MM} - SDF_{MM} interface or on one of these entities itself. Resulting threat: Eavesdropping of the regular subscriber's communication on the air interface. The attacker must be able to perform the DECT Cipher algorithm in order to decipher. Eavesdropping of the over-the-air communication is possible only for the communication following this authentication procedure, and for further communications as long as the DCK is not changed. In case of access to the SDF_{MM}, several DCKs belonging to a CTM-id may be read and subsequently be used for several eavesdropping attacks of communication over the air interface.	E3, C2, supported by Change of authentication data for each authentication
7.3.1.3.1 b) **1**	Eavesdropping of CTM-id and KS, or eavesdropping of CTM-id and RES, respectively on SCF_{MM} - SDF_{MM} interface, on SCF_{MM} - SCF_{SL} interface, or on SCF_{SL} - SDF_{SL} interface or on one of these entities itself. Resulting threat: In case that session keys are used and the KS is eavesdropped, masquerading as network to the user is possible even if network authentication is required, e.g. in order to perform a subscription de-registration procedure leading to a denial of service to that user.	E3, C2, A6, supported by Change of authentication data for each authentication
7.3.1.3.2 a) **2**	Eavesdropping of CTM-id and DCK on SCF_{MM} - SDF_{MM} interface, on SCF_{MM} - SCF_{SL} interface, on SCF_{SL} - SDF_{SL} interface, or on one of these entities itself. Resulting threat: Eavesdropping of the regular subscriber's communication on the air interface. This threat is relevant only if the method to transmit triples is used, it is not relevant if the method to transmit session key is used. Depending on the validity time of the DCK, the subsequent eavesdropping of communication on the air interface can be performed once only or several times. The attacker has to be able to perform the DECT Cipher algorithm in order to decipher.	E3, C2, supported by Change of authentication data for each authentication
7.3.1.3.3 b) **1-2**	Masquerading as SCF_{MM} in order to get authentication data (CTM-id, and session keys or triples) from the SDF_{SL} on request. Resulting threat: Masquerading of the network if session keys are used, e.g. in order to perform a subscription de-registration procedure leading to a denial of service to that user.	A6
7.3.1.4.1 a) **2**	Eavesdropping of CTM-id and related DCK on SCF_{MM} - SDF_{MM} interface or on SCF_{MM} - CUSF interface or on CUSF - SCUAF interface or on one of these entities itself. Resulting threat: Eavesdropping of the regular subscriber's communication on the air interface by deciphering.	E3, E4, C2, supported by C3, C4, C5
7.3.1.4.2 a) **2**	Deletion of Ciphering Request message on the SCF_{MM} - CUSF interface or on the SCUAF - CUSF interface and (if necessary) modification of the Ciphering Reply and/or Report Ciphering Reply message on the same interfaces. Resulting threat: Eavesdropping of the regular subscriber's communication on the air interface. This communication is then not ciphered and hence the attacker needs neither know the algorithm nor the relevant key.	C2, C4, C5, I1

Threat number and Risk	Threat description	Security requirements and services
7.3.1.4.3 a) **2**	Deletion of Ciphering Request message on the air interface, and (if necessary) modification of the according Reply message. Resulting threat: Eavesdropping of the regular subscriber's communication on the air interface. This communication is then not ciphered and hence the attacker needs neither know the algorithm nor the relevant key.	Protocol Integrity
7.3.1.4.4 a) **1**	Encryption failure If encryption fails for whatever reason (on purpose or by system failure), the connection may proceed without protection from eavesdropping - according to the CTM service descriptions (EN 301 175 and EN 301 273). Resulting threat: Eavesdropping of the regular subscriber's communication on the air interface. This communication is then not ciphered and hence the attacker needs neither know the algorithm nor the relevant key.	Protocol Integrity, P5, P9
7.3.3.1 **1**	Eavesdropping of old address. Knowledge of where a PT was.	E2, E3, E4, C2
7.3.3.2 **1**	Masquerading network entities to delete data In this procedure, a deletion can be done in the following entities: SDF_{MM}, CUSF and SCUAF. This can be done by manipulating these entities or by sending them cancellation request. In the case of a deletion in CUSF or SCUAF, outgoing calls can be performed as a new location registration is done, incoming calls can also be performed as the PT address is in the SDF_{MM}. In the case of a deletion in SDF_{MM}, outgoing calls can be performed as a new location registration is done, however, to perform incoming calls the PT address is to be known by the SDF_{MM}, to do this the location registration suggest procedure is necessary. Resulting threat: Incoming calls to a PT may not happen (in case of deletion in SDF_{MM}) before location registration suggest procedure is performed.	A6
7.3.4.1 b) **2**	Eavesdropping of data in an over-the-air registration process and subsequent exhaustive search for AC: Assuming that the attacker knows the DECT algorithms and has attained RAND_F, RS, RES and CTM-id from eavesdropping a subscription process over-the-air, he could find the corresponding AC by exhaustive search and thereby also the UAK. The effort to search for the AC depends on the length of the AC, which is set to a maximum of 8 entered decimal digits in the GAP and the CAP. The attacker could e.g. produce a table with all possible ACs and look for a matching of his calculated RES with the eavesdropped RES. If the random numbers RAND_F and RS are not changed for each subscription registration, the attacker could reuse his table for the data of other subscribers. Resulting threat: Masquerade as the network towards the real subscriber to eavesdrop his communications	Secure over-the-air subscription registration, Change of random numbers for the subscription registration process, AC of maximum length
7.3.4.1.c) **2**	Same as 7.3.4.1 b) Resulting threats: Eavesdropping of the user's communications later on	Secure over-the-air subscription registration, Change of random numbers for the subscription registration process, AC of maximum length

Threat number and Risk	Threat description	Security requirements and services
7.3.4.2 b) **2**	Copying an AC directly from the real subscriber or from the distribution process to him/her, eavesdropping of data in the over-the-air registration process and subsequent calculation of the UAK A valid AC can be obtained by an attacker during the distribution (e.g. by phone or mail) of the AC to a real subscriber or by copying it without the knowledge of the real subscriber/user. The attacker can now wait for and eavesdrop on the real user's over-the-air subscription registration and get the RAND_F, RS and CTM-id then. He can then calculate the UAK (knowledge of the DECT algorithms are needed) and enter it together with the CTM-id or simulate an over-the-air registration process to his equipment to load these values. Resulting threat: Masquerade as the network towards the real subscriber to eavesdrop his communications	Secure over-the-air subscription registration, Secure distribution process of key data
7.3.4.2.c) **2**	Same as 7.3.4.2 b) Resulting threat: Eavesdropping of the user's communications later on	Secure over-the-air subscription registration, Secure distribution process of key data
7.3.4.3. a) **2**	Copying an AC directly from the real subscriber or from the distribution process to him/her, masquerade as the network towards him in an over-the-air registration process and subsequently masquerade as network to him ("stolen subscriber"). An AC can be obtained by an attacker during the distribution (e.g. by phone or mail) of the AC to a real subscriber or by copying it without the knowledge of the real subscriber. The attacker can now masquerade as the network towards the subscriber in an over-the-air subscription registration, using his own RAND_F, RS and CTM-id. He can then calculate the UAK (knowledge of or access to the DECT algorithms are needed) and subsequently masquerade as the network against the subscriber/user. The subscriber now believes (for a while) that he is subscribing to and using the real service provider's network, while technically he can only have services in the faked network. The fraud should be discovered by the subscriber at time of first billing. Resulting threat: Masquerade as network towards the subscriber, which may allow redirecting of calls	Secure over-the-air subscription registration, Secure distribution process of key data
7.3.4.3 b) **2**	Same as 7.3.4.3 a) Resulting threat: Masquerade as network towards the subscriber to eavesdrop his communications	Secure over-the-air subscription registration, Secure distribution process of key data
7.3.4.3.c) **1**	Same as 7.3.4.3 a) Resulting threat: Masquerade as network towards the subscriber in order to bill him for calls he makes (in the faked network)	Secure over-the-air subscription registration, Secure distribution process of key data

Threat number and Risk	Threat description	Security requirements and services
7.3.4.4 a) **1-2**	Masquerading of a user during the over-the-air subscription registration procedure after obtaining the AC illicitly directly from the service provider or from the distribution process to a real subscriber (stealing of identity). A valid AC can be obtained by an attacker, maybe with assistance of an insider, from the service provider's premises or network (e.g. on the SMP-SCP interface or by unauthorized accesses to network entities or data bases). Alternatively a valid AC can be stolen during the distribution (e.g. by mail) to a real subscriber. The AC can then be inserted in the CTM equipment and used in an over-the-air registration process, instead of the real user doing it. However, the real user may detect the attack quite early since he cannot perform the subscription registration procedure himself (as in threat no. 2). Resulting threat: Masquerade as the regular subscriber (for a while)	Secure over-the-air subscription registration, Secure distribution process of key data
7.3.4.5.a) **1**	Masquerading of a user during the over-the-air subscription registration procedure by guessing an AC successfully (stealing of identity). This threat is relevant if the ACs are very short. However, the real user may detect the attack quite early since he cannot perform the subscription registration procedure himself. Resulting threat: Masquerade as the regular subscriber (for a while).	AC of maximum length
7.3.5.1 **1**	Illegal de-registration by an attacker masquerading as service provider: The de-registration process over-the-air requires network authentication. Hence only in situations where the attacker has knowledge of the user's UAK, is this possible. Resulting threat: Illegal de-registration leads to denial of service for the user.	A2, A6, E2, E3, E4, C2
7.3.5.2 **1**	Subscriber does not allow de-registration by manipulating his terminal: If the PT is manipulated not to accept the network authentication which should accompany a withdrawal of the PT's access rights, the user can inhibit the de-registration from taking effect in his terminal. Alternatively he can let the PT send back a reject answer to the network's request, which indicates to the network that the re-register procedure has failed. Resulting threat: The attacker may be able to perform outgoing calls in a visited network, as long as authentication to the home network is not required.	C3
7.3.6.2 a) **2**	Masquerading by using someone's CTM-id and authentication information: Even if authentication and/or ciphering is required for incoming calls, a masquerading attack is possible by knowing the CTM-id and the authentication information which can be known by one of the methods described earlier. Resulting threat: Incoming long distance calls will be (partly) billed to the regular subscriber in case of charging split. If the attacker gives the CTM number of that CTM subscriber to his friends, they can avoid high phone bills at the cost of the threatened subscriber.	P1, P4, P5
7.3.6.2 b) **2**	Same as 7.3.6.2 a) Resulting threat: The attacker can receive incoming calls intended for the regular subscriber. This is relevant especially for data services.	Change of authentication data for each authentication
7.3.6.2 c) **3**	Same as 7.3.6.2 a) Resulting threat: Duplication of CTM-id within inter-network. Both the attacker and the legitimate subscriber may attempt to register at the same time. The network cannot distinguish between a good and bad variant of the same CTM-id.	Change of authentication data for each authentication

Threat number and Risk	Threat description	Security requirements and services
7.3.6.3 **2**	Eavesdropping of the communication on the air interface by use of the DCK: The attacker may have got the DCK by one of the methods described earlier. He needs also be able to perform the DECT cipher algorithm (e.g. using a manipulated portable equipment). Hence, he can decipher the intercepted communication.	Change of authentication data for each authentication
7.3.6.4 **2**	Eavesdropping of the communication on the air interface by deletion of Ciphering Request message on the SCF_{MM} - CUSF interface or on the SCUAF - CUSF interface and (if necessary) modification of the Ciphering Reply and/or Report Ciphering Reply message on the same interfaces, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm nor to know the relevant key (see 7.3.1.4.2).	Protocol Integrity
7.3.6.5 **2**	Eavesdropping of the communication on the air interface by deletion of Ciphering Request message on the air interface and (if necessary) modification of the according Reply message, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm nor to know the relevant key (see 7.3.1.4.3).	Protocol Integrity
7.3.6.7 **2**	Eavesdropping of the start of a communication on the air interface: This may be possible since call set up may have been successfully performed before the authentication has been completed and the ciphering has started. Hence, some secret data may be eavesdropped.	Ciphering active already at call set-up)
7.3.6.8 **1**	Eavesdropping of roaming number or routing number (e.g. at CCF_o), or of FT address. This may occur at the LE entities of either the calling or called party. Resulting threat: This may lead to the knowledge of a CTM user's location.	C2, E3, E4
7.3.6.9 **2**	Modification of routing data in order to re-route the communication to another address (which the attacker has access to). Resulting threat: The attacker may receive (possibly secret) information intended for the regular subscriber. This threat is relevant especially for data services.	I1
7.3.6.10 **2**	Deletion of Release message in case of authentication failure at the SCF_{MM} - SSF_t/CCF_t interface or at one of these entities. Resulting threat: Since the result of authentication is not forwarded to the relevant CCF, the requested call would be proceeded, i.e. a masquerading threat can be performed.	Protocol Integrity
7.3.7.2 **3**	Masquerading by using someone's CTM-id and authentication information: Even if authentication and/or ciphering is required for outgoing calls, a masquerading attack is possible by knowing the CTM-id and the authentication information which can be known by one of the methods described earlier. Resulting threats: Outgoing calls will be billed to the regular subscriber.	Change of authentication data for each authentication, P1
7.3.7.3 **2**	Eavesdropping of the communication on the air interface by use of the DCK: The attacker may have got the DCK by one of the methods described earlier. He needs also be able to perform the DECT cipher algorithm (e.g. using a manipulated portable equipment). Hence, he can decipher intercepted communication.	Change of authentication data for each authentication
7.3.7.4 **2**	Eavesdropping of the communication on the air interface by deletion of Ciphering Request message on the SCF_{MM} - CUSF interface or on the SCUAF - CUSF interface and (if necessary) modification of the Ciphering Reply and/or Report Ciphering Reply message on the same interfaces, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm (see 7.3.1.4.2).	Protocol Integrity

Threat number and Risk	Threat description	Security requirements and services
7.3.7.5 **2**	Eavesdropping of the communication on the air interface by deletion of Ciphering Request message on the air interface and (if necessary) modification of the according Reply message, in order to subsequently eavesdrop the (hence not ciphered) communication of the concerned user on the air interface. For this threat, the attacker need not be able to perform any DECT algorithm nor to know the relevant key (see 7.3.1.4.3).	Protocol Integrity
7.3.7.7 **2**	Eavesdropping of the start of a communication on the air interface: This may be possible since call set up may have been successfully performed before the authentication has been completed and the ciphering has started. Especially the called phone number and - in case of specific services requiring e.g. a PIN - secret data may be eavesdropped.	Ciphering active already at call set-up
7.3.7.8 **2**	Eavesdropping of the phone number of the called party: This may be possible since call set-up may start prior to authentication result and start of ciphering. Resulting threat: This may lead to the knowledge of a communication partner's identity.	Ciphering active already at call set-up, E2, E3, E4, C2
7.3.7.9 **2**	Modification of the dialled number in order to direct the communication to another address (which the attacker has access to). Resulting threat: The attacker may receive (possibly secret) information intended for the CTM subscriber's communication partner. This threat is relevant especially for data services. Here it is not CTM specific.	I1
7.3.7.10 **2**	Deletion of Release message in case of authentication failure at the SCF_{MM} - SSF/CCF interface or at one of these entities. Resulting threat: Since the result of authentication is not forwarded to the relevant CCF, the requested call would be proceeded, i.e. a masquerading threat can be performed.	Protocol Integrity
7.3.8.1 **2-3**	Misuse of emergency call. An attacker can send some emergency calls e.g. to the police, without any reasons, e.g. to give false indications. In the case where giving the CTM-id without authentication is sufficient, he can masquerade as somebody else (if he knows his CTM-id). Then the emergency call seems to come from somebody else. In CTM phase 2, it is not even necessary to have a CTM subscription. Hence, an attacker can just send some false indications when performing an emergency call, without giving any CTM-id. In that case, the misuse of emergency calls is even easier to perform. NOTE: Emergency calls should be delivered with data identifying the location of the calling party. Resulting threat: Masquerading and giving some false indication during emergency calls.	
7.3.8.2 **3**	Manipulate data to give an emergency number to somebody. An attacker can give to a friend an emergency number by manipulating data in the emergency data base. In that case, this new number will be free of charge. Resulting threat: Masquerading as an emergency entity, so that calls to this number are free of charge.	C1, C2, C4, C5
7.3.9.1 a) **1**	Eavesdropping of transmitted information during Service Profile Transfer. Resulting threat: Personal data is divulged to unauthorized persons.	E2, E3, E4, C2

Threat number and Risk	Threat description	Security requirements and services
7.3.9.2 a) **2**	Manipulation of transmitted information during Service Profile Transfer. Resulting threat: The service is increased without authorization.	I1
7.3.9.3 a) **1**	Unauthorized access to the service profile of somebody by unauthorized use of Service Profile Interrogation. Resulting threat: Personal data is divulged to unauthorized persons.	A3, A4, A5
7.3.10.3 a) **1-2**	An unauthorized user may interrogate the status of the call forwarding service for someone else. Resulting threat: Information of someone's call forwarding number is divulged.	C1, C2, C4, C5
7.3.12.1 a) **2**	The DCK may be eavesdropped at some IN interface while transmitted from home network to visited network. Resulting threat: Eavesdropping of a user's communication.	E3, C2 OR Authentication performed in the visited network
7.3.12.2 a) **2**	If authentication is performed in the home network, the result may be modified at some IN interface during transmission (especially the notification "authentication failed" may be changed to "authentication successful"). Resulting threat: Masquerading as chosen user will succeed without valid authentication.	I1
7.3.12.4 a) **1**	Home network refuses to pay visited network, claiming (falsely) that the visited network has stated too much traffic for the roaming users. Home network could claim that visited network has not performed authentication as agreed and also claim that the visited network operator has manipulated call data records (as in the previous threat). Resulting threat: Visited network gets too little compensation for the roaming visitors.	P7

Bibliography

The following material, though not specifically referenced in the body of the present document (or not publicly available), gives supporting information.

ETR 083 (1993): "Universal Personal Telecommunication (UPT); General UPT security architecture".

ETS 300 391-1 (1995): "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: Specification".

ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

History

Document history				
V1.1.1	November 1998	Membership Approval Procedure	MV 9902:	1998-11-10 to 1999-01-08
V1.1.1	January 1999	Publication		

ISBN 2-7437-2833-7
Dépôt légal : Janvier 1999