SLOVENSKI STANDARD
SIST ETS 300 929 E2:2003

01-december-2003

Digitalni celiļ ni telekomunikacijski sistem (faza 2+) ï Omreģne funkcije v zvezi z varnostjo (GSM 03.20, razliļ ica 5.1.1)

Digital cellular telecommunications system (Phase 2+) (GSM); Security related network functions (GSM 03.20 version 5.1.1)

Ta slovenski standard je istoveten z: ETS 300 929 Edition 2

ICS:

33.070.50	Globalni sistem za mobilno telekomunikacijo (GSM)	Global System for Mobile Communication (GSM)

SIST ETS 300 929 E2:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 929

August 1997

Second Edition

Source: ETSI SMG

Reference: RE/SMG-030320QR

ICS: 33.020

Key words: Digital cellular telecommunications system, Global System for Mobile communications (GSM)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 version 5.1.1)

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Foreword

This European Telecommunication Standard (ETS) has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).

This ETS defines the security related network functions within the digital cellular telecommunications system.

The specification from which this ETS has been derived was originally based on CEPT documentation, hence the presentation of this ETS may not be entirely in accordance with the ETSI rules.

Transposition dates	
Date of adoption:	25 July 1997
Date of latest announcement of this ETS (doa):	30 November 1997
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 May 1998
Date of withdrawal of any conflicting National Standard (dow):	31 May 1998

Blank page

0 Scope

This European Telecommunication Standard (ETS) specifies the network functions needed to provide the security related service and functions specified in GSM 02.09.

This ETS does not address the cryptological algorithms that are needed to provide different security related features. This topic is addressed in annex C. Wherever a cryptological algorithm or mechanism is needed, this is signalled with a reference to annex C. The references refers only to functionalities, and some algorithms may be identical or use common hardware.

0.1 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

[1] GSM 01.04 (ETR 350): "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Station (MS) features".

[3] GSM 02.09 (ETS 300 920): "Digital cellular telecommunications system; Security aspects".

[4] GSM 02.17 (ETS 300 922): "Digital cellular telecommunications system; Subscriber Identity Modules (SIM) Functional characteristics".

[5] GSM 03.03 (ETS 300 927): "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".

[6] GSM 04.08 (ETS 300 940): "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[7] GSM 05.01: "Digital cellular telecommunication system (Phase 2+); Physical layer on the radio path; General description".

[8] GSM 05.02 (ETS 300 908): "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path".

[9] GSM 05.03 (ETS 300 909): "Digital cellular telecommunications system (Phase 2+); Channel coding".

[10] GSM 09.02 (ETS 300 974): "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification".

0.2 Abbreviations

Abbreviations used in this ETS are listed in GSM 01.04.

Specific abbreviations used in annex A are listed in clause A.3.

1 General

The different security related services and functions that are listed in GSM 02.09 are grouped as follows:

- Subscriber identity confidentiality;

- Subscriber identity authentication;

- Signalling information element and connectionless user data confidentiality and data confidentiality for physical connections (ciphering).

It shall be possible to introduce new authentication and ciphering algorithms during the systems lifetime. The fixed network may support more than one authentication and ciphering algorithm.

The security procedures include mechanisms to enable recovery in event of signalling failures. These recovery procedures are designed to minimize the risk of a breach in the security of the system.

General on figures in this ETS:

- In the figures below, signalling exchanges are referred to by functional names. The exact messages and message types are specified in GSM 04.08 and GSM 09.02.

- No assumptions are made for function splitting between MSC (Mobile Switching Centre), VLR (Visitor Location Register) and BSS (Base Station System). Signalling is described directly between MS and the local network (i.e. BSS, MSC and VLR denoted in the figures by BSS/MSC/VLR). The splitting in annex A is given only for illustrative purposes.

- Addressing fields are not given; all information relates to the signalling layer. The TMSI allows addressing schemes without IMSI, but the actual implementation is specified in the GSM 04-series.

- The term HPLMN in the figures below is used as a general term which should be understood as HLR (Home Location Register) or AuC (Authentication Centre).

- What is put in a box is not part of the described procedure but it is relevant to the understanding of the figure.

2 Subscriber identity confidentiality

2.1 Generality

The purpose of this function is to avoid the possibility for an intruder to identify which subscriber is using a given resource on the radio path (e.g. TCH (Traffic Channel) or signalling resources) by listening to the signalling exchanges on the radio path. This allows both a high level of confidentiality for user data and signalling and protection against the tracing of a user's location.

The provision of this function implies that the IMSI (International Mobile Subscriber Identity), or any information allowing a listener to derive the IMSI easily, should not normally be transmitted in clear text in any signalling message on the radio path.

Consequently, to obtain the required level of protection, it is necessary that:

- a protected identifying method is normally used instead of the IMSI on the radio path; and
- the IMSI is not normally used as addressing means on the radio path (see GSM 02.09);
- when the signalling procedures permit it, signalling information elements that convey information about the mobile subscriber identity must be ciphered for transmission on the radio path.

The identifying method is specified in the following subclause. The ciphering of communication over the radio path is specified in clause 4.

2.2 Identifying method

The means used to identify a mobile subscriber on the radio path consists of a TMSI (Temporary Mobile Subscriber Identity). This TMSI is a local number, having a meaning only in a given location area; the TMSI must be accompanied by the LAI (Location Area Identification) to avoid ambiguities. The maximum length and guidance for defining the format of a TMSI are specified in GSM 03.03.

The network (e.g. a VLR) manages suitable data bases to keep the relation between TMSIs and IMSIs. When a TMSI is received with an LAI that does not correspond to the current VLR, the IMSI of the MS must be requested from the VLR in charge of the indicated location area if its address is known; otherwise the IMSI is requested from the MS.

A new TMSI must be allocated at least in each location updating procedure. The allocation of a new TMSI corresponds implicitly for the MS to the de-allocation of the previous one. In the fixed part of the network, the cancellation of the record for an MS in a VLR implies the de-allocation of the corresponding TMSI.

To cope with some malfunctioning, e.g. arising from a software failure, the fixed part of the network can require the identification of the MS in clear. This procedure is a breach in the provision of the service, and should be used only when necessary.

When a new TMSI is allocated to an MS, it is transmitted to the MS in a ciphered mode. This ciphered mode is the same as defined in clause 4.

The MS must store its current TMSI in a non volatile memory, together with the LAI, so that these data are not lost when the MS is switched off.

2.3 Procedures

This subclause presents the procedures, or elements of procedures, pertaining to the management of TMSIs.

2.3.1 Location updating in the same MSC area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on the same MSC. The part of this procedure relative to TMSI management is reduced to a TMSI re-allocation (from TMSIo with "o" for "old" to TMSIn with "n" for "new").

The MS sends TMSIo as an identifying field at the beginning of the location updating procedure.

The procedure is schematized in figure 2.1.

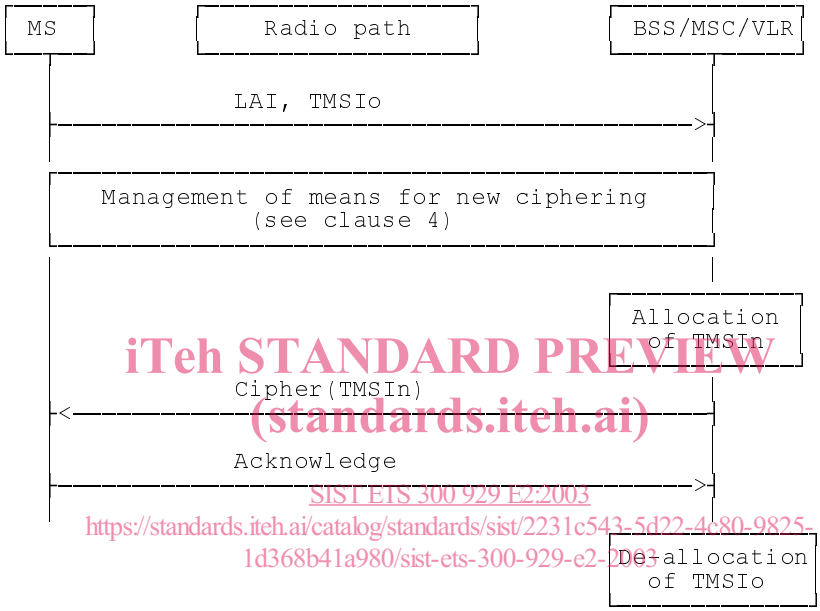


Figure 2.1: Location updating in the same MSC area

Signalling Functionalities:

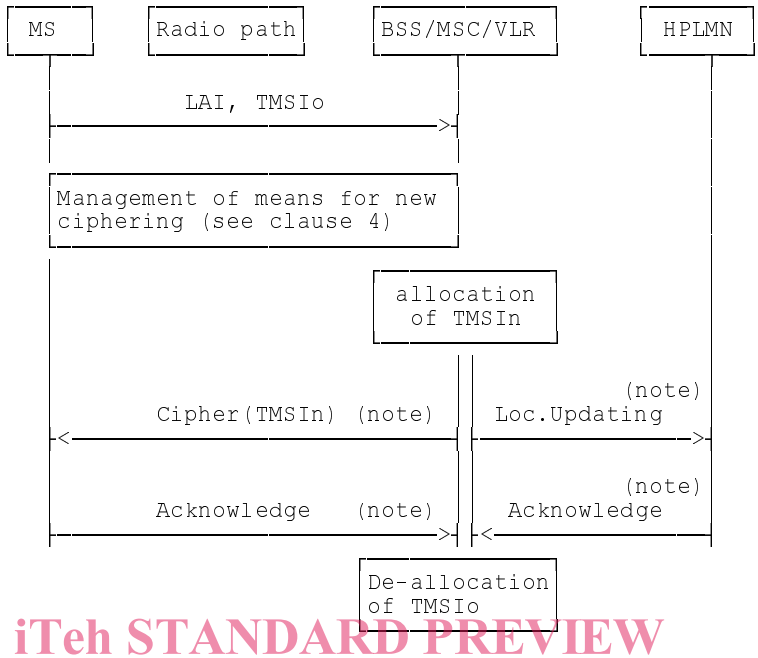
Management of means for new ciphering:

The MS and BSS/MSC/VLR agree on means for ciphering signalling information elements, in particular to transmit TMSIn.

2.3.2 Location updating in a new MSCs area, within the same VLR area

This procedure is part of the location updating procedure which takes place when the original location area and the new location area depend on different MSCs, but on the same VLR.

The procedure is schematized on figure 2.2.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.2: Location updating in a new MSCs area, within the same VLR area

Signalling functionalities:

Loc.Updating:

stands for Location Updating

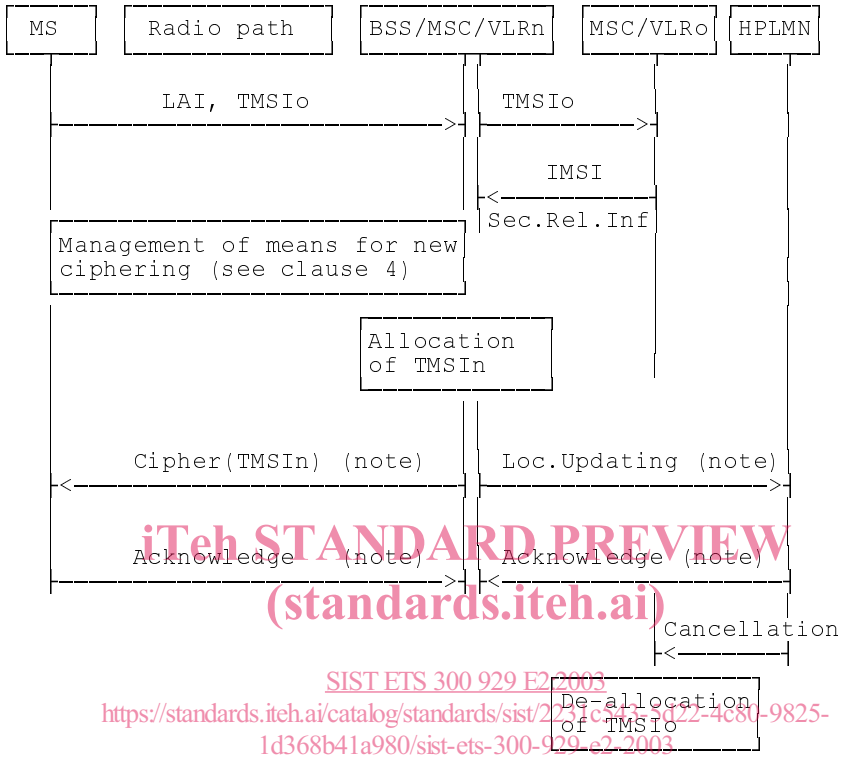
The BSS/MSC/VLR indicates that the location of the MS must be updated.

2.3.3 Location updating in a new VLR; old VLR reachable

This procedure is part of the normal location updating procedure, using TMSI and LAI, when the original location area and the new location area depend on different VLRs.

The MS is still registered in VLRo ("o" for old or original) and requests registration in VLRn ("n" for new). LAI and TMSIo are sent by MS as identifying fields during the location updating procedure.

The procedure is schematized in figure 2.3.



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.3: Location updating in a new VLR; old VLR reachable

Signalling functionalities:

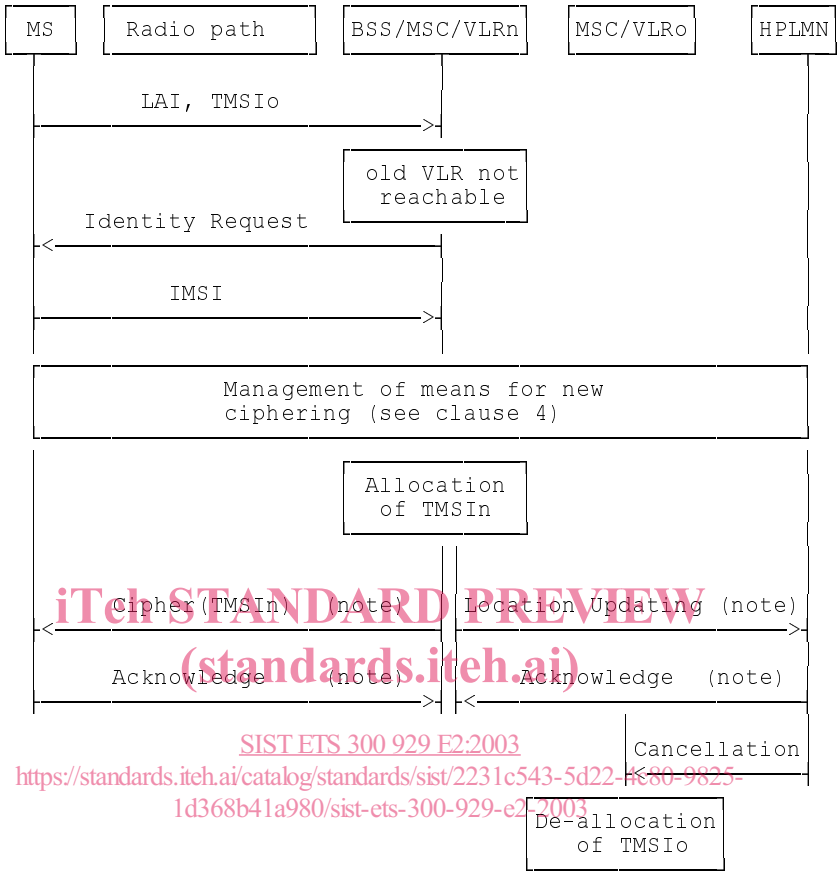
Sec.Rel.Info.:
Stands for Security Related information
The MSC/VLRn needs some information for authentication and ciphering; this information is obtained from MSC/VLRo.

Cancellation:
The HLR indicates to VLRo that the MS is now under control of another VLR. The "old" TMSI is free for allocation.

2.3.4 Location Updating in a new VLR; old VLR not reachable

This variant of the procedure in subclause 2.3.3 arises when the VLR receiving the LAI and TMSIo cannot identify the VLRo. In that case the relation between TMSIo and IMSI is lost, and the identification of the MS in clear is necessary.

The procedure is schematized in figure 2.4



NOTE: From a security point of view, the order of the procedures is irrelevant.

Figure 2.4: Location Updating in a new VLR; old VLR not reachable