



# SLOVENSKI STANDARD SIST ETS 300 929 E3:2003

01-december-2003

---

8 [[ [HJb]`W`] b]`H`Y`\_ca i b]\_UW`g\_]`g]ghYa `fZ`hU`&Z`L`E`Ca fYybY`Z b\_W`Y`j `nj Yn]`n  
j Ufbcghc`f GA `\$` "&\$žfUn] ]WU) "&`%L

Digital cellular telecommunications system (Phase 2+) (GSM); Security related network functions (GSM 03.20 version 5.2.1)

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

Ta slovenski standard je istoveten z: **ETS 300 929 Edition 3**  
SIST ETS 300 929 E3:2003  
<https://standards.iteh.ai/catalog/standards/sist/55d92b45-1543-4611-8038-bcc26350411e/sist-ets-300-929-e3-2003>

---

**ICS:**

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

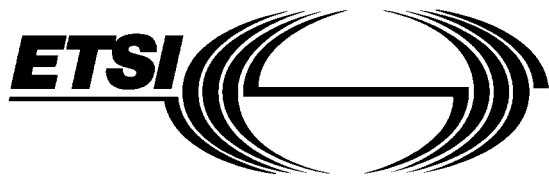
**SIST ETS 300 929 E3:2003**

**en**

## **iTeh STANDARD PREVIEW** **(standards.iteh.ai)**

SIST ETS 300 929 E3:2003

<https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003>



# EUROPEAN TELECOMMUNICATION STANDARD

**ETS 300 929**

July 1998

Third Edition

Source: SMG

Reference: RE/SMG-030320QR1

ICS: 33.020

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



## Digital cellular telecommunications system (Phase 2+); Security related network functions (GSM 03.20 version 5.2.1)

**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

**Internet:** secretariat@etsi.fr - <http://www.etsi.fr> - <http://www.etsi.org>

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

**Copyright Notification:** No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1998. All rights reserved.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ETS 300 929 E3:2003](https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003)

<https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003>

## Contents

Foreword .....	7
Introduction .....	7
0 Scope .....	9
0.1 Normative references .....	9
0.2 Abbreviations .....	9
1 General .....	10
2 Subscriber identity confidentiality .....	11
2.1 Generality .....	11
2.2 Identifying method .....	11
2.3 Procedures .....	12
2.3.1 Location updating in the same MSC area .....	12
2.3.2 Location updating in a new MSCs area, within the same VLR area .....	13
2.3.3 Location updating in a new VLR; old VLR reachable .....	14
2.3.4 Location Updating in a new VLR; old VLR not reachable .....	15
2.3.5 Reallocation of a new TMSI .....	16
2.3.6 Local TMSI unknown .....	17
2.3.7 Location updating in a new VLR in case of a loss of information .....	18
2.3.8 Unsuccessful TMSI allocation .....	18
2.3.9 Combined location area updating with the routing area updating \$(GPRS)\$ .....	19
3 Subscriber identity authentication .....	21
3.1 Generality .....	21
3.2 The authentication procedure .....	21
3.3 Subscriber Authentication Key management .....	22
3.3.1 General authentication procedure .....	22
3.3.2 Authentication at location updating in a new VLR, using TMSI .....	23
3.3.3 Authentication at location updating in a new VLR, using IMSI .....	24
3.3.4 Authentication at location updating in a new VLR, using TMSI, TMSI unknown in "old" VLR .....	25
3.3.5 Authentication at location updating in a new VLR, using TMSI, old VLR not reachable .....	25
3.3.6 Authentication with IMSI if authentication with TMSI fails .....	26
3.3.7 Re-use of security related information in failure situations .....	26
4 Confidentiality of signalling information elements, connectionless data and user information elements on physical connections .....	27
4.1 Generality .....	27
4.2 The ciphering method .....	27
4.3 Key setting .....	28
4.4 Ciphering key sequence number .....	29
4.5 Starting of the ciphering and deciphering processes .....	29
4.6 Synchronization .....	29
4.7 Handover .....	30
4.8 Negotiation of A5 algorithm .....	30
5 Synthetic summary .....	31
Annex A (informative): Security issues related to signalling schemes and key management .....	32
A.1 Introduction .....	32

A.2	Short description of the schemes .....	32
A.3	List of abbreviations .....	33
Annex B (informative): Security information to be stored in the entities of the GSM system .....		47
B.1	Introduction .....	47
B.2	Entities and security information .....	47
B.2.1	Home Location Register (HLR) .....	47
B.2.2	Visitor Location Register (VLR) .....	47
B.2.3	Mobile services Switching Centre (MSC)/Base Station System (BSS) .....	47
B.2.4	Mobile Station (MS) .....	48
B.2.5	Authentication Centre (AuC) .....	48
Annex C (normative): External specifications of security related algorithms .....		49
C.0	Scope .....	49
C.1	Specifications for Algorithm A5 .....	49
C.1.1	Purpose .....	49
C.1.2	Implementation indications .....	49
C.1.3	External specifications of Algorithm A5 .....	51
C.1.4	Internal specification of Algorithm A5 .....	51
C.2	Algorithm A3 .....	51
C.2.1	Purpose .....	51
C.2.2	Implementation and operational requirements .....	51
C.3	Algorithm A8 .....	52
C.3.1	Purpose .....	52
C.3.2	Implementation and operational requirements .....	52
Annex D (normative): Security related network functions for General Packet Radio Service \$(GPRS)\$ .....		53
D.1	General .....	53
D.2	Subscriber identity confidentiality .....	53
D.2.1	Generality .....	53
D.2.2	Identifying method .....	54
D.2.3	Procedures .....	54
D.2.3.1	Routing area updating in the same SGSN area .....	54
D.2.3.2	Routing area updating in a new SGSN; old SGSN reachable .....	55
D.2.3.3	Routing area updating in a new SGSN; old SGSN not reachable .....	56
D.2.3.4	Reallocation of a TLLI .....	57
D.2.3.5	Local TLLI unknown .....	58
D.2.3.6	Routing area updating in a new SGSN in case of a loss of information .....	59
D.2.3.7	Unsuccessful TLLI allocation .....	59
D.3	Subscriber identity authentication .....	60
D.3.1	Generality .....	60
D.3.2	The authentication procedure .....	60
D.3.3	Subscriber Authentication Key management .....	60
D.3.3.1	General authentication procedure .....	60
D.3.3.2	Authentication at routing area updating in a new SGSN, using TLLI .....	61
D.3.3.3	Authentication at routing area updating in a new SGSN, using IMSI .....	62
D.3.3.4	Authentication at routing area updating in a new SGSN, using TLLI, TLLI unknown in 'old' SGSN .....	63
D.3.3.5	Authentication at routing area updating in a new SGSN, using TLLI, old SGSN not reachable .....	64
D.3.3.6	Authentication with IMSI if authentication with TLLI fails .....	64
D.3.3.7	Re-use of security related information in failure situations .....	64

D.4	Confidentiality of user information and signalling between MS and SGSN.....	65
D.4.1	Generality.....	65
D.4.2	The ciphering method.....	65
D.4.3	Key setting .....	65
D.4.4	Ciphering key sequence number .....	66
D.4.5	Starting of the ciphering and deciphering processes.....	66
D.4.6	Synchronisation .....	67
D.4.7	Inter SGSN routing area update .....	67
D.4.8	Negotiation of GPRS-A5 algorithm .....	67
D.5	Synthetic summary.....	68
D.6	Security of the GPRS backbone.....	69
Annex E (informative):	Status of Technical Specification GSM 03.20 .....	70
History.....		71

## iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST ETS 300 929 E3:2003

<https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003>

Blank page

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ETS 300 929 E3:2003](https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003)

<https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003>



## 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 of this ETS:	3 July 1998
Date of latest announcement of this ETS (doa):	31 October 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	30 April 1999
Date of withdrawal of any conflicting National Standard (dow):	30 April 1999

## Introduction

The present document includes references to features which are not part of the Phase 2+ Release 96 of the GSM Technical specifications. All subclauses which were changed as a result of these features contain a marker (see table below) relevant to the particular feature. GSM 10.01 defines the correspondence between these features and GSM yearly releases.

The following table lists all features that were introduced after Release 96.

Feature	Designator
General Packet Radio Service	\$(GPRS)\$

Blank page

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ETS 300 929 E3:2003](https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003)

<https://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003>

## 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 02.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 1".
- [6] GSM 03.03 (ETS 300 927): "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".
- [7] GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".
- [8] GSM 04.08 (ETS 300 940): "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".
- [9] GSM 04.64: "Digital cellular telecommunications system (Phase 2+), General Packet Radio Service (GPRS); Logical Link Control (LLC)".
- [10] GSM 05.01: "Digital cellular telecommunication system (Phase 2+); Physical layer on the radio path; General description".
- [11] GSM 05.02 (ETS 300 908): "Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path".
- [12] GSM 05.03 (ETS 300 909): "Digital cellular telecommunications system (Phase 2+); Channel coding".
- [13] 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

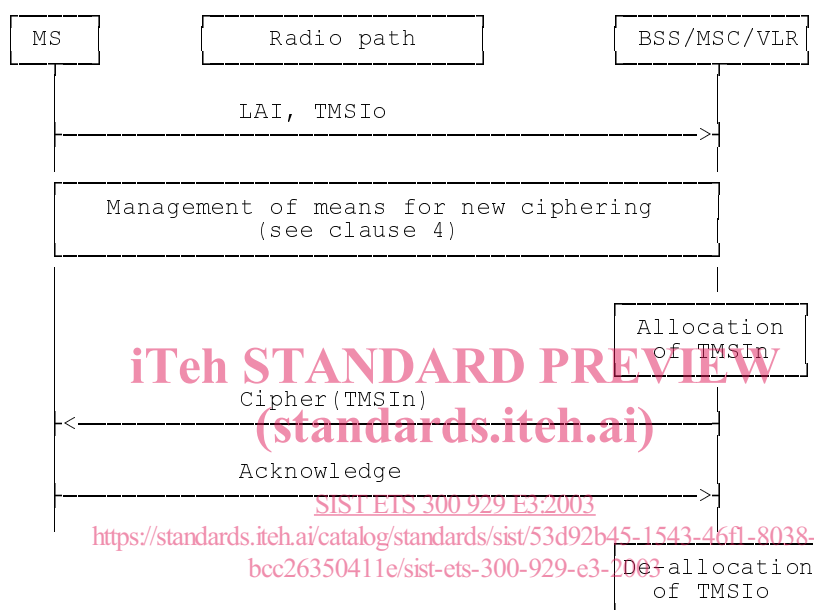
This subclause presents the procedures, or elements of procedures, pertaining to the management of TMSIs.

### 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:

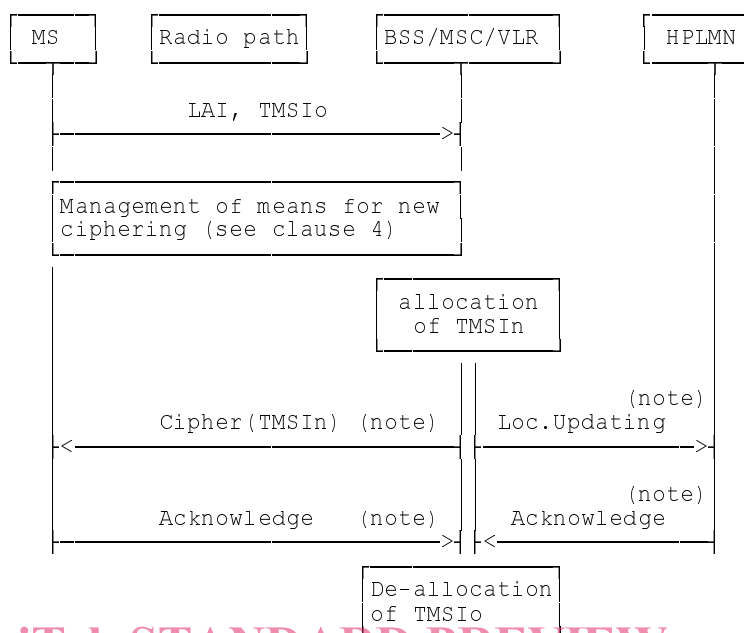
Management of means for new ciphering:

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**

[SIST ETS 300 929 E3:2003](http://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003)

Signalling functionalities: <http://standards.iteh.ai/catalog/standards/sist/53d92b45-1543-46f1-8038-bcc26350411e/sist-ets-300-929-e3-2003>

Loc.Updating:

stands for Location Updating

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