



SLOVENSKI STANDARD
SIST ETS 300 614 E1:2003

01-december-2003

8 [[]HJb]`WV] b]`hY`_ca i b]_UW`g_]`g]ghYa `fZuU&L`%E`I dfUj `Ub`Y`j Ufbcgh]`f] GA
%&`\$' Ł

Digital cellular telecommunications system (Phase 2) (GSM); Security management
(GSM 12.03)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Ta slovenski standard je istoveten z: **ETS 300 614 Edition 1**
SIST ETS 300 614 E1:2003
<https://standards.iteh.ai/catalog/standards/sist/ab7edeb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003>

ICS:

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

SIST ETS 300 614 E1:2003

en

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST ETS 300 614 E1:2003

<https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003>



EUROPEAN
TELECOMMUNICATION
STANDARD

ETS 300 614

August 1996

Source: ETSI TC-SMG

Reference: DE/SMG-061203P

ICS: 33.060.50

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

GSM

**GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS**
(standards.iteh.ai)

**Digital cellular telecommunications system (Phase 2);
Security management
(GSM 12.03)**

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 92 94 42 00 - Fax: +33 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 1996. All rights reserved.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ETS 300 614 E1:2003](https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003>

Contents

Foreword	7
Introduction	7
1 Scope	9
2 Normative references	9
3 Abbreviations	11
4 Management of security features	12
4.1 Subscriber Identity (IMSI) confidentiality management	12
4.2 Subscriber Identity (IMSI) authentication management	12
4.3 Data confidentiality over the air interface	12
4.3.1 Encryption and algorithm management	12
4.3.2 Key management	13
4.4 Management of Mobile Equipment security	13
5 Security management mechanisms	14
5.1 System control mechanisms	14
5.2 Information gathering mechanisms	14
5.2.1 Use of scanners	14
5.2.2 Audit trail mechanisms	14
5.3 Alarm reporting mechanisms	15
6 Security procedures	16
6.1 Subscriber Identity confidentiality management procedures (TMSI)	16
6.1.1 Timer for Periodic Location Update	16
6.1.2 Selector when TMSI reallocation shall be done	16
6.2 Subscriber Identity authentication management procedures	17
6.2.1 Selector when authentication shall be performed	17
6.2.2 Open Identification of MS (authentication retried)	17
6.2.3 Parameters for generation and use of authentication vector	18
6.3 Encryption and algorithm management procedures	18
6.3.1 Encryption Management Procedures	18
6.3.2 Algorithm management procedures	19
6.4 IMEI management procedures	19
6.4.1 Selector when IMEI check shall be performed	19
6.5 Use of counters for security purposes	19
6.5.1 Open transfer of IMSI	19
6.5.2 IMEI related counters	19
6.5.3 Authentication failure	20
6.5.4 Additional security counters	20
6.5.5 Security-related scan reporting	20
6.6 Security reporting	21
6.6.1 Security alarm reports	21
6.6.1.1 Authentication failure in VLR	21
6.6.1.2 IMEI check violation in VLR	21
6.6.1.3 IMEI request failure in VLR	22
6.6.1.4 IMSI request failure in VLR	22
6.6.1.5 Unknown subscriber in HLR (VLR)	22
6.6.1.6 Unknown subscriber in HLR	22
6.6.1.7 Unknown subscriber in AuC(HLR)	22
6.6.1.8 IMSI confidentiality failure In MSC	22
6.6.2 Security audit trail reports	22

7	Security management object model	23
7.1	Security object classes	24
7.1.1	vlr1203AuthenticationFunction	24
7.1.2	vlr1203SubscriberIdFunction	24
7.1.3	vlr1203EquipmentIdFunction	24
7.1.4	msc1203EncryptionFunction	25
7.1.5	msc1203IMSIConfidentialityFunction	25
7.1.6	hlr1203SubscriberIdFunction	25
7.1.7	bts1203EncryptionFunction	25
7.2	Security attributes definitions	26
7.2.1	authenticationNecessaryWhen	26
7.2.2	authenticationRetriedAllowed	26
7.2.3	numberOfAuthenticationVectorsKept	26
7.2.4	authenticationVectorReuseAllowed	26
7.2.5	allocateNewTMSIWhen	26
7.2.6	checkIMEIWhen	26
7.2.7	encryptionControl	26
7.2.8	algorithmListMSC	27
7.2.9	algorithmListBTS	27
7.2.10	threshold	27
7.2.11	vlr1203AuthenticationFunctionId	27
7.2.12	vlr1203SubscriberIdFunctionId	27
7.2.13	vlr1203EquipmentIdFunctionId	27
7.2.14	msc1203EncryptionFunctionId	27
7.2.15	msc1203IMSIConfidentialityFunctionId	28
7.2.16	hlr1203SubscriberIdFunctionId	28
7.2.17	bts1203EncryptionFunctionId	28
7.3	Notifications	29
7.4	Name bindings	29
7.4.1	vlr1203AuthenticationFunction	29
7.4.2	vlr1203SubscriberIdFunction	29
7.4.3	vlr1203EquipmentIdFunction	29
7.4.4	msc1203EncryptionFunction	29
7.4.5	msc1203IMSIConfidentialityFunction	29
7.4.6	hlr1203SubscriberIdFunction	30
7.4.7	bts1203EncryptionFunction	30
7.5	Parameters	31
7.5.1	authenticationFailureInVLRParameter	31
7.5.2	imsiRequestFailureInVLRParameter	31
7.5.3	imsiRequestFailureInVLRParameter	31
7.5.4	imeiCheckViolationInVLRParameter	31
7.5.5	imeiRequestFailureInVLRParameter	31
7.5.6	imsiConfidentialityFailureInMSCParameter	31
7.5.7	imsiConfidentialityFailureInHLRParameter	31
7.6	Abstract syntax definitions	32
7.7	Application contexts	37
Annex A (normative):	Relation between the authentication and encryption attributes	38
Annex B (normative):	Additional security counters	41
B.1	MSC security measurement function	41
B.1.1	Encrypted connection used	41
B.1.2	Unencrypted connection used	41
B.1.3	Connection to be Cleared Due to Incompatible Encryption	42
B.2	VLR Security Function	42
B.2.1	Authentication Vectors Unavailable	42
B.2.2	Subscriber unknown in HLR(VLR)	42
B.3	HLR Security Function	43
B.3.1	Subscriber Unknown in HLR	43
B.3.2	Subscriber Unknown in AuC(HLR)	43

Annex C (normative):	Security measurement Object Model	44
C.1	Model structure and content.....	44
C.2	Security measurement managed object classes	45
C.2.1	mscSecurityMeasurementFunction	45
C.2.2	vlrSecurityMeasurementFunction	45
C.2.3	hlrSecurityMeasurementFunction	45
C.3	Security measurement package definitions	46
C.3.1	General Security Measurement Function Packages	46
C.3.1.1	basicSecurityMeasurementFunctionPackage	46
C.3.2	MSC Security Measurement Function Packages	46
C.3.2.1	encryptedConnectionPackage	46
C.3.2.2	incompatibleEncryptionPackage	46
C.3.3	VLR Security Measurement Function Packages	46
C.3.3.1	authenticationVectorsUnavailablePackage	46
C.3.3.2	unknownSubscriberInHlrFromVlrPackage	46
C.3.4	HLR Security Measurement Function Packages	47
C.3.4.1	unknownSubscriberInHlrPackage	47
C.3.4.2	unknownSubscriberInAucPackage	47
C.4	Security measurement attribute definitions	48
C.4.1	General Security Measurement Function Related Attributes.....	48
C.4.1.1	securityMeasurementFunctionId	48
C.4.2	MSC Security Measurement Function Related Attributes.....	48
C.4.2.1	encryptedConnectionUsed	48
C.4.2.2	unencryptedConnectionUsed	48
C.4.2.3	callClearedIncompatibleEncryption	48
C.4.3	VLR Security Measurement Function Related Attributes.....	48
C.4.3.1	authVectorsUnavailable	48
C.4.3.2	subsUnknownInHlrFromVlr	48
C.4.4	HLR Security Measurement Function Related Attributes	49
C.4.4.1	subsUnknownInHlr	49
C.4.4.2	subsUnknownInAuc	49
C.5	Security measurement name bindings	50
C.5.1	MSC Name Binding	50
C.5.1.1	mscSecurityMeasurementFunction-"gsm1200:1993":mscFunction.....	50
C.5.2	VLR Name Binding	50
C.5.2.1	vlrSecurityMeasurementFunction-"gsm1200:1993":vlrFunction.....	50
C.5.3	HLR Name Binding	50
C.5.3.1	hlrSecurityMeasurementFunction-"gsm1200:1993":hlrFunction	50
C.6	Security measurement behaviour definitions	51
C.6.1	general security measurement function behaviour	51
C.6.2	general security measurement package behaviour	51
C.6.3	general security measurement attribute behaviour.....	51
C.7	Security measurement abstract syntax definitions.....	52
Annex D (informative):	Index.....	53
History.....		55

Blank page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST ETS 300 614 E1:2003](https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003>

Foreword

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

This ETS describes the management of the security related aspects in the GSM/DCS PLMN within the Digital cellular telecommunications system. This ETS corresponds to GSM technical specification, GSM 12.03, version 4.2.1.

NOTE: TC-SMG has produced documents which give technical specifications for the implementation of the Digital cellular telecommunications system. Historically, these documents have been identified as GSM Technical Specifications (GSM-TSs). These specifications may subsequently become I-ETTs (Phase 1), or European Telecommunication Standards (ETTs)(Phase 2), whilst others may become ETSI Technical Reports (ETRs). These ETSI-GSM Technical Specifications are, for editorial reasons, still referred to in this ETS.

Transposition dates	
Date of adoption of this ETS:	31 August 1996
Date of latest announcement of this ETS (doa):	30 November 1996
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 May 1997
Date of withdrawal of any conflicting National Standard (dow):	31 May 1997

(standards.iteh.ai)

Introduction

The radio communications aspect of the GSM system makes it particularly sensitive to unauthorized use. For this reason, security mechanisms are defined for the GSM system:

- Subscriber identity (IMSI) confidentiality.
- Subscriber identity (IMSI) authentication.
- Data confidentiality over the air interface.
- Mobile equipment security.

The use of these security features, is at the discretion of operators for non-roaming subscribers. For roaming subscribers however, the use of these security features is mandatory, unless otherwise agreed by all the affected PLMN operators (GSM 02.09 [1]).

A number of security parameters have been defined in the core specifications to support these security features. The IMSI is used to uniquely identify subscribers and the TMSI to provide subscriber identity confidentiality. The authentication vectors (Kc,RAND,SRES) are used in the authentication process and the ciphering key (Kc) is used to encrypt signaling and user data over the air interface. Finally the IMEI can be used to establish whether a piece of mobile equipment is suitable to be used on the network, i.e., approved and neither stolen nor faulty.

Formal definitions of these security mechanisms and their technical realization can be found in recommendations GSM 02.09 [2] and GSM 03.20 [3] respectively. The relevant messaging and procedures can be found in recommendations GSM 04.08 [4], GSM 08.08 [22], GSM 08.58 [23], and GSM 09.02 [5].

It is the objective of this ETS to provide a standard mechanism for the management of the aforementioned security features and parameters.

Blank page

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST ETS 300 614 E1:2003](https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003)

<https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003>

1 Scope

This European Telecommunication Standard (ETS) describes the management of the security related aspects in the GSM/DCS PLMN. The management of the relevant security services is addressed with respect to the following aspects:

- Overview of the security features;
- Description of the relevant management procedures;
- Modeling using the object oriented paradigm.

The definitions and descriptions of the security features and mechanisms are contained in the specifications of the underlying procedures and are not defined in this ETS. References to appropriate GSM/DCS specifications have been made throughout the ETS, where necessary. Issues relating to the security of management (e.g. file transfer security, database security, inter-operator security, etc.) are not covered in this ETS.

2 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 02.09 (ETS 300 506): "Digital cellular telecommunication system (Phase 2); Security aspects".
- [2] GSM 03.03 (ETS 300 523): "Digital cellular telecommunication system (Phase 2); Numbering, addressing and identification".
- [3] GSM 03.20 (ETS 300 534): "Digital cellular telecommunication system (Phase 2); Security related network functions".
- [4] GSM 04.08 (ETS 300 557): "Digital cellular telecommunication system (Phase 2); Mobile radio interface layer 3 specification".
- [5] GSM 09.02 (ETS 300 599): "Digital cellular telecommunication system (Phase 2); Mobile Application Part (MAP) specification".
- [6] GSM 12.00 (ETS 300 612-1): "Digital cellular telecommunication system (Phase 2); Objectives and structure of Network Management (NM)".
- [7] GSM 12.02 (ETS 300 613): "Digital cellular telecommunication system (Phase 2); Subscriber, Mobile Equipment (ME) and services data administration".
- [8] CCITT M.3010: "Principles for a Telecommunication Management Network"
- [9] GSM 02.16 (ETS 300 508): "Digital cellular telecommunication system (Phase 2); International Mobile station Equipment Identities (IMEI)".
- [10] GSM 12.04 (ETS 300 615): "Digital cellular telecommunication system (Phase 2); Performance data measurements".
- [11] CCITT Recommendation X.720 (1992) (ISO/IEC 10165-1 (1992)): "Information technology - Open Systems Interconnection - Structure of management information : Management information model".
- [12] CCITT Recommendation X.721 (1992) (ISO/IEC 10165-2 (1992)): "Information technology - Open Systems Interconnection - Structure of Management Information : Definition of Management Information".

- [13] CCITT Recommendation X.722 (1992) (ISO/IEC10165-2 (1992)): "Information technology - Open Systems Interconnection - Structure of Management Information: Guidelines for the Definition of Managed Objects".
- [14] CCITT Recommendation X.731 (1992) (ISO/IEC10164-2 (1992)): "Information technology - Open Systems Interconnection - Systems Management :Part 2: State management function".
- [15] CCITT Recommendation X.733 (1992) (ISO/IEC10164-4 (1992)): "Information technology - Open Systems Interconnection - Systems Management :Part 2: Alarm Reporting Function".
- [16] CCITT Recommendation X.734 (1993) (ISO/IEC10164-5 (1993)): "Information technology - Open Systems Interconnection - Systems Management :Event Report Management Function".
- [17] CCITT Recommendation X.735 (1992) (ISO/IEC10164-6 (1992)): Information technology - Open Systems Interconnection - Systems Management: Log Control Function".
- [18] CCITT Recommendation X.736 (1992) (ISO/IEC10164-7 (1992)): "Information technology - Open Systems Interconnection - Systems Management :Part 2: Security Alarm Reporting Function".
- [19] CCITT Recommendation X.740 (1992) (ISO/IEC10164-8 (1992)): "Information technology - Open Systems Interconnection - Systems Management :Security Audit Trail Function".
- [20] GSM 12.20 (ETS 300 622): "Digital cellular telecommunication system (Phase 2); Base Station System (BSS) Management Information".
- [21] GSM 12.08 (ETS 300 627): "Digital cellular telecommunication system (Phase 2); "Subscriber and Equipment Trace".
<https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-1e003825903a-3>
- [22] GSM 08.08 (ETS 300 590): "Digital cellular telecommunication system (Phase 2); Mobile Switching Centre - Base Station System (MSC - BSS) interface Layer 3 specification".
- [23] GSM 08.58 (ETS 300 596): "Digital cellular telecommunication system (Phase 2); Base Station Controller - Base Transceiver Station (BSC - BTS) interface Layer 3 specification".
- [24] CCITT M.3100: "Generic Network Information Model"
- [25] GSM 12.30 (ETR 128): "ETSI object identifier tree; Common domain Mobile domain; O&M managed Object registration definition"

3 Abbreviations

For the purposes of this ETS the following abbreviations apply.

A3	Authentication Algorithm
A5	Ciphering Algorithm
A8	Ciphering Key Computation Algorithm
AuC	Authentication Centre
BCCH	Broadcast Control Channel
BSC	Base Station Controller
BSS	Base Station Sub-system
BTS	Base Transceiver Station
CKSN	Ciphering Key Sequence Number
CM	Call Management
EIR	Equipment Identity Register
GDMO	Guidelines for the Definition of Managed Objects
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
Kc	Ciphering Key
Ki	Individual Subscriber Authentication Key
LU	Location Update
MAP	Mobile Application Part
ME	Mobile Equipment
MM	Mobility Management
MO	Mobile Originating, Managed Object
MOC	Managed Object Class
MS	Mobile Station
MSC	Mobile Switching Centre
MT	Mobile Terminating
NE	Network Element
OS	Operations System
PLMN	Public Land Mobile Network
RAND	Random Number
Rec.	Recommendation
SIM	Subscriber Identity Module
SMS	Short message service
SRES	Signed Response to RAND
SS	Supplementary Service
TMN	Telecommunications Management Network
TMSI	Temporary Mobile Subscriber Identity
TS	Technical Specification
VLR	Visitor Location Register

ITeH STANDARD PREVIEW
(standards.iteh.ai)

<https://standards.iteh.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-910000000000/sist-ets-300-614-e1-2003>

4 Management of security features

Clause 4 identifies the manageable aspects of the security features in the previous clause. The security management mechanisms which can be used are listed in clause 5. Clause 6 defines the procedures introduced in clause 4, and clause 7 provides the object model for the management these parameters.

4.1 Subscriber Identity (IMSI) confidentiality management

Subscriber confidentiality in the GSM PLMN is provided by the use of the Temporary Mobile Subscriber Identity (TMSI) on the air interface. Avoiding the use of the International Mobile Subscriber Identity (IMSI) over the air interface by substituting the TMSI, provides both a high level of confidentiality for user data and signaling, and protection against the tracing of a user's location. This mechanism is described in GSM 03.20 [3] and the structure of the TMSI is described in GSM 03.03 [2].

As the frequency of reallocation of the TMSI has an effect on the subscriber confidentiality, a parameter is defined to provide control over it.

If the (old) TMSI is unknown to the Visitor Location Register (VLR) or wrong, the mobile subscriber can only be identified by using the IMSI. As encryption is not possible during that stage, the IMSI has to be sent unencrypted over the air interface. The occurrence of such an event (or similar) affects the quality of the subscriber confidentiality service. Counters are defined to provide information about this service.

4.2 Subscriber Identity (IMSI) authentication management

The GSM PLMN offers a mechanism for the authentication of subscriber identity. The purpose of this feature, is to protect the network against unauthorized use. It also enables the protection of the GSM PLMN subscribers, by making it practically impossible for intruders to impersonate authorized users.

Subscriber authentication may be included in the Mobile Application Part (MAP) procedures for access request and location update. The use of authentication should be under the control of the operator and a parameter is defined for this purpose.

Authentication may be retried to recover from failure due to incorrect TMSI by requesting open transfer of the IMSI over the air interface. This should be under the control of the operator and a parameter to this effect is defined.

To support authentication, vectors are generated in the AuC. The VLR requests these authentication vectors for use in the authentication procedures. Under exceptional conditions, these vectors may need to be reused. This may have an effect on the security of the network, and should be under the control of the operator.

4.3 Data confidentiality over the air interface

4.3.1 Encryption and algorithm management

In a GSM PLMN, encryption may be used to protect the confidentiality of data and signaling on the air interface. Two algorithms are essentially involved in the encryption process; the ciphering algorithm (A5) and the cipher key generation algorithm (A8). In general, the authentication algorithm (A3) and the A8 algorithm, are implemented as one in the AuC and the SIM, and may be operator-specific. The A5 algorithm is implemented in the ME and at the BTS.

The negotiation (between the MS and the MSC) of up to seven versions of the ciphering algorithm (A5/1, A5/2...,A5/7), is catered for in signaling. The MSC will then identify which of these versions are allowed by the network for this call (perhaps based on the user identity) and will pass the list of acceptable versions to the BSS. The BSS must then select a version from this list. If any versions in this list are supported by the BTS, then encryption must be used. For the case where multiple choices are available, the order of preference for this BSS selection should be set by the operator. A BTS related attribute specifying a priority ordered list of version choices is defined in this ETS. If no version match is available, the MSC must decide whether or not to complete the call in unencrypted mode. An MSC related attribute to allow/prohibit unencrypted communications is defined in this ETS.

4.3.2 Key management

Two types of keys are defined in GSM; the authentication key (Ki) and the cipher key (Kc).

The Ki is unique to the subscriber. It is stored in the SIM during pre-personalization and in the authentication centre

The Kc is normally generated at the same time as the authentication parameters. The same random number (RAND) that is passed through the A3 algorithm with the Ki during authentication, is passed through a different algorithm, the A8, again with the Ki to generate the Kc. The key Kc may be stored and used by the mobile station, until it is updated at the next authentication. Attention is necessary to achieve key consistency during all these operations and after (re)synchronization of nodes. This consistency is provided for by the use of the Ciphering Key Sequence Number (CKSN) and authentication retry.

The administration of the (IMSI,Ki) pair is described in recommendation GSM12.02 [7]. The generation of the Kc is described in recommendation GSM 03.20 [3].

4.4 Management of Mobile Equipment security

For equipment security, the international mobile equipment identity (IMEI) has been defined. The IMEI is physically secure in the ME, as defined in GSM 02.09 [1].

Equipment identification is achieved by requesting the IMEI from the ME. To control this identification, a parameter is defined in subclause 6.4.1 of this ETS. It is used to select which MAP procedures shall include the request of the IMEI.

The Equipment Identity Register (EIR) is used to store IMEIs in the network. An IMEI is classified as white, gray or black.

The IMEI management functions related to the EIR are described in GSM 12.02 [7].

IMEI tracing can be used for the detection and elimination of security breaches. This process is also described in GSM 12.08 [21].

[SIST ETS 300 614 E1:2003
https://standards.itih.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003](https://standards.itih.ai/catalog/standards/sist/ab7edcb1-21e5-420c-9f90-73151007b582/sist-ets-300-614-e1-2003)