Draft EG 201 227 V1.2.1 (1997-10)

ETSI Guide

ETSI numbering system for telecommunication; ALgorithm IDentifiers (ALID)

European Telecommunications Standards Institute

Reference

REG/ICC-00013 (bd000ioq.PDF)

Keywords

ID

ETSI Secretariat

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

X.400

c= fr; a=atlas; p=etsi; s=secretariat

Internet

secretariat@etsi.fr
http://www.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 ETR 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.fr/ipr).

Pursuant to the ETSI Interim 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 ETR 314 (or the updates on http://www.etsi.fr/ipr) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Guide, formerly a Technical Report (TR) has been produced by ETSI Technical Committee Integrated Circuits Cards (ICC) and is now submitted for the Membership Approval Procedure.

NOTE: The present document has been prepared by the former ETSI TC TE/STC TE9.

1 Scope

The present document describes the numbering system for ALgorithm IDentifiers (ALID) for ETSI telecommunication Integrated Circuits (IC) card applications according to ETSI documents.

The numbering system described in the present document provides a means for an algorithm and related services offered by a provider to identify if a given card contains the algorithms required by its related services.

An ALID is used to address an algorithm in the card. It consists of a 7-bit IDentifier (ID) as described in EN 726-3 [1].

The present document describes the coding of the ALID as well as the registration procedure.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

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

[1] EN 726-3: "Identification card systems - Telecommunications integrated circuit(s) cards and terminals - Part 3: Application independent card requirements".

[2] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange".

[3] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following definitions apply (the first two from ISO/IEC 7816-5 [3]):

application: An application consists of a set of security mechanisms, files, data, protocols (excluding transmission protocols) which are located and used in the IC card and outside the IC card (external application).

Application Provider (AP): The entity which is responsible for the application after its allocation. One AP may have several applications in one card. The files allocated in the card, corresponding to one application, are called a card-application. There may exist several applications on a given card from the same AP.

ALgorithm IDentifier (ALID): A data element which identifies an algorithm in a card.

3.2 Abbreviations

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

ALID	ALgorithm IDentifier
AP	Application Provider
BARAS	Baseline Algorithm Recommended for Audio-Visual Services (former ETSI STC TE10)
BEANO	Block Encryption Algorithm for Network Operators
DECT	Digital Enhanced Cordless Telecommunications (ETSI Project)
DSAA	DECT Standard Authentication Algorithm (former ETSI STC RES03, now DECT Project)
DSC	DECT Standard Cipher (former ETSI STC RES03, now DECT Project)
GSM	Global System for Mobile communication
HIPERLAN	HIgh PERformance Local Area Network (former ETSI STC RES10)
IC	Integrated Circuit(s)
ICC	IC Card
ID	IDentifier
PTS	Pay Terminals and Systems (ETSI Project)
RES	Radio Equipment and Systems (former ETSI TC)
STC	Technical Sub-Committee (in ETSI)
TAA1	TETRA Authentication Algorithm No. 1 (former ETSI STC RES06, now TETRA Project)
TC	Technical Committee (in ETSI)
TE	Terminal Equipment (former ETSI TC)
TEA1	TETRA Encryption Algorithm No. 1 (former ETSI STC RES06, now TETRA Project)
TEA2	TETRA Encryption Algorithm No. 2 (former ETSI STC RES06, now TETRA Project)
TESA-7	IC card Authentication Algorithm (former ETSI STC TE09, now PTS Project)
TETRA	TErrestrial Trunked RAdio (ETSI Project)
UPT	Universal Personal Telecommunications (former ETSI STC NA06)
USA-4	UPT Authentication Algorithm (former ETSI STC NA06)

4 Structure of the ALgorithm IDentifier (ALID)

The length of the ALID is 1-byte coded as:

bit 8	bit 7 to bit 1

bit 8: in the relevant keyfile (EF_{KEY_MAN} or EF_{KEY_OP}) indicates if a key is valid for INTERNAL AUTHENTICATION, (bit 8 = 1) or not (bit 8 = 0).

NOTE: Therefore an algorithm can have two ALID (ID1 and ID2; see annex B) for different keys only different in bit 8 indicating if the specific key is valid for internal authentication.

bit 7 - bit 1: ALID (see EN 726-3 [1], subclause 7.6.5).

"00"-"5F" Range of ALID within the scope of the present document.

"60"-"7F" Reserved for propriety algorithms. The use of this ALID is out of scope of the present document.Propriety ALID can be allocated by Application Providers (AP) without notice but without any guarantee of unambiguity.

"6X" shall be used for keys not valid for internal authentication.

"7X" shall be used for keys valid for internal authentication.

A list of allocated ALID is given in annex B.

5 Use of the ALgorithm IDentifier (ALID)

The use of the ALID is specified in EN 726-3 [1].

6 Application and registration procedures

An Algorithm Provider (AP) wishing to get an ETSI ALID should send its request for such a number to the ETSI Secretariat by using the form in annex A, together with a non-refundable registration fee. Method of payment to be determined by the ETSI Secretariat.

Registration forms are also available, on request, from the ETSI Secretariat.

6.1 Criteria for approval and rejection of requests

6.1.1 Criteria for approval of a request for an ETSI ALID

Requests for an ETSI ALID should meet all the following criteria:

a) the applicant should be a provider of telecommunication IC card applications following the specifications laid down in ETSI documents;

b) the applicant has given a statement that the application conforms to the ETSI document referred to by the application code;

c) allocation is approved by the responsible ETSI technical body (TC ICC);

d) the ETSI ALID should be used within a year from time of registration (in accordance with ISO practice).

6.1.2 Criteria for rejection of a request for an ETSI ALID

A request for an ETSI ALID will be rejected if any of the following conditions exist:

a) the applicant is not an Application Provider (AP) as defined in subclause 3.1;

b) the applicant has requested a specific number or the reservation in the register of a specific number or has made a request which is outside the scope of the present document;

c) the use of the algorithm is a limited application which can be handled by a propriety ALID (decision of ETSI TC ICC needed).

6.2 Responsibilities of applicants

The responsibilities of applicants are:

a) to comply fully with the numbering system and the procedures for requesting ETSI ALID as contained in the present document;

b) to forward to the ETSI Secretariat a completed registration form (see annex A), together with a statement that the application conforms to the ETSI document referred to by the algorithm code and the requisite fee;

NOTE: The registration fee is not refundable.

c) to retain the completed registration form containing the ETSI ALID assigned to the applicant by the ETSI Secretariat;

d) to provide at least one application using the ETSI ALID assigned to the applicant by the ETSI Secretariat within a reasonable time frame;

e) to inform the ETSI Secretariat of any modification to the data related to the assigned ETSI ALID;

f) to take responsibility for the interoperability of all of the applicant's devices using the registered algorithm provider code within the algorithm described in the ETSI document related to the algorithm code chosen;

g) to register separately for each algorithm if more than one ETSI ALID is required.

6.3 Responsibilities of the ETSI Secretariat

The responsibilities of the ETSI Secretariat are:

a) to fully comply with the numbering system and procedures for requesting ETSI ALID in the present document;

b) to provide ETSI algorithm code on request to the ETSI technical body responsible for the ETSI document in question;

c) to maintain a register of allocated ETSI algorithm codes and associated ETSI documents;

d) to process requests for ETSI ALIDs within 30 days of receipt of a request;

e) to ensure that clause A.1 of the registration form has been filled in correctly;

f) where requests fulfil the criteria set down in subclause 6.1.1, to notify applicant, in writing, within 30 days of receipt of the request, as to the number assignment, returning the completed registration form containing the number assignment to the applicant informing it of the requirement to retain the completed registration form as a permanent record;

g) to reject requests for a specific number and for reservation of a specific number or any request outside the scope of the present document;

h) where a request is rejected, to advise the applicant, in writing, within 30 days of receipt of the request, that the request has been rejected, informing it of the reason(s) for the rejection;

j) to maintain the register of ETSI ALID (see subclause 6.4) including its recoverability;

k) to retain as a permanent record copies of all requests submitted to it, along with the disposition of each request;

m) to maintain the list of correspondence between the ETSI ALID and the document that specifies the standardized ETSI card algorithm (see subclause 6.5) including its recoverability;

n) to respond to general enquiries covering the present document;

p) to prevent unauthorized use of ETSI ALID and/or registered algorithm code and/or ETSI algorithm provider IDs if misuse is brought to the attention of the ETSI Secretariat.

6.4 The register of ETSI ALID

The ETSI Secretariat maintains a database of information taken directly from the registration form.

The register of ETSI ALID contains the following information:

a) name of organization;

b) information as indicated on the registration form;

c) ETSI ALID assigned to the algorithm provider by the ETSI Secretariat.

NOTE: A copy of each request received is maintained on file by the ETSI Secretariat.

Annex A:
Request registration form for an ETSI ALID

Request form to be filled in and addressed to:

ETSI Secretariat

Postal address:
06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00
Fax: +33 4 93 65 47 16
Internet: secretariat@etsi.fr

This request is submitted in accordance with EG 201 227, i.e. the present document.

A.1 To be completed by the requesting organization

Name of organization:	
Address of organization:	
Principal contact in organization:	
Telephone number:	Fax number:
Address for correspondence/billing:	
European VAT Id:	
Country, if not identical with country in address field:	
Number and title of the ETSI document to which the telecommunication IC card algorithm in question complies:	
ETSI card algorithm code to which the telecommunication IC card algorithm in question complies:	
Date:	Signature:

A.2 To be completed by the ETSI Secretariat

ETSI ALID:	
Date:	Signature:

Annex B: Allocated ALID

Table 6: ALgorithm IDentifiers (ALID) allocated to ETSI standard cryptographic algorithms

Name of algorithm	Application	Export licence required	Price (ECU)	ID 1 (note 1)	ID 2 (note 2)
BARAS	audio-visual services	yes	1 000		
BEANO (note 4)	network operators				
COMP 128				"40"	"50"
COMP NAT				"02"	"12"
DSAA	DECT	yes	1 000	"01"	"11"
DSC	DECT	yes	1 000		
HIPERLAN	Radio LAN	yes	1 000		
Proprietary algorithms				"6x"	"7x"
TEA1	TETRA	yes	1 000		
TEA2	TETRA	yes	1 000		
TAA1 (note 4)	TETRA				
TESA-7 (notes 3, 5)	IC cards	yes	1 000	"04"	"14"
USA-4	UPT	yes	1 000		

NOTE 1: ID1 is not valid for INTERNAL AUTHENTICATION.

NOTE 2: ID2 is valid for INTERNAL AUTHENTICATION.

NOTE 3: Algorithms used for encipherment, and available for general use, are not defined in EN 726-3 [1]. However, such algorithms might be incorporated for proprietary use.

NOTE 4: Awaiting authorization from French authorities not yet granted

NOTE 5: TESA-7 consists of four parts:

1) IC card functions
2) Security module functions
3) IC card test data
4) Security module test data

BARAS	Baseline Algorithm Recommended for Audio-Visual Services (former ETSI STC TE10)
BEANO	Block Encryption Algorithm for Network Operators
DECT	Digital Enhanced Cordless Telecommunications
DSAA	DECT Standard Authentication Algorithm (former ETSI STC RES03, now DECT Project)
DSC	DECT Standard Cipher (former ETSI STC RES03, now DECT Project)
HIPERLAN	HIgh PERformance Local Area Network (former ETSI STC RES10)
IC	Integrated Circuit(s)
ICC	IC Card
PTS	Pay Terminals and Systems (ETSI Project)
RES	Radio Equipment and Systems (former ETSI TC)
STC	Technical Sub-Committee (in ETSI)
TAA1	TETRA Authentication Algorithm No. 1 (former ETSI STC RES06, now TETRA Project)
TC	Technical Committee (in ETSI)
TE	Terminal Equipment (former ETSI TC)
TEA1	TETRA Encryption Algorithm No. 1 (former ETSI STC RES06, now TETRA Project)
TEA2	TETRA Encryption Algorithm No. 2 (former ETSI STC RES06, now TETRA Project)
TESA-7	IC card Authentication Algorithm (former ETSI STC TE09, now PTS Project)
TETRA	TErrestrial Trunked RAdio (ETSI Project)
UPT	Universal Personal Telecommunications (former ETSI STC NA06)
USA-4	UPT Authentication Algorithm (former ETSI STC NA06)

History

Document history		
V1.1.1	July 1997	Publication as TR 101 227
V1.2.1	October 1997	Membership Approval Procedure MV 9751: 1997-10-21 to 1997-12-19