ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 035

November 1995

Source: ETSI TC-SAGE

Reference: DTR/SAGE-00009

ICS: 33.020

Key words: Management rules, cryptographic algorithm

Security Algorithms Group of Experts (SAGE); Rules for the management of the BARAS algorithm

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

Contents

Blank page

Foreword

This Technical Committee Reference Technical Report (TCR-TR) has been prepared by the Security Algorithyms Group of Experts (SAGE) of the European Telecommunications Standards Institute. It was given the classification of TCR-TR by the 20th TC Chairmens' Co-ordination (TCC) meeting and postal approval (CL 1227) by the Technical Assembly (TA).

A TCR-TR is a deliverable for use inside ETSI which records output results of ETSI Technical Committee (TC) or Sub-Technical Committee (STC) studies which are not appropriate for European Telecommunication Standard (ETS), Interim European Telecommunication Standard (I-ETS) or ETSI Technical Report (ETR) status. They can be used for guidelines, status reports, co-ordination documents, etc. They are to be used to manage studies inside ETSI and shall be mandatorially applied amongst the concerned TCs. They shall also be utilised by the TC with overall responsibility for a study area for co-ordination documents (e.g. models, reference diagrams, principles, structures of standard, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

This TCR-TR and describes the rules for management for the BARAS cryptographic algorithm which was designed by SAGE for use in audiovisual systems as specified by ETSI STC/TE10 (see refernces [1] and [2]).

Blank page

1 Scope

The purpose of this TCR-TR is to specify the rules for the management of the BARAS cryptographic algorithm for use in the European standards for audiovisual systems as specified by ETSI STC/TE10 and contained in the ETSI standards [1] and [2].

2 References

[1] DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements.

[2] DE/*****: Integrated Services Digital Network (ISDN), Key Management procedures.

3 Abbreviations

BARAS	Baseline Algorithm Recommended for use in Audiovisual Systems
SAGE	Security Algorithms Group of Experts (ETSI)
TE	Terminal Equipment (ETSI)

4 Outline

The outline of this TCR-TR is as follows.

The management structure is defined in clause 5. This structure is defined in terms of the principals involved in the management of the BARAS (ETSI, ETSI TC/TE, BARAS Custodian and Approved Recipients) together with the relationships and interactions between them.

The procedures for delivering the BARAS to Approved Recipients are defined in clause 6. This clause is supplemented by Appendix 1 which specifies the items which are to be delivered.

Clause 7 is concerned with the criteria for approving an organisation for receipt of the BARAS and with the responsibilities of an Approved Recipient. This clause is supplemented by Appendix 2 which contains a Confidentiality and Restricted Usage Undertaking to be signed by each Approved Recipient.

Clause 8 is concerned with the responsibilities of the BARAS Custodian.

5 BARAS Management Structure

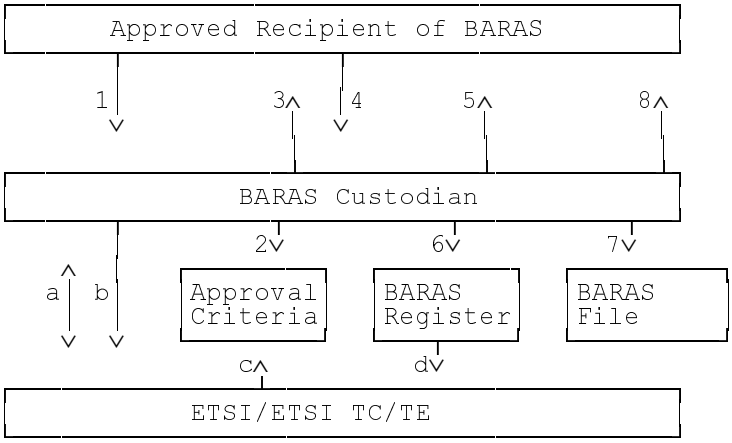
The management structure is depicted in figure 1. The figure shows the three principals involved in the management of the BARAS and the relationships and interactions between them.

ETSI is the owner of the BARAS and together with ETSI TC/TE sets the approval criteria for receipt of the algorithm (see clause 4).

The BARAS Custodian is the interface between ETSI and the Approved Recipients of the BARAS.

The activities of the BARAS Custodian are supported by an agreement between ETSI and the Custodian.

The BARAS Custodian's duties are detailed in clause 5. They include distributing the BARAS specification to Approved Recipients, as detailed in clause 3, providing limited technical advice to Approved Recipients and providing algorithm status reports to ETSI TC/TE.



Key to Figure :

a = Agreement between BARAS Custodian and ETSI

b = Status reports and recommendations

c = Setting of approval criteria

d = Restricted details of the BARAS register.

1 = Request for BARAS

2 = Check of request against approval criteria

3/4 = Exchange of Confidentiality and Restricted Usage Undertaking

5 = Dispatch of BARAS Specification

6 = Update the BARAS register

7 = Document filing

8 = Technical advice

Figure 1: BARAS Management Structure

6 Distribution Procedures

6.1 Distribution by BARAS Custodian

The BARAS specifications consist of the following documents:

Part 1 - BARAS Specification;
Part 2 - BARAS Test Data.

The following procedures for distributing the BARAS to Approved Recipients are defined with reference to Figure 1.

1 The BARAS Custodian receives a written request for N copies of the BARAS Specification (see Note 1), where N should not be bigger than six. The request should indicate that the algorithm is meant for use in the implementation of European standards for audio visual systems as specified by ETSI STC/TE10 and contained in the ETSI standard [1].

2 The BARAS Custodian confirms (or otherwise) whether the requesting organisation meets the approval criteria (see clause 4).

3 If the request is approved, the BARAS Custodian dispatches 2 copies of the Confidentiality and Restricted Usage Undertaking (as given in Appendix 2) for signature by the Approved Recipient (see Note 2 and 6) together with a copy of this document (Rules for the Management of the BARAS Algorithm).

4 Both copies of the Confidentiality and Restricted Usage Undertaking must be signed by the approved recipient (see Notes 5 and 7) and returned to the BARAS Custodian.

5 The BARAS Custodian sends up to N (Note 3) numbered copies of the BARAS Specification to the Approved Recipient, together with one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking and a covering letter (see Notes 4 and 6).

6 The BARAS Custodian updates the BARAS Register by recording the name and address of the recipient, the numbers of the copies of the BARAS Specification delivered and the date of delivery. If the original request is not approved, the BARAS Custodian records the name and address of the requesting organisation and the reason for rejecting the request in the BARAS Register.

7 The BARAS Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the BARAS File together with a copy of the covering letter sent to the Approved Recipient.

NOTE 1: Requests for the BARAS Specification should be made directly to the BARAS Custodian.

NOTE 2: The confidentiality and Restricted Usage Undertaking specifies the number of copies requested.

NOTE 3: The covering letter specifies the numbers of the copies delivered.

NOTE 4: The BARAS Custodian must send all items listed in Appendix 1. Requests for part of the package of items are rejected.

NOTE 5: Under normal circumstances the Custodian is expected to respond within 25 working days. This does not include delays in the process of applying for an export licence.

NOTE 6: The approved recipient must be a legal representative of the receiving organisation.

NOTE 7: If a BARAS Specification is returned to the BARAS Custodian (for example the recipient may decide not to make use of the information), then the BARAS Custodian shall destroy the specification and enter a note to this effect in the BARAS Register.

NOTE 8: The BARAS custodian may impose a reasonable charge to cover administrative costs involved in issuing the BARAS specification documents.

6.2 Transfers by a Beneficiary

An organisation which has already been approved and has obtained BARAS Specifications may transfer one or more of these specifications to a second organisation which requires the specification.

In this case, the first organisation must ensure that the second organisation meets the approval criteria.

The first organisation must get the second organisation to sign two copies of the Confidentiality and Restricted Usage Undertaking. The first organisation then sends these to the BARAS Custodian, together with the numbers of the specifications which are to be transferred.

The BARAS Custodian then enters the transfer details in the BARAS Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the first organisation , and files the other and a copy of the letter in the BARAS File.

The first organisation is responsible for passing (a copy of) the countersigned Confidentiality and Restricted Usage Undertaking to the second organisation.

7 Approval Criteria

The approval criteria are set by the ETSI together with ETSI TC/TE and maintained by the BARAS Custodian. The BARAS Custodian may recommend changes to these criteria.

In order for an organisation to be considered an Approved Recipient of the BARAS for use in the European standards for audio visual systems as specified by ETSI STC/TE10 it shall satisfy at least one of the following criteria:

C1 The organisation is designer of or competent to manufacture systems according to "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", where the BARAS is included in the systems.

C2 The organisation is designer of or competent to manufacture components for systems according to "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", where at least one of the components includes the BARAS.

C3 The organisation is designer of or competent to manufacture a system simulator for a system according to "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", where the simulator includes the BARAS.

The BARAS Custodian will decide whether an organisation requesting the BARAS Specification may be considered to be an Approved Recipient. Any doubtful cases will be referred back to ETSI/ETSI TC/TE, after taking the advice of the ETSI Deputy Director.

8 The BARAS Custodian

8.1 Responsibilities

The BARAS Custodian is expected to perform the following tasks:

T1 To approve requests for the BARAS by reference to the Approval Criteria given in clause 4.

T2 To exchange the Confidentiality and Restricted Usage Undertaking with Approved Recipients as described in clause 3.

T3 To distribute the BARAS Specification as detailed in clause 3 (see Note 1).

T4 To maintain the BARAS Register as described in clause 3.

T5 To hold in custody the contents of the BARAS File as specified in clause 3.

T6 To provide recipients of the BARAS with limited technical support, i.e, answer written queries arising from the specification or test data (see Note 2).

T7 To liaise with the ETSI Deputy Director over any problems of a legal nature concerning the issue of the Specifications or the Confidentiality and Restricted Usage Undertakings.

T8 To advise ETSI TC/TE of any problems arising with the approval criteria.

T9 In the light of written queries from recipients of the BARAS Specification, to make recommendations to ETSI TC/TE for improvements/corrections to the specification and, subject to ETSI TC/TE approval, make and distribute the changes (see Note 3).

T10 To provide ETSI TC/TE with information from the BARAS Register when requested to do so.

T11 To monitor published advances in cryptanalysis and advise the ETSI TC/TE of any advances which have a significant impact upon the continued suitability of the BARAS for the use in the context of "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements".

NOTE 1: Normal postage will be used (e.g., airmail for overseas recipients). If recipients require a different delivery service then they can be excepted to pay the full costs.

NOTE 2: The BARAS Custodian will only endeavour to answer questions relating to the BARAS Specification. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the BARAS Specification must be automatically distributed to all recipients of the specification and a record of the distribution entered in the BARAS Register.

8.2 Appointment

The BARAS Custodian will be appointed by ETSI.

Annex A: Items delivered to Approved Recipient of BARAS

ITEM-1: Up to N numbered copies to the BARAS Specification, for use in the European standards for audio visual systems as specified by ETSI STC/TE10 (as indicated in the request), where N is the number of copies requested.

ITEM-2: A countersigned Confidentiality and Restricted Usage Undertaking.

ITEM-3: A cover letter from and signed by the BARAS Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered (see Note 1).

NOTE 1: In the case of a transfer (see clause 3.2), only ITEM-2 and the cover letter are delivered. Moreover, the cover letter details the numbers of the transferred specifications.

Annex B: Confidentiality and restricted usage undertakings

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the BARAS cryptographic algorithm for use in the European standards for audio visual systems as specified by ETSI STC/TE10 and contained in the ETSI standard:

DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements.

Between

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the BENEFICIARY;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the PROVIDER.

Whereas

The BENEFICIARY has alleged that he fulfils at least one of the following criteria:

* He is designer of or competent to manufacture systems according to "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", where the BARAS is included in the systems.

* He is designer of or competent to manufacture components for systems according to [1]"DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", where at least one of the components includes the BARAS.

* He is designer of or competent to manufacture a system simulator for a system according to "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", where the simulator includes the BARAS.

The PROVIDER undertakes to give to the BENEFICIARY:

- ..... registered copies of the detailed specification of the BARAS cryptographic algorithm for use in the European standards for audio visual systems as specified by ETSI STC/TE10 (DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements).

The BENEFICIARY undertakes:

1. To keep strictly confidential all information contained in the detailed specification of the BARAS and all related communications written or verbal which have been associated with that information before and after the signature of the present undertaking (the "INFORMATION").

2. Not to make copies of the BARAS specifications (all copies of these specifications must be produced, numbered and registered by the BARAS Custodian).

3. Not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the PROVIDER.

4. To the best of his ability to take measures to avoid that his personnel disclose to third parties, without prior and explicit authorization in writing by the PROVIDER, all or part of the INFORMATION.

5. To use the INFORMATION in the BARAS specification exclusively for the provision of components, systems or services according to "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements", thus refraining from making any other use of the BARAS or information in the BARAS specification.

6. Not to register, or attempt to register, any IPR (patents or the like rights) relating to the BARAS and containing all or part of the INFORMATION.

7. To design his equipment, to the best of his ability, in a manner that protects the BARAS from disclosure and ensures that it cannot be used for any purpose other than to provide the services for which it is intended. (These services are defined in "DE/*****: Integrated Services Digital Network (ISDN), Confidentiality for audiovisual services, Procedures and Terminal Requirements".)

8. Not to subcontract any part of the design and build of his equipment, or the provision of his services, which requires a knowledge of the BARAS, to any organisation which has not signed the Confidentiality and Restricted Usage Undertaking.

9. Not to publish a description or analysis of any aspects which may disclose the operation of the BARAS in any document that is circulated outside the premises of the BENEFICIARY, except to the PROVIDER.

The above restrictions shall not apply to information which:

is or subsequently becomes (other than by breach by the BENEFICIARY of its obligations under this agreement) public knowledge; or

is received by the BENEFICIARY without restriction on disclosure or use from a third party and without breach by a third party of any obligations of confidentiality to the PROVIDER.

If, after five years from the effective date hereof, the BENEFICIARY has not used the INFORMATION, or if he is no more active in the business mentioned above, he shall return the written INFORMATION which he has received. The BENEFICIARY is not authorized to keep copies or photocopies; it is forbidden for him to make any further use of the INFORMATION.

In the event that the BENEFICIARY breaches the obligations of confidentiality imposed on him pursuant to clause 1 to 9 above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the BENEFICIARY agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach provided that such indemnity shall not extend to any losses incurred by ETSI as a result of any third party claiming against ETSI for any consequential or incidental losses (including loss of profits) suffered by that third party.

All disputes which derive from the present undertaking or its interpretation shall be settled by the Court of Arbitration of the International Chamber of Commerce situated in Paris, in accordance with the procedures of this Court of Arbitration and with the application of French Law regarding questions of interpretation.

The obligations of confidentiality herein shall not apply vis-à-vis other BENEFICIARIES. Evidence of being a BENEFICIARY shall be given by providing a certified copy of this undertaking duly undersigned.

This undertaking constitutes the entire agreement between the parties. All amendments to this undertaking shall be agreed in writing and signed by a duly authorised representative of each of the parties.

Made in two originals, one of which is for the PROVIDER, the other for the BENEFICIARY.

For the PROVIDER	For the BENEFICIARY
.....	.....
BARAS Custodian	.....
	(Name, Title (typed))
.....	.....
(Date)	(Date)

History

Document history	
March 1995	Draft For endorsement by TCC 20
June 1995	Final draft Endorsement by TCC 20, for approval by TA
November 1995	First Edition
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)