TR 101 054 V1.1.1 (1997-06)

Technical Report

Security Algorithms Group of Experts (SAGE);
Rules for the management of the
HIPERLAN Standard Encryption Algorithm (HSEA)

Reference
DTR/SAGE-00012-1 (9rc00ics.PDF)

Keywords
SAGE, security, algorithm, HSEA

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

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Security Algorithms Group of Experts (SAGE).

1 Scope

The purpose of the present document is to specify the rules for the management of the HIPERLAN Standard Encryption Algorithm HSEA.

The management structure is defined in clause 4. This structure is defined in terms of the principals involved in the management of the HSEA (ETSI, ETSI TC RES, HSEA Custodian and approved recipients) together with the relationships and interactions between them.

The procedures for delivering the HSEA to approved recipients are defined in clause 5. This clause is supplemented by annex A which specifies the items which are to be delivered.

Clause 6 is concerned with the criteria for approving an organization for receipt of the HSEA and with the responsibilities of an approved recipient. This clause is supplemented by annex B which contains a Confidentiality and Restricted Usage Undertaking to be signed by each approved recipient.

Clause 7 is concerned with the appointment and responsibilities of the HSEA Custodian.

2 References

There are no references required for the use of the present document.

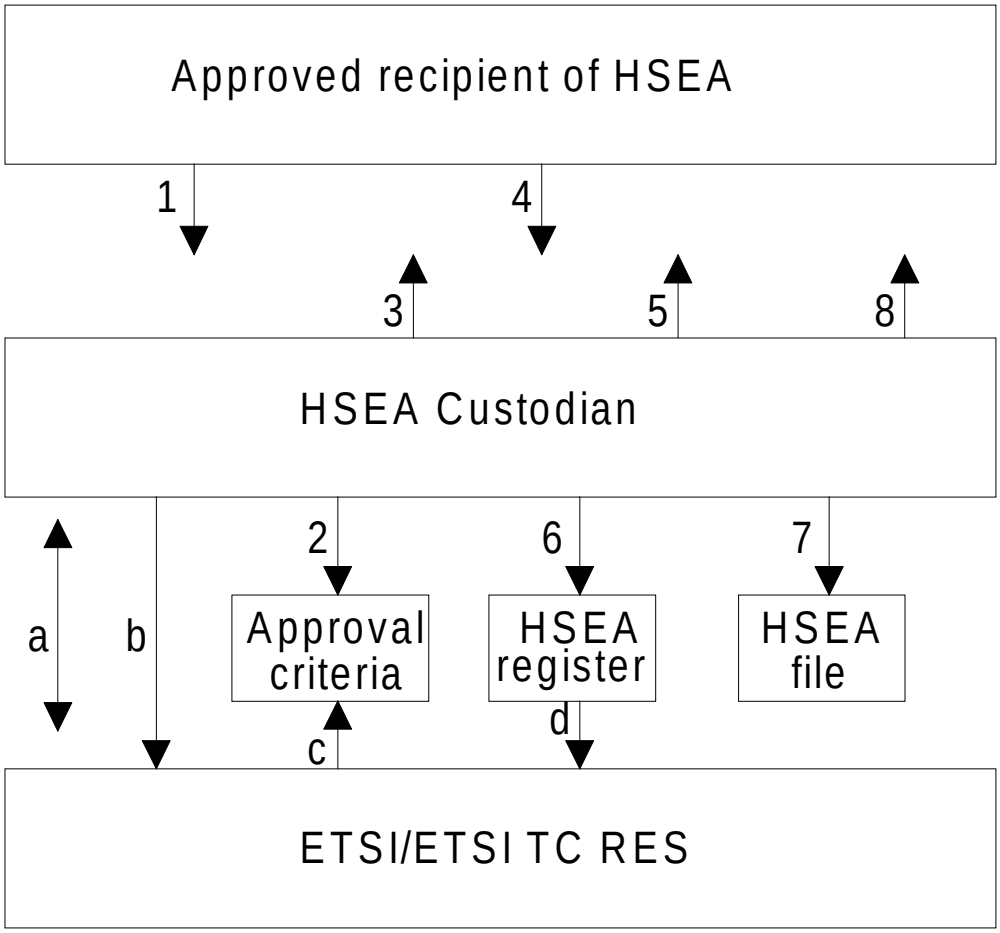
3 Abbreviations

For the purposes of the present document, the following abbreviation applies:

HIPERLAN High Performance Radio Local Area Network

4 HSEA management structure

The management structure is depicted in figure 1.



Key:

a = Agreement between HSEA Custodian and ETSI
b = Status reports and recommendations
c = Setting of approval criteria
d = Restricted details of the HSEA register
1 = Request for HSEA
2 = Check of request against approval criteria
3 and 4 = Exchange of Confidentiality and Restricted Usage Undertaking
5 = Dispatch of HSEA Specification
6 = Update the HSEA register
7 = Document filing
8 = Technical advice

Figure 1: HSEA management structure

The figure shows the three principals involved in the management of the HSEA and the relationships and interactions between them.

ETSI is the owner of the HSEA. The ETSI Secretariat together with ETSI TC RES sets the approval criteria for receipt of the algorithm (see clause 6).

The HSEA Custodian is the interface between ETSI and the approved recipients of the HSEA.

The Custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI TC RES to delegate this task to a third party on the basis of an agreement between the latter and the ETSI Secretariat. The HSEA Custodian's duties are detailed in clause 7. They include distributing the HSEA to approved recipients, as detailed in clause 5, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI TC RES.

5 Distribution Procedures

5.1 Distribution by HSEA Custodian

The following procedures for distributing the HSEA to approved recipients are defined with reference to figure 1:

1) The HSEA Custodian receives a written request for N copies of the HSEA Specification (see note 1),where N should not be greater than six (6).

2) The HSEA Custodian indicates whether the requesting organization meets the approval criteria (see clause 6).

3) If the request is approved, the HSEA Custodian dispatches 2 copies of the corresponding Confidentiality and Restricted Usage Undertaking (as given in annex B) for signature by the approved recipient (see notes 2 and 6) together with a copy of this document (Rules for the Management of the TETRA Standard Encryption Algorithm HSEA).

4) Both copies of the Confidentiality and Restricted Usage Undertaking shall be signed by the approved recipient (see notes 5 and 7) and returned to the HSEA Custodian, together with the payment of charges if any.

5) The HSEA Custodian sends up to N (see note 3) numbered copies of the HSEA 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 HSEA Custodian updates the HSEA Register by recording the name and address of the recipient, the numbers of the copies of the HSEA Specification delivered and the date of delivery. If the original request is not approved, the HSEA Custodian records the name and address of the requesting organization and the reason for rejecting the request in the HSEA Register (see also note 8).

7) The HSEA Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the HSEA File together with a copy of the covering letter sent to the approved recipient.

NOTE 1: Requests for the HSEA Specification may be made directly to the HSEA Custodian or through ETSI, where appropriate.

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 HSEA Custodian sends all items listed in annex A. Requests for part of the package of items are rejected.

NOTE 5: An organization may request the specification on behalf of a second organization to which it is subcontracting work which requires the specification. In this case, the first organization is responsible for returning a Confidentiality and Restricted Usage Undertaking signed by the second organization. Refer to the Transfer details given in subclause 5.2.

NOTE 6: Under normal circumstances the Custodian is expected to respond within 25 working days, excluding the delay of the procedures with the National Authorities.

NOTE 7: The approved recipient has to be a legal representative of the receiving organization.

NOTE 8: If a HSEA Specification is returned to the HSEA Custodian (for example the recipient may decide not to make use of the information), then the HSEA Custodian destroys the specification and enters a note to this effect in the HSEA Register.

5.2 Transfers by a Beneficiary

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

In this case, the first organization has to ensure that the second organization meets the approval criteria. The first organization has to get the second organization to sign two copies of the Confidentiality and Restricted Usage Undertaking. The first organization then sends these to the HSEA Custodian, together with the numbers of the specifications which are to be transferred.

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

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

6 Approval criteria

The approval criteria are set by the ETSI Secreteriat together with ETSI TC RES and maintained by the HSEA Custodian. The HSEA Custodian may recommend changes to these criteria.

In order for an organization to be considered an approved recipient of one of the HSEA it has to satisfy at least one of the following criteria :

C1 The organization is designer of or competent to manufacture HIPERLAN systems, where the HSEA is included in the systems.

C2 The organization is designer of or competent to manufacture components for HIPERLAN systems, where at least one of the components includes the HSEA.

C3 The organization is designer of or competent to manufacture a HIPERLAN system simulator for approval testing of HIPERLAN systems, where the simulator includes the HSEA.

The HSEA Custodian will decide whether an organization requesting the HSEA Specification may be considered to be an approved recipient. Any doubtful cases will be referred back to ETSI Secretariat or ETSI TC RES.

7 The HSEA Custodian

7.1 Responsibilities

The HSEA Custodian is expected to perform the following tasks:

T1 To approve requests for the HSEA by reference to the Approval Criteria given in clause 6.

T2bis To obtain the Administrative authorization and export licences required by the National Authorities of its country if any.

T2 To exchange the Confidentiality and Restricted Usage Undertaking with approved recipients as described in clause 5.

T3 To distribute the HSEA Specifications as detailed in clause 5 (see note 1).

T4 To maintain the HSEA Register as described in clause 5.

T5 To hold in custody the contents of the HSEA File as specified in clause 5.

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

T7 To advise ETSI/ETSI TC RES of any problems arising with the approval criteria.

T8 In the light of written queries from recipients of the HSEA Specifications, to make recommendations to ETSI/ETSI TC RES for improvements/corrections to the specification and, subject to ETSI/ETSI TC RES approval, make and distribute the changes (see note 3).

T9 To provide ETSI/ETSI Project TETRA with information from the HSEA Register when requested to do so.

T10 To monitor published advances in crypto-analysis and advise the ETSI TC RES of any advances which have a significant impact upon the continued suitability of the HSEA for the HIPERLAN application.

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 HSEA Custodian will only endeavour to answer questions relating to the HSEA Specifications. He is not expected to provide technical support for development programmes.

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

7.2 Appointment

The HSEA Custodian is:

ETSI Secretariat

The contact person is:

Mr Pierre De Courcel Fax +33 4 93 65 47 16

ETSI

F-06921 Sophia Antipolis Cedex

France

The HSEA Custodian will ask a fee from the recipient to cover the cost of distribution.

Annex A:
Items delivered to approved recipient of HSEA

ITEM-1: Up to N numbered paper copies to the HSEA Specification 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 HSEA Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered (see note).

NOTE: In the case of a transfer (see subclause 5.2), 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 Undertaking for HSEA

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the HSEA algorithm for the protection of the information exchanged over the radio channels of the High Performance Radio Local Area Network System.

Between

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the BENEFICIARY;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The BENEFICIARY has alleged, supported by additional information provided, that he fulfills at least one of the following criteria:

- He is designer of or competent to manufacture HIPERLAN where HIPERLAN Standard Encryption Algorithm (hereinafter referred to as HSEA) is included in the systems.
- He is designer of or competent to manufacture components for HIPERLAN systems where at least one of the components include the HSEA.
- He is designer of or competent to manufacture HIPERLAN system simulator for approval testing of HIPERLAN systems where the simulator includes the HSEA.

The CUSTODIAN undertakes to give to the BENEFICIARY:

- registered copies of the detailed specification of the confidentiality algorithm for protection of the information exchanged over the radio channels of a HIPERLAN system.

The BENEFICIARY undertakes:

1) To keep strictly confidential all information contained in the detailed specification of the HSEA and all related communications written or verbal which have been associated with that information after the signature of the present undertaking (the "INFORMATION").
2) Not to make copies of the HSEA specifications (all copies of these specifications must be produced, numbered and registered by the HSEA Custodian).
3) Not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the CUSTODIAN.

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 CUSTODIAN, all or part of the INFORMATION.

5) To use the INFORMATION in the HSEA specification exclusively for the provision of HIPERLAN components, systems or services, thus refraining from making any other use of the HSEA or information in the HSEA specification.

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

7) To design his equipment in a manner, to the best of his ability, that protects the HSEA from disclosure and ensures that it cannot be used for any purpose other than to provide the HIPERLAN services for which it is intended.

   These services are specified in the following standard:

   ETS 300 652: "High Performance Radio Local Area Network (HIPERLAN); Functional specification".

8) Not to subcontract any part of the design and build of his equipment, or the provision of his HIPERLAN services, which requires a knowledge of the HSEA, to any organization 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 HSEA in any document that is circulated outside the premises of the BENEFICIARY.

The above restriction does 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 CUSTODIAN.

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 bullets 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. The BENEFICIARY may not be held liable for any indirect or consequential or incidental losses (including loss of profits) suffered by any third party claiming against ETSI.

All disputes which derive from the present undertaking or its interpretation will be settled by the Court of Justice located in Grasse (Alpes Maritimes) and with the application of French Law regarding questions of interpretation.

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

This undertaking supersedes all prior confidentiality and restricted scope undertakings between the parties and constitutes the entire agreement between the parties. All amendments to this undertaking will be agreed in writing and signed by a duly authorized representative of each of the parties.

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

For the CUSTODIAN	For the BENEFICIARY
.....	.....
(Name, Title (typed))	(Name, Title (typed))
.....	.....
(Name, Title (typed))	(Name, Title (typed))
.....	.....
(Date)	(Date)

History

Document history		
June 1997	1.1.1	Publication

ISBN 2-7437-1567-7
Dépôt légal : Juin