ETSI TECHNICAL COMMITTEE REFERENCE TECHNICAL REPORT

TCR-TR 031

November 1995

Source: ETSI TC-SAGE

Reference: DTR/SAGE-00007

ICS: 33.020

Key words: UPT, authentication algorithm, management rules

Security Algorithms Group of Experts (SAGE); Universal Personal Telecommunication (UPT) authentication; Rules for the management of USA-4

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 produced by the Security Algorithms Group of Experts (SAGE) of the European Telecommunications Standards Institute (ETSI). 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 standards, framework and guideline documents) which constitute the agreed basis for several, if not all, TCs and STCs to pursue detailed standards.

Blank page

1 Scope

The purpose of this TCR-TR is to specify the rules for the management of the USA-4 cryptographic algorithm. USA-4 is an authentication algorithm for use in the advanced access devices and corresponding security modules used for performing authentication of Universal Personal Telecommunication (UPT) users according to ETS 300 391-1 [1] and NA-TR 014 [2].

The management structure is defined in clause 3. This structure is defined in terms of the principals involved in the management of the USA-4 (ETSI, TC Network Aspects (TC-NA), USA-4 Custodian and Approved Recipients) together with the relationships and interactions between them.

The procedures for delivering the USA-4 to Approved Recipients are defined in clause 4. This clause is supplemented by annex A which specifies the items which are to be delivered.

Clause 5 is concerned with the criteria for approving an organisation for receipt of the USA-4 and with the responsibilities of an Approved Recipient. This clause is supplemented by annex 2 which contains a Confidentiality and Restricted Usage Undertaking to be signed by each Approved Recipient.

Clause 6 is concerned with the appointment and responsibilities of the USA-4 Custodian.

2 References

This TCR-TR incorporates by dated and undated reference, provisions from other publications. These 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 TCR-TR only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 391-1 (1995): "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT Phase 1; Part 1: Specification".

[2] NA-TR 014 (1993): "Universal Personal Telecommunication (UPT); Authentication algorithm for Phase 1; Requirements specification".

NOTE: NA-TR 014 is available from the TC-NA Chairman.

3 USA-4 Management Structure

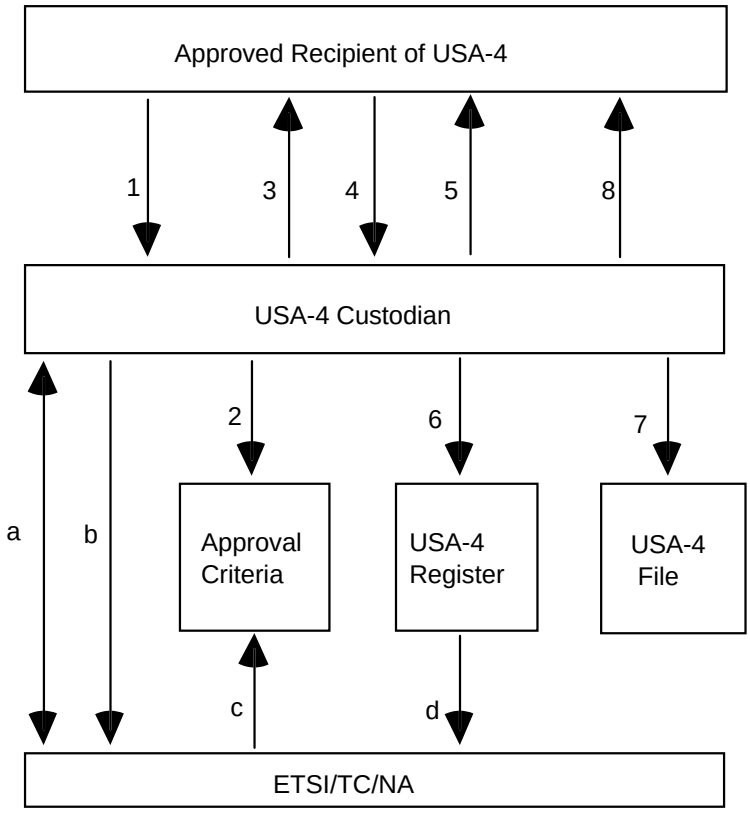
The management structure is depicted in figure 1. The figure shows the three principals involved in the management of the USA-4 and the relationships and interactions between them.

ETSI is the owner of the USA-4 and, together with TC-NA, sets the approval criteria for receipt of the algorithm (see clause 5).

The USA-4 Custodian is the interface between ETSI and the Approved Recipients of the USA-4.

The activities of the USA-4 Custodian are supported by an agreement between ETSI and the custodian.

The USA-4 Custodian's duties are detailed in clause 6. They include distributing the USA-4 algorithm to Approved Recipients, as detailed in clause 4, providing limited technical advice to Approved Recipients and providing algorithm status reports to TC-NA.



Key to figure:

a = agreement between USA-4 Custodian and ETSI;
b = status reports and recommendations;
c = setting of approval criteria;
d = restricted details of the USA-4 Register.

1 = request for USA-4;
2 = check of request against approval criteria;
3 = dispatch of USA-4 Specification;
3/4 = exchange of Confidentiality and Restricted Usage Undertaking;
4 = update the USA-4 Register;
5 = document filing;
6 = technical advice.

Figure 1: USA-4 management structure

4 Distribution procedures

The following procedures for distributing the USA-4 to Approved Recipients are defined with reference to figure 1:

The USA-4 Custodian receives a written request for N copies of the USA-4 Specification (see note 1), where N should not be greater than six. The request should indicate that the algorithm is needed for implementing a UPT security architecture or otherwise.

The USA-4 Custodian confirms (or otherwise) whether the requesting organisation meets the approval criteria.

If the request is approved, the USA-4 Custodian dispatches 2 copies of the appropriate Confidentiality and Restricted Usage Undertaking (as given in annex B) for signature by the Approved Recipient together with a copy of this TCR-TR.

Both copies of the Confidentiality and Restricted Usage Undertaking shall be signed by the Approved Recipient and returned to the USA-4 Custodian.

The USA-4 Custodian sends up to N (note 3) numbered copies of the USA-4 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).

The USA-4 Custodian updates the USA-4 Register by recording the name and address of the recipient, the numbers of the copies of the USA-4 Specification delivered and the date of delivery. If the original request is not approved, the USA-4 Custodian records the name and address of the requesting organisation and the reason for rejecting the request in the USA-4 Register.

The USA-4 Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the USA-4 File together with a copy of the covering letter sent to the Approved Recipient.

NOTE 1: Requests for the USA-4 specification should be made directly to the USA-4 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 and the intended usage.

NOTE 4: The USA-4 Custodian sends all items listed in annex A. 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 is the legal representative of the receiving organisation.

NOTE 7: If a USA-4 Specification is returned to the USA-4 Custodian (for example the recipient may decide not to make use of the information), then the USA-4 Custodian destroys the specification and enters a note to this effect in the USA-4 Register.

NOTE 8: The USA-4 Custodian may impose a reasonable charge to cover administrative costs involved in issuing the USA-4 specification documents.

5 Approval criteria

The approval criteria are set by ETSI together with TC-NA and are maintained by the USA-4 Custodian. The USA-4 Custodian may recommend changes to these criteria.

In order for an organisation to be considered an Approved Recipient of the USA-4 algorithm for use in a UPT system it shall satisfy at least one of the following criteria:

C1 the organisation is a designer of, or competent to, manufacture systems according to ETS 300 391-1 [1], where the use of USA-4 is included;

C2 the organisation is designer of or competent to manufacture components for systems according to ETS 300 391-1 [1], where at least one of the components includes the USA-4;

C3 the organisation is designer of or competent to manufacture a system simulator for a system according to ETS 300 391-1 [1], where the simulator includes the USA-4;

C4 the organisation will provide UPT services as an operator of a system according to ETS 300 391-1 [1] using the USA-4.

The USA-4 Custodian will decide whether an organisation requesting the USA-4 Specification may be considered to be an Approved Recipient. Any doubtful cases will be referred back to ETSI/TC-NA, after taking the advice of the ETSI Deputy Director.

6 The USA-4 Custodian

6.1 Responsibilities

The USA-4 Custodian is expected to perform the following tasks:

T1 to approve requests for the USA-4 by reference to the Approval Criteria given in clause 5;
T2 to exchange the Confidentiality and Restricted Usage Undertaking with Approved Recipients as described in clause 4;
T3 to distribute the USA-4 Specification as detailed in clause 4 (see note 1);
T4 to maintain the USA-4 Register as described in clause 4;
T5 to hold in custody the contents of the USA-4 File as specified in clause 4;
T6 to provide recipients of the USA-4 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-NA of any problems arising with the approval criteria;
T9 in the light of written queries from recipients of the USA-4 Specification, to make recommendations to ETSI/TC-NA for improvements/corrections to the specification and, subject to ETSI/TC-NA approval, make and distribute the changes (see note 3);
T10 to provide ETSI/TC-NA with information from the USA-4 Register when requested to do so;
T11 to monitor published advances in crypt analysis and advise the TC-NA of any advances which have a significant impact upon the continued suitability of the USA-4 for the use in the context of UPT.

NOTE 1: Registered mail will be used. If recipients require a different delivery service they will be excepted to pay the full costs.

NOTE 2: The USA-4 Custodian will only endeavour to answer questions relating to the USA-4 Specification. He is not expected to provide technical support for the general development of UPT authentication or implementing of the algorithm.

NOTE 3: Numbered copies of any changes to the USA-4 Specification are automatically distributed to all recipients of the specification and a record of the distribution entered in the USA-4 Register.

6.2 Appointment

The USA-4 Custodian is:

Per Christoffersson

Telia Promotor AB
Box 168
13623 Haninge
Sweden

Fax: +46 8 7073599
Fax: +46 8 7772815

Annex A: Items delivered to Approved Recipient of USA-4

ITEM-1: up to N numbered copies to the USA-4 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 USA-4 Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered.

Annex B: Confidentiality and restricted usage undertaking

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the USA-4 authentication algorithm for use in European systems for Universal Personal Telecommunications (UPT) as specified in the ETSI standard ETS 300 391-1 [1].

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 ETS 300 391-1 [1], where the use of USA-4 is included;

- he is designer of or competent to manufacture components for systems according to ETS 300 391-1 [1], where at least one of the components includes the USA-4;

- he is designer of or competent to manufacture a system simulator for a system according to ETS 300 391-1 [1], where the simulator includes the USA-4;

- he will provide UPT services as an operator of a system according to ETS 300 391-1 [1] using the USA-4.

The PROVIDER undertakes to give to the BENEFICIARY:

- registered copies of the detailed specification of the authentication algorithm USA-4.

The BENEFICIARY undertakes:

1) to keep strictly confidential all information contained in the detailed specification of the USA-4 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 USA-4 specification (all copies of these specifications shall be produced, numbered and registered by the USA-4 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 USA-4 specification exclusively for the provision of UPT components, systems or services, thus refraining from making any other use of the USA-4 or information in the USA-4 specification;

6) not to register, or attempt to register, any IPR (patents or the like rights) relating to the USA-4 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 USA-4 from disclosure and ensures that it cannot be used for any purpose other than to provide the UPT services for which it is intended, (these services are defined in ETS 300 391-1 [1]).

8) not to subcontract any part of the design and manufacture of his equipment, or the provision of his UPT services, which requires a knowledge of the USA-4, to any organisation which has not signed the Confidentiality and Restricted Usage Undertaking;

9) not to communicate a description or analysis of any aspects which may disclose the operation of the USA-4 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 his 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
.....	.....
USA-4 Custodian	.....
	(Name, Title (typed))
.....	.....
(Date)	(Date)

History

Document history		
December 1994	Draft	For endorsement by TCC 19
June 1995	Final draft	Endorsed by TCC 20, for approval by TA
November 1995	First Edition	
March 1996	Converted into Adobe Acrobat Portable Document Format (PDF)	