ETSI

ETSI TECHNICAL REPORT

ETR 324

December 1996

Source: ETSI TC-NA

Reference: DTR/NA-007012

ICS: 33.020

Key words: UPT, security

Universal Personal Telecommunication (UPT); Authentication algorithm for Phase 1; Requirements specification

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 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Network Aspects (NA) Technical Committee of the European Telecommunications Standards Institute (ETSI).

ETRs are informative documents resulting from ETSI studies which are not appropriate for European Telecommunication Standard (ETS) or Interim European Telecommunication Standard (I-ETS) status. An ETR may be used to publish material which is either of an informative nature, relating to the use or the application of ETSs or I-ETSs, or which is immature and not yet suitable for formal adoption as an ETS or an I-ETS.

This ETR was prepared in 1992.

Blank page

1 Scope

This ETSI Technical Report (ETR) provides a requirements specification on the Universal Personal Telecommunication (UPT) authentication algorithm for Phase 1.

The algorithm is a secret-keyed one-way function, and is to be used for the non-interactive authentication of the UPT users for Phase 1, using the procedures defined in ETS 300 391-1 [1].

Although it is primarily intended for Phase 1, the algorithm is specified in such a way that it should also be possible to use it in an interactive way in Phase 2.

2 References

This ETR incorporates by dated or undated reference, provisions from other publications. These references are cited at the appropriate places in the text and the publications are listed below. For dated references subsequent amendments to, or revisions of, any of these publications apply to this ETR 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: "Universal Personal Telecommunication (UPT); Specification of the security architecture for UPT phase 1; Part 1: Specification".

3 Algorithm parameters

The algorithm parameters are as follows:

- Input: 64 bits labelled X[0] to X[63];
- Output: 32 bits labelled Y[0] to Y[31];
- Key: 128 bits labelled K[0] to K[127].

The input will be a non-repeating number generated by the UPT device (counter). The mapping from the counter value into the bits X[0] to X[63] is described in ETS 300 391-1 [1].

When the UPT device is a DTMF generator, the output value is to be converted into a Dual Tone Multi-Frequency (DTMF) signal for transmission across the network. The mapping from the bits Y[0] to Y[31] into the DTMF characters is described in ETS 300 391-1 [1].

4 Strength

For any set of inputs, it shall be computationally unfeasible to use the knowledge of the corresponding outputs under an unknown key to deduce the key, or to deduce the output corresponding to any additional input value.

5 Algorithm confidentiality

The algorithm specification will be kept confidential (i.e. not published). The algorithm will be made available to the service providers and to those who need to know how to implement the standard, but will not be published as part of this ETR, or be publicly available.

6 Algorithm distribution

An algorithm custodian, appointed by ETSI, will be entrusted with the algorithm distribution.

Anyone receiving a copy of the algorithm specification will have to sign a non disclosure and restricted usage undertaking.

7 Dimensioning constraints

A software oriented solution is preferred, with the following constraints:

SPEED: 100 milliseconds maximum (input/output non included) on a 6 805 family of microprocessors, e.g. the Motorola SC21 series, with a 4 MHz clock;

ROM: 1 000 bytes maximum (if possible 500 bytes);

RAM: 64 bytes.

It should be feasible to implement the algorithm in a smart card.

8 Acceptance criteria

The design and the evaluation work will be done under the control of the ETSI/SAGE group, which is responsible for the final approval of the algorithm.

9 Algorithm presentation

ETSI/SAGE will produce two documents:

1) the algorithm specification, which will be kept secret and will consist of:

   - a word mathematical description of the algorithm;
   - conformance test vectors;
   - Pascal/C sample implementations;
   - dimensioning/performance estimates;

2) a final report to Network Aspects Technical Committee containing some dimensioning/performance estimates.

History

Document history	
December 1996	First Edition

ISBN 2-7437-1149-3
Dépôt légal : Decembre 1996