ETSI

ETSI TECHNICAL REPORT

ETR 277

March 1996

Source: ETSI TC-SAGE

Reference: DTR/SAGE-00013

ICS: 33.020

Key words: Audio visual systems, encryption algorithm, management data

Security Algorithms Group of Experts (SAGE); Requirements specification for an encryption algorithm for use in audio visual systems

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 ETSI Technical Report (ETR) has been produced by the Security Algorithms Group of Experts (SAGE) and the Terminal Equipment (TE) Technical Committee of the European Telecommunications Standards Institute (ETSI).

The work on this ETR was undertaken in response to the CEC mandate reference BC-T-239.

Blank page

1 Scope

A specification for a confidentiality system for audio visual services is currently being defined by CCITT WP XV (1). This specification does not contain a cryptographic algorithm, but caters for the use of different algorithms. The algorithms are to be used to encrypt the data streams.

This ETSI Technical Report (ETR) provides the requirements specification for a cryptographic algorithm which may be used with this CCITT standard.

ETSI STC TE10 is considering converting ITU-TS Recommendations in the field of security and privacy for telecommunication in full or partly into ETSs.

The cryptographic algorithm required by this ETR will be developed by SAGE Project Team 38V, it will be registered in ISO 9979, and it will be proposed to ITU-TS SG15 for inclusion into CCITT Recommendation H.233 [1].

2 References

For the purposes of this ETR, the following references apply:

[1] CCITT Recommendation H.233 (1995): "Confidentiality system for audiovisual services".

NOTE: This Recommendation describes the use of the algorithm in detail.

[2] ETS 300 144: "Integrated Services Digital Network (ISDN); Audiovisual services; Frame structure for a 64 kbit/s to 1 920 kbit/s channel and associated syntax for inband signalling".

NOTE: This ETS describes the (framing) structure of the data which is to be encrypted.

[3] ITU-T Recommendation H.234 (1994) Key : "Encryption key management and authentication system for audiovisual services".

3 Abbreviations

For the purposes of this ETR, the following abbreviation applies:

SAGE Security Algorithms Group of Experts

4 External interface specification

The use of the algorithm is specified in detail in CCITT Recommendation H.233 [1].

The inputs for the algorithm are a cryptographic key, KEY, and an Initialization Vector (IV).

The key is, in principle, a random parameter established using key management procedures as described in CCITT Recommendation H.234 [3]. Its length is 64 bits.

IV is a random number which is regularly updated and transmitted via a control channel and is used to initialize the algorithm. Its length is 64 bits.

Re-synchronization of the algorithm takes place after a new IV is received (which happens normally after a number of multi-frames).

At re-synchronization of the algorithm, the KEY and IV are loaded in the algorithm. The algorithm produces a cipher bit stream which is bitwise added modulo 2 with the data stream. In this process certain bits, determined by the framing, of the cipher stream are ignored, i.e. not used for encryption (see CCITT Recommendation H.233 [1] and ETS 300 144 [2]).

5 Functional requirements specification

5.1 Operation speed requirements

The algorithm should operate at a speed of 2 Mbit/s using a hardware (chip) implementation with a 20 MHz clock.

5.2 Implementation complexity requirements

It should be possible to realize a hardware implementation of the algorithm which is much smaller than a Personal Computer (PC) add-on board. A single chip implementation is preferable.

Simplicy of implementation should not be sacrificed for too high a degree of security.

5.3 Algorithm usage, distribution and management

In principle there is no restriction on the use of the algorithm to a specific user group. The algorithm should be subject to minimal export restrictions.

The algorithm specification will be distributed strictly on the basis of a restricted usage and non-disclosure undertaking prepared by ETSI. Distribution of the algorithm will be restricted to manufactures of hardware implementing the algorithm for the specified use.

A custodian will be appointed by ETSI to manage the distribution of the algorithm.

5.4 Technical requirements

The minimum life time of the algorithm is 5 years (commensurate with the life time of the audiovisual equipment in which the algorithm is used).

6 Algorithm presentation

The algorithm specification should include:

- a mathematical description of the algorithm (including, e.g. a functional diagram or information flow chart);
- example conformance test vectors;
- software simulation code.

7 Acceptance procedure

Acceptance of the specification will be solely on the basis of the internal SAGE acceptance procedures.

History

Document history	
March 1996	First Edition

ISBN 2-7437-0555-8
Dépôt légal : Mars 1996