Draft new Recommendation J.96 (J.encryp)

TECHNICAL METHOD FOR ENSURING PRIVACY IN LONG-DISTANCE INTERNATIONAL MPEG-2 TELEVISION TRANSMISSION CONFORMING TO REC. J.89

1 SCOPE

This ITU-T Recommendation constitutes a common standard for a conditional access system for long distance international transmission of digital television according to MPEG Professional Profile (4:2:2). Practical implementations are also provided in annexes.

2 REFERENCES

2.1 Normative reference


[3] ETR 289: "Digital broadcasting systems for television, sound and data services; Support for use of scrambling and conditional access (CA) within digital broadcasting systems.


2.2 Bibliographic reference

Common Scrambling Algorithm is used according to the DVB specification including the section for DSN applications.

A. Fixed local "control word"

B. Variable local "control word"

C. Full conditional access system

Fig. 1 GENERAL DESCRIPTION OF THE SCRAMBLING/DESCRAMBLING PROCESSES

More information about the application of the DVB Common Scrambling Algorithm can be found in the ETSI publications available on the ETSI Website (http://www.etsi.org/).

The three implementations illustrated above are described in the Annexes A, B of this recommendation.

APPLICATION IN THE MPEG/DVB ENVIRONMENT.

SCRAMBLING

Scrambling is a process used to make an information incomprehensible for unauthorised receivers during transmission of this information.

For this process, adopted the "common scrambling algorithm" specified by DVB.

This algorithm uses common keys to initialise the scrambling-descrambling process at each transport packet. These common keys are issued from control words (CW) that are sent in the stream.

Scrambling can be done at transport or PES packets level.
DVB Common Scrambling Algorithm V.2.0

The Common Scrambling Algorithm, approved by the Steering Board of the DVB Project, is comprised of the Common Descrambling System and Scrambling Technology. The specification for each is distributed separately under arrangements with the European Telecommunications Standards Institute, which acts as Custodian for the four Companies which have developed the Common Scrambling Algorithm.

The Common Descrambling System will be licensed to manufacturers of Decoders and their components, and to providers, designers and other entities engaged in conditional access.

The Scrambling Technology will be licensed to manufacturers of Scramblers, which will in turn sublicense the purchasers of Scramblers.

The conditions for receiving the confidential information are specified in the summary of distribution arrangements for the Common Descrambling System or for the Scrambling Technology.

DVB Common Descrambling System Licence and Non-Disclosure Agreement or the DVB Scrambling Technology Licence and Non-Disclosure Agreement have to be signed for receiving the confidential information.

For further information please consult the explanatory note on certain terms governing the distribution agreements of the common scrambling algorithm.

Or contact

European Telecommunications Standards Institute (ETSI)
F-06921 Sophia Antipolis CEDEX
France
fax: (33) (0) 4 92 94 4270
attention: Gina Ebenezersson

Last updated: 2006-02-09 09:43:52