EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT

pr **ETS 300 747**

February 1997

Source: ETSI TC-Security

Reference: DE/SEC-002308

ICS: 33.020

Key words: Audio, security, service

Telecommunications Security; Service access control and synchronisation for audiovisual services

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 final draft European Telecommunication Standard (ETS) has been produced by the Security Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

This European Telecommunication Standard (ETS) fits into the series of standards about audiovisual communication over the Integrated Services Digital Network (ISDN), which is introduced in the ITU-T H.200 series of Recommendations.

In ITU-T Recommendations H.233 [1] and H.234 [2], the basic mechanisms for confidentiality and key exchange are specified.

On top of these, this ETS specifies the confidentiality related protocol extensions needed for the establishment, modification and termination of audiovisual conferences using one or more Multipoint Control Units (MCUs).

2 Normative references

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

[1] ITU-T Recommendation H.233: "Confidentiality system for audiovisual services".

NOTE 1: ITU-T Recommendation H.233 forms the basis of ETS 300 840 [6].

[2] ITU-T Recommendation H.234: "Encryption key management and authentication system for audiovisual services".

NOTE 2: ITU-T Recommendation H.234 forms the basis of ETS 300 841 [7].

[3] ITU-T Recommendation H.243: "Procedures for establishing communication between three or more audiovisual terminals using digital channels up to 2 Mbit/s".

[4] ITU-T Recommendation H.231: "Multipoint control units for audiovisual systems using digital channels up to 2 Mbit/s".

[5] ITU-T Recommendation H.230: "Frame-synchronous control and indication signals for audiovisual systems".

[6] ETS 300 840: "Telecommunications Security; Integrated Services Digital Network (ISDN); Confidentiality system for audiovisual services".

[7] ETS 300 840: "Telecommunications Security; Integrated Services Digital Network (ISDN); Encryption key management and authentication system for audiovisual services".

3 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

CCK	Chair Command Kill
CCT	Chair-Control Terminal
ECS	Encryption Control Signal
MCU	Multipoint Control Unit
NMCU	Non-trusted MCU
TMCU	Trusted MCU

4 General functions

4.1 Trusted MCUs (TMCUs) versus Non-trusted MCUs (NMCUs)

4.1.1 TMCU

In the case of a "trusted MCU" (in which the signals are all decrypted at the inputs to the MCU, and therefore the MCU needs to be in a secure location) the communication between each audiovisual terminal and the MCU may be encrypted as described in ITU-T Recommendation H.233 [1]. Clearly this method is not applicable to the connection of telephone terminals to the conference via the analogue telephone network.

4.1.2 NMCU

A NMCU is not able to decrypt the audio, video, or other data. The point-to-point environment specified in ITU-T Recommendations H.233 [1] and H.234 [2], suitable for a TMCU, should be enhanced to include a NMCU.

The conference is carried out in switching mode as mixing of encrypted data is not possible at the MCU. A possible mode of switching may be that all participants receive the picture and the voice of the speaker, except the speaker himself, who receives the video and audio of the Chair Control Terminal (CCT). The switching of the speaker is controlled directly by the CCT using the BAS codes specified in ITU-T Recommendation H.230 [5].

The existence of a CCT for the distribution of keys is mandatory. Each participant has to open the Encryption Control Signal (ECS) channel as specified in ITU-T Recommendation H.233 [1] and the MCU has to route it between the participants and the CCT. The routeing information is also coded in the ECS channel as described in subclause 4.4. This provides a configuration to exchange keys and other information over a point-to-point link, i.e. from CCT to the participants.

4.2 Chair-Control Functions for Confidentiality

For the control of audiovisual conferences, the confidentiality related functions of the MCU as described in ITU-T Recommendation H.231 [4] may be divided into switching and chair-control functions. In the case of a TMCU both groups of functions may be implemented within the MCU; for confidentiality purposes, an explicit CCT is not required.

If a NMCU is used, the CCT has to take over the chair-control functions as below:

- it is responsible for the authentication of the participants;
- it is responsible for the distribution of keys in regular or irregular intervals;
- when a partner joins or leaves during a session, new session keys should be distributed;
- the speaker switching should be carried out by the chair control.

4.3 Authentication

Generally, all participants including the session chair have to authenticate themselves before joining the session. Optionally, mutual authentication may be applied.

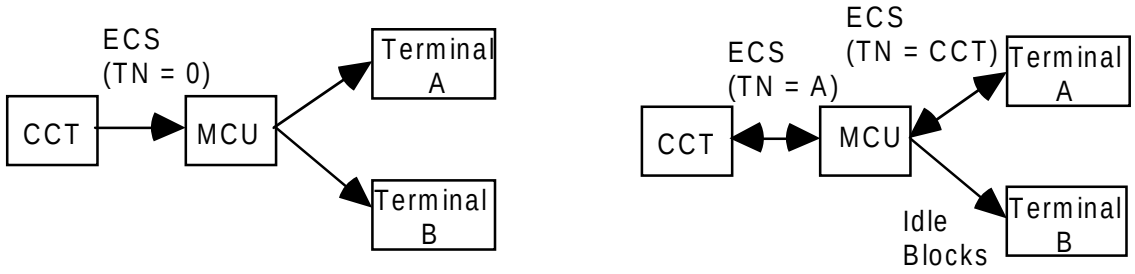
In the case of a TMCU, the MCU is in charge of authenticating all terminals (cf. ITU-T Recommendation H.234 [2]). When a NMCU is used, the CCT has to take over this function; in this case, no authentication for the CCT takes place, but all other terminals have to authenticate themselves against the CCT.

Once the connection between the MCU and the CCT is running, the conference is considered as established. All other participants are treated as joining an existing conference; therefore their entry into the conference is equivalent to a modification of a running session.

4.4 Routeing of ECS channel messages

In the case of a NMCU, a routeing function within the NMCU is required for the point-to-point signalization between specific terminals and the CCT.

The MCU has to route the ECS channel corresponding to the routeing information coded in the IV blocks. The IV block is extended to include the terminal number of the participant with whom the CCT communicates. 16 bits from the 20 spare bits are used for this.



a) MCU broadcasts the message (Terminal Number TN = 0)

b) MCU routes CCT to A and vice versa All others receive idle packets

Figure 1: Routeing of the ECS channel

5 Access control

5.1 Initialization of a session

If a TMCU is used, the session initialization takes place as specified in ITU-T Recommendations H.234 [2] and H.243 [3].

In the case of a NMCU, a session is initialized with the first terminal with Chair Control capability connected to the MCU. The Chair Control token is passed over to this terminal. If this terminal does not have the Chair Control capability, then the connection is dropped. All other initialization procedures are carried out as specified in ITU-T Recommendation H.234 [2].

5.2 Modifications during a session

5.2.1 Participants joins a session

The procedures for authentication and/or key exchange take place as specified in ITU-T Recommendation H.234 [2], clause 2.

If a TMCU is used, the central part of these procedures is carried out by the MCU.

In the case of a NMCU, the MCU informs the CCT that a new participant intends to join the session. The CCT transmits P0 to the respective terminal. If the terminal replies with P1 or P2, the new terminal should be excluded from the session.

NOTE: Exchange of session keys necessitates synchronization as described in clause 6.

5.2.2 Participant leaves a session

After a participant has left the session (cf. ITU-T Recommendation H.243 [3], subclause 7.3), the MCU (or the CCT in case of a NMCU) shall initiate a key exchange procedure and thereby the distribution of a new key-encrypting key for the remaining participants. Thereafter new session keys shall be distributed, and synchronization shall be carried out.

The same procedure applies for the case, where a terminal is dropped by the CCT (cf. ITU-T Recommendation H.243 [3], subclause 7.5).

5.2.3 Handover of session responsibility

The handover of the Chair Control token may be handled in two ways on the MCU:

- **restricted mode:** the initial terminal is the CCT and cannot be changed during the session;

- **flexible mode:** The initial participant is the Chair Control, and it may transfer this role to another participant during a session. If no other participant can handle the Chair Control token, the session should be terminated.

This function is mandatory for a NMCU, and is optional for a TMCU. The applicable protocol is described in ITU-T Recommendation H.243 [3], subclause 7.2.

5.3 Termination of a session

When a MCU receives the BAS code Chair Command Kill (CCK) from the CCT, it drops the connections at all its ports, releasing all associated conference resources (cf. ITU-T Recommendations H.243 [3] and H.230 [5]).

5.4 Abnormal events

In the case of a NMCU, an abrupt termination of the CCT should be identified by the MCU and cause the termination of the session.

In the case of a TMCU, the conference may be continued with the remaining terminals.

6 Synchronization of the confidentiality system

6.1 Introduction

After each modification of a session a synchronization of the confidentiality system in all terminals has to be carried out.

6.2 Synchronization of session key activation

The MCU broadcasts the session keys to all participants, using message P6 as specified in ITU-T Recommendation H.234 [2]. Each participant, after receiving the message P6, confirms it using P12. The MCU sequentially establishes connection over the ECS channel to each participant to receive the confirmation. The MCU should repeat P6 until it receives P12 from the participant or until a specified period of time has elapsed. In case no confirmation is received, the partner is dropped from the conference.

Message Name:	Key Received Confirmation P12
Message Identifier:	1 0 P t_1 t_2 t_3 t_4 t_5 = 1 0 0 0 1 0 1 0
Meaning:	The terminal has received the new session key supplied by the MCU.
Contents:	The message has no content.

After the MCU has received the confirmation from all participants it sets the key-loading synchronization flag in the IV block to use the new key.

If a NMCU is used, the respective protocol steps are carried out by the CCT.

History

Document history			
April 1996	Public Enquiry	PE 105:	1996-04-08 to 1996-08-30
February 1997	Vote	V 9715:	1997-02-11 to 1997-04-11