INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.93

(03/98)

SERIES J: TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

Ancillary digital services for television transmission

Requirements for conditional access in the secondary distribution of digital television on cable television systems

ITU-T Recommendation J.93

(Previously CCITT Recommendation)

ITU-T J-SERIES RECOMMENDATIONS

TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

General Recommendations	J.1–J.9
General specifications for analogue sound-programme transmission	J.10–J.19
Performance characteristics of analogue sound-programme circuits	J.20–J.29
Equipment and lines used for analogue sound-programme circuits	J.30–J.39
Digital encoders for analogue sound-programme signals	J.40–J.49
Digital transmission of sound-programme signals	J.50–J.59
Circuits for analogue television transmission	J.60–J.69
Analogue television transmission over metallic lines and interconnection with radio-relay links	J.70–J.79
Digital transmission of television signals	J.80–J.89
Ancillary digital services for television transmission	**J.90–J.99**
Operational requirements and methods for television transmission	J.100–J.109
Interactive systems for digital television distribution	J.110–J.129
Transport of MPEG-2 signals on packetised networks	J.130–J.139
Measurement of the quality of service	J.140–J.149
Digital television distribution through local subscriber networks	J.150–J.159

For further details, please refer to ITU-T List of Recommendations.

ITU-T RECOMMENDATION J.93

REQUIREMENTS FOR CONDITIONAL ACCESS IN THE SECONDARY DISTRIBUTION OF DIGITAL TELEVISION ON CABLE TELEVISION SYSTEMS

Summary

This Recommendation considers the requirements, hardware and command interfaces, policies, and procedures appertaining to conditional access for the secondary delivery of digital television and data on cable systems.

Source

ITU-T Recommendation J.93 was prepared by ITU-T Study Group 9 (1997-2000) and was approved under the WTSC Resolution No. 1 procedure on the 18th of March 1998.

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

The ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. The ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, the ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

Recommendation J.93

REQUIREMENTS FOR CONDITIONAL ACCESS IN THE SECONDARY DISTRIBUTION OF DIGITAL TELEVISION ON CABLE TELEVISION SYSTEMS

(Geneva, 1998)

1 Scope

This Recommendation lists the requirements for the Conditional Access (CA) systems related to the secondary distribution of digital television and data signals over a cable television system. The actual conditional access features selected for implementation in a specific system should be derived from the system requirements for that system.

2 References

The following ITU-T Recommendations, and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; all users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

[1] ITU-T Recommendation J.83 (1997), *Digital multi-programme systems for television, sound and data services for cable distribution*.

[2] ITU-T Recommendation J.84 (1997), *Distribution of digital multi-programme signals for television, sound and data services through SMATV networks*.

3 Definitions

This Recommendation defines the following terms.

3.1 **algorithm**: A mathematical process which can be used for the scrambling and descrambling of a data stream.

3.2 **authentication**: The process intended to allow the system to check with certainty the identification of a party.

3.3 **authorization coding**: A digital word which describes the personality or service access capability of the subscriber decoder unit.

NOTE – This code word, which is based on the service access authorized by the billing system, determines which keys are distributed to each customer, and is required at the subscriber decoder to authorize the descrambling of any specific program.

3.4 **Conditional Access system (CA)**: The complete system for ensuring that cable services are accessible only to those who are entitled to receive them, and that the ordering of such services is not subject to modification or repudiation.

3.5 **cryptanalysis**: The science of recovering the plaintext of a message without access to the key (to the electronic key in electronic cryptographic systems).

3.6 **cryptographic duty cycle**: The maximum secure capacity of a cryptographic process, based on the total number of bits that can be securely encrypted before it becomes advisable to change the key.

3.7 **descrambling**: The process of reversing the scrambling function (see "scrambling") to yield usable pictures, sound, and data services.

3.8 **electronic key**: The term for data signals which are used to control the descrambling process in subscriber decoders.

NOTE – There are at least three types of electronic keys: those used for television signal streams, those used for protecting control system operations, and those used for the distribution of electronic keys on the cable system. See also "authorization coding" which is also effectively a key.

3.9 **encryption**: The process of scrambling signals to avoid unauthorized access.

3.10 **full period terminated service**: A subscription service that is always available to subscribers during the operating hours of the delivery system.

NOTE – By contrast, other services, such as a pay-per-view feature film, are only available for a specific period of time.

3.11 **host**: A device with generalized functionality where modules containing specialized functionality can be connected.

3.12 **integrity**: The ability of a function to withstand being usurped for unauthorized use, or modified to yield unauthorized results.

3.13 **intrusion resistance**: The ability of a hardware object to deny physical, electrical, or irradiation-based access to internal functionality by unauthorized parties.

3.14 **module**: A small device, not working by itself, designed to run specialized tasks in association with a host.

3.15 **non-repudiation**: A process by which the sender of a message (e.g. a request on a pay-per-view) cannot deny having sent the message.

3.16 **one-way hash**: A mathematical process or algorithm whereby a variable length message is changed into a fixed length digital word, such that it is very difficult to calculate the original message from the word, and also very difficult to find a second message with the same word.

3.17 **pay-per-view**: A payment system whereby the subscriber can pay for an individual program or specified period of time.

3.18 **piracy**: The act of acquiring unauthorized access to programs, usually for the purpose of reselling such access for unauthorized reception.

3.19 **public key cryptography**: A cryptographic technique based upon a two-key algorithm, private and public, wherein a message is encrypted with the public key but can only be decrypted with the private key. Also known as a Private-Public Key (PPK) system.

NOTE – Knowing the public key does not reveal the private key.

Example: Party A would devise such a private and public key, and send the public key openly to all who might wish to communicate with Party A, but retain the private key in secret. Then, while any who have the public key can encrypt a message for Party A, only Party A with the private key can decrypt the messages.

3.20 **scrambling**: The process of using an encryption function to render television and data signals unusable to unauthorized parties.

3.21 **secure signature**: A mathematical process by which the origin and integrity of a transmitted message can be ascertained.

NOTE – If a secure signature system is used, the originator cannot deny having sent the message, and the receiver can determine if the message has been modified.

3.22 **transport stream**: An MPEG-2 Transport Stream.

4 Background

With the advent of digital cable television and data, new standards are required for the Conditional Access (CA), or security, subsystem which performs the several functions associated with this system element. There are numerous standards activities directly addressing the conditional access of cable television and data signals currently in progress worldwide. There are other organizations which address security for these signals tangentially by targeting a larger issue which also includes television and data.

4.1 Television

Just as with analogue cable television transmissions today, there are varying requirements for the different types of digital television programming material which will be carried to the user's premises on cable delivery systems. These include:

- basic tier full period terminated subscription television services;
- premium channel full period terminated subscription television services;
- transaction coherent television services such as pay-per-view;
- short-term television which is part of a multimedia transmission for the purpose of marketing, commerce, or communications.

Cable delivery of television programming has the same basic security challenges found on broadcast, satellite, SMATV (Satellite Master Antenna Television), and Multichannel Multipoint Distribution Systems (MMDS), mainly resulting from the requirement to place an operational decoder with current keying material inside of the user's premises, one of whom happens to also be the pirate, where it can be subjected to sophisticated attack without fear of physical detection. In a traditional governmental or military symmetric key system, this is equivalent to giving the enemy the current cryptographic key. Physical measures, such as secure microprocessors, make the job more difficult, but no such countermeasures will delay the professional for long. Cable delivery has the advantage that in being a closed system, certain policies and procedures discussed below can be implemented to make the pirate's efforts unprofitable.

In setting CA requirements, attention must be paid to the assessments of risk and threats, and the capital and operational costs of recommended countermeasures. Risk refers to that which might be lost if the CA system were compromised. In the case of cable systems, the risk is the loss of system revenue through signal theft, or the usurpation of control of the system by an unauthorized party. The threat is the individual, organization, or mechanism by which the CA countermeasures are compromised and the risk incurred. All countermeasures, even if they are procedures only, represent some cost to the operating cable system. If the cost to negate the threat is too large relative to the risk, then it is not a workable option.

4.2 Secondary distribution of cable data

(For further study.)

5 Conditional Access requirements on cable systems

The general area of Conditional Access (CA), as applied to the secondary distribution of digital television and data on cable systems, can be subdivided and defined as shown in Table 1 below.

Table 1/J.93 – Conditional Access requirements and explanations

Conditional Access requirement	Explanation
Signal Security	Provides the encryption of the digital television signals and/or related messaging to prevent unauthorized access to the contents (see 5.1)
Key Distribution	Refers to that subsystem which generates, distributes and stores the cryptographic keys for the headend encoders and for the customer premises decoders (see 5.2)
Secure Signature	The process by which user authentication and transactional non-repudiation are accomplished (see 5.3)
Control System Integrity	Prevents the usurpation of system control by an unauthorized entity (see 5.4)
Authorization Coding	A process whereby the access personality of the subscriber decoding unit is protected against unauthorized modification (see 5.5)

5.1 Signal security requirements

It is required that any digital television or data channel carried on a cable operating system be subject to scrambling via digital encryption, at the option of the system management. Access to all differentiated services should be controlled by a scrambling process. The following general requirements apply to such cryptographic processes:

- the cryptographic process chosen should operate in a Private-Public Key (PPK) mode, a symmetric key mode, or should use PPK processes to distribute secret keys for specific transactions;

- the cryptographic engine selected for the scrambling and descrambling of a television or data stream associated with a single RF carrier should be applicable to the distribution systems described in Recommendations J.83 [1] and J.84 [2];

- the duty cycle of the cryptographic process supporting scrambling should be sufficient to meet good cryptographic design criteria;

- the cryptographic algorithm selected for scrambling should be one which is sufficiently robust to make direct cryptographic attack both initially and subsequently by a third party cost and time ineffective;

- operating characteristics of the cryptographic process such as error extention, latency, data rate, data rate dialation, and interface parameters should be optimized to the MPEG-2 or data transport stream characteristics, as appropriate;

- the cryptographic algorithm selected for signal scrambling should be approved for use worldwide;

- control system overhead required for continuous operation of the scrambling algorithm should be minimized;

- the algorithm should be designed in such a fashion as to facilitate the hardware, software, and firmware diagnostic entry points needed for intensive security system audits and tamper countermeasures.

5.2 Key distribution and storage requirements

The root element of all CA systems is the binary cryptographic key which is used in conjunction with the other hardware and software elements of the CA system to limit access to the content to authorized users only. Key may be assigned to a group or tiering of television services consisting of several channels scrambled with the same key. Key may also be assigned to an individual television channel, as in the case of a separate premium programmer. A key may also be assigned to an individual television channel, but only for a pre-determined period of time, as in the case of pay-per-view services. Therefore, it is required that the CA mechanism have the ability to store multiple keys as required.

In addition to the above operational keys, each encoder or decoder should have the capability to store a permanent and unmodifiable binary unique identification number which can be used for identification of the unit or as a type of key for the narrowcasting of signals to that unit. For television, it may be required that the encoders and decoders have the ability to store and utilize additional keys as may be required for system compartmentalization to lessen the risk resulting from subscriber/pirates, an example of which may be a trunk-coherent key system whereby some piece of key is changed according to the trunk address of the subscriber. The exact number and nature of these system-coherent keys is a feature left to the vendors of CA products for specification.

All keys, whether operational, of the unique identifier type, or system-coherent, should be stored in intrusion resistant circuitry which is cost prohibitive to access by physical or electrical means, by irradiation, or by cryptographic methodology.

The length of any key is dependent upon the unique characteristics and weaknesses of the selected cryptographic algorithm, but should be sufficiently long to protect against known attacks of the cryptographic system for a period which is sufficient to meet individual system operational security requirements.

The actual required data rate for the transmission of keying material depends upon the rekeying cycle requirements, the size of the keyed universe, the number of operational keys utilized, and the length of the individual keys. These design specifications should be clearly stated in any description of a CA system destined for cable system usage.

Key distribution may be accomplished in-band via data packets within the MPEG-2 packet stream, or out-of-band by a stand-alone data carrier on the system. In either case, the key distribution transmissions represent a high value target for the signal pirate and must be protected to a degree considerably beyond that required for television signal security. If the algorithm selected for signal security does not provide that degree of protection, then another algorithm must be utilized for key distribution. Under all circumstances, a separate key is used for the protection of the key distribution system. The protection of the keying material must be sufficient to withstand compromise for a period consistent with the security requirements of the individual cable operating system.

5.3 Secure signature

The secure signature uniquely guarantees that received messages come from the source indicated, that they have not been modified, and that the sender cannot repudiate having sent the message. This process should protect control and ordering messages which may be sent in either direction on the cable network.

There are several well-known examples of this kind of functionality, including but not limited to the RSA (Rivest-Shamir-Adleman) or DSA (Digital-Signature-Algorithm) algorithms. These systems include a secure one-way hashing algorithm which reduces the arbitrary length message to a fixed length hash which is highly unique to the original message, and has the following characteristics:

- given any message, it is quick and easy to calculate its unique hash;

- given any hash, it is virtually impossible to calculate the original message;

- given any message and its unique hash, it is virtually impossible to find another message which generates the same hash.

Certain classic attacks on hashes effectively limit the number of analytic operations to attack the algorithm to about $2^{(1/2 \text{ hash length})}$. This means that a hash of 64 bits could be broken with 2^{32} operations, perhaps an hour's work for a modern high-speed personal computer. For this reason, any hash used for the secure signature function on a cable system should be of sufficient length to meet system operational requirements.

5.4 Control system integrity

This functionality is implemented to assure that the control system cannot be entered by unauthorized parties for the purpose of signal theft or disruption of services. Control signals wherein the risk of theft or disruption is reasonably low are encrypted in their normal form for transmission to an individual decoder, a group of decoders, or globally to all decoders on the system. Control messages which are of high value may be subjected to additional countermeasures. The control system requires a separate and unique key from those used for either signal security or key distribution.

5.5 Authorization coding

In addition to the process of cryptographically protecting programming material, a secure process for setting the entitlement or authorization of each individual subscriber is required. In the headend, this service personality determines which cryptographic keys are authorized for downloading to each subscriber, and serves in the subscriber unit as a protection against the unauthorized insertion of pirated cryptographic keys from an external source. It may be implemented by any of a number of techniques.

6 Manufacturing and distribution security

Hardware which is manufactured for the CA of digital television and data signals on cable systems are required to meet certain practices to ensure the integrity of their systems. These are:

- all integrated circuit design and test vector documentation will be numbered and audited on a regular basis with any missing pieces documented for the examination of potential customers;

- all manufactured integrated circuits for use in CA hardware will be audited and every piece documented as to its final disposition, including its integration in a host device and the host's serial number, its distribution path, and the identification of the cable operating system wherein it is operating. Additionally, all integrated circuits will be marked with an unchangeable unique identification number which is both physically and electrically readable.

7 Failure and compromise recovery

For financial, operational, and security reasons, it is required that the CA circuitry or software be easily removable and replaceable, without having to also replace the host device(s) with which it interacts. Such replacements may be necessary because of failure of the mechanical, electrical, or software elements of the CA functionality, because changing business and architectural structures requires new or different functionality, or because some attack, which has led to a cost-effective compromise of security, has been devised and deployed, resulting in the unacceptable loss of system revenues or control.

Removability implies that all of the CA circuitry and software be contained within a module which interfaces with a host device, such as a set top or set back decoder unit, a television receiver or VCR, a data modem, or a personal computer. Replaceability means that there are no interface, operational, legal, or financial factors which would make replacing the CA functionality impossible.

To meet these requirements, the interface between the removable CA module and the host device must be non-proprietary and open in architecture. There are a number of such interfaces and module form factors commonly defined for other international applications which may be appropriate in this instance, for example the DVB common interface specification (see [I.3]) or the specification defined by the National Renewable Security Standard (see [I.4]). (For further study.)

8 Key escrow provision

If the national law of any country requires the inclusion of a key escrow capability within the CA system, then functionality should be included to implement such. At the time of this Recommendation, no such requirement exists in any country which is a treaty member of the ITU.

9 Policies and procedures

No cryptographic system is truly secure without a set of underlying policies and operational procedures which support the function. How these policies and procedures are implemented in a given cable operating system is situationally dependent. Therefore, the following guidelines should be taken as recommended practices and adapted to each operational situation as required:

- personnel who have access to the CA control system at the cable headend or regional hub, or who routinely handle subscriber units, should fall under a human reliability program;

- access to key elements of the CA system should be restricted and surveillence of such areas maintained;

- large cable systems or conglomerations should be compartmented by cryptographic procedures to reduce the market area of subscriber/pirates;

- unproven CA systems which are being considered for purchase should be submitted to an independent certifying agency for testing;

- a system of regular security audits should be initiated and maintained;

- procedures should be in place so that if an active illegal CA unit is captured, the identification of the pirate/subscriber can be ascertained by examination of the unique identifier in the unit and its authorization code.

Appendix I

Bibliography

The following regional and international standards are included herein as applicable background information:

[I.1] ISO/IEC 13818-1:1996, *Generic coding of moving pictures and associated audio information: Systems*.

[I.2] ISO 7816: *Identification Cards*, Parts 1-6.

[I.3] Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, *DVB A007*, July 1995.

[I.4] National Renewable Security Standard, *EIA/NCTA IS-679*, Parts A and B.

[I.5] Digital Video Broadcasting – Support for use of Scrambling and Conditional Access with Digital Broadcasting Systems, *EBU*.

[I.6] CCIR Report 1079-1 (1990), *General Characteristics of a Conditional Access Broadcasting System*.

[I.7] ITU-T Recommendation J.81 (1993), *Transmission of component-coded digital television signals for contribution-quality applications at the third hierarchical level of ITU-T Recommendation G.702* .

[I.8] ITU-T Recommendation J.91 (1994), *Technical methods for ensuring privacy in long-distance international television transmission*.

[I.9] ITU-T SG 9 Delayed Contribution D.19 (1997-2000): *The conditional access system of digital cable television in Japan*.

ITU-T RECOMMENDATIONS SERIES

Series A	Organization of the work of the ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communication
Series Y	Global information infrastructure
Series Z	Programming languages