International Telecommunication Union

ITU-R

Radiocommunication Sector of ITU

Recommendation ITU-R BT.1852-1

(10/2016)

Conditional-access systems for digital broadcasting

BT Series

Broadcasting service (television)

Foreword

The role of the Radiocommunication Sector is to ensure the rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services, including satellite services, and carry out studies without limit of frequency range on the basis of which Recommendations are adopted.

The regulatory and policy functions of the Radiocommunication Sector are performed by World and Regional Radiocommunication Conferences and Radiocommunication Assemblies supported by Study Groups.

Policy on Intellectual Property Right (IPR)

ITU-R policy on IPR is described in the Common Patent Policy for ITU-T/ITU-R/ISO/IEC referenced in Annex 1 of Resolution ITU-R 1. Forms to be used for the submission of patent statements and licensing declarations by patent holders are available from http://www.itu.int/ITU-R/go/patents/en where the Guidelines for Implementation of the Common Patent Policy for ITU-T/ITU-R/ISO/IEC and the ITU-R patent information database can also be found.

Series of ITU-R Recommendations

(Also available online at http://www.itu.int/publ/R-REC/en)

Series	Title
BO	Satellite delivery
BR	Recording for production, archival and play-out; film for television
BS	Broadcasting service (sound)
BT	**Broadcasting service (television)**
F	Fixed service
M	Mobile, radiodetermination, amateur and related satellite services
P	Radiowave propagation
RA	Radio astronomy
RS	Remote sensing systems
S	Fixed-satellite service
SA	Space applications and meteorology
SF	Frequency sharing and coordination between fixed-satellite and fixed service systems
SM	Spectrum management
SNG	Satellite news gathering
TF	Time signals and frequency standards emissions
V	Vocabulary and related subjects

Note: *This ITU-R Recommendation was approved in English under the procedure detailed in Resolution ITU-R 1.*

Electronic Publication
Geneva, 2017

RECOMMENDATION ITU-R BT. 1852-1

Conditional-access systems for digital broadcasting

(Question ITU-R 49-1/6)

(2009-2016)

Scope

This Recommendation describes principles intended to facilitate the development of effective conditional-access methods for digital broadcasting that uses either MPEG-2 transport streams or MPEG media transport protocol (MMTP). It provides information on reliable protection of broadcasting services from unauthorized access.

Keywords

Conditional access, scramble system, access control, content protection, MPEG-2 TS, MMT

The ITU Radiocommunication Assembly,

considering

a) that there is a growing demand in many countries to protect broadcast programmes against unauthorized reception;

b) that an efficient way of ensuring such protection of MPEG-2 transport stream packets, multiplexed according to Recommendation ITU-T H.222.0, is to implement conditional-access broadcasting systems;

c) that an efficient way of ensuring such protection of MMTP packets formed on the basis of Recommendation ITU-R BT.2074 is to implement conditional-access broadcasting systems;

d) that examples of conditional-access systems have been designed and are operated for digital terrestrial, digital cable, digital satellite and IP (Internet Protocol) television, as well as sound, multimedia and data services;

e) that there are many cases of implementing digital broadcasting systems based on relevant BT and BO Series Recommendations, such as Recommendation ITU-R BO.1516 for satellite digital broadcasting systems;

f) that it is desirable to limit the number of different conditional-access systems, while taking into account the different requirements of various broadcast services and transmission systems;

g) that putting as many common elements of conditional access as possible into the receivers at the outset would give the greatest potential to the general public to access protected services at a reduced equipment cost;

h) that conditional-access systems provide a protection against and that copyright owners, programme suppliers and service providers desire highly secured broadcast/distribution networks to allow protection of their programmes through access control,

recommends

1 that conditional-access systems for digital broadcasting services protecting either MPEG-2 transport stream packets or MMTP packets should:

– provide the services available to authorized receivers only;

– share the largest number of common elements in the receiver; and

– be designed according to the fundamental principles listed in Annex 1.

NOTE 1 – Examples of implementations of conditional-access systems for digital broadcasting are given in Annex 2.

Annex 1

Fundamental principles for the design of conditional-access systems for digital broadcasting

1 Introduction

The principles described in this Annex should facilitate the development of effective conditional-access systems for digital broadcasting that are convenient for both subscribers and service providers, assuring reliable protection of information from unauthorized access.

The principles apply generally to the delivery of digital television services, sound services as well as multimedia and data broadcasting services. These principles apply to both Recommendation ITU-T H.220.0 transport stream packet and MMTP packet delivery to consumers over different media, such as digital terrestrial, digital cable, digital satellite and IP (Internet Protocol) broadcasting.

2 Normative references

Recommendation ITU-T H.222.0 | ISO/IEC 13818-1 – Information technology – Generic coding of moving pictures and associated audio information: Systems

Recommendation ITU-R BT.2074 – Service configuration, media transport protocol, and signalling information for MMT-based broadcasting systems

3 Terms, definitions and abbreviations

3.1 Terms and definitions

Scrambling in digital broadcasting

Cipher encoding of broadcast content including vision/sound/data in order to prevent unauthorized reception of the information in non-encrypted format. This cipher encoding is a specified process under the control of the conditional-access system (sending end).

Descrambling in digital broadcasting

Cipher decoding of broadcast content including vision/sound/data in order to allow reception of the information in non-encrypted format. This cipher decoding is a specified process under the control of the conditional-access system (receiving end).

Conditional access

A user accesses a protected service by interacting via conditional-access functionality in the receiver. If, in the session, all the access conditions are met, authorization occurs, the cipher decoding key is released, and the content is recovered.

Subscriber authentication, account confirmation, and validation of service availability or other programme control parameters activate the session encryption/decryption key to let the session conclude the authorization process.

Conditional-access control

The function of the conditional-access control at the sending end is to generate the scrambling control information and the encryption "keys" associated with the service.

The function of the conditional-access control at the receiving end is to produce the descrambling control information in conjunction with the "keys" associated with the service.

Encryption and decryption

These are terms used for methods which are used to protect (and interpret) some of the information within the "access-related messages" which have to be transmitted from the sending end to the receiving end of the conditional-access control functions.

Point of origination

This is the point in a distribution system where programme or other content first becomes a signal in its final broadcasting/distribution format. It marks the start of end-to-end protection. Entry content may be any form, not necessarily a humanly sensible form. The content input need not itself be intelligible.

NOTE 1 – The copyright owners, service providers, and distributors form a huge hierarchy of many possible points of origination in a flow of information to a consumer and thus in the flow of scrambled content and encrypted keys to a consumer. The point of origination ought to begin with a copyright holder or producer. In practice, most points of origination will be simply the points of entry wherever they may be in the system for business and operational reasons. While there may be many such points of entry, each is a unique and independent point from which the information can be consistently maintained in whatever format it may be input all the way through to a consumer.

Point of presentation

This is the point where programme or other content last occurs as a signal in a distribution system before it exists in a humanly sensible form at the receiver's screen and speakers. It marks the output from protection.

Content

This is any form of digital data that can be acquired and presented by a device.

Service

This is one or more data flows intended to be presented together.

Service protection

This is protection of a service such that only authorized devices are able to receive and decode it.

3.2 Abbreviations

Ks Scrambling key

Kw Work key

Km Master key

EMM Entitlement management message

ECM Entitlement control message

CRC Cyclic redundancy check

DES Data encryption standard

AES Advanced encryption standard

CBC Cipher block chaining

CTR Counter

MAC Message authentication code

MMT MPEG media transport

MMTP MPEG media transport protocol

OFB Output feedback

RMP Rights management and protection

4 General description of a conditional-access system

There are two fundamental functions that comprise conditional-access systems for digital broadcasting; scrambling and access control. They are distinct, and in many cases independent, components in a conditional-access system, each of which is a distinct information process.

4.1 Reference model

Conditional access requires that the information be *scrambled* before it is broadcast. This process is obtained by using cipher encoding to broadcast bit-stream.

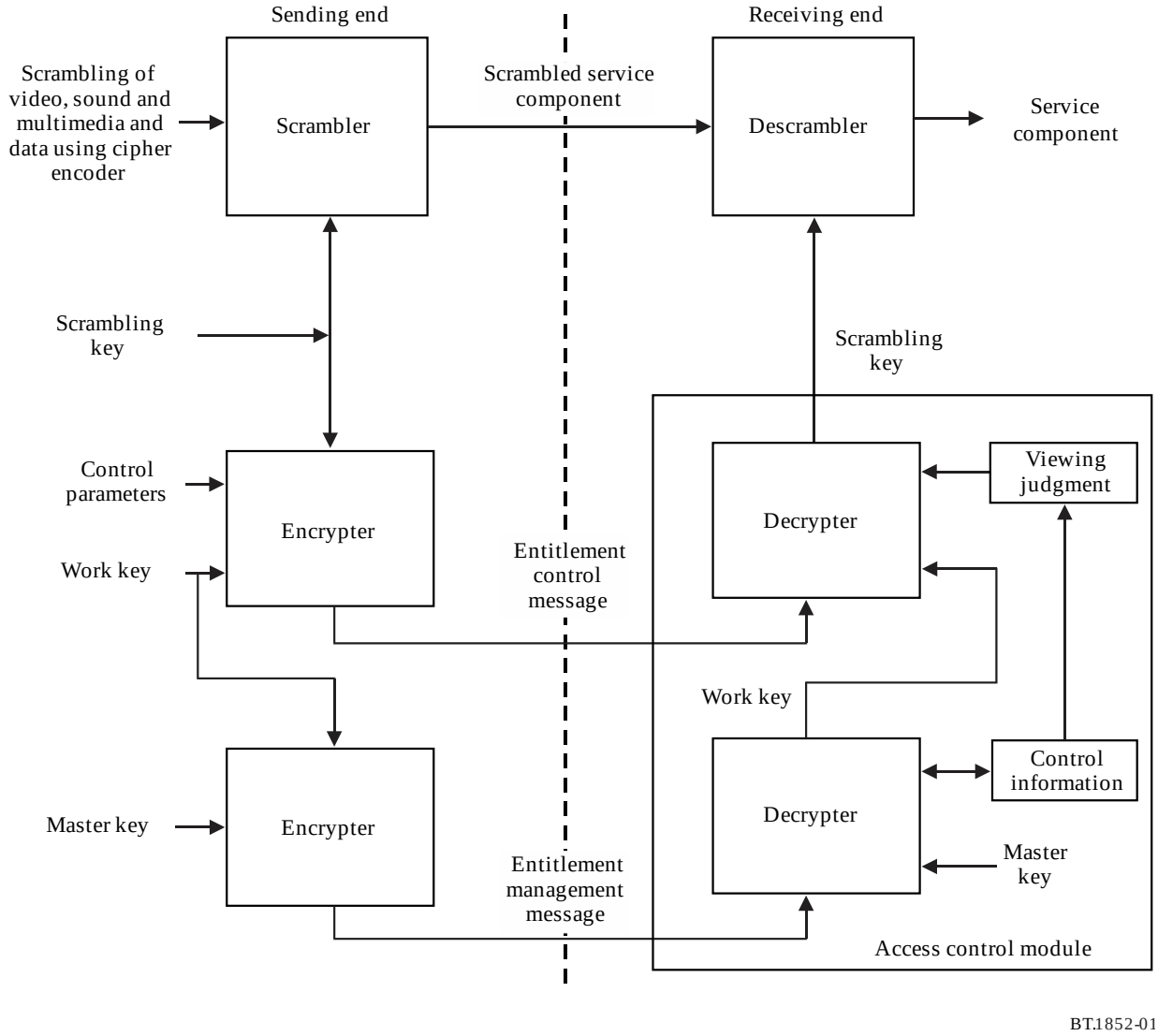
The descrambling process at the receiving end requires the same cipher decoding (in this case the descrambling procedure) to recover the original bit-stream.

To provide this sequence and to ensure synchronism between the sending and receiving processes, the cipher decoding conditions are controlled by a data transmitted from the cipher encoder to decoder according to special protocol.

The detailed structure of this process is given in Fig. 1.

FIGURE 1

An example of block diagram of a conditional-access system for digital broadcasting



BT.1852-01

4.2 Scrambling

This is the process of protecting some or all components of a service to cope with unauthorized accesses by using cipher encoding under the control of the conditional-access system at the sending end.

4.3 Access control

This is a provision of information to enable authorized users to descramble the protected service. The availability of this information is controlled by the conditional-access system.

Between the transmitter and the receiver(s), this information is structured in special messages, which may be multiplexed within the broadcast bit-stream itself, or may be delivered by some other means, such as over a telecommunication line.

At the receiving end(s), these messages are interpreted by the access-control system in order to control the descrambling of the authorized parts from received bit-stream in the authorized receiver(s).

5 User requirements

5.1 Anti-hacking strength of a cipher for scrambler and descrambler

A cipher used in scrambler and descrambler blocks should be well tested for anti-hacking capability. A cipher selected from international standards is recommended.

5.2 Security

The security of a system is the degree of difficulty encountered by an unauthorized user in attempting to gain access to the protected service.

– *Descrambling the signal without reference to the access control process*. This is a function of the nature of the services and the scrambling method. Television, sound and data broadcasting services are predominantly digital in nature and thus will allow for highly secure scrambling processes.

– *Obtaining the access control key in an unauthorized manner*. This is a function of the security of the key encryption algorithms.

5.3 Selection of common or private scrambling algorithm

Access is made available, to any authorized user meeting the conditions for access, via a common (universal) or private scrambling algorithm.

The use of a common scrambling algorithm implies that descrambling would be common to all receivers, based on a standard scrambling algorithm, independent to delivery media used, permits lower cost and flexible equipment and would still allow competition through service-provider-specific implementations.

The use of private scrambling algorithm implies that the descrambling process would be carried out on the receivers with specific algorithm implemented only.

5.4 Access modes

A conditional-access system may support a range of access modes, for example:

– period availability (subscription of the service) – authorization runs from a starting time to a finishing time;

– programme or service item (purchase of an event) – availability is for a specific service item, whether or not it is completely used;

– service charge (token based) – the charge or use of credit is proportional to the duration of use and/or the value of the service involved;

– free-to-air – service is protected, but the access is provided free of charge.

The access modes need to be variable with respect to several parameters, for example:

– time;

– various segments of the service;

– groups of intended users.

5.5 Equipment standardization

To provide maximum economy of manufacturing scale for receiving equipment and to simplify management and maintenance:

– common equipment should be standardized so that it can cater for as many service options as possible;

– A consumer's receiver architecture is required to support the conditional-access functionality requirements of the selected conditional-access system. Depending on the selected system, the functionality may require support such as embedded or detachable security functionality (e.g. smart card).

5.6 Access management

The definition of conditional access is based on the formal concept of *entitlement* to access, which can be implemented in various forms. An entitlement gives to its holder an *authorization* to access the related service. Uneconomic use of the resources due to management or transmission overheads should be avoided.

5.7 Avoidance of interruptions to the service

Interruptions due to faulty or unreliable acquisition of the access control data should be avoided.

6 Entitlement control messages (ECMs)

ECM provides the scrambling key to descramble the protected service.

Access on the scrambling key in ECM is controlled by means of entitlements, or rights, provided in EMM.

Typically ECM is provided in the broadcast stream, together with the protected service.

The scrambling keys are usually changed frequently to minimize the harm caused by scrambling key leaking.

The content of ECM is system specific.

7 Entitlement management messages (EMMs)

The processing of an entitlement management message validates or provides the entitlement required to descramble the protected service. EMM may contain a work key to provide encryption and decryption of the scrambling key. Messages and/or work keys addressed to individual receivers are encrypted. The encryption may use the master key. The master key may be stored in the receiving device.

In conditional-access systems for digital broadcasting, the entitlement management messages are distributed over the broadcast or by other media.

– Distribution over the broadcasting services is known as "over-the air addressing". The cycle time associated with the distribution of over-the air keys may be reduced by the application of the principles of shared key encryption. The entitlement management messages may also be distributed by other media.

– Distribution over another media typically is accomplished over a point-to-point connection, thus providing an additional security measure to ensure the messages are accessed by the targeted devices only.

Following is an example of operation:

In the case of payment, per unit of time or per programme, the management messages can convey an encrypted cost code, transmitted as part of the service. The credit may be held in the receiver and may take the form of encrypted money tokens which are transmitted as part of an over-the air addressing service. Alternatively credit may take the form of stored money tokens distributed by other means. Payment consists of decrementing the stored credit according to the received cost code.

The content of EMM is system specific.

8 Receiver access control functionality

At the receiving end, the conditional access may be introduced in many ways, including the following are:

Type 1: The security functionality (that may include key encryption algorithm and master keys) and the descrambling functionality are carried out in the receiver.

Type 2: The security functionality is detachable (for example, smart card) and the descrambling functionality is carried out in the receiver.

Type 3: The security and descrambling functionality are detachable; all the functions performing input data stream restoration are implemented in a detachable module, communicating with the receiver through a standardized interface (for instance, Common Interface); in this case any receiver with such interface may be used.

When requested, security functionality checks for conditions, and if met, provides the scrambling key to the descriptor. These conditions may include:

– a time period requirement, with the date in the control parameter falling between the starting and expiry dates in the authorization parameter;

– a price requirement by which an authorization may be provided only if a charge is accepted by the security module.

A conditional-access system may realize a transaction involving the security functionality which includes different stages, such as:

– preliminary instructions, if present (e.g. password, user acceptance, etc.);

– operating instructions using the security module;

– result processing (e.g. delivery of scrambling word).

Annex 2 (informative)

Examples of the implementation of a conditional-access system for digital broadcasting

TABLE 1

Examples of the implementation

Reference in Annex 1	"Roscrypt" system	"CAS-R" system	"ARIB B61-CAS"	"IEC 62455 with DVB systems"
§ 4 Type of cipher for scrambler and descrambler	Based on Russian Federation State Standard 28147-89	MULTI2 (ISO/IEC 9979)	– AES (128-bit key length) (ISO/IEC 18033-3) – Camellia (128-bit key length) (ISO/IEC 18033-3)	DVB-CSA or AES-128 (mandatory for devices); also DES, 3DES and MULTI2 are possible (optional for devices)
§ 4 Scrambling process	Cyclical multi-step transition based on shift registers using polynomials of 64th Based on non-linear algorithms and is practically a random sequence (does not have an analytic form)	a) For 64-bit encoded sequences, the original encoding is replaced with another binary code string using 64- and 256-bit variables b) For code strings of less than 64 bits, the method described in a) above is used to generate a series of pseudo-random encoded sequences, which are combined to create the scrambled signal	– For MPEG-2 TS packets, CBC+OFB mode – For MMTP packets, CTR mode	DVB-CSA: according to ETSI ETR-289; AES-128: according to FIPS PUB 197:2001 using ECB or CBC mode; DES or 3DES: according to FIPS PUB 46-3:1999 and FIPS PUB 81:1980; MULTI2 according to ISO/IEC 9979
§ 4 Synchronization of scrambling process	Mutual synchronization of random sequence and DVB stream shaping circuits	Associated information in ECMs (programme and control information), EMMs (individual information), EMM common messages, and EMM individual messages are used in order to synchronize the scrambling process	Associated information in ECMs (programme and control information), EMMs (individual information), EMM common messages, and EMM individual messages are used in order to synchronize the scrambling process	Odd_even_flag and initial_vector are included in the key stream message delivering the Traffic Encryption Key to facilitate the synchronization. Corresponding values of transport_scrambling_control bits and pes_scrambling_control bits indicate which key is to be used at a given time

TABLE 1 (*continued*)

Reference in Annex 1	"Roscrypt" system	"CAS-R" system	"ARIB B61-CAS"	"IEC 62455 with DVB systems"
§ 6 Entitlement control messages (ECM)	ECM content: – Work key identifier – Scrambling key (odd/even) – Encrypted counter and cryptographic checksum DVB stream structural redundancy or additionally assigned reserves are used	ECM section and its basic architecture of the ECM payload: – The entire ECM section is subject to a section CRC – The ECM payload consists of a fixed part that is always transmitted and a variable part whose content varies by transmission objective – Only necessary ECM function information is inserted into the variable part of the ECM	ECM section and its basic architecture of the ECM payload: – The entire ECM section is subject to a section CRC – The ECM payload consists of a fixed part that is always transmitted and a variable part whose content varies by transmission objective – Only necessary ECM function information is inserted into the variable part of the ECM	The ECM carries a key stream message, which includes fields for carrying the following information: – content_key_index – odd_even_flag – cipher mode – next_initial_vector – encrypted_traffic_key_material – traffic_key_lifetime – timestamp – access_criteria_descriptors – permissions_category – encrypted_programme encryption key – programme_CID_extension – programme_MAC – service_CID_extension – service_MAC Which of these fields are included in a particular key stream message depends on several factors, e.g. whether the service provider wants to enable access on an individual programme basis

TABLE 1 (*end*)

Reference in Annex 1	"Roscrypt" system	"CAS-R" system	"ARIB B61-CAS"	"IEC 62455 with DVB systems"
Master Key	256 bits	Master Key length depends on service operator.	Master Key length depends on service operator.	There is no "Master Key" as such. Protection of service encryption keys (SEK) or programme encryption keys (PEK) is based on RSA keys, which have 1 024, 2 048 or 4 096 bits, depending on the trust authority. In the broadcast mode, the 128-bit inferred encryption key (IEK) has a similar role. It is derived from a set of keys which are delivered to the receiver during registration. Protection of the keyset is based on 1 024, 2 048 or 4 096 bits RSA keys
§ 6 Change of scrambling key and flag	Scrambling key is changed as necessary. All the four states of scrambling flag are used	Scrambling keys (Odd/Even) are changed typically every two seconds	Scrambling keys (Odd/Even) are changed every more than one second	The traffic encryption key changes frequently in the order of once per minute to once per second
§ 7 Entitlement management message (EMM)	EMM content: – Protocol number – Broadcaster group identifier – Work key – Programme identifier – Security module identifier – Access rights – Encrypted counter and cryptographic checksum – DVB stream structural redundancy or additionally assigned reserves are used	The EMM section can carry multiple payloads. – The entire EMM section is subject to CRC error detection. – The EMM payload consists of a fixed part that is always transmitted and a variable part whose content varies by transmission objective. – Only necessary EMM functional information is inserted into the variable part of the EMM. The card ID (6 bytes) and the associated information byte length (1 byte) are sent at the beginning of the EMM fixed part (unencrypted part). The receiver filters this area to identify EMM payloads addressed to itself	The EMM section can carry multiple payloads. – The entire EMM section is subject to CRC error detection. – The EMM payload consists of a fixed part that is always transmitted and a variable part whose content varies by transmission objective. – Only necessary EMM functional information is inserted into the variable part of the EMM. The device ID (8 bytes) in the RMP case or the module ID (6 bytes) in the CAS case, and the associated information byte length (1 byte) are sent at the beginning of the EMM fixed part (unencrypted part). The receiver filters this area to identify EMM payloads addressed to itself	In the interactive mode, OMA DRM 2.0 Rights Objects are used instead of Entitlement Management Messages to deliver rights and service encryption keys (SEK) or programme encryption keys (PEK) to the receivers. They are delivered over an interactivity channel. In the broadcast mode, special binary version (called BCRO) of these Rights Objects is used

TABLE 1 (*end*)

Reference in Annex 1	"Roscrypt" system	"CAS-R" system	"ARIB B61-CAS"	"IEC 62455 with DVB systems"
§ 8 Access control functionality	It is inside the Conditional Access Module (CAM) or built into the STB	Type 2: Security module is detachable and descrambling module is built into the receiver	Type 1: Security and descrambling modules are carried out in the receiver. Type 2: Security module is detachable and descrambling module is built into the receiver	Type 1 is anticipated, but other implementations are not ruled out, either
Encrypted counter and cryptographic checksum	ECM, EMM	MAC (message authentication code) is included in both ECM and EMM packets	MAC (message authentication code) is included in both ECM and EMM. The MAC can be added to each MMTP packet as well.	MAC (message authentication code) is included in key stream messages and broadcast mode rights objects. Interactive mode rights objects are protected with a signature
§ 8 Security functionality	It is inside the Conditional Access Module (CAM) or built into the STB	Mutually authenticated between smartcard and receiver	Mutually authenticated between smartcard and receiver for Type 1 and Type 2. In the case of Type 1, security of the access control system can be maintained and improved by downloading and updating it.	Implementation is not dictated by the standard. Compliance and robustness rules are set by the trust authority

1 Description of "Roscrypt" system

A conditional-access system (CAS) "Roscrypt" is being implemented at the present time in Russia in connection with the conversion to digital TV broadcasting. The "Roscrypt" system is designed to protect DVB data streams against unauthorized receiving. It possesses a wide range of utilization with the different DVB chains of satellite and terrestrial broadcasting and flexibility in managing their subscribers.

The "Roscrypt" system consists of:

- the *scrambler*, which performs an encryption of preselected DVB transport stream components; it can work autonomously and under PC control;
- a *CAM-module*, inserted into the receiver common interface (CI) slot to descramble selected components;
- a *security module*, which has a built-in Set-Top-Box.

The equipment needed for working of the common control and monitoring system is installed at the sending end.

"Roscrypt" solves the following problems:

- broadcasting limitation within the country area to protect the rights of programme owners to limited broadcasting;
- protection of corporate and departmental broadcasting against unauthorized access;
- organization of commercial broadcasting.

"Roscrypt" takes into account characteristic features of the chains protected against unauthorized access.

1.1 Functional and technical features of "Roscrypt":

- Common working model of CAS "Roscrypt" corresponds to Fig. 1 of Annex 1.
- *Scrambling algorithm*: There are two private scramble algorithms, which were realized in CAS "Roscrypt" scramble and descramble. The operator can change the current scramble algorithm at any point.
- *Security keys*: The following keys are used in CAS "Roscrypt":
  - The scrambling key and work key provide scramble/descramble of content.
  - The base of unique master keys provides ECM deciphering (work key) and access control under the subscriber.
  - The programme keys group allows the isolation of subscribers of different operators from each other and the division of all subscribers by any criterion.
  - Operators can make a quick change of keys without physical and electronic distribution.
- *Access mode*: There are two access modes to effectively manage the subscribers: period availability, programme and service item.
  - Access mode parameters: subscriber manage time is 1 000 subscribers per sec; the number of subscribers is not limited; the number of scrambling components is 150; groups of intended users – 64 000.

– *EMM and ECM*: The structure of EMM and ECM signals is in accordance with §§ 6 and 7 of Annex 1.
  – There is an encrypted counter and cryptographic checksum at the end of each EMM and ECM packet.
  – For managing commands (EMM and ECM) delivery both additional resources of DVB stream bandwidth and structural speed reserves (structural redundancy) of DVB transport stream can be used.
– *Receiving equipment*: Two types of conditional-access system "Roscrypt" are possible at the receiving side:
  – A security module, that includes a key decryption algorithm of security keys and a descrambling module, is built into the Set-Top-Box.
  – A conditional access module (CAM) that includes security and descrambling modules, communicating with the receiver through a standardized common interface (CI), is detachable. The single CAM module can restore scrambled components of input transport stream simultaneously.

1.2 Other:

– A single transmitting equipment set "Roscrypt" can encipher content of several independent providers. This property is used for large satellite and terrestrial broadcasting operators.
– The common control and monitoring system allows controlling subscriber access to content.
– The common control and monitoring system allows a remotely centralized operation and the monitoring of transmitting equipment set "Roscrypt" all over the net. This property is used for large satellite and terrestrial broadcasting operators.

2 Description of "CAS-R" system

2.1 Purpose of the system

ARIB STD-B25 addresses a conditional-access control system for use in digital broadcasting, defining scrambling and associated information specifications as well as related reception specifications for a system that provides control during signal reception (called "CAS-R" hereinafter).

This standard specifies the CAS systems for both terrestrial and satellite digital broadcasting systems currently used in Japan.

2.2 Requirement of CAS-R and its deliberative systems

ARIB STD-B25 specifies CAS systems to fulfil the following requirements:

1 The maximum number of subscribers:

The system can be expanded for providing customer management functions for all households in the coverage area.

2 System lifetime:

The system can be managed by supporting applicable broadcast media.

3 Anti piracy:

The system offers advanced security functionality and can take measures in the event of a security attack.

4 The systems are applicable to all digital broadcasting systems in the specific area.

5 Reception types:

a) Real-time reception including A/V streaming and data broadcasting using file format. (CAS-R).

b) Stored reception (non-real-time reception).

c) Recorded reception (including reserved reception).

6 The system can be applied to the following fee structures; flat/tier, pay per view (Impulse PPV (IPPV)), and free of charge.

2.3 Requirement for security module

1 Associated information encryption:

The encryption system uses three layered architecture with DES-equivalent and private keys. From the perspective of implementation on a smart card, the encryption system should feature a compact programme size and be conducive to high-speed processing using at least an 8-bit microcontroller.

2 Administration functionality:

The system may change the encryption protocol in order to counter piracies.

3 A mutual authentication should be implemented between smart card and receiver:

When using the CAS smart card to eliminate receivers that do not respond to rights protection information in applications using this conditional-access system as a rights protection technology for digital broadcasting, a system is provided for mutual authentication between this smart card and the receiver.

2.4 A detailed description of the system is provided in the following document

The specifications of the ARIB STD B-25 conditional-access system can be found at: http://www.arib.or.jp/english/html/overview/doc/6-STD-B25v5_0-E1.pdf.

3 Description of ARIB STD-B61 based second-generation CAS (ARIB B61-CAS)

3.1 Characteristics of system

ARIB STD-B61 specifies a scramble system, content protection system, and CAS program download system for digital broadcasting as the second-generation CAS. The following are characteristics of the second-generation CAS:

– supports both MPEG-2 TS and MMT as the underlying media transport protocol;

– supports 128-bit length AES and Camellia as the cipher algorithm;

– supports secure transmission of associated information;

– has the capability of continuously maintaining and improving the security level of an access control system by the download mechanism of CAS programs.

3.2 Requirements for system

1 Requirements for scrambling sub-system

– The sub-system provides advanced security functionality and can take measures in the event of a security attack.

2 Requirements for associated information sub-system

- Associated information is a common format to the utmost extent.
- Information for individual receivers can be transmitted.
- Associated information can be transmitted securely.
- The security of an access control system can be maintained and improved continuously.

3.3 Scrambling sub-system

In the scrambling sub-system, two cipher algorithms are selected in order to maintain high level of security of the system: 128-bit length AES or Camellia. Both algorithms are used for MMTP packets as well as MPEG-2 TS packets.

In the MPEG-2 TS case, the scrambling unit is an MPEG-2 TS packet excluding its packet header. Since an MPEG-2 TS packet is a fixed-length packet, cipher block chaining (CBC) and output feedback (OFB) modes are used in combination as the operation mode of the cipher algorithm. The cipher algorithm is identified by Scramble_system_id in a scrambler descriptor, which is part of the Service Information.

In the MMT case, the scrambling unit is an MMTP packet excluding its packet header. Since an MMTP packet is of variable length and relatively large, the counter (CTR) mode is used as the operation mode of the cipher algorithm. The cipher algorithm is identified by Scramble_system_id in a scrambler descriptor, which is part of the Signalling Information. The scrambling control information is placed in an MMTP packet header extension field in order to identify the following three scrambling statuses: non-scrambled payload, payload scrambled with even key, and payload scrambled with odd key.

3.4 Associated information sub-system

There are two types of reception control: one is a CAS and the other is a content protection system. Each system has its own associated information.

The second-generation CAS includes a content protection system called “Rights Management and Protection (RMP)” system for free-to-air broadcasting services in addition to reception control. The RMP system enables broadcasters to distribute a scrambling key to each receiver, which is used for decrypting content.

While the RMP system is basically the same as that for the CAS-R system described above, it can be applied to the MMT case as well as the MPEG-2 TS case.

3.5 Three-layer architecture and ECM/EMM

The second-generation CAS uses the three-layer architecture with the ECM/EMM described in the reference model.

In the MPEG-2 TS case, the ECM provides common information for all receivers. The scrambling key is carried in the ECM. Access to the scrambling key in the ECM is controlled by means of entitlements or rights provided in the EMM. The EMM provides information for individual receivers. The work key is carried in the EMM.

In the MMT case, the ECM provides common information for all receivers. The scrambling key is carried in the ECM. Access to the scrambling key in the ECM is controlled by means of entitlements or rights provided in the EMM. The EMM provides information for individual receivers. The work key is carried in the EMM. The ECM and EMM are carried in an M2 section message, which is specified in Recommendation ITU-R BT.2074. The message authentication code (MAC) can be added to each MMTP packet so that a receiver can check the integrity and authenticity of the packet.

3.6 Downloadable CAS

The second-generation CAS includes a downloadable CAS in order to continuously maintain the security of an access control system and support new broadcasting services. A receiver can securely download an updated CAS program via broadcast and/or broadband.

A three-layer key structure and scrambling are used for downloading a CAS program via broadcast channels. A CAS program in broadcast channels is encrypted with a transmission channel protection key (Kt), which is distributed to each receiver by using a download control message (DCM) and download management message (DMM).

In addition to encrypting a CAS program, it is signed by its provider in order to maintain its integrity and authenticity.

4 Description of the "IEC 62455 with DVB systems"

IEC 62455 specifies a standardized system for controlling access to broadcast services based on MPEG2 transport stream. The IEC 62455 also specifies how the same system can be used for controlling the access to broadcast services based on Internet Protocol (IP). Thus the specification is widely applicable to different broadcast systems, including systems where the protection cannot be accomplished on MPEG2 transport stream packets (e.g. IP-based services delivered on non-MPEG2 based networks).

For conditional-access broadcasting systems, the IEC 62455 provides a fully specified interface between the sending and receiving ends. By use of this fully specified interface, both server and receiver vendors can independently implement the support for the protection system, rather than being forced to rely on a single security vendor to facilitate the implementation on both server and receiver. Thus an embodiment of the system avoids lock-in into a security vendor, and enables changing the vendor of any specified conditional-access system element without changing the other elements or their vendors.

The IEC 62455 specification covers all of the following layers of the system, but references existing specifications whenever possible:

- registration layer;
- rights management layer;
- key stream layer;
- traffic layer.

The rights management layer is based on the well-established and commercially widely adopted digital rights management standard by Open Mobile Alliance, OMA DRM 2.0. This layer is responsible for delivering rights and related constraints to the receivers, as well as long-term keys, i.e. service encryption key (SEK) or programme encryption key (PEK), depending on whether the access is granted on a subscription or a programme-by-programme basis.

In the interactive mode, i.e. when a bidirectional communication channel is available between the receiver and the service provider, OMA DRM 2.0 is used as is. For a unidirectional broadcast operation in the absence of an interaction channel, the system has been enhanced with bandwidth-saving binary versions of the OMA DRM 2.0 rights objects (called binary coded rights object, or BCRO), and a method for protecting these BCROs when delivered over the broadcast channel. Addressing the BCROs includes various addressing modes, which further reduce the bandwidth needed for distributing the rights objects. The protection method is based on zero-message broadcast encryption, ensuring that a security breach in a single receiver does not provide access on keys or rights delivered to any other receivers. The usage of the broadcast bandwidth is very optimized.

The keyset required for a broadcast mode operation is delivered to the receiver during registration for the service over the broadcast channel. In order to register for a service, the user only needs to communicate the unique device number (UDN) of the receiver to the service provider, which can then look up the certificate of the receiver from a certificate database. The certificate contains the public key of the receiver, which is used to protect the keyset during transit.

For protecting an MPEG-2 transport stream, the encryption (scrambling) of the actual content of the service employs popular ciphers such as DVB-CSA or AES-128 as specified by IEC 62455. IEC 62455 also specifies support for other encryption standards – such as IPsec, SRTP and ISMAcryp – to facilitate a non-MPEG2 transport stream packet based protection.

To facilitate the frequent changing of traffic encryption keys (TEK) used to protect the content of the service, IEC 62455 specifies a key stream layer that works between the rights management layer and traffic layer. The system supports granting access to the same stream through both service and programme rights objects. If the service provider wants to enable programme-by-programme access in the case that the programme is also available by subscription, the key stream message will carry a PEK encrypted with the SEK in addition to TEK encrypted by PEK. The key stream layer may also carry some other information, such as access criteria, or a permissions category value that can be used to select between different rights in the service rights object, related to the particular fragment of the stream to which the key stream message applies. This makes it possible to have different rights for different programmes, even though the access is based on subscription to a service consisting of multiple consecutive programmes.

Attachment 1 to Annex 2

Bibliography

– Recommendation ITU-R BT.810 – Conditional-access broadcasting systems

– ARIB STD-B25: Conditional access system specifications for digital broadcasting

– ARIB STD-B61: Conditional access system (second generation) and CAS program download system specifications for digital broadcasting

– IEC 62455: Internet protocol (IP) and transport stream (TS) based service access