



Recommendation ITU-R BT.1852-1
(10/2016)

**Conditional-access systems for
digital broadcasting**

BT Series
Broadcasting service
(television)



International
Telecommunication
Union
Documents
Document Sharing Hub

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

© ITU 2017

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without written permission of ITU.

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.