

# ITU-T Technical Report

(05/2023)

## TR.FSR

---

### **Factual subscriber-base reporting and protected content delivery in a conditional access system (CAS)**





# Technical Report ITU-T TR.FSR

## Factual subscriber-base reporting and protected content delivery in a conditional access system (CAS)

### Summary

Technical Report ITU-T TR.FSR on factual subscriber-base reporting and protected content delivery in a conditional access system (CAS) has been prepared to specify the terminology definition, service scenario and use cases related to Recommendation ITU-T J.1036 highlighting the characteristics of related technologies and network architecture. The goal of this Technical Report is to develop a secured network and ecosystem to ensure authorized access to content utilizing the standard CAS in digital addressable systems (DAS) for television broadcasting. An additional objective of this technical report is to supplement under-development of Recommendation ITU-T J.1036 and address two major concerns related to CAS, namely, underreporting of subscriber numbers and content piracy, leading to revenue loss to broadcasters, content providers and governments. Recommendation ITU-T J.1036 elaborates on the various functional requirements of the CAS such as log requirements, reports requirements, database requirements, security requirements and service requirements. Compliance with these requirements in CAS performance will address the twin concerns mentioned above.

### Keywords

CAS, conditional access, misreporting, piracy, SMS, subscriber management system, testbed preparations.

### Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

**Editor:** Avinash Agarwal  
Ministry of Communications  
India  
  
Rakesh S. Desai  
Ministry of Communications, India  
India

Tel: +91-9868171222  
Email: [avinash.70@gov.in](mailto:avinash.70@gov.in)

Tel: +91-9426203403  
E-mail: [rakesh.desai@gov.in](mailto:rakesh.desai@gov.in)

© ITU 2023

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

## Table of Contents

	<b>Page</b>
1 Scope .....	1
2 References.....	1
3 Definitions .....	1
3.1 Terms defined elsewhere.....	1
3.2 Terms defined in this Technical Report .....	1
4 Abbreviations and acronyms .....	2
5 Background of CAS.....	2
6 Service scenario.....	2
7 Use cases.....	4
8 Testbed preparations.....	4
9 Functional requirements .....	4
10 Conclusion .....	5

## **Introduction**

This Technical Report describes the essential elements of the conditional access system (CAS) with the headends in the cable networks or direct to home (DTH) (herein jointly referred as distribution platforms owners (DPOs)). The objective of this Technical Report is to supplement Recommendation ITU-T J.1036 and addresses two major concerns related to CAS, namely, underreporting of subscriber numbers and content piracy, leading to revenue loss to broadcasters, content providers and governments. Recommendation ITU-T J.1036 elaborates on the various functional requirements of the CAS such as log requirements, reports requirements, database requirements, security requirements and service requirements. Compliance with these requirements in CAS performance will address the concerns mentioned above. The objective of this report is also to assist CAS providers and DPOs in the implementation of the CAS in distribution networks. Correct implementation is a critical element for the factual and accurate reporting of the subscriber numbers, the channels subscribed and the reporting to the content providers, and the efficient working of the headend and the consumer premises equipment. This will also help in optimizing the resources at the headend and ensuring that consumers receive an uninterrupted service.



# Technical Report ITU-T TR.FSR

## Factual subscriber-base reporting and protected content delivery in a conditional access system (CAS)

### 1 Scope

This Technical Report specifies the terminology definition, service scenario, system architecture and use cases related to [ITU-T J.1036].

### 2 References

- [ITU-T J.93] Recommendation ITU-T J.93 (1998), *Requirements for conditional access in the secondary distribution of digital television on cable television systems.*
- [ITU-T J.95] Recommendation ITU-T J.95 (1999), *Copy protection of intellectual property for content delivered on cable television systems.*
- [ITU-T J.1036] Recommendation ITU-T J.1036 (2023), *Factual subscriber-base reporting and protected content delivery in conditional access system – Requirements.*
- [ITU-R BT.1852-1] Recommendation ITU-R BT.1852-1 (2016), *Conditional-access systems for digital broadcasting.*
- [TRAI] Telecom Regulatory Authority of India (2020), *TRAI Consultation Paper On Framework for Technical Compliance of Conditional Access System (CAS) and Subscriber Management Systems (SMS) for Broadcasting & Cable Services.*  
[https://www.trai.gov.in/sites/default/files/CP\\_22042020.pdf](https://www.trai.gov.in/sites/default/files/CP_22042020.pdf)

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

**3.1.1 conditional access system (CA)** [ITU-T J.95]: 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.

**3.1.2 piracy** [ITU-T J.93]: The act of acquiring unauthorized access to programs, usually for the purpose of reselling such access.

**3.1.3 content** [ITU-R BT.1852-1]: This is any form of digital data that can be acquired and presented by a device.

**3.1.4 service** [ITU-R BT.1852-1]: This is one or more data flows intended to be presented together.

#### 3.2 Terms defined in this Technical Report

This Technical Report defines the following terms:

**3.2.1 factual subscriber-base reporting:** In the context of a conditional access system, the accurate and truthful representation of the number of subscribers of each service in a distribution platform without any manipulation or distortion of the underlying data.

**3.2.2 protected delivery of content:** in the context of a conditional access system used in broadcasting and distribution platforms, the secure encrypted transmission of digital content, such as TV programmes, films or music, to authorized users while preventing unauthorized access or piracy.

## **4 Abbreviations and acronyms**

This Technical Report uses the following abbreviations and acronyms:

CAS	Conditional Access System
DPO	Distribution Platform Operator
DTH	Direct To Home
HITS	Headend In The Sky
IPTV	Internet Protocol Television
LCN	Logical Channel Number
LCO	Local Cable Operator
SMS	Subscriber Management System
STB	Set Top Box
VC	Viewing Card

## **5 Background of CAS**

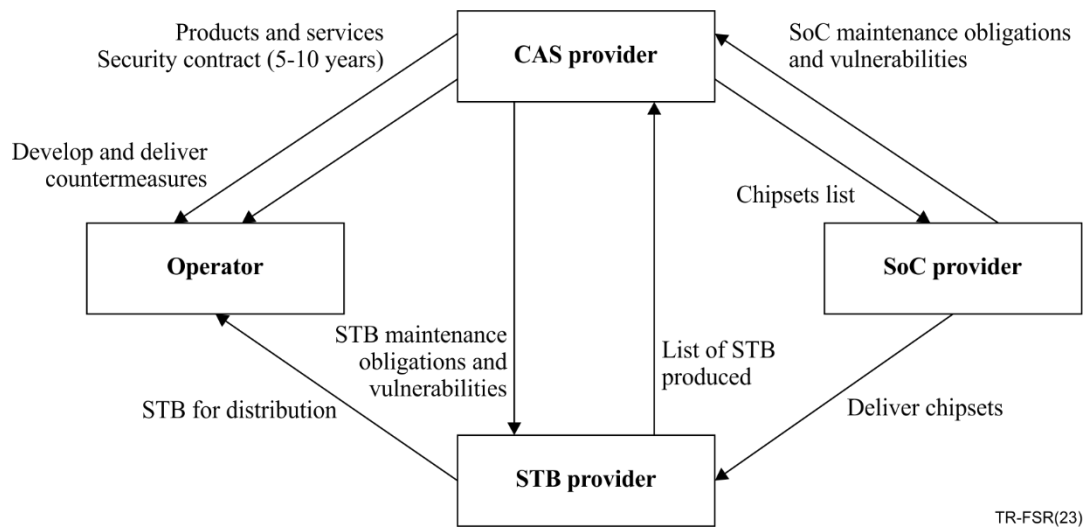
Most countries have implemented digital addressable systems (DAS) for distribution platforms such as cable TV, direct to home (DTH), internet protocol television (IPTV) and headend in the sky (HITS). DAS enables subscribers to have a choice and option to select their channels and packages. A conditional access system (CAS) and subscriber management system (SMS) are integral parts of a DAS environment. While CAS is responsible for encrypting the content and its delivery in a secure and encrypted manner to authorized subscribers only, SMS handles the subscriber management functions. The quality of service depends on the CASs and SMSs deployed by the distribution platform owner (DPO). Since the content providers and broadcasters have no control over the CAS and SMS, as these are deployed at the DPO end, they often complain about loss of revenue due to various malpractices, such as under-reporting of subscriber base, distribution of channels to unauthorized users and content piracy. Therefore, it is necessary to frame benchmarks for the CASs, prescribing technical specifications focusing on functional requirements to ensure factual reporting of subscriber-base and protected delivery of content to authorized subscribers. Creating a framework that prevents the deployment of a sub-standard CAS will bring preventive control from potential threats and revenue losses arising due to the vulnerability of such systems, increase economic efficiency and improve quality of service and the end-consumer experience.

## **6 Service scenario**

Conditional access systems are an important and integral part of the pay TV broadcast and cable environment. The distribution platforms use CAS to ensure that content is securely encrypted and available to authorized subscribers. An SMS is another key link between the content provisioning to the authorized subscribers, the customer relations management system of the distribution platform and payment to the pay TV content providers based on the numbers of the subscribers authorized to watch their content. The quality of service depends on the CASs and SMSs deployed by the DPO.

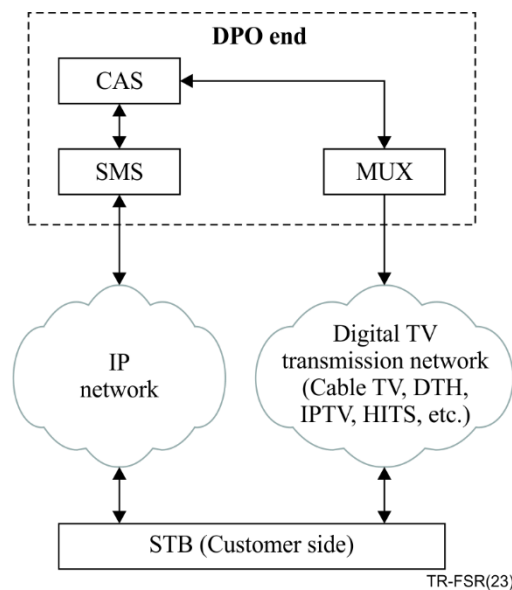
In any market there are a number of CAS and SMS solutions deployed and a framework needs to be developed that ensures that all the CAS and SMS solutions meet a minimum basic performance requirement.





**Figure 1 – Relationship of key players in a pay TV ecosystem (Source: [TRAI])**

Distribution platforms depend on various subsystem (see Figure 1) and have a relationship and dependency not only for a smooth operation but also for the introduction of the newer features, meeting regulatory and business needs and also keeping the system fool proof. The working of the DAS ecosystem is explained in Figure 2 below.



**Figure 2 – Digital addressable system (DAS) architecture**

The implementation of a CAS and SMS solution that does not meet minimum required criteria and functionalities can lead to:

- i) The CAS and SMS providers being unable to maintain and upgrade products and offerings to the subscribers to meet the growing business requirements;
- ii) Consumer choices being limited as there are limitations on product creations and provision;
- iii) Invoice generation to the subscribers not being generated on time thus impacting the service provisioning to them.

## **7 Use cases**

Market systems need CAS and SMS to enable secure, safe systems that enable the content provider to provide content without the fear of being redistributed in an unauthorized manner and that the distribution platform gives a transparent and accurate number of distributions.

All established solutions of CAS and SMS deploy advanced security to ensure that content and implementation are secure; however, sometimes some exceptions are seen. This leads to the disruption of the services to the distribution platforms as they do not receive the content and subscribers are also not able to view the content. The content providers do not get their due share of the revenue. It is sometimes seen that a few DPOs also take advantages of the shortcomings in the CASs and the SMSs and take that route to shortchange the content provider.

The CASs and SMSs should comply with the below requirements:

- a) The CAS through its user interface or application or direct command line interface shall not allow the DPO to directly activate/deactivate the set top box (STB) or viewing card (VC), channels or packages, to create, modify or delete channels and/or packages, or to add, modify or delete a subscriber, etc. The CAS must execute commands initiated from its designated SMS only.
- b) Historical logs of package creation and modifications along with date and time stamp should be available in the CAS and SMS.
- c) Every individual channel should be available only on one unique logical channel number (LCN) in the entire network, which also includes the local cable operator (LCO) networks. The channel descriptor should match the channel name. The same channel cannot be distributed in the entire network under another LCN or channel descriptor or in an unencrypted form.
- d) The CAS and SMS should be able to handle in à-la-carte mode all the channels distributed by the DPO.
- e) The CAS and SMS shall be able to tag and blacklist VC and STB numbers that have been involved in piracy in the past to ensure that they cannot be re-deployed.
- f) The CAS shall be capable of generating reports pertaining to channel/bouquet subscriptions and active/deactivated subscribers, or any combination thereof; start and end date of the subscribers subscription per package/channel, VC number or virtual card number of the STB, as the case may be. The CAS shall share such report with SMS as a scheduled activity, and also upon request.

## **8 Testbed preparations**

To test the CAS, it is essential that the testing agency is able to simulate the right conditions of a network. It should have signal sources, encoders/transcoders, multiplexers (which can handle the CASs working in the region), upconverters, down converters, a model SMS and relevant STBs.

The signal sources at the headend at the test lab has to be configured to the MPEG2/MPGE4/H.264 or the H.265 encoders and the same has to be configured in the multiplexing equipment.

The CAS has to be configured with the respective multiplexing equipment and the SMS. The STBs are to be put in the networks in the lab to test the features of the CAS.

## **9 Functional requirements**

The CAS shall meet the following functional requirements:

- 1) Log and reporting requirements
- 2) CAS database requirements

- 3) Security requirements
- 4) Service requirements.

Detailed information on the above-mentioned functional requirements may be found in [ITU-T J.1036].

## **10 Conclusion**

Conformance to the functional requirements prescribed in [ITU-T J.1036] prevents the deployment of sub-standard CASs and will bring preventive control from potential threats and revenue losses arising due to the vulnerability of such systems, bring economic efficiency, improve quality of service and improve the end-consumer experience.

---