Date: 07-10-2022
Panaccess
CAS-DRM-IPTV

To,
Shri Anil Kumar Bhardwaj, Advisor (B&CS),
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan, Jawaharlal Nehru Marg,
New Delhi, Delhi 110002

RESPONSE TO THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) (FOURTH AMENDMENT) REGULATIONS, 2022 (___ of 2022)

We thank the Telecom Regulatory Authority of India (TRAI) for providing the opportunity to participate on this consultation process regarding the draft TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) (FOURTH AMENDMENT) REGULATIONS, 2022 (___ of 2022). Panaccess is specialized in providing high-end one-way or two-way CAS and DRM security solutions to its customers all around the globe. Satellite, cable, terrestrial, and IPTV operators. We hope that the inputs and comments given by us shall be given a thought into by TRAI in resolving issues pertaining to IPTV Framework, OTT setup, Digital Rights Management System, Fingerprinting, watermarking, and transactional capacity of DRM and SMS system. We appreciate TRAI’s efforts to ensure elimination of rampant piracy and under declaration existent on the ground even as on date.

Please find below our response to the draft Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fourth Amendment) Regulations, 2022 (___ of 2022):

For any Queries or Clarification please contact:

Reveesh R Nair

rn@panaccess.com

Table.1 Responses on issues related to Draft Regulations 2022 raised in this CP

S no	Clause number of Draft Regulations 2022 Consultation Paper No. 12/2022	Do you agree with the Draft Regulations proposed in this CP (Yes/No)	If you do not agree with the amendment proposed in this CP, then provide amended Clause proposed by you	Reasons with full justification for your response
1	D 15	No	D 15	If not regulated there may arise the different versions of the clause mentioned.
2	D 16	No	D 16	DRM should be independent to define Packages so
3	D 27	No		Needed to know if it's to enable logging in from other device to check subscription status or to use OTP to activate the box
4	E 14	Yes		DRM should be capable of updating packages on real-time basis
5	E 19 to E 25	Yes		Security of the Content in Multicast streams is and should be of highest priority for a Secure System
6	E 30 E 31 E 33 E 34 E 36 E 38	Yes		
7	E 45 E 46	Yes		
8	G 1 to G 23	Yes		

Table 2: Response on issues related to 'System Requirement for Digital Right Management (DRM)' on issues other than those proposed in this CP

S no	New Clause number proposed in the Draft Regulations 2022	Suggested Amendment (additional clause)	Reasons/ full justification for the proposed amendment
1	D 15	Clarification needed on File output formats needed from DRM	This mismatch is normally found through audits, so it is assumed that the active count file is uploaded into SMS UI to cross check with its data.
2	D 16	SMS creates and manages packages based on Product ID and composition provided from DRM	DRM API's cannot allow Packages to be directly be created/modified from SMS subject to DRM database security. Clause E14 is acceptable which is in line with and agreeable.
3	E 34	If CDN is not allowed how the catchup content to be accessed?	How the catchup content of linear services is stored and retransmitted on request on the device needs to be regulated.
4	E 52	In line with E 25 mentioned DRM System to be deployed on secured server	It has to be 24/7 x 365 days accessible remotely (via private VPN) or directly with session based logging to ensure accessibility.
5	E 53	OTT Apps currently transmitting Linear Channels to be verified their mode of transmission. As HLS or Dash is not allowed.	No one should have any unfair advantage over the transmission and subscriber base.

❖ References as mentioned in the Consultation Paper No. 12/2022

PAGE 13

D 15.

The file output of DRM shall be processed by SMS system to compare and generate a 100% match or mismatch error report

D 16.

Channel/Bouquet management: SMS shall support the following essential requirements:

(a) Create and manage all channels and bouquets along with the relevant details such as name, tariff, broadcaster, or DPO bouquet, etc.

(b) Manage changes in the channel/bouquet, as may be required, from time to time.

(c) Link the Products IDs for à-la-carte channels and bouquets (Single and Bulk) created in DRM with the product information being managed in SMS, for smooth working of SMS and DRM integration.

(d) Management of historical Data of Product name, i.e., Broadcasters (name), maximum retail price (MRP), distributor retail price (DRP).

PAGE 15

D 27.

User Authentication: SMS should have the capability to authenticate its subscribers through registered mobile number (RMN) through one-time password (OTP) system

PAGE 17

E 14.

DRM shall be capable of adding/modifying channels/bouquets as may be required on real time basis in line with the activity performed in SMS.

PAGE 18

E 19.

DRM should support encryption of individual tracks of a content stream with individual keys, i.e.,

track level protection

E 20.

DRM should support key rotation, i.e., periodic changing of security keys

E 21.

In case DPO has deployed hybrid STBs, DRM shall ensure that the over-the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs.

E 22.

There shall not be any active unique subscriber outside the database tables. Further, there shall not be an option to split DRM database for creation of more than one instance by a DPO or a vendor.

E 23.

It must support the following options with reference to uploading of unique access (UA)/MAC ID details in DRM database:

(a) A secure un-editable file of MAC ID details, as purchased by the distributor, to be uploaded by the DRM vendor on the DRM server directly,

(b) If it is uploaded in any other form, UA/MAC ID in DRM database shall be captured in logs,

(c) Further, DRM shall support an automated, application programming interface (API)-based mechanism to populate such UA/MAC ID details in the SMS, without any manual intervention.

E 24.

It shall be mandatory to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers:

Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server:

Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB UA/MAC ID details, entitlement level information, etc

E 25.

DRM and SMS shall ensure that the access to database is available to authorized users only, and in "read only" mode only. Further, the database audit trail shall be permanently enabled.

PAGE 19

E 30.

There shall be unique license key required for viewing every 10 minutes in DRM deployed by DPO.

E 31.

For every change in channels, fresh license keys should be issued by the DRM. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB from any other source other than the one specified by the IPTV system.

E 33.

IPTV transmission has to be in multicast mode only just like cable TV transmission. There cannot be any such case where unicast is allowed. STBs with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device.

E 34.

IPTV transmission should not be allowed to configure any content delivery network (CDN) in their system to deliver linear content to STBs.

E 35.

IPTV should not be allowed to deliver linear content to any other device except STB which has been whitelisted in DRM.

PAGE 20

E 36.

IPTV should have capability to implement session based/token authentication with token authentication duration to be controllable to few minutes.

E 38.

The DRM should have following policies implemented:

(a) It should restrict user to editing or saving content in part or full.

(b) It should restrict user from sharing or forwarding or mirroring the content from the STB

(c) It should disallow user to take screen shots or screen grabs or screen-recording.

(d) It should lock access to authorized STBs only.

(e) It should have Geo blocking, that enables a broadcaster to determine and instruct the DPO/IPTV service provider to restrict the broadcast of TV channels in locations.

(f) It should be able to set expiry date to recorded content at STB end based on various policies.

E 45.

DRM should ensure that the integrated STBs are verifiably located within India by reference to internet protocol address and service address. Further, the DRM shall not permit delivery to an Internet/mobile device. The DRM must use industry-standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.

E 46.

DRM should ensure that channels are accessible on integrated STBs of only such subscribers who are then-current, valid subscribers of the distributor of channels, and such confirmation must take place prior to the DRM actually delivering (or authorizing the delivery of) channel to the integrated STBs of such subscribers.

PAGE 23.

G 14.

DRM deployed should be able to geo tag STB deployed in the network for security.

G 16.

STB should not have feature to download (direct or side download) any 3rd party App/APK (Including on Hybrid STB's if any) and should not have access to any browser.

G 17.

STB should not be able to access the authorization keys from any other source except from the IPTV system through the IPTV closed network. DRM must ensure that the authorization keys are not received by the STB from any other source other than the one specified by the IPTV system

G 19.

STB should have copy protection – HDCP with version 2 and above, DHCP, CGMS & macrovision with version 7 and above.

G 21.

The DRM should not allow delivering linear TV channels on HLS, Smooth Streaming, Dash & HTTP/TCP.