

From : srrao@ulka.tv(srrao@ulka.tv)
To : cp@traigov.in
Cc :
Subject : IPTV Service in Smart TV
Date : Oct 19 2022 13:51 PM

To,
Shri Dr.P.D.Vaghela,
Chairman,
Telecom Regulatory Authority of India,
Jawaharlal Nehru Marg, Mahanagar Doorsanchar Bhawan,
New Delhi – 110002

Subject: Distribution of IPTV services in Smart TV.
Reference: TRAI consultation Paper No.12/2022.

Dear Sir,

Distribution of television channels via IPTV using existing internet broadband networks greatly contributes to growth of internet services in the country

SMART Televisions are rapidly increasing their market share in television sales in India and global market.

All the requirements for IPTV distribution can be accomplished using DPO/MSO Application in the SMART TV in place of IPTV STB as per TRAI guidelines except the Device Manufacturer Declaration Certificate.

It should be noted that all the requirements are implemented from the DPO/MSO Application integrated with the DRM installed in the SMART TV and hence approval of the Application is important than the device.

Smart TV offers enhanced security for the content since the encrypted channel streams are decrypted inside the Smart TV and there is no TV signal output cable similar to CABLE TV / DTH Set-top-Box.

As per TRAI guidelines MSO provides all types of fingerprinting to their Smart TV Application similar to CATV/DTH STB which is an additional security compared to OTT Applications.

Introduction of SMART TV for IPTV distribution by MSO is the perfect solution for Interoperability of consumer devices between MSOs as per TRAI recommendations to Ministry of Information and Broadcasting.

The consumers who are already having Smart TV can migrate to IPTV subscription without any upfront investment and experience enhanced quality of linear TV channels compared to OTT services and migrate to other IPTV operators without changing the STB/CPE.

If the DRM deployed by MSO for their IPTV distribution is of equal standard compared to OTT applications MSO should be allowed to use Smart TV as their IPTV CPE (Customer Premise Equipment)

The Premium content providers like Youtube, Netflix, Disney, and most of the popular broadcasters in India have launched their OTT service Applications in Smart TV platforms.

When most of the popular broadcasters in India are distributing their content using their OTT Applications in Smart TV there is no reason to restrict licensed MSOs to use Smart TV as per IPTV Regulations.

Licensed MSO follow TRAI guidelines to honor consumer rights to allow them to choose only the channels they desire and transmit all the mandatory Doordarshan Channels unlike OTT players of live channels.

Consumers are migrating from licensed MSOs to OTT Applications provided by most of the popular broadcasters and hence MSOs should be given opportunity to use Smart TV as their IPTV CPE and compete with the unregulated OTT players in the market.

MSO and OTT players should have level playing field both in technology and Commercial aspects.

We have already sent our response to TRAI Consultation paper CP12/2022 and the copy of the same is in the attachment. I am also attaching the digitally signed letter in the attachment.

We request you to consider our proposal to enable Television Distribution Platform Operators in India to deliver world class services and compete in quality with major global content players.

Thanking you,
Regards,
S Raghava Rao
Director
City Online Media Private Ltd. (ULKA TV)
Ph:+919848028638
www.ulka.tv

To,
Shri Dr.P.D.Vaghela,
Chairman,
Telecom Regulatory Authority of India,
Jawaharlal Nehru Marg, Mahanagar Doorsanchar Bhawan,
New Delhi – 110002

Subject: Distribution of IPTV services in Smart TV.

Reference: TRAI consultation Paper No.12/2022.

Dear Sir,

Distribution of television channels via IPTV using existing internet broadband networks greatly contributes to growth of internet services in the country

SMART Televisions are rapidly increasing their market share in television sales in India and global market.

All the requirements for IPTV distribution can be accomplished using DPO/MSO Application in the SMART TV in place of IPTV STB as per TRAI guidelines except the Device Manufacturer Declaration Certificate. It should be noted that all the requirements are implemented from the DPO/MSO Application integrated with the DRM installed in the SMART TV and hence approval of the Application is important than the device.

Smart TV offers enhanced security for the content since the encrypted channel streams are decrypted inside the Smart TV and there is no TV signal output cable similar to CABLE TV / DTH Set-top-Box. As per TRAI guidelines MSO provides all types of fingerprinting to their Smart TV Application similar to CATV/DTH STB which is an additional security compared to OTT Applications.

Introduction of SMART TV for IPTV distribution by MSO is the perfect solution for Interoperability of consumer devices between MSOs as per TRAI recommendations to Ministry of Information and Broadcasting.

The consumers who are already having Smart TV can migrate to IPTV subscription without any upfront investment and experience enhanced quality of linear TV channels compared to OTT services and migrate to other IPTV operators without changing the STB/CPE.

If the DRM deployed by MSO for their IPTV distribution is of equal standard compared to OTT applications MSO should be allowed to use Smart TV as their IPTV CPE (Customer Premise Equipment)

The Premium content providers like Youtube, Netflix, Disney, and most of the popular broadcasters in India have launched their OTT service Applications in Smart TV platforms. When most of the popular broadcasters in India are distributing their content using their OTT Applications in Smart TV there is no reason to restrict licensed MSOs to use Smart TV as per IPTV Regulations.

Licensed MSO follow TRAI guidelines to honor consumer rights to allow them to choose only the channels they desire and transmit all the mandatory Doordarshan Channels unlike OTT players of live channels.

Consumers are migrating from licensed MSOs to OTT Applications provided by most of the popular broadcasters and hence MSOs should be given opportunity to use Smart TV as their IPTV CPE and compete with the unregulated OTT players in the market.

MSO and OTT players should have level playing field both in technology and Commercial aspects.

We request you to consider our proposal to enable Television Distribution Platform Operators in India to deliver world class services and compete in quality with major global content players.

We have already submitted our response to TRAI CP No.12/2022.

Thanking you,

Regards, Signature:

S Raghava Rao

Director

City Online Media Private Ltd.

Ph:+919848028638

Date: 18-10-2022.

To,
 Sh. Anil Kumar Bhardwaj,
 Advisor (B&CS)
 Telecom Regulatory Authority of India.

Reference: Consultation Paper No.12/2022.
 Subject: Our response and comments on issues related to Draft Regulations 2022 raised in this CP with detailed reasons and Justifications including supporting Annexures.

Dear Sir,

City Online Media Private Ltd is an MSO with registration No.N-450009/52/2020-DAS dated 10/11/2020. We have submitted all the mandatory self-declarations to TRAI , MIB and DOT. Ministry of Information and Broadcasting has issued a letter No.16/3/3033-BP&L dated 21st February, 2022 stating that we may provide IPTV services in India during the validity of our MSO registration i.e. currently upto 09-11-2030.

We have already submitted Technical Audit reports to all the major broadcasters and completed the RIO agreements as per the list below

- 1) Star India Private Ltd - Star
- 2) Sony Pictures Networks India Private Ltd- SONY
- 3) Indiacast Media Private Ltd -TV18
- 4) Indiacast Media Private Ltd – Warner
- 5) Sun Distribution Services Private Ltd – SUN TV
- 6) Gemini TV Distribution Services Private Ltd – Gemini
- 7) Eenadu Television Private Ltd – ETV
- 8) Bennet Coleman & Company Ltd – Times
- 9) T.V.Today Network Limited
- 10) New Delhi Television Ltd – NDTV
- 11) Discovery Communication India – Discovery
- 12) Celebrities Management Private Ltd – Travel XP
- 13) Odisha Television Limited
- 14) Epic Television Networks Private Ltd – EPIC

As a stake holder we are submitting our written comments in reply to the consultation paper issued on 9th September 2022 as per the prescribed format. We have also submitted our response on issues related to ‘System Requirement for Digital Rights Management (DRM)’ on issues other than those proposed in this CP in Table-5. Detailed explanations and justification for our responses for some of the Clauses were submitted in Annexures-1,2,3 and 4.

Table 1: Proposed DRM requirements for SMS

S No	Clause No.	Yes / No	AMENDED Clause proposed by us for the disagreed amendments proposed in this CP	Reasons with full justification for our response
1	1 (1), (2), (3)	Yes		
2		No	Password Policy Creation for Users: SMS shall have a defined password	Mac id of the STB or the CPE are unique and if they are paired or locked with the

			policy, with minimum length criteria and composition (upper and lower-case characters, numeric, alphabets or special characters), forced password changes or any other appropriate mechanisms or combinations thereof or alternatively user account has to be locked/paired to the Mac Id of the STB or the CPE	user account, support for the password validation and recovery for users are not required.
3	3	Yes		
4	4	Yes		
5	5	No	Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs is reflected in the reports generated from the SMS integrated with the DRM and DRM Session logs should be able to validate the access of the channels between period of activation and deactivation of the STBs	As per clause 4, All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM. When the DRM is not involved in activation and deactivation of the STB it cannot generate activation and deactivation logs. The SMS sends the command to the DRM to decrypt the channel as per the subscription details of the user and the DRM creates the session log for each access of the channels of each user.
6	6	Yes		
7	7	Yes		
8	8 (j)	No	(j) Unique STB number / user name	DRM and Middleware systems work with user names which are more user friendly than STB numbers.
9	9	Yes		
10	10	Yes		
11	11	Yes		
12	12	Yes		
13	13	Yes		
14	14	Yes		
15	15	Yes		
16	16	Yes		
17	17	Yes		
18	18	Yes		
19	19(b)	No	(b) SMS/DRM shall have the provision of generating the user activity log report to enable tracking user's work history. It shall not be allowed to delete the records from the log.	(b)DRM maintains the session logs whenever a user views a channel including the time stamp. These logs facilitate the viewership analysis and provides validation for the channel access as per the user's subscription.
20	20	Yes		
21	21	Yes		
22	22	No	STB/Username and MAC ID shall be paired from the SMS to ensure security of channel.	Usernames can also be used in place of STB number. DRM is not involved when the pairing is done in the SMS.
23	23	Yes		

24	24	No	SMS should have a facility to carry out monthly reconciliations of channels/ala carte and bouquet (with their respective ID created in SMS with DRM and the variance report should be available from the DRM and SMS logs and made available during audits.	As per clause 4. All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM. SMS maintains the activation and deactivation logs and DRM maintains the session logs. Middleware or a dedicated log server which maintains the logs of both SMS and DRM in synchronization via the API's provided by SMS and DRM systems can be used to maintain the logs to verify the user's subscription status.
25	25	Yes		
26	26	yes		
27	27	Yes		
28	28	Yes		

Table 2: Proposed DRM Requirements for conditional access by subscribers and encryption

S No	Clause No.	Yes / No	AMENDED Clause proposed by us for the disagreed amendments proposed in this CP	Reasons with full justification for our response
1	1	Yes		
2	2	No	DRM shall ensure all logs are un-editable, stamped with date and time of all transactions (all session logs of the users, channel wise, date wise with user id or mac id should be available). The DRM shall not allow altering or modification of any logs. There shall be no facility for the distributor/users to purge logs. Provision for validation of session logs with subscription status should be available via middleware or an equivalent software.	As per Table 1 Clause 4 and Table 2 Clause 3 (All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM and DRM do not have the facility to activate and deactivate a STB.) When there is no option of activation and deactivation, assignment or de-assignments of channels for user/STB it cannot generate the log of the same activities on its own. However ever validation of the session logs as per the subscription status of the user/STB can be done via middleware or an equivalent server which can sync the logs of SMS and DRM via read only API's provided by the respective vendors. Most of the Global popular DRM vendors provide encryption and decryption facility as per authorization of the billing systems. They do not have facilities like maintaining complete data of users, channels, bouquets etc.
3	3	Yes		
4	4	No	The SMS and the DRM should be integrated in such manner that activation and deactivation of STB are synchronized in real time.	When a user subscribes a channel it not necessary that he watches the channel. When user watches a channel only the session log is created in the DRM and the DRM enables the decryption only when the SMS/billing systems sends a valid

				subscription status to DRM via API integration and this can happen in real time.
5	5	Yes		
6	6	Yes		
7	7	Yes	The DRM deployed should be able to generate, record, maintain independent reports and logs for verification purpose during audits corresponding to each command executed in the DRM issued by the SMS integrated with the DRM for last two (2) years minimum. The reports must have date and time stamp. Proposed reports should include:	
7	7(a)	No	(a) Unique active STB count as well as Unique MAC ID/User ID/DRM ID wise on any desirable date	(a)The unique id for each subscriber is required. It can be MAC ID / User id / unique ID generated by DRM for each user.
7	7 (b)	No	(b) Unique channel active for a specific STB/User on any desirable date	(b)Bouquet info is not maintained in DRM unlike traditional CAS but all the channels contained in the particular bouquet can be obtained for a specific STB/User id on any desirable date or duration.
7	7(c)	No	(c) MAC ID/User ID wise Channel viewership report for service requests	(c) As per Table 1 Clause 4 and Table 2 Clause 3 (All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM and DRM do not have the facility to activate and deactivate a STB.) When there is no option of activation and deactivation of user/STB it cannot generate the log of the same activities on its own. However ever validation of the session logs as per the subscription status of the user/STB can be done via middleware or an equivalent server which can sync the logs of SMS and DRM via read only API's provided by the respective vendors.
7	7(d)	No	(d) Any alteration in bouquet and/or channels configured in DRM if the facility is available in DRM	(d)Assignment of bouquets or channels is not done in most of the popular DRMs unlike traditional CAS. It is implemented only in SMS.
7	7(e)	No	(e) Blacklist STB should not have access / session log in the DRM. This clause can be removed also.	(e) Blacklist STB is done only in SMS and when it is blacklisted in SMS it will not send the request to DRM for viewer ship so no activity can be recorded in DRM.
7	7(f)	No	(f) Product code pertaining to channels should be available in DRM	(f)bouquets are created and managed only in SMS. SMS sends the decryption request to DRM if the requested channel is included in the bouquet subscribed by the STB/User.

7	7(g)	No	(g) Channel Viewership Access by STB /User for a particular date / week / a period (from date to date)	(g)Authorization / Assignment of channels / bouquets are defined only in SMS
7	7(h)	No	(h) STB-VC pairing / de-pairing or User id- Mac-id Pairing / de-pairing (If applicable) in SMS/DRM	(h)Mac-id is unique globally for the IP/STB and it can be used for pairing in place of VC card. This is usually implemented in SMS and not in DRM
7	7(i)	No	(i) Session Log validation should be possible for each active subscribed channel per user during subscription period of the user for any particular channel	(i) As per Table 1 Clause 4 and Table 2 Clause 3 (All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM and DRM do not have the facility to activate and deactivate a STB.)
7	7(j)	No	(j) DRM should not have facility for assignment of channel / bouquets to STB/User. If the facility is available the corresponding logs should be available.	(j) Most of the popular DRM systems does not have facility of management of channels or bouquets they only enable decryption of the content as per the request from the SMS/Billing systems. When the activity is not available in the DRM system it cannot generate the logs on its own. Session logs of user per channel can be validated for the subscription period.
7	7(k)	No	(k) Report of the activations or the deactivations of a particular channel for a given period available in SMS should be able to validate the session logs available in DRM.	(k) As per Table 1 Clause 4 and Table 2 Clause 3 (All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM and DRM do not have the facility to activate and deactivate a STB.)
7	7(l)	No	(l) The total number of registered subscribers if the DRM has the facility to register subscribers	(l)Registration of subscribers are done only in SMS and most of the DRM systems do not have the facility of subscriber's registration and depend on SMS or the billing system for the same data.
7	7(m)	Yes		
7	7(n)	No	(n) The total number of temporary suspended subscribers if the subscribers have registration facility in the DRM.	(n) Registration, Activation, De-activation and suspension of users is available only in SMS and DRM does not have the facility as per Table-1 Clause 4 and Table-2 Clause 3
7	7(o)	No	(o) The total number of deactivated subscribers if the registration of subscribers is available in DRM	As per Table 1 Clause 4 and Table 2 Clause 3 (All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM and DRM do not have the facility to activate and deactivate a STB.)
7	7(p)	No	(p) List of blacklisted STBs in the DRM if the registration of subscribers is available in DRM	Blacklisting of STBs is implemented in SMS and SMS do not send any type of information to DRM related to Blacklisted STBs

7	7(q)	No	(q) Channel and User wise monthly viewership report in the prescribed format	Bouquets are maintained only in SMS and DRM systems do not have access to Bouquets in SMS.
7	7(r)	No	(r) The names of the channels in relation to their names registered in SMS	Bouquets are not managed in most of the DRM systems they depend on SMS.
7	7(s)	No	The total number of active subscribers subscribing to a particular channel at a given time	Bouquets are not managed in most of the DRM systems they depend on SMS.
7	7(t)	No	(t) The name of the channels per user viewership records with respect to subscription status of a subscriber	The subscription status of channels and bouquets are maintained only in SMS. DRM decrypts the channel as per the command from the SMS and records the session log.
7	7(u)	No	(u) The ageing viewership report of a particular channel for a particular time period.	Bouquets are not managed in most of the DRM systems they depend on SMS.
8	8	No	DRM deployed should not have any facility to activate the blacklisted STB.	Most of the Popular DRM systems do not manage the STBs they depend on the SMS.
9	9	Yes		
10	10	Yes		
11	11	Yes		
12	12	Yes		
13	13	No	DRM shall not support carriage of channel with same name or nomenclature in the distributor's network served by each headend under more than one instance, and another channel descriptor. Further, each channel available in DRM shall be uniquely mapped with channels available in SMS.	Most of the DRM systems do not have facility of management of LCN they depend on the SMS however they allow only unique names for the channels during encryption which are mapped against the respective channels in the SMS.
14	14	No	DRM shall be capable of executing SMS requests for channels as may be required on real time basis in line with the activity performed in SMS	Most of the DRM systems do not have any facility for assignment of channels / bouquets and they depend on SMS and declaration by the DRM vendor can be obtained.
15	15	No	DPO should deploy and activate only the approved branded / proprietary STBs which are tested as per the technical Audit Manual and DPO's should include the STB models in their Annexure-3 declaration and should submit the updated Annexure-3 declaration if any new model STB is deployed for the viewership of pay channels.	Most of the popular DRM systems are global players and supports the STB Models depending on their technical security evaluation of the chipsets deployed in the STB. It is the responsibility of the DPO to ensure the firmware / operating system of the STB to be compatible to the TRAI regulations and submit the required declarations in the prescribed format.
16	16	Yes		
17	17	No	DRM should support content protection and usage viewership data for B2C model	Unable to interpret "usage rules enforcement for B2C model"
18	18	Yes		

19	19	No	DRM should support encryption of individual channel with individual keys and encrypt all the content available in the channel	This is applicable only in MPTS (Multiple Program Transport streams) in traditional DTH and CATV systems.
20	20	Yes		
21	21	No	In case DPO has deployed hybrid STBs, DPO Application integrated with the 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, DPO Application integrated with 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.	The DPO application system integrated with the DRM and the firmware / operating system are involved in the required implementation. It is not just the DRM which is responsible for the required implementation.
22	22	Yes		
23	23	Yes		
24	24	Yes		
25	25	Yes		
26	26	Yes		
27	27	Yes		
28	28	Yes		
29	29	No	DRM should have the following features: (b) The entitlement end date in DRM shall be open and SMS shall manage entitlements based on the billing cycles and payments.	Point (a) and Point(b) are contradicting each other. As per Table 1 Clause 4 and Table 2 Clause 3 (All activation and deactivation of STBs shall be done with the commands of the SMS integrated with the DRM and DRM do not have the facility to activate and deactivate a STB.)
30	30	Yes		
31	31	Yes		
32	32	Yes		
33	33	No	IPTV transmission has to be in Local Network only and the IPTV streams should use only Private IP Address space as per Internet Assigned Numbers Authority (IANA) . STBs with facilities for recording programs shall have a copy protection system (i.e.,the recorded content should be encrypted with the same DRM and decryption should be allowed only during the subscription period of the subscriber for that content) and such recorded content should not be transferrable to any other device.	As per Table 2 Clause 5 (DRM deployed should be able to support two-way networks only). Multicast is only a one-way network and Unicast is a two-way Network. When the content is encrypted at the source headend and decrypted only in the STB/CPE unicast or multicast transmission do not compromise the security of the content in any manner. Table-2 Clause 45 is not applicable if it is multicast transmission. A detailed explanation is submitted in Annexure -1

34	34	No	IPTV transmission should be in encrypted format and only the STB/CPE should be allowed to decrypt as per the subscription status. If CDN/Stream Multiplexer/Stream Multiplier is involved it should not have any facility to decrypt and encrypt and should distribute the stream in the same format of the source stream in real-time.	CDN performs the activity similar to EDFA in traditional Cable TV networks. CDN offers the scalability of the network. CDN offers an extra layer of security and management of users per LCO or a Reseller and avoids the bandwidth bottlenecks from the source Headend. A detailed explanation is submitted in Annexure-2
35	35	Yes		
36	36	Yes		
37	37	Yes		
38	38	Yes		
39	39	Yes		
40	40	Yes		
41	41	Yes		
42	42	Yes		
43	43	Yes		
44	44	Yes		
45	45	No	DRM should ensure that the integrated STBs are verifiably located within India by reference to internet protocol address and service address. 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.	The hybrid STB is an internet device which is already permitted as per Table-2 Clause 21 and Table-4 clause 16.
46	46	Yes		
47	47	Yes		
48	48	Yes		
49	49	Yes		
50	50	Yes		
51	51	Yes		

Table 3: Fingerprinting requirements under DRM

Sl No	Clause No.	Yes / No	AMENDED Clause proposed by us for the disagreed amendments proposed in this CP	Reasons with full justification for your response
1	1	Yes		
2	2	Yes		
3	3	Yes		
4	4	Yes		
5	5	Yes		
6	6	Yes		

7	7	No	The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), settings, blank screen and in all screens of the Linear channel Interface in case of Hybrid STB	In case of hybrid STB the user exits the Linear channel interface and switches to other applications in the HYBRID STB it is no more relevant since the linear channels are not accessible as per Table-2 Clause 21
8	8	Yes		
9	9	Yes		
10	10	Yes		
11	11	Yes		
12	12	Yes		
13	13	Yes		
14	14	Yes		
15	15	Yes		

Table-4: STB Requirements for DRM for IPTV services

Sl No	Clause No.	Yes / No	AMENDED Clause proposed by us for the disagreed amendments proposed in this CP	Reasons with full justification for your response
1	1	Yes		
2	2	Yes		
3	3	Yes		
4	4	Yes		
5	5	Yes		
6	6	Yes		
7	7	Yes		
8	8	Yes		
9	9	Yes		
10	10	Yes		
11	11	Yes		
12	12	No	The watermarking network logo for all channels shall be inserted at encoder/Transcoder end only. In case of infrastructure sharing, it shall be as per terms and conditions of infrastructure sharing.	If watermarking network logo is not inserted for the FTA Channels they can be redistributed without an MSO License including in OTT platforms. For some channels IRD with IP/OUT were used in place of encoders and transcoder can be used in place of encoders for insertion of logo
13	13	No	DRM/SMS deployed should be able to send scroll messaging which should be only available in the lower part of the screen.	SMS can execute the required function without DRM involvement by sending the commands to the DPO Application.
14	14	Yes		
15	15	No	STB should take all commands directly from SMS/DRM not from any intermediate servers.	As per Table-2 Clause 3, DRM deployed do not have facility to activate and deactivate a Set Top Box (STB) directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs shall be done with the

				commands of the SMS integrated with DRM.
16	16	Yes		
17	17	Yes		
18	18	Yes		
19	19	No	STB should have copy protection – HDCP with version 2	DHCP, CGMS & Macrovision with version 7 and above are designed only for the Analog output devices
20	20	Yes		
21	21	No	Only the DRM supported streaming containers/formats (MPEG-TS , Mpeg-Dash, hls etc) and network protocols (http , hls, TCP, UDP etc) are to be deployed	As per the latest enhanced security polices some of the older streaming formats are not supported by the Popular DRMs and the latest 4k HEVC Codec. TCP is a two-way reliable protocol unlike UDP and as per Table-2 Clause 5 DRM should be able to support two-way networks only and TCP is the only option in this case. Detailed information is given in Annexure-3
22	22	Yes		
23	23	Yes		

Response for Digital Rights Management (DRM) on issues other than those Proposed in the CP

Tabel-5: SMART TV Requirements for DRM for IPTV Services

S No	Clause No.	Additional Clause Suggested for Amendment	Reasons with full justification for the proposed Amendment
1	1	The DRM should support the operating system and the related hardware chipset in the SMART TV	DRM decryption is handled by end-user device hardware and not the Software Application.
2	2	The DPO Application should accept only the commands from the SMS and DRM	The DPO Application should not give access to any third party Applications via its API or other means.
3	3	The DPO Application in the Smart TV should not give access to any other content or streaming applications available in the SMART TV	OTT content should not be accessible from the DPO application similar to HYBRID STB.
4	4	The DPO Application in the SMART TV should not gives access to its linear channels or other content to any 3 rd Party applications installed in the Smart TV	OTT or other Applications installed in the Smart TV should not get access to the linear channels or other content in DPO Application similar to HYBRID STB.
5	5	The DRM should support and enable forensic watermarking for the Smart TV	Forensic watermarking gives enhanced security for tracking the content piracy.
6	6	The DPO Application should have overlay permission for execution of all types of Fingerprinting as per Table 3. If by any means the overlay permission is disabled for the DPO Application it should prompt to re-enable overlay permission to proceed for the startup of the Application. If the overlay	Smart TV have the special permission features for the individual Applications installed in it. Overlay permission is one them used for fingerprinting to display fingerprint over the top most layer of the linear channel.

		permission is not granted the DPO application should not startup.	
7	7	The DPO shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals from its Application installed in the Smart TV	In case of IPTV STB also only the Application is involved not the STB hardware/firmware or the operating system.
8	8	The DPO Application installed in Smart TV should support both visible and covert types of finger printing	This provides additional Security for tracking piracy compared to OTT Applications.
9	9	The fingerprinting should not get invalidated by use of any device or any third party Application installed in the Smart TV	The DPO Application is responsible for the security and should not give access
10	10	The finger printing should not be removable by pressing any key on the remote of the Smart TV until the user exits the DPO IPTV Application.	This provides additional Security for tracking piracy compared to OTT Applications.
11	11	The fingerprinting should be on the topmost layer of the video.	Always provides the visibility
12	12	The finger printing should be such that it can identify the unique Smart TV id or the MAC ID of its network interface	Facilitates the blacklisting of the Smart TV for the DPO Application in case it is involved in piracy.
13	13	The finger printing should appear on the screens in all scenarios, such as menu, Electronic Program Guide (EPG), settings within the DPO Application until the user exits the IPTV Application.	Similar feature of the IPTV STB
14	14	The location, font color and background color of fingerprint should be changeable from head end and should be random on the CPE	Similar feature of the IPTV STB
15	15	The finger printing should be possible on global as well as on the individual user Account registered in the Smart TV	Similar feature of the IPTV STB
16	16	The overt fingerprinting/watermarking should be displayed by the DPO without any alteration with regard to the time, location, duration and frequency	Similar feature of the IPTV STB
17	17	The DRM deployed should be able to generate fingerprinting/watermarking both global fingerprinting as well as targeted channel fingerprinting/watermarking.	Similar feature of the IPTV STB
18	18	The DRM shall support and enable forensic watermarking for the Smart TV	Similar feature used by popular OTT Applications
19	19	The Smart TV deployed should be capable to support content decryption, decoding and DRM License evaluation from the installed DPO Application.	Similar feature of the IPTV STB
20	20	The Smart TV should be individually addressable from the headend using the installed DPO Application.	Similar feature of the IPTV STB

21	21	The Smart TV should be able to receive messages from the headend using the installed DPO Application	Similar feature of the IPTV STB
22	22	The Smart TV should be able to display messages with minimal character length of 120 characters in the DPO Application installed.	Similar feature of the IPTV STB
23	23	There should be provision for global messaging and the individual user messaging to the DPO Application installed in the Smart TV	Similar feature of the IPTV STB
24	24	The Smart TV must be complaint to the applicable Bureau of Indian Standards	Similar feature of the IPTV STB
25	25	The DPO Application installed in the Smart TV should be addressable over the air to facilitate OTA software upgrade of the DPO Application.	Similar feature of the IPTV STB
26	26	The Smart TV should not have any facilities for recording the linear tv channels from the DPO Application installed in the Smart TV	Similar feature of the IPTV STB
27	27	The watermarking network log for all the channels shall be inserted at encoder or transcoder level only. In case of infrastructure sharing, it shall be as per terms and conditions of the infrastructure sharing.	Similar feature of the IPTV STB
28	28	The DPO Application deployed in the Smart TV should be able to send scroll messaging which should be only available in the lower part of the screen.	Similar feature of the IPTV STB
29	29	The DPO Application in the Smart TV should be able to geo tag the Smart TV deployed in the network for security.	This feature helps in tracking the location of the users and prevent them in using the services outside India.
30	30	The DPO Application in the Smart TV should take all commands directly from the SMS/DRM and not from any intermediate servers.	This will protect the subscription accounting of the users
31	31	The DPO Application 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 DPO Application in the Smart TV from any other source other than the one specified by the IPTV system.	This will protect the subscription accounting of the users
32	32	The DPO Application installed in the Smart TV should have forced messaging capability including forced finger printing display	Similar feature of the IPTV STB
33	33	DPO system should have capability to maintain un-editable logs of all activity and configurations including DPO OTA upgrades.	This feature prevents the mismanagement of the subscription accounting. OTA

			upgrade logs will help in bugfixes of a particular version of the DPO Application.
34	34	The DRM should log the model no of the Smart TV along with unique user id in its session logs.	The DPO can identify if any particular model of the Smart TV requires bugfixes.
35	35	If a particular Smart TV model is compromised in DRM Security feature the DPO should have a system to de-activate all the Smart TVs of the that particular Model No.	If any particular Model of the Smart TV is not compatible as per the Regulations they can be deactivated.

Annexure-1

Unicast Vs Multicast Transmission for IPTV Networks

- 1) The content is encrypted with the DRM at the source headend and decrypted only in the STB/CPE, unicast or multicast transmission does not effect security of the content in any manner.
- 2) Multicast is only a one-way network which uses UDP (User Datagram Protocol) as transport layer protocol. There is no reliability, flow control or error recovery functions in UDP and Unicast is a two-way Network uses TCP as the transport layer protocol which uses a three-way handshake to check for data transmission errors.
- 3) As per Table 2 Clause 5 (DRM deployed should be able to support two-way networks only)
- 4) In order to stream effectively with Multicast the MSO/LCO need to have their own managed network end to end and it cannot operate in most of the existing broadband networks of ISPs. Every device deployed in the network should support multicast with the same performance level. It's not a solution that's suitable for MSO/LCO who don't have their own network.
- 5) Multicast streaming model does not scale easily to heterogeneous networks which are predominant in ISP's broadband networks.
- 6) Multicast does not support Point to Point Wireless Links, home Wi-Fi devices and PM-WANI Networks.
- 7) Most of the IPTV Android devices have Wi-Fi option which enables wireless connectivity to user's television sets which avoids Lan cable installation for IPTV STB.
- 8) Multicast assumes that everyone receiving the stream has the same bandwidth capabilities and that they are using a similar device to access the content. This makes it difficult to scale and cater to viewers who have lower or fluctuating bandwidth.
- 9) As per scope of Technical Audit IPTV linear services should not be available on Internet/public network. The solution for this is restricting the IPTV distribution to private unicast networks instead of restricting the distribution only to multicast networks. For setting up private networks, three IP address ranges have been reserved by IANA as per below table

S No.	Reserved IP Address Range	Network Class
1	10.0.0.0 ----- 10.255.255.255	Class A
2	172.16.0.0 ----- 172.31.255.255	Class B
3	192.168.0.0 --- 192.168.255.255	Class C

The Internet Assigned Numbers Authority (IANA) is a standards organization that oversees global IP address allocation.

These private IP address ranges have been documented in RFC 1597 and RFC 1918. Private IP address ranges are not routed in the internet and can be used without registration in any number of private networks.

- 10) Table-2 Clause 45 is not applicable if it is multicast transmission.
- 11) Restricting IPTV transmission to multicast mode only just like cable TV transmission as per Table-2 clause 33 prevents the licensed MSOs in adopting the latest technology for enhanced user experience including the future 4k transmission and compete with unlicensed OTT content providers.
- 12) Unicast streaming allows the use of existing networks of ISPs broadband networks and this encourages the ISP provider to expand their network to television households who does not have internet and contributes to penetration of internet in rural India and narrows the digital divide between urban and rural population for the success of Digital India Mission.
- 13) Rolling out exclusive multicast network for IPTV distribution is not a suitable revenue model for the NCF charges specified by TRAI.
- 14) Most of the popular Broadcasters in India are having their OTT applications with DRM which uses unicast internet transmission and there is no reason to discriminate licensed MSOs preventing them to use unicast transmission.
- 15) Fourteen Broadcasters have already approved our unicast distribution in private networks and signed the RIO agreements including major broadcasters like Star India (P) Ltd, Sony Pictures Networks India (P) Ltd, India Cast Media Distribution (P) Ltd, Sun Distribution Services (P) Ltd, Eenadu Television (P) Ltd and others.

Annexure – 2

Use of Stream Multiplexer or CDN (Content Delivery Network)

- 1) The Content of all the channels were encrypted with the DRM at the source headend before the distribution network and decrypted only in the STB as per the subscription status of the STB/user.
- 2) Amended clause is proposed in Table-2 Clause 34 for use of CDN in unicast networks (IPTV transmission should be in encrypted format and only the STB/CPE should be allowed to decrypt as per the subscription status. CDN/Stream Multiplexer involved should not have any facility to decrypt and encrypt and should distribute the stream in the same format of the source stream in real-time)
- 3) Advantages of Unicast transmission and its relevance with DRM systems is already explained in Annexure-1
- 4) CDN provides an extra layer of security and control. The resellers can select only the channels and bouquets as per local regional demand in the local CDN and as per the minimum requirement of TRAI regulation and can save the Point-to-Point Link transmission cost.
- 5) CDN helps in Users segmentation location wise and contributes to viewership analytics.
- 6) The subscribers of a reseller can be locked to their local CDN and can be migrated to other reseller only after approval, considering the existing commercial transactions.
- 7) Stream multiplexers or CDN's are used for multiplication of streams for unicast stream transmission and multicast switches and devices are used in multicast transmission.
- 8) CDN's performs similar function of EDFA in traditional CATV systems.
- 9) Prohibiting the use of CDNs/Stream Multiplexers limits the scalability of IPTV distribution and discourages the investment in IPTV platforms which is the best option of competing the growing market share of OTT platforms which are not regulated as per MSO guidelines.

- 10) CDNs help in overcoming the bandwidth bottlenecks in the distribution trunk lines.
- 11) CDNs can be connected with multiple redundant trunk lines and helps in maintaining 100% uptime and compete with OTT platform services.
- 12) Major global Premium Content providers like Netflix, Primevideo, Disney Hotstar are using CDNs for their distribution and when MSO is offering additional finger printing features as per TRAI guidelines there is no security reason to prevent them from using CDNs in their distribution network.
- 13) Fourteen Broadcasters have already approved our unicast distribution with CDN in private networks and signed the RIO agreements including major broadcasters like Star India (P) Ltd, Sony Pictures Networks India (P) Ltd, India Cast Media Distribution (P) Ltd, Sun Distribution Services (P) Ltd, Eenadu Television (P) Ltd and others.

Annexure-3

DRM support for Stream Container formats and transmission Protocols

- 1) The streams are encrypted using the DRM at the source Headend of the MSO and decrypted only inside the user's STB/CPE and hence the stream container format or the protocols do not compromise the security of the content.
- 2) The latest HEVC codec which is used for 4k and above resolutions has limitations in adapting to all available stream container formats and protocols. MSOs should be given opportunity to upgrade to the latest technology available instead of limiting them to use the age old technology.
- 3) Mpeg-Dash is the only streaming solution certified by ISO (International Organization for Standardization) and the latest which support HEVC codec which has the benefit of highest compression in the industry with best quality.
- 4) When the DRM supports a particular stream container format or a codec there is no purpose to restrict the use of them since DRM is responsible for the security of the content.
- 5) MPEG-DASH is a company independent, open and international standard, which has broad support from the industry.
- 6) Major Content providers like Youtube and Netflix are using MPEG-DASH and restricting MSOs in adapting to the latest technology is not recommended.
- 7) Restricting licensed MSOs in adapting to the latest technologies encourages the subscribers to migrate to OTT platforms.

Annexure-4

SMART TV as an IPTV CPE for MSO

- 1) SMART Televisions are rapidly increasing their market share in television sales in India and global market.
- 2) As per Table-5 all the requirements for IPTV distribution can be accomplished using DPO Application in the SMART TV in place of IPTV STB as per TRAI guidelines except the Annexure-4 Certificate from the device manufacturer. It should be noted that all the requirements are implemented from the DPO Application integrated with the DRM installed in the SMART TV and not directly from the SMART TV.
- 3) Copy Protection systems - HDCP, DHCP, CGMS and Macrovision are not required since there is no cable between the decoder and the television, the encrypted channel streams are decrypted inside the Smart TV offering better security.

- 4) As per TRAI guidelines MSO provides all types of fingerprinting to their Smart TV Application similar to CATV STB which is an additional security compared to OTT Applications.
- 5) Introduction of SMART TV for IPTV distribution by MSO is the perfect solution for Interoperability of consumer devices between MSOs as per TRAI recommendations to Ministry of Information and Broadcasting.
- 6) The consumers who are already having Smart TV can migrate to IPTV subscription without any upfront investment and experience enhanced quality of linear TV channels compared to OTT services and migrate to other IPTV operators without changing the STB/CPE.
- 7) If the DRM deployed by MSO for their IPTV distribution is of equal standard compared to OTT applications MSO should be allowed to use Smart TV as their IPTV CPE (Customer Premise Equipment)
- 8) The Premium content providers like Youtube, Netflix, Disney, and most of the popular broadcasters in India have launched their OTT service Applications in Smart TV platforms.
- 9) When most of the popular broadcasters in India are distributing their content using their OTT Applications in Smart TV there is no reason to restrict licensed MSOs to use Smart TV as per IPTV Regulations.
- 10) Licensed MSO follow TRAI guidelines to honor consumer rights to allow them to choose only the channels they desire and transmit all the mandatory Doordarshan Channels unlike OTT players of live channels.
- 11) Consumers are migrating from licensed MSOs to OTT Applications provided by most of the popular broadcasters and hence MSOs should be given opportunity to use Smart TV as their IPTV CPE and compete with the unregulated OTT players in the market.

Thanking You,

Regards,

S Raghava Rao Signature:

Date:6-10-2022

Director

City Online Media Private Ltd. (M.S.O), Contact: srrao@ulka.tv , Ph.9848028638

Chairman & Managing Director

City Online Services Limited (I.S.P), Contact: srrao@cityonlines.com

Address: City Online Media (P) Ltd, 701, Aditya Trade Center, Ameerpet, Hyderabad - 500038