COMMENTS/RESPONSES TO THE CONSULTATION PAPER ON:

THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES DIGITAL ADDRESSABLE SYSTEMS AUDIT MANUAL

SUBMITTED BY:

TEV AUDIT AND TECH SOLUTIONS PVT. LTD.

Q1. Whether it should be mandatory for every DPO to notify the broadcasters (whose channels are being carried by the DPO) for every change made in the addressable system (CAS, SMS and other related systems)?

We feel that it should be mandatory for every DPO to notify the Broadcasters (either individually or through IBF/NBA) for every change, modification and alteration made to the configuration or version of the addressable system (CAS, SMS and other related component which have commercial implication or affects the technical compliance of the DAS system).

Such information should be communicated to the Broadcasters (either individually or through IBF/NBA) definitely within 7 days of such a change having been effected by the DPO.

Further, then, the previously issued Report/Certificate of compliance issued by the previous Audit Agency would also become invalid and the Broadcasters should have the right to Audit the DPO's system once again under Clause 10 (7) of the Interconnect Regulations, 2017 as has been rightly observed in 3.1.4 of General Guidelines for Conducting Audits.

Q2. Whether the Laptop is to be necessarily provided by the Auditee DPO or the Audit Agency may also provide the Laptop? Please provide reasons for your comment.

We acknowledge that the Regulator has rightly proposed that the DPO and the Audit Company should enter into a Mutual Non-Disclosure Agreement which should bind the Audit Company, its Auditors and other employees to maintain absolute confidentiality about the DPO's DAS System/Network Design and the Data extracted there from.

Generally, the Auditors carry their own laptop while conducting DAS audits. However, as these laptops contain sensitive and confidential data pertaining to the audit company, it is not possible for the auditors to leave their laptop behind at the DPO's premise at the end of every day's work during the audit.

Hence, for any reason, if the DPO is not comfortable with the Auditor taking the extracted data out of the DPO's premises (even though there is a signed NDA in place) for further data analysis and report preparation, it is only fair that a Laptop/PC is provided to the Auditors by the DPO with all the required softwares/application installed in it, in order to carry out this part of their job.

Q3. Whether the Configuration of Laptop vide Annexure 1 is suitable? If not, please provide alternate configuration with reasons thereof.

The configuration of laptops/systems vide Annexure 1 is suitable.

Q4. Do you agree with the provisions regarding seeking of TS recording and ground sample information from IBF/ NBA for verification/ checking by the Auditor?

Comparing the TS recorded at the DPO's Headend with the same recorded at its network (on pre-audit as well as post-audit dates) is very crucial for the Auditors to understand the possibility of any Revenue Leakage in the DPO's Digital Addressable System/Network Design.

In order to ensure the accuracy of such network TS Recordings, we believe it is only apt that the IBF/NBA should facilitate the field TS recordings and the same should be carried out by the Auditors.

Also, the ground sample STB/VC data provided to the Auditors for necessary checking/verification should be provided by IBF/NBA prior to commencement of the Audit as has been stated in clause 4.1 x.

Q5. Do you agree that Data Dump may be cross-checked with weekly data of sample week's basis? If yes, do you agree with checking of random 20 % sample weeks? Please support your comments with justification and statistical information.

Yes. We agree with this methodology of cross-checking of weekly data on sample week's basis.

We also agree with the suggested 20% sample weeks for random checking of the data dump as we feel that a 20% sample is a sufficiently high statistical sample for checking the sanctity of the data that is being extracted.

Q6. Do you agree with the proposed Data extraction methodology? If not, suggest alternates with reasoning thereof.

Yes. We agree with the Data Extraction methodology.

Further, since this extraction of data is being done in the presence of the Auditors, all the data being extracted should be in a format which is more suitable for accurate data analysis (like csv, txt, xlsx, xls, etc.). This is important since converting tabular data stored in PDF format to csv/txt/xlsx is very much prone to errors. In many instances it has been observed that the converted data tends to overflow the column width and results in erroneous conversion and needs further cleansing before the same can be used for reconstruction/analysis.

Q7. Do you agree with verification and reporting of City-wise, State-wise and Head-end wise subscription report? Please provide supporting reasons/ information for your comment.

In order to maintain sanctity of the data being reported, the subscription report should be City-wise, State-wise and Head-end wise, however, the verification of this City-wise, State-wise and Head-end wise data is possible only from the SMS in most of the cases.

The reason for this is that at present, most of the CA Systems do not have a provision of storing the data in the database basis City/State/Head-end wise bifurcations. Even in the case of DPOs/Distributors using multiple Area Servers for each Area being catered to by the DPO/Distributor, no City-wise/State-wise/Head-end wise bifurcation is found in the CAS database of these Area Servers.

Q8. Do you agree with the tests and procedure provided for checking covert and overt fingerprinting? Provide your comments with reasons thereof?

We agree with the tests and procedures as laid down in the Audit Manual for checking covert fingerprinting.

However, for checking overt fingerprinting, we suggest the following alternate tests and procedures (along with the reasoning/explanations for the same):

a) ECM Based Fingerprinting:

*Every service/channel in a Digital Addressable System should have its unique ECM streams for each CAS in order to be compliant with **Schedule III A10** clause of the Regulation. It depends up on the stored entitlements (active packages/channels), which enables the STB to retrieve the Control Word (which is encrypted and transmitted though ECM(s) by the Scrambler and Simulcrypt Synchronizer) and decrypt the encrypted service/channel. In case the STB doesn't have proper entitlement active in it to view a particular service/channel, it will not be able to decipher its ECM and retrieve the Control Word. This also means that, if ECM based fingerprinting is triggered on any such channel for which the STB doesn't have proper*

entitlement (in simple words, a channel which is not active on that STB), theoretically the STB shouldn't be able to display that fingerprinting either.

Hence, we believe in an ideal scenario, ECM based fingerprinting triggered on a channel should be visible only on that particular channel on all the STBs at the same time, barring those STBs on which that channel is not active/authorized.

Suggested test and procedure for checking ECM Based Overt Fingerprinting

1. *ECM based fingerprinting should be triggered from SMS/CAS targeting a particular channel and such triggering should not require any target STB Range (Single/Group/All) parameter to be mentioned.*
2. *Triggered ECM based fingerprinting should be visible only on that particular channel on all the STBs at the same time, barring those STBs on which that channel is not active/authorized.*
3. *The time gap between the ECM based fingerprinting triggered in CAS and the same getting displayed at the STB output should be less than or equal to the ECM Cycle Time defined in CAS or Crypto Period defined in Mux/Scrambler.*

b) EMM Based Overt Fingerprinting:

EMMs are specific to each subscriber as identified by the unique STB/VC identifier. An EMM Based fingerprinting can be triggered targeting a single STB/Group of STBs/all the STBs in the Network. Basis this target range, fingerprinting should be displayed at the STB(s) output visible on the TV screen irrespective of the channel which is being viewed at that point in time. Even if the targeted STB(s) is/are tuned to a channel which is not active/authorized for viewing, EMM based fingerprinting should be visible on that channel as well.

Suggested test and procedure for checking EMM Based Overt Fingerprinting

1. *EMM based fingerprinting should be triggered from SMS/CAS targeting a STB Range (Single/Group/All) and need not require any channel parameter to be mentioned on which the FP will be visible.*

2. *Triggered EMM based fingerprinting should be visible on all the STBs mentioned in the target range irrespective of the channel being viewed at that point in time even if the channel is not authorized for viewing.*

Q9. Any other suggestions/comments on the provisions or methodology proposed in the Audit Manual.

ADDITIONAL SUGGESTIONS/COMMENTS ON THE PROVISIONS AND METHODOLOGY PROPOSED IN THE AUDIT MANUAL

Regulation Clause 15 (3) – "Every distributor of television channels shall offer necessary assistance to auditors so that audits can be completed in a time bound manner"

It is suggested in the Audit procedure that:

"(b) DPO to allow auditors to run queries to extract data / logs / reports from live SMS and CAS systems (Auditors to not accept any pre-extracted data/reports from SMS & CAS systems)"

Our Comments:

It has been observed by us that many CA Systems do not have a ready Report or a Database Query/Script available in their systems, that allows extraction of following data as proposed in this Audit Manual:

- *Historical month-end active and de-active STB/VC wise subscriber counts for the audit period*
- *Historical month-end active and de-active package and channel-wise subscriber counts along-with details of such STB/VC for the audit period*

Alternatively, In order to comply with the Regulation, those CA Systems have a mechanism in place that automatically extracts these data at a pre-defined time in the system on a daily basis and stores it in a pre-defined format (txt/csv/xlsx/pdf) under a certain folder in the CAS server.

We feel that the following issues also should be clarified in the Audit Manual in order to avoid any dispute between the Auditors and the DPOs/Distributors at the time of Audit:

Should the Auditors accept these pre-extracted data for such CA Systems, if:

1. *The CAS Vendor acknowledges this system limitation in its Declaration and also certifies the Specific Time and folder location of this data getting saved automatically every day.*
2. *Date/Time Stamp (of creation and last modification) and folder location of these pre-extracted data files are in line with that certified by the CAS vendor in its declaration.*

Schedule III A2 – "The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands."
And
Schedule III A3 – "It shall not be possible to alter the data and logs recorded in the CAS and the SMS."

It is suggested in Audit Procedure that:

"Auditor to download log from SMS and CAS and check the following:
i. These have date & time stamp.
ii. They are in un-editable format (including PDF format)"

Our Comments:

Every transaction in CAS and SMS are recorded and stored in their respective database table(s) chronologically according to their date/time of execution and a unique "log_id" is also assigned to each of these logs.

CAS/SMS Providers who do not allow the Auditors to access their database, generally have a mechanism in place to export these logs on a daily basis and store it in separate files in a pre-defined format under a certain folder. In such cases, these files should be checked for proper Date & Time stamp (of creation and last modification) and also should be in un-editable format (including PDF Format) in order to ensure Schedule III compliance.

Our Suggestions:

1. *Since this Audit Manual also proposes that the auditor should be allowed to access the CAS/SMS database and run queries to extract necessary Data/Logs/Reports, we suggest that all the logs with all the relevant data fields (including "log_id" and "date/time" of each log) should be extracted directly from the CAS/SMS database using necessary queries under the auditor's supervision and the same should be saved in a file format (csv/txt/xlsx) which is less prone to errors and much easier to work with for data-reconstruction than the same stored in PDF file format.*

2. *Like CAS Vendors, SMS vendors should also certify in its Declaration that:*
   "It is not possible to alter the data and logs recorded in the SMS"*.*

Schedule III B13 – "The watermarking network logo for all pay channels shall be inserted at encoder end only"

Our Comments:

We feel that the procedure suggested in the Proposed Audit Manual to check compliance of this requirement is not infallible.

The suggested procedure in the Audit Manual is based on the idea that:-

a. *If the watermarking network logo for all Pay Channels is actually inserted at the encoder end, it is already present in the Digital Stream. Hence, if the RF signal carrying this Digital Stream is disconnected from the STB, the watermarking network logo should also disappear from the STB Output visible on the TV Screen.*
b. *If the Logo is still visible on the TV Screen, then it is inserted at the STB Level, and not at the Encoder end.*

*We know that whenever the STB detects absence of a proper RF Signal at its input, it is programmed to display an error message at the output TV screen, for example: "**Signal not found**". In a similar way while inserting watermarking network logo at the STB level, the STB can be easily programmed to display this logo only when it detects presence of a proper RF signal at its input. In such cases, whenever the RF Signal is lost at the input for any reason whatsoever, the logo will disappear and the error message will be displayed.*

The STB can also be programmed to display watermarking network logo only on those channels where it detects the presence of a custom Service Specific Descriptor in the PSI/SI data. This way the STB will display the watermark logo only on the pay channels, not on the DTA channels, making it further impossible to track whether the logo is inserted at the encoder end or at the STB level.

This way, the system will comply with the requirement as per the Audit Procedure suggested in the audit manual, even while the watermarking network logo is actually inserted at the STB level, not at the pay channel encoder end as mandated in the regulation.

Our Suggestions:

1. *Almost all the DVB Encoders in common use presently, generate its SPTS/MPTS output over IP Multicast which is further routed to the MUX/Edge QAM via managed switches. The auditor should be allowed access to these IP Multicasts in order to play it on a PC/Laptop via VLC Player and check the presence of watermarking network logo in the video.*
2. *Also the DPO should be asked by the Auditor to switch off and switch back on the watermarking network logo from the encoder's management interface (test to be performed on at least one encoder of each make and model) in order to check for its desired effect on the output TV screen.*

Schedule III C8 – "The STB should have forced messaging capability including forced finger printing display."

It is suggested in Audit Procedure that:

"Auditor should trigger scroll messaging from SMS or CAS to all STB in the network which should display the fingerprint as the message. Auditor should take screenshot of the display"

Our Suggestions:

1. *Additionally, tests should be conducted by the Auditor to ensure that the user is not able to abort/discard such forced scroll messages by pressing any button from Remote Control or STB front panel.*
2. *Also, the Auditor should check that once the STB is rebooted while such message is still active on screen, such message should start playing automatically once again when the STB comes back online.*

Monthly Subscription Report as per Regulation Clause 14 (1) and 14 (3) and its format as suggested in Schedule VII of the Interconnection Regulation:

The regulation mandates that Channel/Package/STB wise active count of subscriber to be recorded at any point of time between 1900Hrs and 2300Hrs on 7th, 14th, 21st and 28th day of every month and reported in the monthly subscription report.

Our Comments:

For the purpose of verification of such counts as declared by the DPO in Monthly Subscription Report, the exact time of recording these counts should be mentioned in the Report itself so that the auditors can observe this time while cross checking these counts on a random week basis from the Data Dump extracted from CAS.

The CAS server should also be capable of generating Data Dump for these dates as on that particular time.
