ETSI TR 103 656 V1.1.1 (2020-07)

Lawful Interception (LI);
Study on high bandwidth delivery

Reference
DTR/LI-00166

Keywords
bandwidth, filtering, interception

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The scope of the present document is to assess and characterize the problems associated with interception and secure onward delivery of high-bandwidth user traffic using TCP or TLS, identify whether there is a need to solve these problems, and identify potential technical and other measures that can be used to mitigate or address them.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] CM-SP-CBI2.0-I11-160602: "Cable Broadband Intercept Specification (CBIS)".

[i.2] ETSI TS 103 120: "Lawful Interception (LI); Interface for warrant information".

[i.3] ETSI TS 103 221-1: "Lawful Interception (LI); Internal Network Interfaces; Part 1: X1".

[i.4] ETSI TS 103 221-2: "Lawful Interception (LI); Internal Network Interfaces; Part 2: X2/X3".

[i.5] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[i.6] ETSI TS 102 232-2: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".

[i.7] ETSI TS 102 232-3: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".

[i.8] ETSI TS 102 232-4: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".

[i.9] ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

[i.10] ETSI TS 102 232-6: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".

[i.11] ETSI TS 102 232-7: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".

[i.12] ETSI TS 122 261: "5G; Service requirements for next generation new services and markets (3GPP TS 22.261)".

[i.13] Recommendation ITU-R M.2083: "Framework and overall objectives of the future development of IMT for 2020 and beyond".

[i.14] ETSI TS 103 643: "Techniques for assurance of digital material used in legal proceedings".

[i.15] IETF RFC 6733: "Diameter Base Protocol".

[i.16] IETF RFC 893: "Trailer Encapsulations".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ADMF	Administration Function
API	Application Program Interface
ASN.1	Abstract Syntax Notation 1
BER	Basic Encoding Rules
CC	Content of Communication
CDN	Content Delivery Network
CNLP	Connectionless Network Layer Protocol
COTS	Commercial Off-The-Shelf
CP	Content Provider
CPU	Central Processing Unit
CSP	Communications Service Provider
CUPS	Control and User Plane Separation
DASH	Dynamic Adaptive Streaming over HTTP
DDOS	Distributed Denial Of Service
DER	Distinguished Encoding Rules
DNS	Domain Name System
DPI	Deep Packet Inspection
EIDR	Entertainment Identifier Registry
EVC	Ethernet Virtual Circuit
GW	GateWay
HI2	Handover Interface 2
HI3	Handover Interface 3
HoL	Head of Line
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IRI	Intercept Related Information
ISO	International Organization for Standardization
ITU-R	International Telecommunication Union - Radiocommunication sector
JSON	JavaScript Object Notation
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
LI	Lawful Interception
LIID	Lawful Interception IDentifier
LVSF	LI Video State Function
MAC	Media Access Control
MDF	Mediation and Delivery Function
MEC	Multi-access Edge Computing
MPLS	Multiprotocol Label Switching

MTU	Maximum Transmission Unit
PDHR	Packet Data Header Reporting
PDSR	Packet Data Summary Reporting
PoI	Point of Interception
QUIC	Quick UDP Internet Connection
RAN	Radio Access Network
RFC	IETF Request For Comments
SCTP	Stream Control Transmission Protocol
TC	ETSI Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type Length Value
TR	Technical Report
TS	Technical Specification
UDP	User Datagram Protocol
UE	(3GPP) User Equipment
UGC	User Generated Content
URI	Uniform Resource Identifier
URLLC	Ultra Reliable Low Latency Communications
VPP	Vector Packet Processing
XML	eXtensible Markup Language

4 Context

4.1 Problem statement

The problem of high-volume delivery of user traffic includes the following aspects:

- Issues with HI3 mediation performance with respect to fixed-line accesses.
- Consideration of alternative ways of handing over data in both HI3 and X3.
- Concerns over 5G user-plane data rates.

4.2 High level requirements

This study aims to find the ideal combination of the following two approaches:

- Deliver everything, but more efficiently. Any solution should be able to deliver packets in a reliable fashion ensuring that the traffic seen on is delivered successfully.
- Filter out content. This could consist of suppressing publicly available broadcast content (and including a unique identifier which would allow the content to be recovered) i.e. in theory a lossless form of filtering. Removing content which is likely to be of no operational value i.e. lossy filtering.

The identification of a formal input requirements for 5G defining the actual throughput data rate to be supported for CC delivery (i.e. 20 Gbit/s as peak data rate to be always guaranteed for LI) has not yet been addressed by ETSI TC LI. Such a clarification is quite relevant for implementers when designing the MDF systems to support the new 5G LI solution.

The 3GPP stage 1 service requirements for 5G system ETSI TS 122 261 [i.12] does not detail any CC data rates number in terms of maximum peak rate, it only specifies in table 7.1-1 (Performance requirements for high data rate and traffic density scenarios) experienced data rates which for an indoor hotspot is up to 1 Gbps. Note that the user experienced data rate is the achievable data rate that is available ubiquitously across the coverage area to a mobile user/device.

A clear reference on peak rate traffic is within the Recommendation ITU-R M.2083 [i.13], see Figure 3 page 14.

5 Key Issues

5.1 Transmission, routing and encoding

5.1.1 Encoding/decoding overhead

Generally, encoding only occurs once.

Decoding is done at least once or twice, if not many more times, including during:

- transmission, including retransmission through topologies such as data diodes;
- storage and retrieval; and
- analysis.

When considering protocol changes, it is recommended to optimize for decoding and transmission without being overly costly on the encoder. This is similar pattern to compression, where many compression techniques prioritize decompression performance.

5.1.2 Efficient routing

There may be multiple points along a handover path where the message framing is required to retransmit (e.g. through a data diode). Many formats (including ASN.1 BER, XML) require non-trivial effort to determine the framing of a message, including up to a full decode of the message to determine framing (e.g. see ASN.1 indefinite length encoding).

This is similar to considerations about message size and fixed-length headers in clause 5.1.1 - ability to extract routing information (such as LIID) without full decode may help.

5.1.3 Concentration of CC from POI at MDF

The MDF should collect all CC from a PoI and transform it between X interfaces to H interfaces, sometimes enriching information in the CC with extra information in addition to that coming from PoI and route the flow to the right LEMF. Such COTS/Nodes for legacy systems will face a dimensioning issue at their inputs, even before the problems of encapsulation and encoding, enrichment of headers and delivery to the right LEMF.

This may imply that the Mediation and Delivery Function (MDF) faces an internal higher bandwidth issue than the one related to the delivery to the LEMF. The solution may have to cover the case of virtual MDF and legacy one.

5.1.4 Distributed LI for URLLC/MEC

CDNs based on MEC and URLLC of 5G may need local PoIs in order to reach the required low latency around 10 ms (below 100 km between UE and data centre) and 40 ms on regional basis (i.e. below 1 000 km). However, CUPS (separation of control to user plane) may lead to more complex race conditions and local internal output that may cause issues related not only to backhaul and LI detection/triggering. This also generates issues with the LI architecture related to high bandwidth due to limitation on it for the services to be intercepted, that do not need such extra bandwidth in the backhaul, such as:

- Should the MDF3, next to MDF2, be based locally at the PoI to cover the low latency and CDN issues but extra cost to the delivery to the LEMF due to the distance?
- Should the LI system be based on centralized architecture even for CC delivery to the LEMF next to ADMF and control plane? If so, would such a scenario generate issues on race condition and on internal bandwidth on the backhaul?
- Should there be hybrid architecture with only MDF3 local and the rest of the LI system central?

Such different architectures should be studied with respect to secure packet duplication as it creates some high bandwidth issues either in the internal backhaul either in the delivery to LEMF.

5.1.5 Transmission

The use of TCP as a transport protocol is prevalent throughout an operator's network and extends to delivery to a LEMF and may extend beyond within LEMF facilities.

A TCP connection has a number of problems that restrict its use for high bandwidth situations:

- Head of Line (HoL) blocking.
- Congestion control.
- Slow start.
- Delay-bandwidth product restrictions.
- Requires message framing.

TCP works well in relatively short links with little congestion or network errors. Within the CSP core network, TCP is likely still a good choice. Its limitations are more obvious in:

- the link the between the CSP and LEMF; and
- less reliable RAN links at the edge (where error and retry mechanisms may be necessary).

5.2 Volume of Data

5.2.1 General high-bandwidth services

Interception of an Internet Access Service requires the interception and delivery of the entire communications content of the target which can be quite large. On top of this, there is the additional and necessary LI metadata which increases the volume of data even further.

5.2.2 Video on demand services/publicly available media

As of May 2020, video on demand made up approximately 58 % of mobile internet bandwidth. Investigative value derived from video on demand services is low compared with the resources required to transport, process and store it. It could be of value to create a function to enable an LEA to request that this data is not delivered or summarized. There are legal precedents in some countries around not delivering broadcast video (arising from historical differences in how broadcast services were delivered).

5.2.3 Data integrity

It is important to consider the integrity of material if it is intended to be used as part of legal proceedings.

It is not necessarily the case that removing/filtering material means that integrity has been lost and that the material is no longer suitable for use in court. It is important that the criteria for removing data are well-understood, are well-formatted, are stored and are correctly applied.

6 Potential solutions

6.1 Efficient Transmission, routing and encoding

6.1.1 Fixed-length headers

Being able to determine the full message size by examining a smaller (relatively fixed size) header before reading/processing the entire message payload is a huge benefit for implementations. ASN.1 BER with indefinite length encoding is not adequate here, because that requires a full recursive decode of the ASN.1 TLVs to find the message framing boundary. ASN.1 DER with enforced definite length encoding enables to read the first few bytes of the first TLV to provide the message framing.

With fixed-length headers (e.g. ETSI TS 103 221-2 [i.4]), further efficiencies can be considered including aligning fields on 32 bit boundaries, having the payload at a fixed offset with options/extensions moved to trailing octets, etc. See protocols such as Diameter (IETF RFC 6733 [i.15]), and historically, Ethernet trailers in the 1980s (see IETF RFC 893 [i.16]).

Hardware offload of traffic routing is more likely with fixed headers rather than variable length encoding such as ASN.1/XML/JSON.

6.1.2 Use of UDP

While UDP does not suffer some of the concerns raised against TCP in clause 5.1.5, use of UDP as a transport protocol for LI has significant weaknesses which are incompatible with the main LI requirement. These are:

- Packet loss caused by no automatic retransmission; erroneous packets are discarded.
- Packet loss caused by no flow control. This allows destinations to be overwhelmed, causing more packet loss.
- Out of order packets.
- Increased CPU utilization when handling large numbers of small messages. This is because each packet is sent in a single UDP message.
- Fragmentation of UDP messages exceeding MTU (Maximum Transmission Unit) bytes. The LI-header (~64 byte) prefixed to each packet leads to earlier fragmentation.

Some of these limitations could be addressed with UDP/Ack on the application layer. However, this is much slower than the transport layer and the risk of improper implementation is increased. UDP/Ack would increase the problem with out-of-order packets.

6.1.3 Use of IP/SCTP

Used by telcos internally, but many protocols (e.g. Diameter) that support IP/SCTP also permit IP/TCP.

6.1.4 Use of ISO CNLP

The ISO stack is effectively dead outside of some niche areas.

6.1.5 Use of Ethernet Virtual Circuit (EVC)

The use of Ethernet Virtual Circuit (EVC) might be useful if the underlying user service is layer 2 (without layer 3 IP), but even then it appears that it is often tunnelled over MPLS anyway, in which case extra Ethernet layers (and packet bytes) are being transported unnecessarily.

6.1.6 Use of QUIC/HTTP/3

QUIC and HTTP/3 might be an option because that has explicitly been designed to use IP/UDP and transit existing middleware infrastructure.

HTTP/3 is notionally split into two layers, a QUIC transport layer and an HTTP abstraction that assumes and optimizes performance based upon its knowledge of the underlying transport.

It is built on top of UDP but providing reliable in order delivery as well as multi-homing, multi-stream capabilities.

This variant is not recommended for CC data transport due to the overhead of the HTTP abstraction and interpretation.

6.1.7 QUIC transport

A more promising solution (compared to clause 6.1.6) would be to use only the QUIC transport layer as an alternative to TCP. It may also suffer some of the issues of UDP with small message sizes (though packing multiple logical stream messages into one larger physical packet may mitigate this drawback. It may also require significantly more CPU in order to implement most of QUIC in the CPU rather than via network interface card offload/kernel support.

6.1.8 Developing a custom transport protocol

It is not productive for ETSI TC LI to consider working on transport protocols already developed or being developed in IETF.

6.1.9 IP/TCP with explicit multi-connection support

While there are variants of TCP that give a protocol-level multi-home and multi-stream support, these would require changes at an LEMF receiver. Instead, a backward compatible solution requires a collection of TCP connections directed to the same endpoint. Those connections could originate from different physical links to spread throughput or could be based on several connections through one physical path. The key benefit is that each connection has independent HoL blocking, congestion control and delay-bandwidth product.

Multi-connection support is also allowed and discussed as part of ETSI TS 102 232-1 [i.5] as an extension to single connection support. A LEMF already needs to support this use case when receiving data from multiple CSPs so it is likely to have a relatively low impact and it scales as the number of available physical links increases. Load balancing across the various connections would be achieved by selecting a particular path on a per LIID basis at task allocation. Delivery details would reflect the selected logical delivery endpoint. It is important that all traffic relating to a single LIID (including all its sessions) is directed to the same endpoint so that independent hold-ups on other connections do not affect the management of the warranted sessions on the current connection. It is assumed that LEMF receiving processes do not require in-order delivery across different warrants.

The strategy for choosing which route to use for a new warrant could be explicit from the LEA. In practice, selecting the next available delivery endpoint based on random or round-robin selection between available endpoints may be sufficient and would lower the barrier for LEAs. A LEMF not requiring the performance or not wishing to define the extra endpoints would continue with a choice of 1 and always select it.

6.2 Filter excess data volume

6.2.1 Use of 3GPP PDSR/PDHR capabilities

Bearing in mind that not all of the communications content may be needed by LEAs, then a mechanism could be devised to exclude certain large bandwidth data flows from being intercepted and delivered to the LEMF at the direction of the LEA. Such a mechanism would require defining the criteria for identifying the flows to be excluded (e.g. IP Packet header information such as the 5-tuple or 6-tuple set of information). It could also take into account identification of any specific carrier provided/managed service for which flows could be excluded.

6.2.2 Identification of publicly available media via IP address lists

A list of IP addresses and ports associated with known lawful public content (i.e. material that should be excluded from LI delivery) may be available. It would be important to note that this will need to be updated in order to aid trigger mechanisms. This introduces a maintenance issue and would mean LEA would get some Lawful Public Content streams until the list of IP addresses and ports are updated.

Note that the Entertainment Identifier Registry (EIDR) http://eidr.org/ (assuming access to clear text) could be considered as a used to strip out the meta data. This would impact trigger points, i.e. content might not even be captured as the header would already indicate all meta data required. Attaching additional meta data (e.g. hashed user ID, public IP address consuming the content) would also aid the meta data collection. This would require standards development in this area.

Various content providers use their own or modified clients to deliver content in order to protect their copyrighted material, improve the user experience, adapt the quality based on the access mechanism or support network topologies where agreements are in place (caching). This may require codex support for all public content providers and the ongoing maintenance and updates.

Stakeholders in ETSI, 3GPP and other standardization fora should be surveyed on some of these points, to ask about codecs, meta data or stream formats that may be required in the mediation devices to determine content type and meta data extraction.

It would be important to investigate whether sites could allow to make User Generated Content (UGC) available within material that is marked as lawful public content. Some means is required to distinguish these feeds in order not to miss these UGC, bearing in mind there may be modes of distributing hidden intelligence that is required for a case. UGC may not last on a site and may be removed pending its content.

6.2.3 Identification of publicly available media via DNS

One way to reduce high-bandwidth delivery is to reduce the amount data (via filtering, suppression, and meta data support) that is delivered when the subject is accessing publicly available media.

The assumption is that one is accessing lawful public content from the internet. This means web-supported versions of broadcast content, which are made available for free or provided as a video-on-demand service for a fee or to increase viewership and revenue streams associated with that use.

While a DNS query might be used as trigger (it identifies or pre-triggers logic that a video feed is imminent), it does not allow access to the titles (meta data) that might be required for digital evidence. The web sites (usually using encrypted links) may provide links to content but may use a picture to indicate the content or internal dynamic links. These web pages will undergo revision as new content become available and as new picture art is generated for the icon of the content. It is not clear if this can be used to create the meta data of the content or if the meta data created can locate the same content later if required for evidence. It would require a database of known IP addresses of public content.

One could argue that the DNS query points to a public content site. However, these are internet sites that may host additional services (e.g. allowing comments to be made) that are still in the jurisdiction of collection, so cannot on its own be used to trigger.

6.2.4 Identification of publicly available media via EIDR

6.2.4.1 Use of EIDR in CSP Network

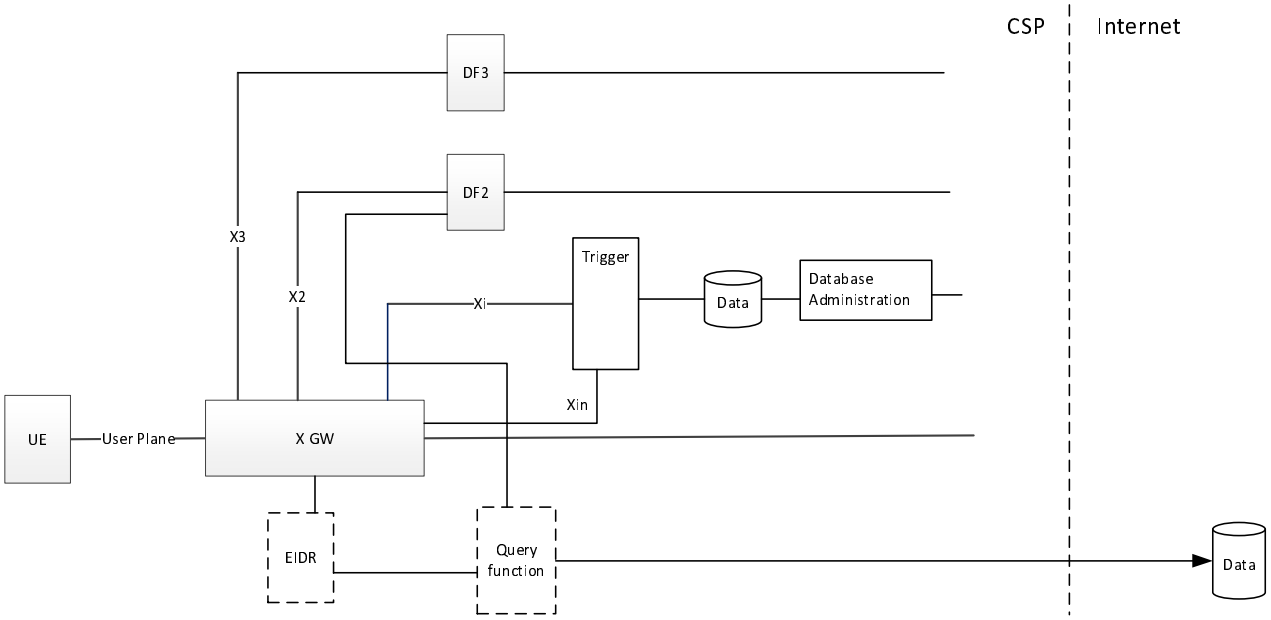

Figure 6.2.4.1-1: Use or EIDR in CSP Network

Figure 6.2.4.1-1 provides an example and describes using IP address to filter. This solution provides additional scrutiny of the filtering request by analysing the users stream for EIDR labels or identifications. It then queries a public database that manages these assets for information regarding the asset. That query is used to provide additional information into the IRI data when available. This function could be within the gateway, where it could also be used to trigger the filtering along with the IP trigger data. Additionally, the use of the EIDR and or similar databases could be used to update or summarize new CP sources that need to be vetted prior to installation in the databases. The EIDR in the CSP can be a copy of the public database and synced on new request of unknown asset tags, or periodically depending any business relationship with the EIDR.

6.2.4.2 Use of EIDR in LEA

Figure 6.2.4.2-1 shows a situation where the function is located in the LEA. In this situation it would be important to choose whether database data is used or not. Information on the stream is provided to the LVSF, from which a EIDR tag or information is retrieved. An EIDR query of the database is used to retrieve information on the asset, title, packet length estimate. This additional information is applied to logic that can check the EIDR asset information from other information gathered from the LVSF and collected from Data2 if used. A filter request is sent to the CSP, and additional metadata from the EIDR is included that is used to be provided back in IRI data when the filtering is activated. Requests to the EIDR should help scrutinize legitimate public content. Security used by EIDR needs to be reviewed to watch out for cases where actors could find EIDR tags for content and ensure it is embedded in a stream that used for other purposes.

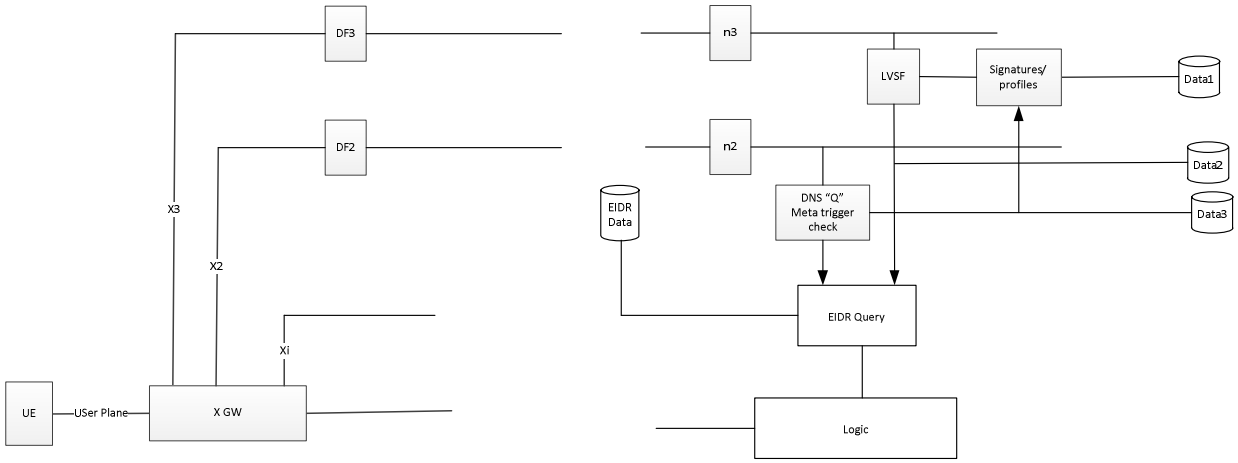

Figure 6.2.4.2-1: Use of EIDR in LEA

6.2.5 Identification of publicly available media via digital watermarks

Some content providers may be required to watermark the content, either under redistribution contracts, or to protect their own content from copyright infringement. The content would have a digital watermark with viewer information and other meta data spread out over the content, such that if the content is found on other sites, it can be tracked to those that infringed on the copyrights. This might interact with techniques used to assure digital evidence, so some discussion on this point may be required. This question should be considered: if sufficient meta data is collected in the LI interface, could a URI be constructed back to the provider to provide the same feed if required as digital evidence? It is important to bear in mind the situation if dates are used in the watermark. It would be important to consider whether confirmation that this IP address consumed that data on this time is acceptable (on the assumption that those records are available e.g. in the viewing history). If clear text recording (as above) is acceptable then this may not be an issue in some regions.

NOTE: It is noted that many CSPs are disputing copyright law in some regions with regards to the level of support required to find and deter those users that infringe. There are potentially privacy issues. Some are prevented from using DPI systems that may limit or control the delivery of user content.

6.2.6 Identification of encrypted public content

6.2.6.1 Middlebox in the CSP Network

Figure 6.2.6.1-1 provides a view if a middlebox is used. A middlebox is an appliance that can provide security, privacy, and access when lawfully authorized and required. The middlebox could be in the gateway or as an external function.

This particular middlebox will use a key set provided by the Content Provider (CP). A user may obtain keys for the CP, but the middlebox will proxy the request and provide a similar key set as provided by the CP. The middlebox will provide clear text access to other functions required to determine validity of the content, as described in Issue 1. Key access and management are out of scope, but keys may be via the CP and stored locally in the CSP. The assumption is that the clear text that is made available is with the confines of the middlebox and its associated function, and not available to the CSP for access to third party content and techniques or schema.

The keys should be held in accordance with appropriate regulation.

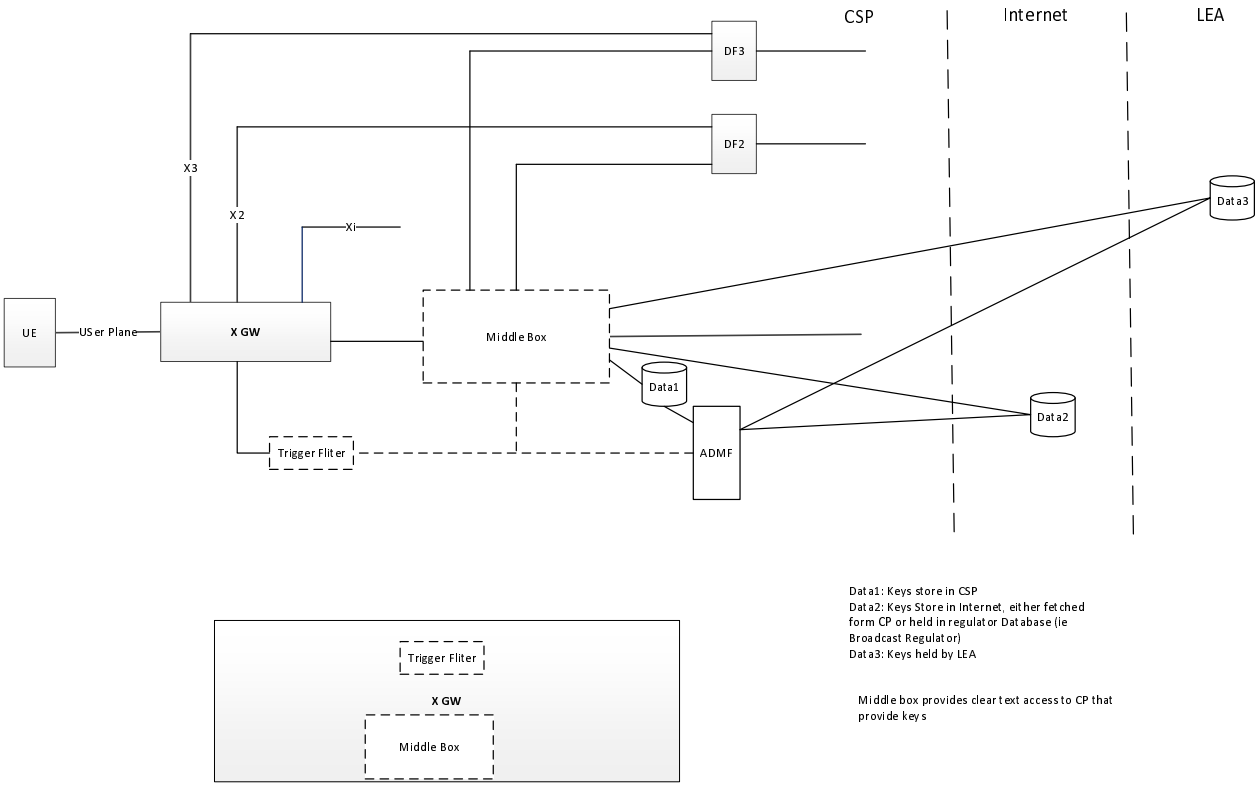

Figure 6.2.6.1-1: Middlebox in the CSP network

In essence the middlebox will appear to the user as the CP end point and terminate its session. The middlebox will have provided keys, and if and when they are authenticated back to the CP, the CP will validate these are valid keys sets to use with the CP. The middlebox can now provide clear text to other functions. The middlebox may also obtain keys set from the CP, i.e. acting as a client, and with these re-encrypt the session to the CP providing privacy on access networks.

6.2.6.2 Middlebox for the CSP with network slicing

In Figure 6.2.6.2-1 where network slicing is enabled and available, the CP may enter into agreements to distribute content over a CSP network. A network slice may be provided that provides functional measurement, caching and other services. It is also expected that it provides login/ username and TLS decryption functions. It may provide access to navigation features and functions. However, only data that is required for evidence and to request filtering is required. This function may provide additional triggers, i.e. release of session, and or new navigations, assuming IP and ports do not change. It is not clear if one slice will be used for all content providers or one per CP.

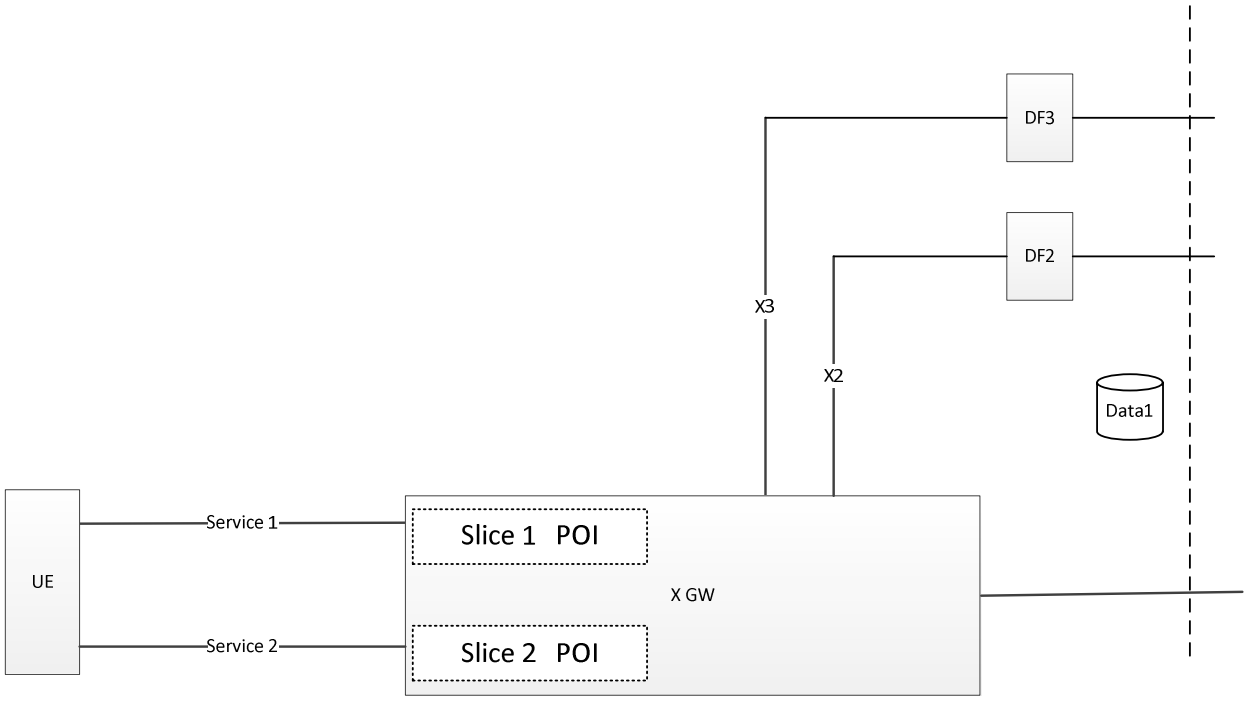

Figure 6.2.6.2-1: Middlebox for CSP with Network Slicing

6.2.6.3 Middlebox in the LEA Network

In Figure 6.2.6.3-1 the middlebox is in the LEA network. The middlebox will access keys as above (however these are different keys). It will not have to re-encrypt towards the CP. It will have additional logic or optional logic to decode stream content. It should be sufficient (pending CP navigation and business models) that accessing the key material and successfully accessing clear text would trigger a filter request identifying CP.

The filtering request should have the reason code, hash, and any other metadata required for the region.

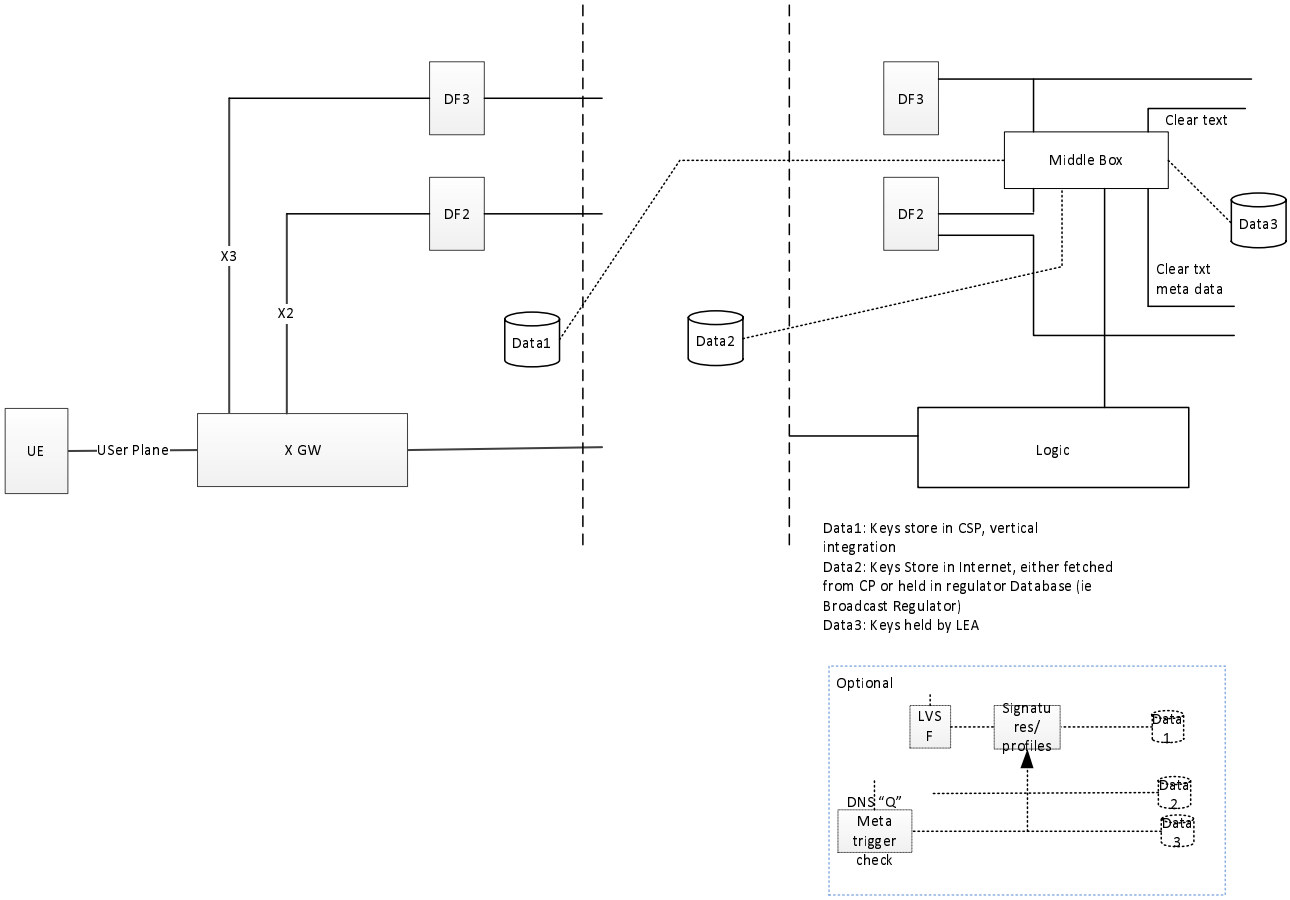

Figure 6.2.6.3-1: Middlebox in the LEA network

6.2.6.4 DPI function to identify audio/video characteristics

If there is no middlebox solution or access to keying information, nor user login, then DPI functions could be used to look at characteristic of the various audio/video protocols in order to identify it. This is similar to virus scanning, and might be useful in characterizing Lawful Public Content from other content delivery mechanisms.

It would be important to consider whether the IP address and port numbers associated with transport protocols would be sufficiently accurate triggers for use in evidence. Potentially a database is required that is also used to create the metadata. It should be considered whether a Packet Data summary on the stream would be required. It is useful as it does suggest the content type, but includes network issues and retransmission that are not a function of the content. Note that there could be other metadata that can be used to describe the service that was filtered.

6.2.7 Filtering based on kernel networking solutions

The following two tools are relevant to high bandwidth output management with COTS:

- Extended Berkeley Packet Filters could improve some aspect of networking and security if the COTS is not shared with third party. It may help create firewall and intrusion/DDOS detection solution but also packet duplication, remote logging, sandboxing, tracing or filtering based on IP (at least faster than an IP table solution). The performance of processing is linked to the size of the header and of the payload.

- Vector Packet Processing (VPP) are tools based on packet processing graphs that may be used as NFV/SDN accelerator with or without external hardware. It could provide a low-level LI API at very high performance but with some security risk. The performance is linked to number of packets with the same header as the first packet consumes a lot of processing. Such a system brings down the average processing cost per packet. As a result, throughput and latency are very stable and lower than many other solutions. It could be used also to create IP Packet Summary Report which is required by some national regulations.

6.2.8 Databases of known public content

6.2.8.1 CSP updates and manages database

Figure 6.2.8.1-1 outlines a view of the database attached to the ADMF though it can be associated with GW. In this figure it is added to the ADMF to address how the ADMF would respond to updates in the databases. This is not shown and is out of scope. It assumed the ADMF - when setting up the targeting - would pull IP addresses that are known Content Provider IP addresses. It would provision the GW with these addresses and might provision the X2 with information to provide in the meta data reported for the filtering of these addresses. That meta data may include Content Provider information.

If the data bases changes during the warrant period, the ADMF could update the provision data (pending regional conditions) and new filtering rules could apply with associated meta data. New streams could be filtered and old streams that were filtered could be un-filtered. This solution would apply to encrypted and or unencrypted content.

The solution should allow packet summary reporting of the filtered streams, and these should be aligned to any changes in the filtering during the warrant period.

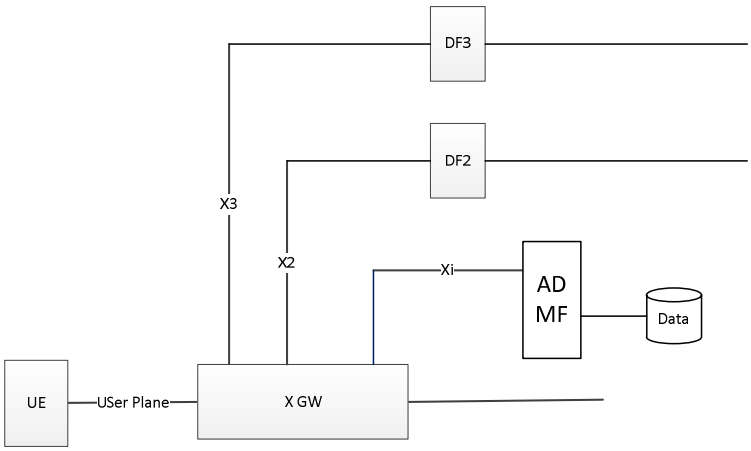

Figure 6.2.8.1-1: CSP provided database

This solution is valid for vertically-integrated companies that have and vet these IP addresses. It may filter non-public IP address, i.e. internal CDN address. This solution adds a level of uncertainty for LEAs, and a mechanism is required to LEA to vet the data in the database. This process should take into account access to the data and rogue employees of the CSP.

The solution requires modification to X1 and X2 protocols to support delivery of messages associated with filtering of IP addresses.

The proposed solution is a per-CSP and not per-target invocation. This may require additional work on protocols.

6.2.8.2 LEA updates and manages a database that resides in the CSP

Figure 6.2.8.2-1 outlines a high-level view of the location of the database. In this view it is shown attached to the ADMF and it is updated by the LEA. How and when the updates occur are out of scope although there should be a trusted platform and secure links. The ADMF as above needs to update the collection platforms based on its scheduling needs and regional conditions.

If LEA updates the database, a hash, and other information should be delivered and used in the IRI reporting. This would prevent a rogue entity in the LEA from providing filtering of essential information required in the warrant. The hash may include the authorizing identity in the LEA. Not shown is the LEA collection, where the IRI data received should be validated against authorized transactions. As a minimum, it would be a record of the individual who authorized the filter on a specific IP address, and when this occurred.

The structure of the database should provide required information which could include internal CSP addresses if these were known, shared with and vetted by the LEA. It is possible that this database is co-shared, with the CSP providing vertical addresses and the LEA providing public IP addresses.

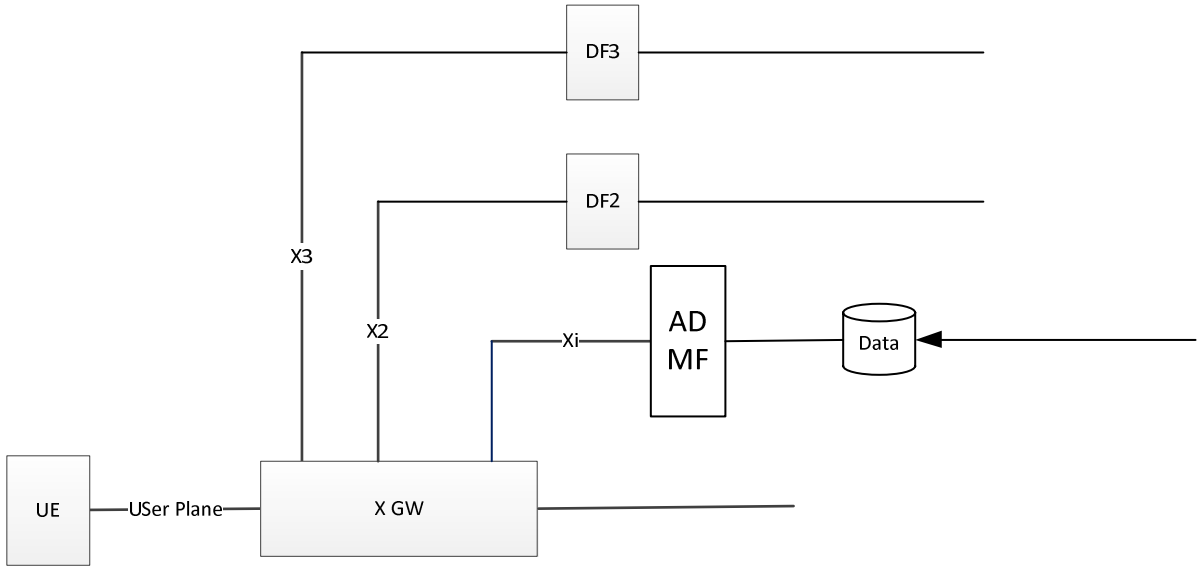

Figure 6.2.8.2-1: LEA manages database hosted in CSP

6.2.8.3 LEA updates and manages database

Figure 6.2.8.3-1 outlines a high-level view of where the database is located. In this view it is shown attached to the ADMF and is updated by the LEA. Other locations would require additional interfaces.

How and when the update occurs are out of scope. The ADMF (as in clause 6.2.8.1) needs to update the collection platforms based on its scheduling needs and regional conditions. In this view an existing interface could be updated to pass the IP address and meta data information from the LEA to the CSP.

This model could also handle internal IP addresses of the CSP if they are provided to the LEA.

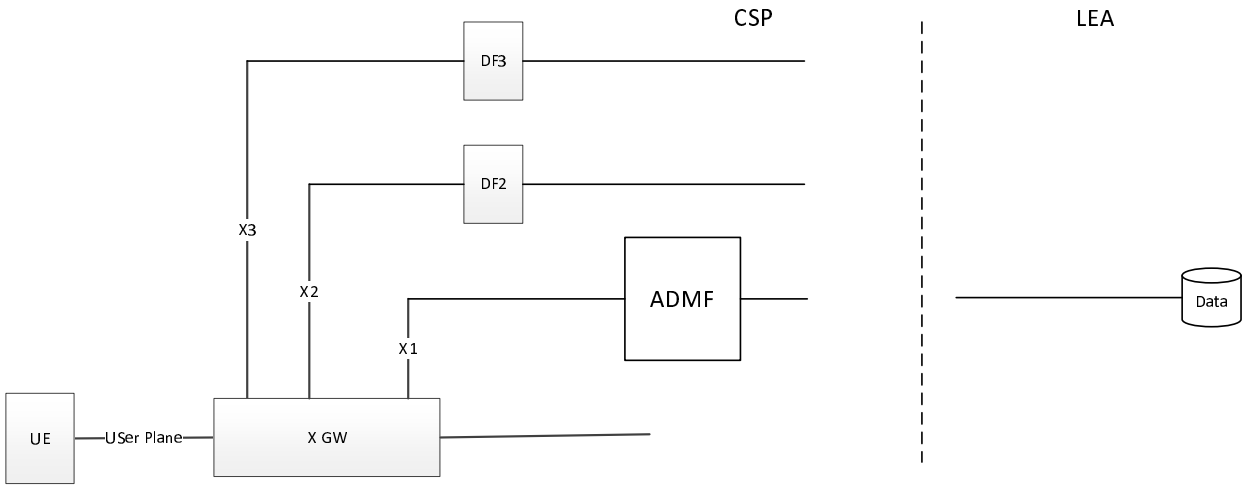

Figure 6.2.8.3-1: LEA updates and manages database

6.2.8.4 LEA updates and manages database (alternative view)

Figure 6.2.8.4-1 outlines a high-level view of where the data base is located. In this view it is managed by the LEA. This solution addresses the navigation aspects descripted in the Issue 1 that may be required by regional requirements.

This solution could be on a per target or regional basis. On a per target basis, IRI data is collected and analysed for DNS queries for CP (Content Provider) content. The IRI data can be fetched from the information on the CP, which can be used to request profiles from another database on CP construction of media sources. If the data is encrypted, it might provide signatures of data flows.

As CC arrives, it is supplied to a LI Video State Function (LVSF) that has profiles loaded to provide de-encapsulation of the media into components. From this information, IRI is gathered to query content title databases, if that is required, for title, and other information. The LVSF may also be able to provide transport stream information and estimated size of the program.

This information is provided to a function that determines when and if it should send a filter request to the CSP.

It will contain information that is required to be fed back in IRI data which can be checked by the LEA for accuracy and compliance as described in other options.

This option allows for navigation of the site and could provide additional back end signalling needed by the LEA to follow navigation, and then initiate a filter request when the video stream is requested by the target.

If, on updating of the filtering, the addresses are provided as per options in 1 to 3, then additional information is required to know when navigation stops and a video begins. This could be simply based on port numbers or protocol types.

This reduces the signalling between the LEA and ADMF compared to the above (which would be real time signalling).

This mode would require additional information to trigger the filtering.

The LVSF can still be used on the LEA side; it would provide the Content title and assess the trigger functions on the data it acquires.

Upon failure of hashes, or determination of hacking (triggered filtering IP address) the LEA can release (or not filter) the IP address.

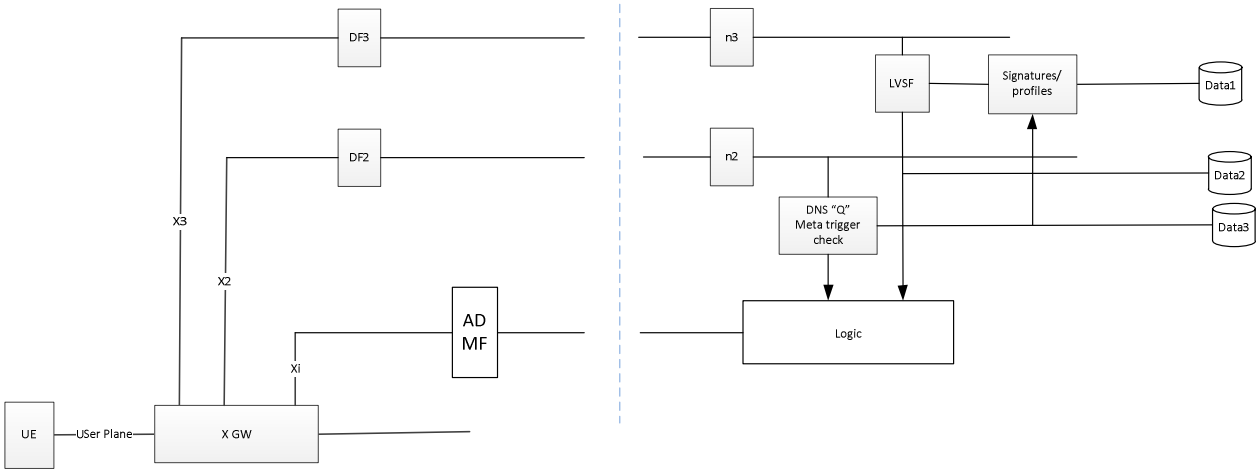

Figure 6.2.8.4-1: LEA updates and manages database (alternative view)

6.3 Digital evidence

6.3.1 Introduction

ETSI TS 103 643 [i.14] describes how to maintain an accurate chain of evidence when applying processing or filtering to digital material which may be used in evidence. It explains how accurate, well-specified, correctly-versioned filtering can be a part of a process which is used for material used in evidence.

If material already has a hash (i.e. a known piece of public content) then this is valuable for evidential purposes and it should be kept and stored securely (perhaps using techniques from ETSI TS 103 643 [i.14]).

6.3.2 Location of functions

Figure 6.3.2-1 shows a scenario in which the LEA hosts this solution. All these components could be in the CSP domain, however the CSP may be a vertically-integrated CP in competition with other CP and those CPs may not want to expose their distribution network function and capabilities to competitors. As such it is assumed that the CP would be able to share their profiles and schema to the LEA. If these functions are CP-provided or LEA-provided virtualized services providing some level of security for the CP, then they could exist in the CSP network.

In Figure 6.3.2-1, target data is analysed, upon receiving a DNS query, or recognizing an IP address that associated with public content. Then information is loaded into a signatures/profile engine which queries a CP profile database on schema to be used to analyse the upcoming content. This could include navigation tools, codex, transport schema (i.e. MPEG2/4 DASH), decryption (where needed), digital water marking algorithms or a means to obtain a decrypt key from CP (this has potentially identifying to the CP target ID).

As content is presented to the LVSF, the engine gathers information. Pending digital watermarking, several seconds or minutes might be required to gather sufficient data. Digital watermarking may include the IP address that is receiving the content, device information, MAC ID of the device, mobile information, user ID, title of the content, date and time stamp. This same information may be available in the transport schema.

At some point meta data is received, and that is used to query a title database.

Pending regulator rules for digital evidence, the information gathered by the LVSF and via meta data initiates a trigger to the CSP, that provides authorization to filter, generates IRI messages and other LI requirements.

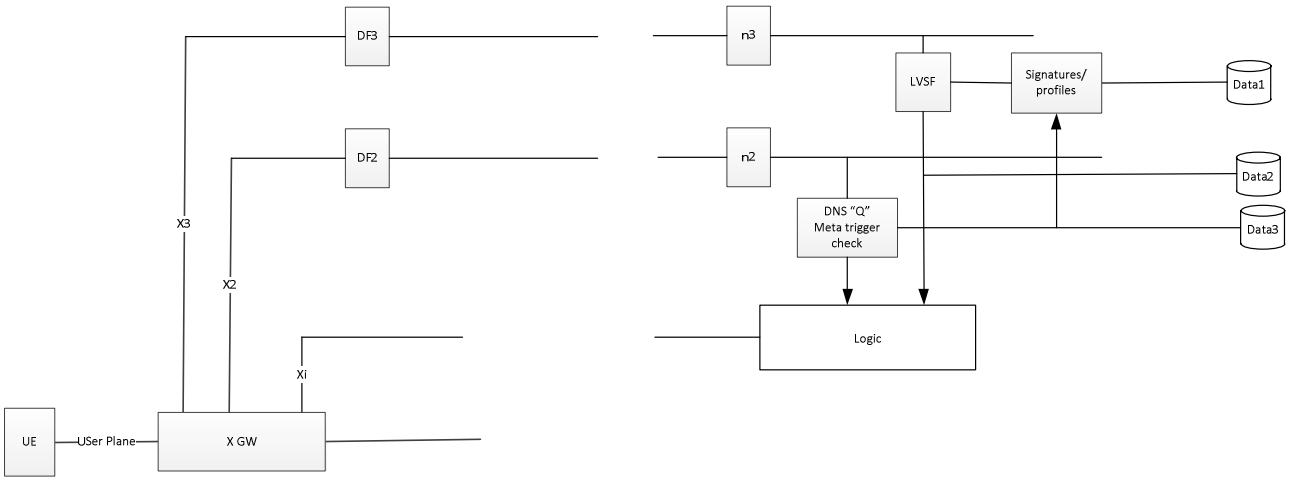

Figure 6.3.2-1: Digital Evidence collection for public content

If the IRI information needs to have the title, it is delivered from the LEA along with the filtering request. It is placed in the IRI message sent back to LEA as part of the reason for filtering. If this logic was in the CSP network, the title would be sent as IRI when the filtering was enabled from the logic. If the LEA sends the filter request, a hash or signature is set that can be used to validate the request at the CSP end (to show that it is an authorized request). A similar signal is sent over the IRI to provide the hash to the LEA. This is used as a feedback mechanism to ensure that a filter request was authorized and can be tracked through the LEA systems.

The LEA systems - upon validating the returned IRI information - can respond, do nothing or send back a request to stop filtering pending national requirements. On a Stop filtering request an alarm should be raised in the CSP if it occurs within a defined period of the filter request.

7 Recommendations

7.1 Isolation of flows recommendation

Ever-increasing data rates delivered by fixed line broadband and future data rates of 5G services will need to be addressed either by scaling infrastructure, or by more efficient delivery or by more selective delivery. Each stakeholder will always need to assess their own cost/benefit assessment of scaling infrastructure. Therefore the present document aims to offer a standardized alternative to increased investment to transmitting and receiving more data.

It is therefore the recommendation of this study that effort is focused towards a process to isolate flows. This aims to reduce the volume of low or no intelligence value traffic being delivered from the CSP to the LEA whilst maintaining evidential integrity.

Focusing on reducing traffic volume rather than delivery efficiency will provide benefits throughout the network and processing systems but does contain a risk that data of value could be isolated. It is therefore critical that the tasking LEA holds full control of rules applied to all their LIIDs, with the flexibility to amend these rules at any time.

The option to apply no rules to an LIID should remain. Clear auditing is also crucial to enable understanding of the impact of a profile and to assist with the assurance of the material when used in legal proceedings.

It is therefore recommended that the most basic isolation rules would be based on managing IP traffic flows through the use of IP address rules as described in clause 6.2.4.

This places an obligation on the LEA to maintain and update those lists with a recommendation that some level of automation (via appropriate DNS queries) and occasional verification of normally discarded data to confirm the initial assessment.

This would be achieved by adding an isolation of flows messaging protocol (see ETSI TS 103 120 [i.2] and ETSI TS 103 221-1 [i.3]) which defines the tasking, traffic management and audit. Annex E of the Cable Broadband Intercept Specification [i.1] contains a very similar process definition.

There should be three primary states of any isolation of flows:

- None: Where no isolation is applied.
- Full LEA control: Where exact rules are applied as solely defined by the LEA.
- Hybrid control: Where requirement is defined by the LEA, but the CSP has dynamic ability to adapt the exact rules based on internal network changes.

Updates to normative work in ETSI TS 103 120 [i.2] (eWarrant interface) and ETSI TS 103 221-1 [i.3] are required to define and implement additional HI1 objects and control messages:

- Isolation details and isolation of flows profile definition and loading:
  - Owned by LEA and implemented by CSP.
  - New messages required for maintenance of isolation details and their collection by reference in isolation of flow profiles.
  - Changes to isolation details or isolation of flows profiles should have no immediate impact to LIID delivery:
    - Create isolation details or profile.
    - Update isolation details or profile:

      "Should be versioned".

      "Migration to updated profiles should be independent of the isolation of flows profile update to enable test and assurance of the new profile".
    - Delete isolation of flows profile.

  - Each isolation of flows profile may include a set of rules for rejecting content and/or specific exclusions.
  - Rules should allow matching against a range of IPv4 5-tuples or IPv6 6-tuples.
  - Both should contain auditable fields, as a minimum name, creation date, version number.
  - Isolation details should also contain rules for its intended purpose.
  - Isolation details should also contain supporting content isolation configuration information.
- Isolation of flows profile application to LIID:
  - Owned by LEA and implemented by CSP.
  - Isolation of flows profiles may be applied once provisioned, causing pending updates to affect both new and existing warrants:
    - Apply isolation of flows profile.
    - Remove isolation of flows profile.
- Warrantry tasking changes:
  - A warranted task details may contain a list of relevant isolation of flows profile IDs.
  - Regularly updated to reference the latest applied isolation of flows profiles.

Updates to normative work in ETSI TS 102 232 parts 1 to 7 [i.5], [i.6], [i.7], [i.8], [i.9], [i.10] and [i.11] defining HI2 for additional metadata messages:

- Traffic Management:
  - Traffic which has been isolated should be reported via HI2. This allows for measuring the isolation of flows profiles effectiveness, identifying faults and providing contextual IRI. Utilizing PDSR and PDHR should be considered for this process.
  - Isolation of flows profiles should be applied as early in the process as possible to allow for most efficiency gains and integrity checking.
  - An isolation start and stop message is required in HI2 to indicate the actual isolation implementation times to the LEA.
- Audit:
  - Auditable data should be available to accurately inform of the exact isolation rules applied to any LIID at any time.

7.2 Transmission recommendation

QUIC is likely to be a more efficient transmission protocol to TCP without the risk of packet loss which would be introduced with UDP.

Delivery using TCP should be extended to support horizontal scaling (clause 6.1.9).

Multiple connections to a single LEMF is a backward compatible low-risk improvement.

Annex A (informative): Change History

Status of ETSI TR 103 656		
TC LI approval date	**Version**	**Remarks**
June 2020	1.1.1	First publication after approval by ETSI TC LI#54e

History

Document history		
V1.1.1	July 2020	Publication