Interception Légale
Principes et Architecture

EFORT
http://www.efort.com

1. Introduction

Tout opérateur de services de télécommunications est tenu de mettre en place les moyens nécessaires pour intercepter les communications échangées sur un réseau publique.
L'interception légale (Lawful interception, LI) est la collecte de données sur le réseau de communications et transmises à une autorité légale à des fins d'analyse ou de preuve. De telles données sont généralement constituées de signalisation ou d'information de gestion de réseau ou, dans des cas plus rares, le contenu des communications. Ce tutoriel présente l'architecture, les fonctions et données d'interception légale et l'application de l'interception légale au domaine circuit mobile.

2. Architecture d'interception légale

L'interception légale est une des obligations nationales imposée aux opérateurs au même titre que les obligations telles que le numéro d'urgence, la portabilité du numéro, la rétention des données, etc.
LI est souvent confondu avec la rétention des données. Le but de la rétention des données est de conserver les données de sessions de tous les usagers.
Le principe de LI est de dupliquer en temps réel le trafic d'une cible, et de l'envoyer aux autorités. Les IRI (Intercepted Related Information) et les CC (Content of Communications) sont délivrés.
Les principaux organismes de normalisation sont 3GPP pour les réseaux mobiles et l'IMS et l'ETSI.
LI est aujourd'hui implantée dans le réseau circuit (e.g., réseau circuit mobile, réseau RTC), le réseau IP (e.g., réseaux paquet mobile, Internet), l'IMS (e.g., VoLTE, VoWiFi, etc).

Il existe deux domaines:
- Le domaine LEA qui représente les organismes d'application de la loi (autorités)
- Le domaine Opérateur

Deux types d'interface sont présents :
- HI: Interface de transfert entre les domaines opérateur et LEA. C'est une interface physique et logique à travers laquelle les mesures d'interception sont demandées à un AP / NWO / SvP, et les résultats d'interception sont délivrés d'un AP / NWO / SvP à une LEMF (Law Enforcement Monitoring Facility)
- INI: Interfaces internes dans le domaine opérateur entre la fonction d'interception interne et une fonction de médiation.

La LEMF est désignée comme destination des résultats d'interception relatifs à un sujet d'interception particulier.
La MF (Mediation Function) représente un mécanisme qui transmet des informations entre un fournisseur d'accès ou un opérateur de réseau ou un fournisseur de services et une interface de transfert

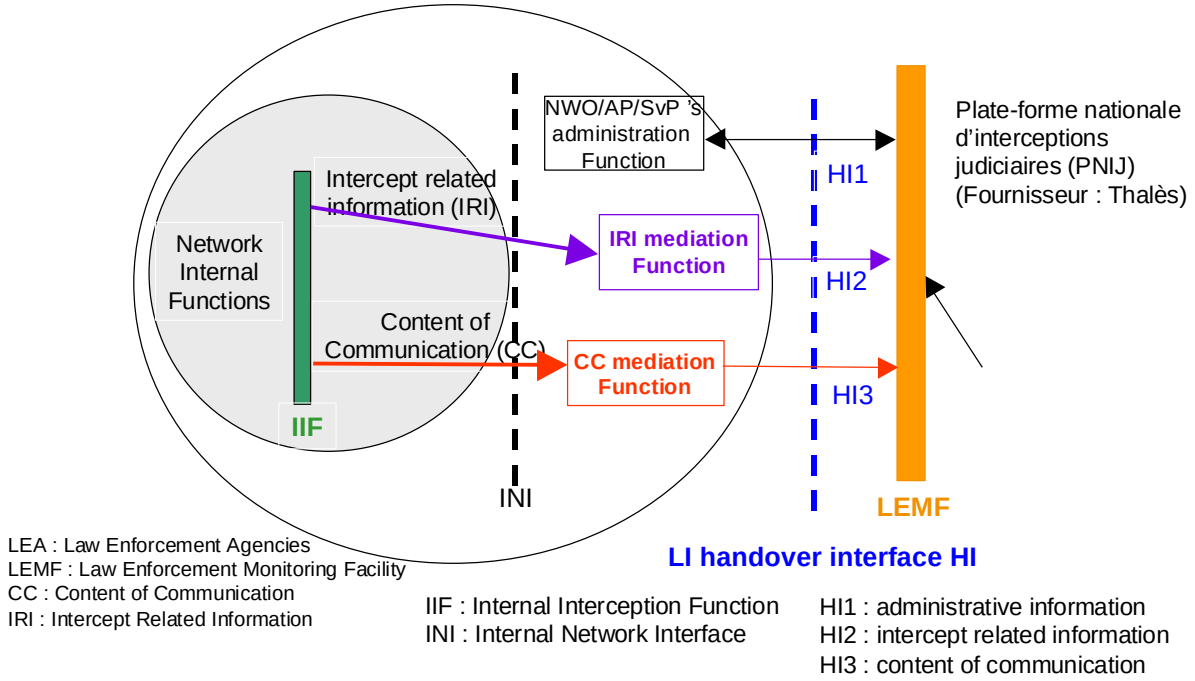

Figure 1 : Architecture d'interception légale

Le négoce de l'interception légale est partagé entre trois types de fournisseurs :

- Les fournisseurs de points d'accès d'interception (IAP, Intercept Access Points) localisés dans le domaine de l'opérateur (e.g., Cisco, Ericsson, Nokia, etc.)
- Les fournisseurs de plate-formes de médiation localisées dans le domaine de l'opérateur et qui embarquent les entités fonctionnelles administration function,, IRI mediation function et CC mediation function (e.g., Verint, Utimaco, SS8, Aqsacom)
- Les fournisseurs de LEMF localisée dans le domaine LEA (e.g., ATIS, Thales, Verint, etc)

3. Structure de nœud avec les interfaces internes et application au domaine circuit mobile

Il existe deux types d'interfaces de base :

- Interfaces internes (X) comme montrées à la figure 2, qui sont supposées être propriétaires du fournisseur ou selon des normes industrielles ad hoc.
- Interfaces de transfert (HI, Handover Interface), qui sont spécifiées dans les normes internationales avec plus ou moins d'adaptation pour un contexte national.

Les interfaces internes sont adaptées à la technologie propriétaire du fournisseur et optimisées avec les fonctions de communication du nœud respectif. Il est important d'éviter l'augmentation du coût et la diminution des performances lors de l'introduction de la fonction d'interception interne dans les nœuds qui sont produits et commercialisés en grands volumes. Par conséquent, il peut être nécessaire de fournir les informations dans les interfaces sous la forme purement binaire et d'utiliser des piles de protocole simples, telles que UDP au lieu de TCP pour la couche de transport.
Il existe certaines initiatives récentes pour le développement de normes pour les interfaces internes, comme la RFC 3924. Cette technologie d'interface est basée sur le protocole de gestion de réseau simple (SNMP), qui peut bien sûr imposer une certaine charge supplémentaire sur la conception du nœud, à moins que SNMP soit déjà utilisé à d'autres fins dans le nœud en question.
L'interface pour positionner / modifier la cible et souscrire à des événements, peut contenir des informations sur l'adresse de livraison interne ou externe pour IRI (Information relative à

l'Interception) et CC (Contenu de la communication). Il y aura également des informations sur le fait que l'interception requiert uniquement des IRI ou des IRI + CC.

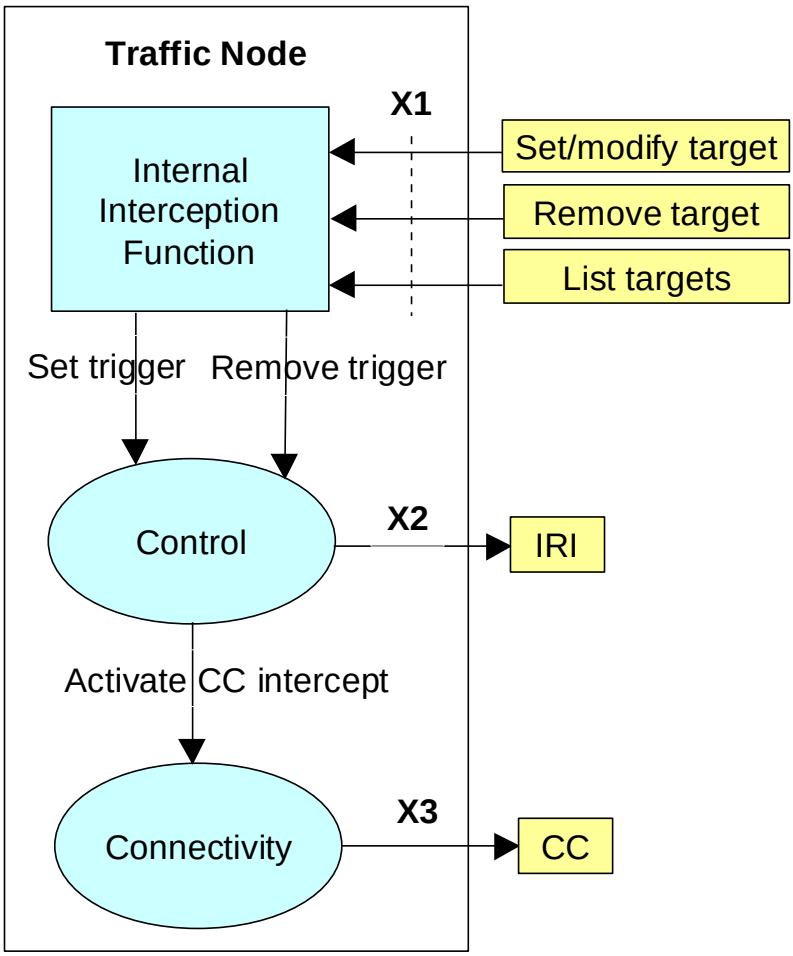

Figure 2 : Structure de nœud avec les interfaces internes

Si l'on considère le domaine circuit, les interfaces HI2 et HI3 représentent les interfaces entre la LEA et deux fonctions de livraison. Les fonctions de livraison sont utilisées:

- Pour distribuer l'information relative à l'interception (IRI, Intercept Related Information) aux LEA pertinentes via HI2.
- Pour distribuer le Contenu de la communication (CC) aux LEA pertinentes via HI3.

Les interfaces du domaine de commutation de circuits sont normalisées (HI2, HI3), tandis que les interfaces internes dans le domaine de commutation de circuit (X1, X2, X3) sont propriétaires. La fonction de médiation agit comme une passerelle à partir du domaine de commutation de circuit vers le réseau de la LEA.
Il existe également une fonction de gestion (ADMF), qui reçoit des données HI1 et envoie des commandes sur X1 pour positionner les nœuds de communication dans le domaine de commutation de circuit et le système LI MF / DF pour effectuer une interception et relayer les résultats aux destinataires désignés.
Les fonctions de livraison DF2 et DF3 sont utilisées:

- Pour convertir les informations sur l'interface X2 en les informations correspondantes sur l'interface HI2;
- Pour convertir les informations sur l'interface X3 en les informations correspondantes sur l'interface HI3;
- Pour distribuer les informations relatives à l'interception (IRIs) à la ou aux LEA pertinentes,

- Pour distribuer le contenu d'interception des communications (CC) à la (aux) LEA (s) concernée (s)

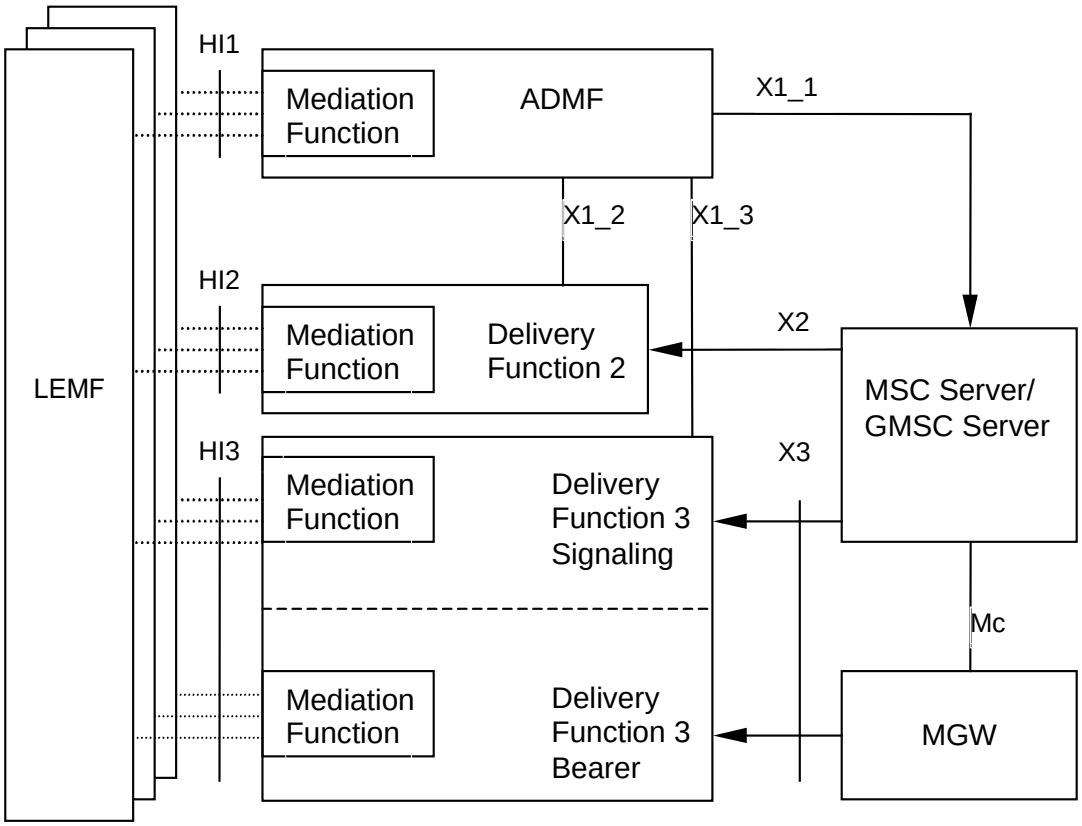

Figure 3 : Configuration d'interception de la communication de circuit

A la figure 4, l'interface HI2 représente l'interface entre la LEA et la fonction de livraison. La fonction de livraison est utilisée pour distribuer l'information relative à l'interception (IRI) aux LEA pertinentes via HI2.
L'interception CC ne s'applique pas au HLR. C'est la raison pour laquelle il n'y a pas d'interface HI3.

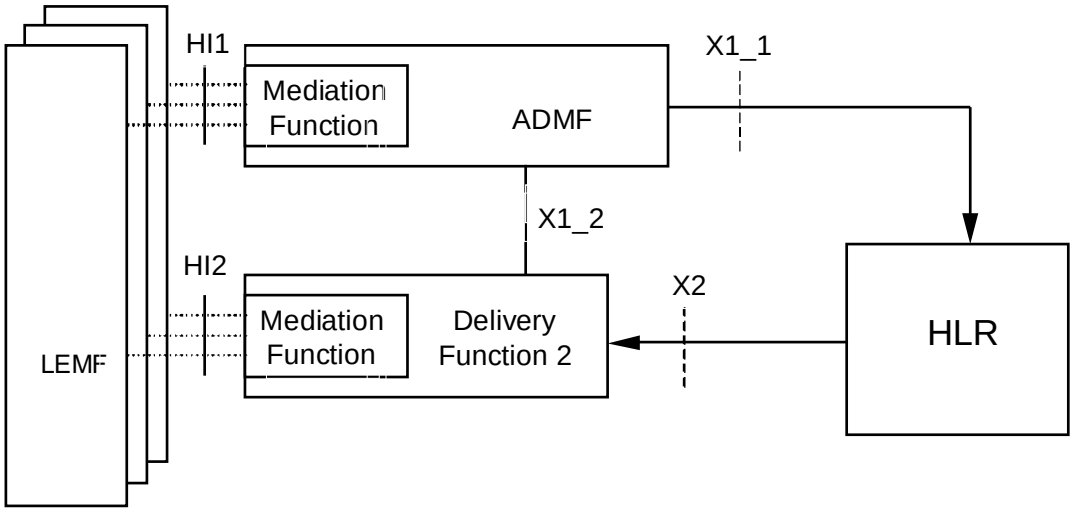

Figure 4 : Configuration d'interception HLR

4. Evénements de commutation de circuit mobile

Les informations envoyées à DF2 sont déclenchées par 13 différents événements liés à un appel et non liés à un appel. Les événements d'interception sont configurables (s'ils sont envoyés à DF2) dans le MSC Server et peuvent être supprimés dans la DF2. Les événements sont répertoriés comme suit:

- Evénements relatifs à un appel : Call Establishment, Call Answer, Supplementary Service, Handover, Call Release
- Evénements non relatifs à un appel : SMS, Location Update, Serving System, HLR subscriber record change, Subscriber Controlled Input, Cancel Location, Register Location, Location Information Request

Les événements sont utilisés pour générer des enregistrements pour la livraison via HI2 à la LEMF si cela est nécessaire. Le tableau 1 donne le mappage entre type d'événement et type d'enregistrement.

Event	IRI Record Type	
Call establishment	BEGIN	MSC
Answer	CONTINUE	MSC
Supplementary service	CONTINUE	MSC
Handover	CONTINUE	MSC
Release	END	MSC
Location update	REPORT	MSC
Subscriber controlled input	REPORT	MSC
SMS	REPORT	MSC
Serving system	REPORT	HLR
HLR subscriber record change	REPORT	HLR
Cancel location	REPORT	HLR
Register location	REPORT	HLR
Location information request	REPORT	HLR

Tableau 1 : Evénements de commutation de circuit mobile

Si l'on considère l'événement *Register location* généré par le HLR, il consiste en les informations suivantes :

- MSISDN ou IMSI : Au moment de l'attachement de l'usager, ce dernier fournit son IMSI. Le HLR associe l'IMSI au MSISDN de l'usager. Lorsque le HLR génère cet événement, il indique au moins l'une de ces deux identités qui identifie l'usager qui s'est attaché.
- Event type : Il s'agit de l'événement « Register Location Report ».
- Event date and time : Date et heure de l'événement.
- Lawful intercept identifier : Identité de la cible (target) assignée par autorité d'interception lors de la demande d'interception.
- Network Identifier : L'élément de réseau qui est en mesure de produire cet événement est le HLR (Global Title du HLR). Même si l'usager est dans un réseau visité, c'est le HLR du réseau nominal qui prend en charge l'usager pour son authentification et la fourniture de son profil au MSC/VLR visité.
- Previous Serving System : Lorsque l'usager s'attache, le HLR disposait de l'adresse de l'ancien MSC/VLR qui prenait en charge l'usager avant que ce dernier se détache. Toute adresse de MSC/VLR commence par le country code et le network code qui permet de savoir à quel réseau était attaché l'usager. Lors de ce nouvel attachement, le HLR indique le précédent réseau auquel était attaché ce même usager avant son nouvel attachement (il peut s'agir du même réseau).
- Previous serving MSC number : Global Title (GT) du MSC Server précédent sur lequel était attaché l'usager.
- Previous serving MSC address : Adresse IP du MSC Server sur lequel était attaché l'usager.

- Current Serving System : Réseau (MCC et MNC) sur lequel est attaché actuellement l'usager. Lorsque l'usager s'attache, le HLR disposait de l'adresse de l'ancien MSC/VLR qui prenait en charge l'usager avant que ce dernier se détache. Toute adresse de MSC/VLR commence par le country code et le network code qui permet de savoir à quel réseau était attaché l'usager. Lors de ce nouvel attachement, le HLR indique le précédent réseau auquel était attaché ce même usager avant son nouvel attachement (il peut s'agir du même réseau).
- Current serving MSC number : Global Title (GT) du MSC Server courant sur lequel est attaché l'usager.
- Current serving MSC address : Adresse IP du MSC Server courant sur lequel est attaché l'usager.

Pour l'établissement d'appel, un événement d'établissement d'appel (*Call establishment*) est généré par le MSC Server. Cet événement est généré au début d'un appel lorsque le MSC Server tente de joindre l'usager. Ces informations seront transmises au DF2 si disponible:

- Oberved MSISDN : MSISDN de la cible.
- Observed IMSI : IMSI de la cible.
- Observed IMEI : IMEI de l'UE de la cible, il doit être vérifié pour chaque appel sur l'interface radio
- Event type : Il s'agit de l'événement Call establishment
- Event date : Date de génération d'événement dans le MSC Server
- Event time : Heure de génération d'événement dans le MSC Server
- Dialled number : Numéro de téléphone composé avant la modification des chiffres, modification via le Réseau Intelligent, etc.
- Connected number : Numéro du répondant
- Other party address : Numéro de téléphone de l'autre partie pour l'appel initié par la cible, numéro de l'appelant pour l'appel entrant à la cible.
- Call direction : information indiquant si la cible appelle ou est appelée par ex. MOC / MTC ou origine / terminaison
- Correlation number : Numéro unique pour chaque appel envoyé au DF, pour aider la LEA, à disposer d'une corrélation entre chaque appel et l'IRI
- Network Element Identifier : Identificateur unique de l'élément réseau MSC Server.
- Location Information : Les informations de localisation sont l'identité de la zone de service et / ou l'identité de zone de localisation connue par le MSC server au moment de la génération de l'événement.
- Basic service : informations sur le téléservice ou le service de transport (bearer service)
- Supplementary service : Services supplémentaires utilisés par la cible, e.g., CF (call forwarding), CW (call waiting), ECT (explicit call transfer).

Références

3GPP TS 33.108 , Handover interface for Lawful Interception (LI)
3GPP TS 33.107, Lawful interception architecture and functions
3GPP TS 33.106, Lawful interception requirements
ETSI TS 101 671, Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic