

FINFISHER

Introduction 2

Scope and Preconditions

The three companies Gamma Group, Desoma and Dreamlab intend to create Telecommunication Intelligence Systems for different telecommunication networks to fulfill the customers' needs and requirements regarding Lawful Interception, Massive Data Interception, Data Retention and traffic/application/protocol Control (Traffic Blocking and Shaping).

These different intelligence methods and technologies are to be deployed in different network environments like "classic" fixed and mobile networks as well as in IP-based (packet oriented) networks. However, not every technology/method will be used in every network in the same way if it will be used at all.

The Intelligence Systems must be modular/scalable and have to be combined depending on the communication environments and needs in different project/countries.

The main expertise of all three partners is the "IP-world". There should be some technological competence on Desoma's side regarding the classic networks (PSTN, Mobile), while Gamma has the world wide marktet access and competence regarding sales and marketing for all technologies mentioned above.

Beside some "restrictions" regarding specific knowledge (which has to be evaluated) there are for sure restrictions regarding man power, time and money.

A strategy has to be defined to create Intelligence System(s) which can be realized in a rather short period of time to generate Rol, being

competitive and making the most use of currently available knowledge and experience of all partners.

The following slides will give an overview of the different Intelligence Solutions' requirements and technologies and an indication regarding the availability of solutions and/or the capability to solve the technial requirements.

Networks <-> Intelligence Methods used

Networks Methods	PSTN (ISDN/POTS)	Mobile (GSM/GPRS/UMTS/ LTE)	IP-Networks			
Lawful Interception	Yes supported by Network	Yes Supported by Network	Yes partly supported by NW mainly own Appliances			
Mass Data Interception	Yes International Gateways	?	Yes Internet Gateways			
Blocking / Shaping	No	partly for/in the IP-part of the NW	Yes i.e. at Internet Gateways			
Data Retention	Yes supported by Network	Yes supported by Network	Yes using NW elements and/or own Appliances			
Infection	Not inside the NW but for PC/Nb indirectly via IP-NW	For PC/Nb possible in Mobile NW or indirectly via IP-NW (FinFly ISP). For mobile Phones/PDA etc. own FinFisher-Application	Yes FinFly ISP			

Networks (Intelligence Methods) <-> Solutions / Technologies

Networks Methods	PSTN (ISDN/POTS)	Mobile (GSM/GPRS/UMTS/L TE)	IP-Networks			
Lawful Interception	Admin HI1: inside NW IRI HI2:IP/X.25-Receiver CC HI3: S2m-Recorder TgtIdent: inside NW	Admin HI1: inside NW IRI HI2:IP/X.25-Receiver CC HI3: S2m-Recorder CC HI3 IP: own IP-Appliance TgtIdent: inside NW	Admin HI1: own Admin HI2 (= HI3): n/a own IP- Appliance TgtIdent: own IP- Appliance			
Mass Data Interception	Admin: own Admin IRI HI2:??? CC HI3: S2m- Recorder	?????	Admin HI1: own Admin HI2 (= HI3): n/a CC HI3: own IP- Appliance			
Blocking / Shaping	n/a	IP-Part of the NW: Admin:own Admin Block/Shape: own IP- Appliance TgtIdent: own IP- Appliances	Admin: own Admin Block/Shape: own IP- Appliance TgtIdent: own IP- Appliance			
Data Retention	Network Elements (OSS/BSS) provide Info for DRS (CDRs)	Network Elements (OSS/BSS) provide Info for DRS (CDRs)	Using Network Elements (OSS/BSS) and/or own IP- Appliances			
Infection	Indirectly: See IP-Networks	See IP-Networks for PC/Nb Mobile Phones: Admin: own Admin TgtIdent: manually (?) Delivery: own "Methods"	Admin: own Admin TgtIdent: own IP- Appliance Delivery: own IP- Appliance			

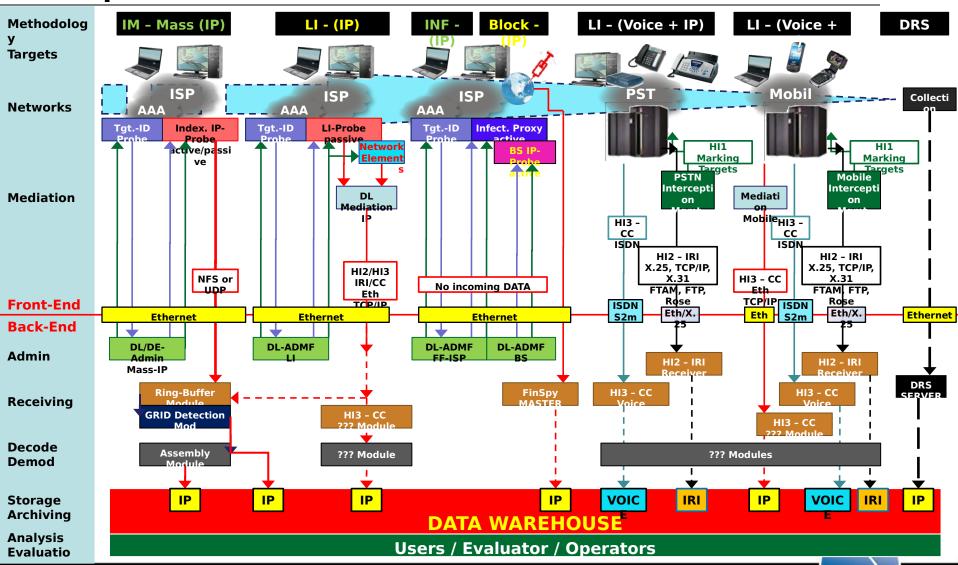
•		PSTN (ISDN/POTS)				Mobile (GSM/UMTS/LTE)				IP-Networks						
	TASKS	ш	Mass Data	B & S	DRS	INFEC	ш	Mass Data	B & S (IP- only)	DRS	INFEC Mobile	LI	Mass Data	B & S	DRS	INFEC
Fro	Administration	NW	Desom a/ 3rd Party		Tbd		NW		Dreaml ab	Tbd	GG	DE/DL	DE/DL	DE/DL	Tbd	DL/GG
	Data Capturing / Handling	NW	Desom a/ 3rd Party		Tbd		NW		Dreaml ab	Tbd	GG	Dreaml ab	Dreaml ab	Dreaml ab	Tbd	DL/GG
En d	Target Identification	NW	Manuall y NW		Tbd		NW		Dreaml ab	Tbd	GG	Dreaml ab	Dreaml ab	Dreaml ab	Tbd	Dreaml ab
	Mediation	IRI only	???		Tbd		IRI-NW IP DL			Tbd		Dreaml ab	Dreaml ab		Tbd	
	Receiving Data	Desoma / 3rd Party	Desom a/ 3rd Party		Tbd		Desom a			Tbd	GG	Desom a	Desom a		Tbd	GG
Ba	DB (Storage/Archive)	Desoma	Desom a		Tbd		Desom a			Tbd	GG	Desom a	Desom a		Tbd	GG
ck-	Decode / Demodul	Desoma	Desom a		Tbd		Desom a			Tbd		DE/DL	DE/DL		Tbd	
En	Reconstruction	Desoma	Desom a		Tbd		Desom a			Tbd		DE/DL	DE/DL		Tbd	
d	Back-End Admin	DE/DL	DE/DL		Tbd		DE/DL			Tbd	GG	DE/DL	DE/DL	DE/DL	Tbd	DL/GG
	User Management	DE/DL	DE/DL		Tbd		DE/DL			Tbd	GG	DE/DL	DE/DL	DE/DL	Tbd	DL/GG

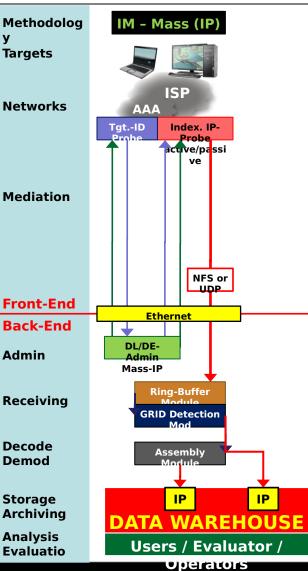


provided/available by eihter the NW or by a partner to be defined OR using 3rd Party solution (DRS)

not needed / not
applicable
to be
done/defined/created







Data Capturing:DAISY from Desoma is curretly using a CS-2000 or PN41-Blade (IBM) to connect play or actively to

the network (Indexing Module = IP-Probe). This has to be changed to use HP-Servers with appropriate

NICs from Dreamlab.

Active will be chosen in case a Man-in-the-Middle attack is planned for SSL certificates (using Bypass

Function). In this module data filtering takes place to search for specific data and reduce the amount of

data to be sent to the Back-End. It has to be defined whether String Search must be integrated into the



IP-Probes to reach a finer granularity for Filtering data of interest.

Target Identif.: Dreamlab has Tgt-Id-Probes available in case Mass IP-Interception has to be specified for dedicated



subscribers (exceptional case)

Data handover: NFS and/or UDP is used currently and will be implemented into the Dreamlab IP-Probes too, to



handover the captured IP-data to the Ring-Buffer / GRID Detection Module.

Admin: Has to take care about the workflow in the Mass IP Interception System. The user can enter Filter

Criteria which are forwarded to the IP-Probe(s) to filter/capture data of interest. If necessary

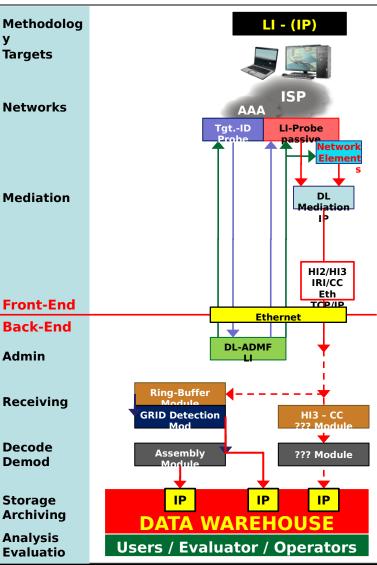
Probes are configured as well.



The Admin has to be designed and has to integrate a User Management with several layers

rights (who has the right to access what kind of data; Admin, User, Auditor etc.)

Ring-Buffer &



Data Capturing: This will be the same kind of HP-Servers used for Mass IP-data In epition to capture

IP-Data for LI passively. In addition Dreamlab is capable of handling IP-data provided by

Network Elements (Juniper, Cisco, Huawei).

Target Identif.: Dreamlab has Tgt-Id-Probes available to capture assinged IP-addresses of Targets by

searching for their nw access credentials.

Data Handover

= Mediation: This Dreamlab appliance can convert the captured IP-data into several dominates

(i.e. ETSI) for IP-datza handover to several Monitoring Centers simultaneously.

Admin: Has to take care about the workflow in the LI System. The user can enter the NW access

credentials for the Targets of interest forwarded to the Tgt-Id-Probe(s). For LI

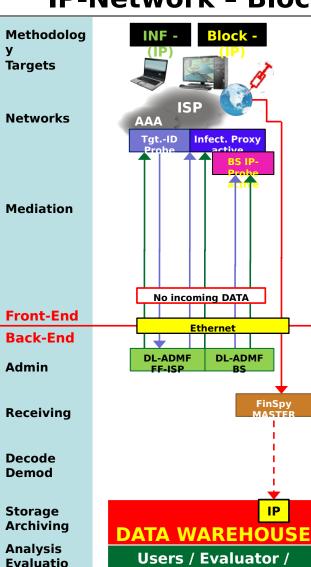
handling of a LIIDs is esssential (to create warrants).

The Admin has to be designed and has to integrate a User and Warrant gement

with several layers of user rights (who has the right to access what kind of data; Admin,

User, Auditor etc.). This LIID structure will aply for LI in PSTN / Mobile NW too.

Receiving Data: It has to be analyzed whether the concept using the Ring-Buffer, GRID and



Remarks: The solutions IP-traffic Blocking & Shaping and the Infection using FF ISP are different form other

Intelligence Methods described because Blocking & Shaping doesn't require any data to be transferred

from the Front to the Back-End. The same applies in the first step for the data provided by remotely

controlled targets. These data are received by FinSpy Server and can be pushed into to warehouse on demand.

Dat Again HP-Servers will be used but for both Blocking & Shaping and Infection these Servers MUST be

actively inline for data manipulations. The Bypass Function is a must have too.

Target Identif.: Tgt-Id-Probes are needed and used in the same way as for LI. In addition they can block

and/or shape the traffic of subscribers of interest. Without Tgt-Id-Probes B&S will take care about

rotocols / applications only without target "awareness".

It has to be defined whether String Search must be integrated into the IP-Probes to reach a finer

granularity for blocking / shaping and maybe infection.

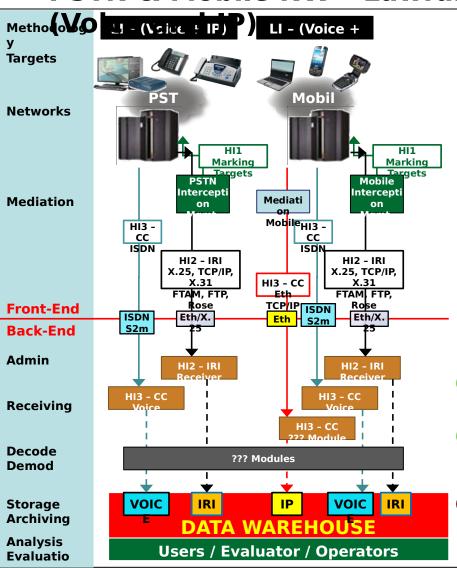
Data handover: Only defined for FinSpy (Master).



Admin: The Admin is available for FF ISP.

An Admin System has to be designed taking care about the workflow in the Blocking/Shaping System.

Operators



Data Capturing:In both Networks (PSTN and Mobile) data capturing is performed inside NW

using NW-vendor specific solutions (assuming the NW-vendor is providing such

kind of solutions). This applies for both Voice (voice, modem, fax) and IP-data.

Targer entif.: This is also part of the NW-LI-functions.

Admin: Also the Admin-Function of the NW is part of the NW-environment. Subscribers

(fixed / mobile) will be marked for LI inside the NW. The Interception $\ensuremath{\mathsf{Mgmt}}$

Systems (PSTN/Mobile) also provide the IRI-data (either ASN.1 encoded or as

ASCII-files). Assigning a LIID is part of this admin process and it has to refer to the

LIID used in the Monitoring Center for admin the LI-warrant.

Datandover

CC-Voice: Voice data will be transferred via ISDN (S2m) to the Back-End (PCM30, A-law

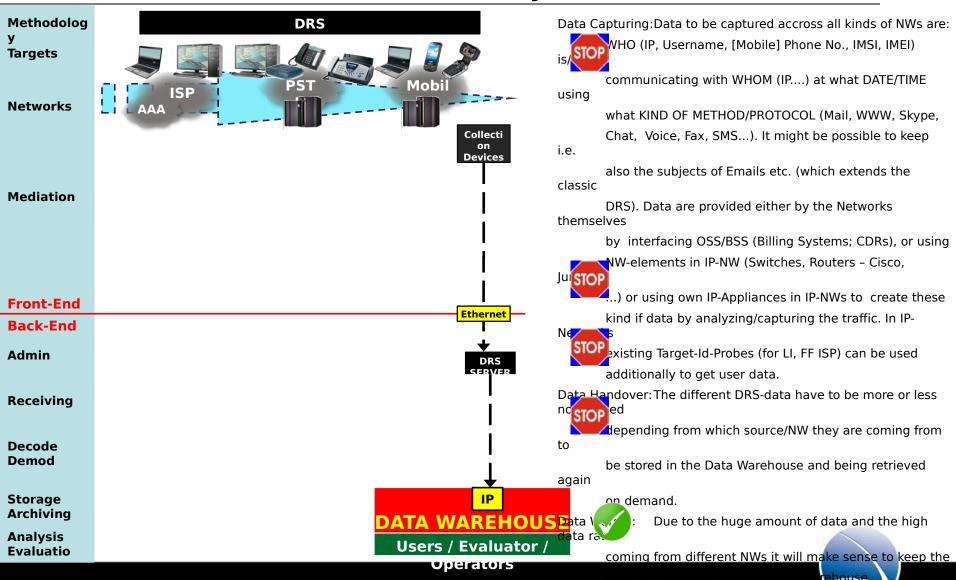
🕢 ?? Coded) from the switches of the NW.

Record can be either FTAM, FTP or Rose on X.25/X.31 or TCP/IP

the NW-LI-Management System(s).

???n: IP-data from GPRS/UMTS will be mediated using Dreamlabs

Appliance to provide i.e. ETSI-formated data to the Back-End.



Conclusion - proposal how to proceed ...

Conclusion

This conclusion is based on the following assumptions and facts:

- 1. More IP-knowledge than classic PSTN/Mobile NW knowledge available within the 3 partners
- 2. Sales experience and market access is available for all solutions
- 3. PSTN/Mobile Voice data need a complete different handling (receiving, decoding, evaluation) than IP-data
- 4. No. 2 becomes even more difficult dealing with decoding of modem and fax transmissions
- 5. LI for classic PSTN/Mobile NWs depend very much on the LI-implementations provided by the different NW-vendors
- 6. DRS is characterized by huge amounts of data, a wide range of different intefaces needed to capture/receive data, different Hand-over-Interfaces (HI-A, HI-B) and different approaches when data are to be retrieved, own/different user management etc.
- 7. Different Intelligence Methods need different kinds of administration functions
- 8. Different Intelligence Methods need different ways of storage (data structures), different decoding and analysis/evaluation methods

The proposed way to go should be:

- 9. Start with Mass IP-Data Interception (for this Intelligence Method the most work is done / solutions are available)
- 10. Next Step will be LI in IP-Networks (a lot of components can be used and/or are available and can be modified accordingly)
- 11. Due to the fact that Infection solutions are products ready to use (FinFly ISP, FinFlyWeb, FinFlyUSB) the data coming from FinSpy Master have to be integrated into the Data Warehouse (like we did for other MCs).
- 12. Blocking and Shaping has no real impact on the Back-End because no data transfer towards the BE has to take place. It can be kept as a separate product, making use of filter criteria also used for Mass IP-data Interception. Having an own GUI running on the same Management Workstation like Mass IP Interception and/or LI and/or Infection will be sufficient.















FINFISHER

IT INTRUSION