



Lawful Interception

Interception challenges and Handover capabilities

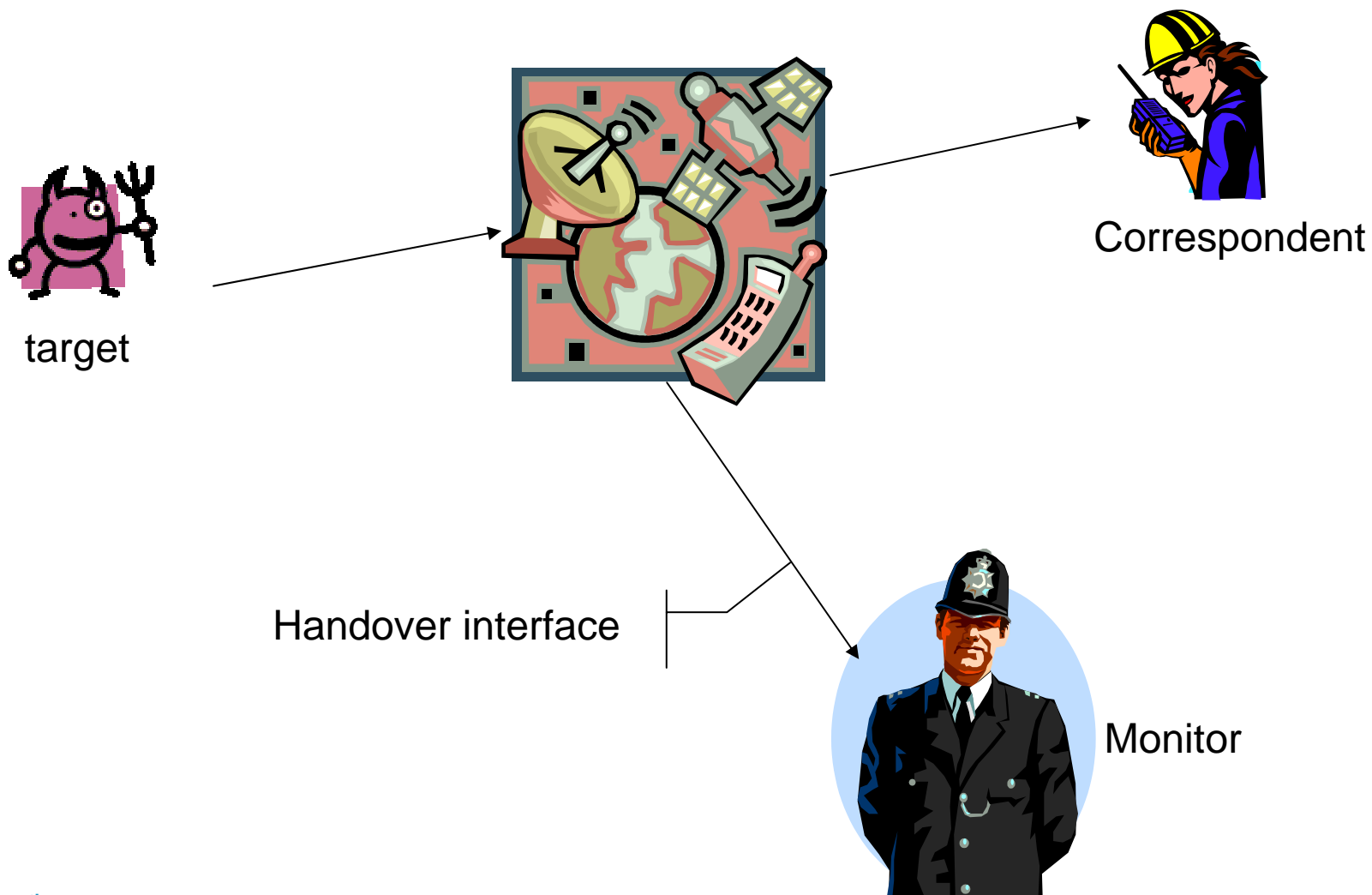
Scott Cadzow
TC LI Vice Chairman
C3L

ETSI Security Workshop
16th January 2006
Sophia Antipolis

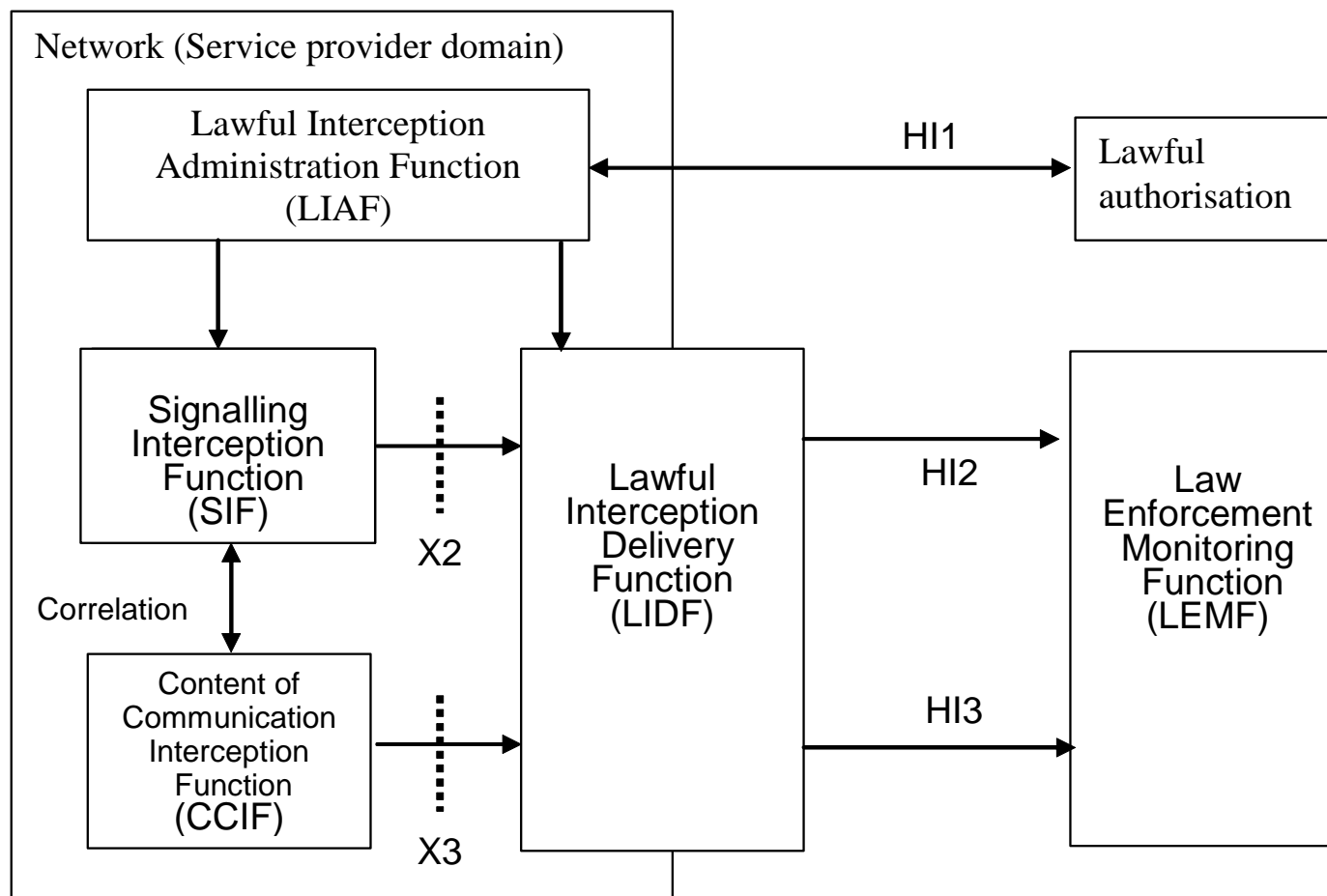
What is lawful interception?

- ❑ Used in the support of criminal investigation and to counter terrorism
- ❑ Applies to data in transit
 - It is not a search of records
- ❑ Applied to any data in transit
 - Signalling
 - Speech
 - Video
 - E-mail
 - Web
 - Etc.

Simple architecture



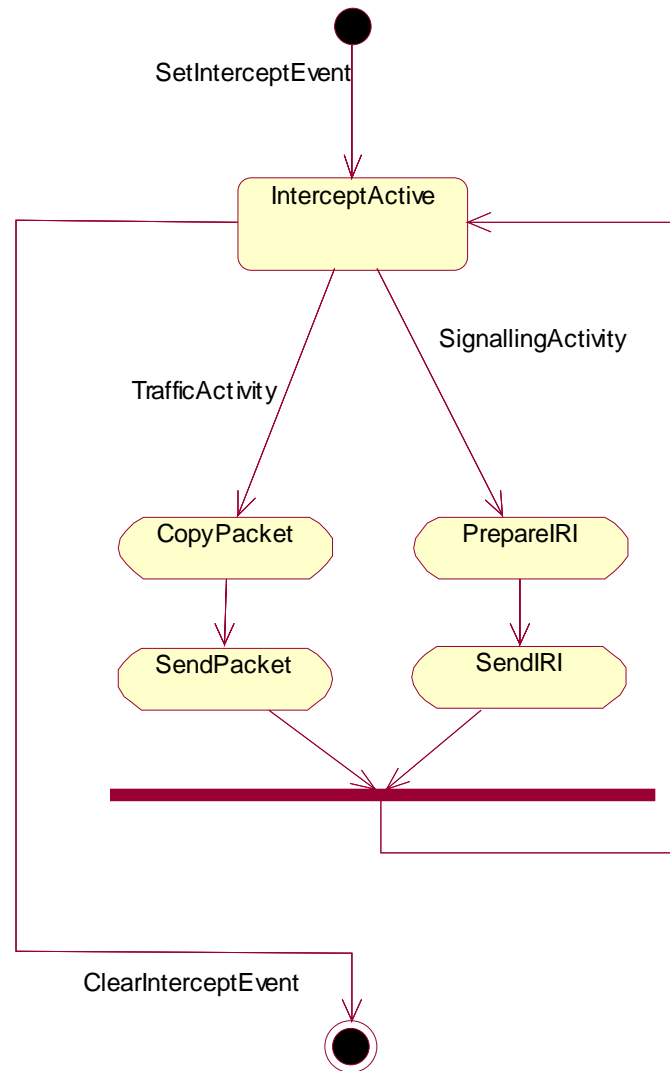
More technically



The architecture - actors

- ❑ **The target**
 - This is the entity against which the interception is made
- ❑ **The correspondent**
 - Who the target is talking to and whose communication with the target is intercepted
- ❑ **The monitor**
 - The entity that any interception is given to (usually a Law Enforcement Monitoring Facility (LEMF))
- ❑ **The operator**
 - The entity that serves the target and manages the interception

What interception protocols do

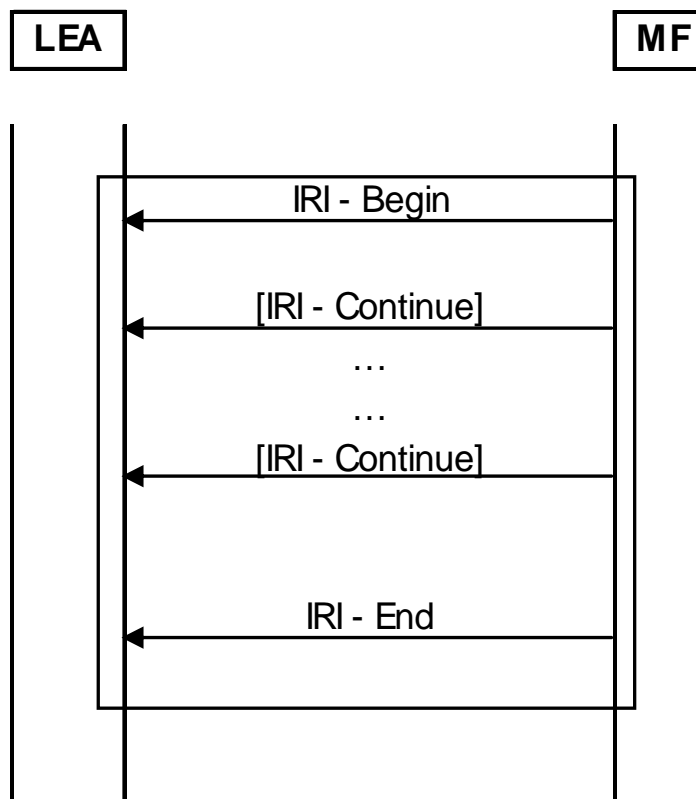


The IRI protocol#1

□ 4 types of IRI record

- **Begin**
- **Continue**
- **End**
- **Record**

IRI Protocol#2



Use of IRI Record Types

Record Type	When record type is used
Begin	First event of a communication attempt, opening the IRI transaction
Continue	Any time during a communication or communication attempt within the IRI transaction
End	The end of a communication or communication attempt, closing the IRI transaction
Report	Used in general for non-communication related events or where there is uncertainty about the event



Processing of intercepted data

□ Two models

- Encapsulation
- Mapping

□ Encapsulation

- Hand over of raw data as it first appears
- IRI-Report only used
- Information and intelligence captured by Law Enforcement Agency

□ Mapping

- Gives information and intelligence to LEA
- IRI Protocol used (Begin-Continue-End)
- Mapping is standardised

Why ETSI?

- ❑ **Source of many communications protocols**
 - Knowledge centre for how to intercept
- ❑ **Membership driven**
 - National and regional requirement to support LI identified to members
 - Lower cost to members if protocol and data model is standard (one model fits wherever the communications protocols are used)

Specification tools

□ Data

- Defined using ASN.1 for handover
- Preferred also using ASN.1 for interception

□ Protocol

- Mostly defined in plain text
- Some interception groups use SDL (TETRA), others use UML (TIPHON/TISPAN) – no fixed rules

Who does what in ETSI?

□ Division by function:

- Handover
- Interception

□ Handover:

- Led by TC LI
- Defines means for delivering intercepted signalling and communication to LEMF

□ Interception:

- Performed within technology TBs
- Defines how technology specific data is intercepted



The documents (handover)

□ Architecture

- TR 101 943v111, Concepts of Interception in a Generic Network Architecture

□ Handover

- ES 201 671, Handover interface for the lawful interception of telecommunications traffic
 - This covers handover for 64kb/s switched networks (Annex A), packet switched handover (Annex B), use of ROSE (or FTP) for HI2 (Annex C)
- TS 102 232, Handover Specification for IP Delivery

The documents (interception)

- TETRA: EN 301 040
- GSM/3GPP: TS 133 108 V5.3.0 (33.108 version 5.3.0 Release 5)
- E-mail: TS 102 233
- Internet access: TS 102 234
- TIPHON/TISPAN: TS 102 277 (in draft)
- ISDN: TR 102 053 V1.1.1
- Cable: TS 101 909-20-1, TS 101 909-20-2 (in draft)

Environment fluidity

- ❑ **Communications models and modes change**
 - Pay as you go models
 - Text and Instant messaging over voice
- ❑ **Operators**
 - Virtual and real operators
 - Small and large operators
 - Bit carriers and service providers
 - Interconnected and discrete
- ❑ **Support of law enforcement stays constant**
 - Criminal behaviour may move, need to stop it remains constant

Challenges

- ❑ **Encapsulation versus Mapping**
 - Who does the processing?
- ❑ **Broadband**
 - Interception and handover
 - Identification and capacity
- ❑ **Multi-provider environment**
 - One target many provider relationships
 - Network
 - Service
 - Content
- ❑ **NGN**
 - Object based capabilities rather than services
 - Open architectures with open provision
 - End user service logic

