5th Generation Crime-fighting in Cyberspace: Lawful Intercept in 5G Networks

Mats Näslund
National Defence Radio Establishment & KTH

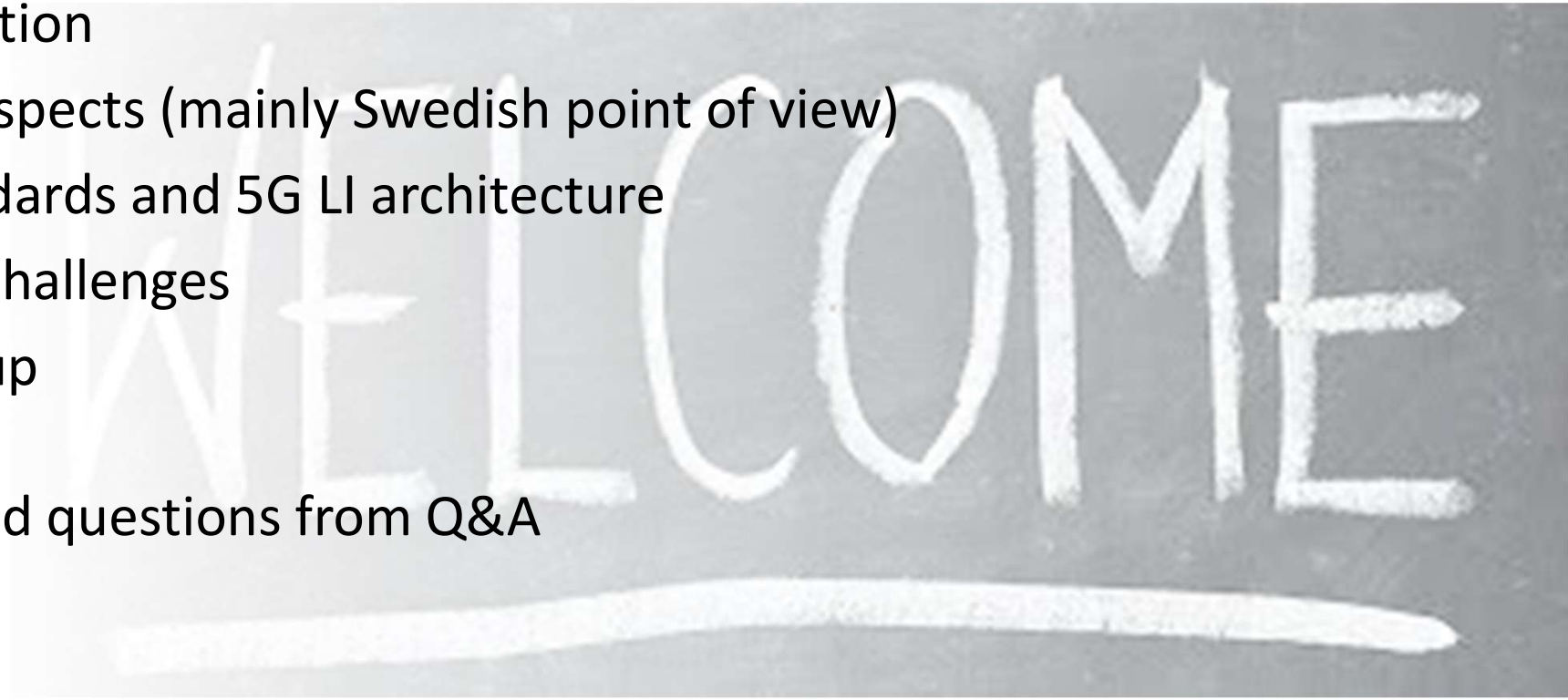
HAIC Talk, October 6 2020

Information in this material was prepared to support an oral presentation and cannot be considered complete without the accompanying discussion.

Talk Outline

- Motivation
- Legal aspects (mainly Swedish point of view)
- LI standards and 5G LI architecture
- Some challenges
- Wrap-up

- Selected questions from Q&A



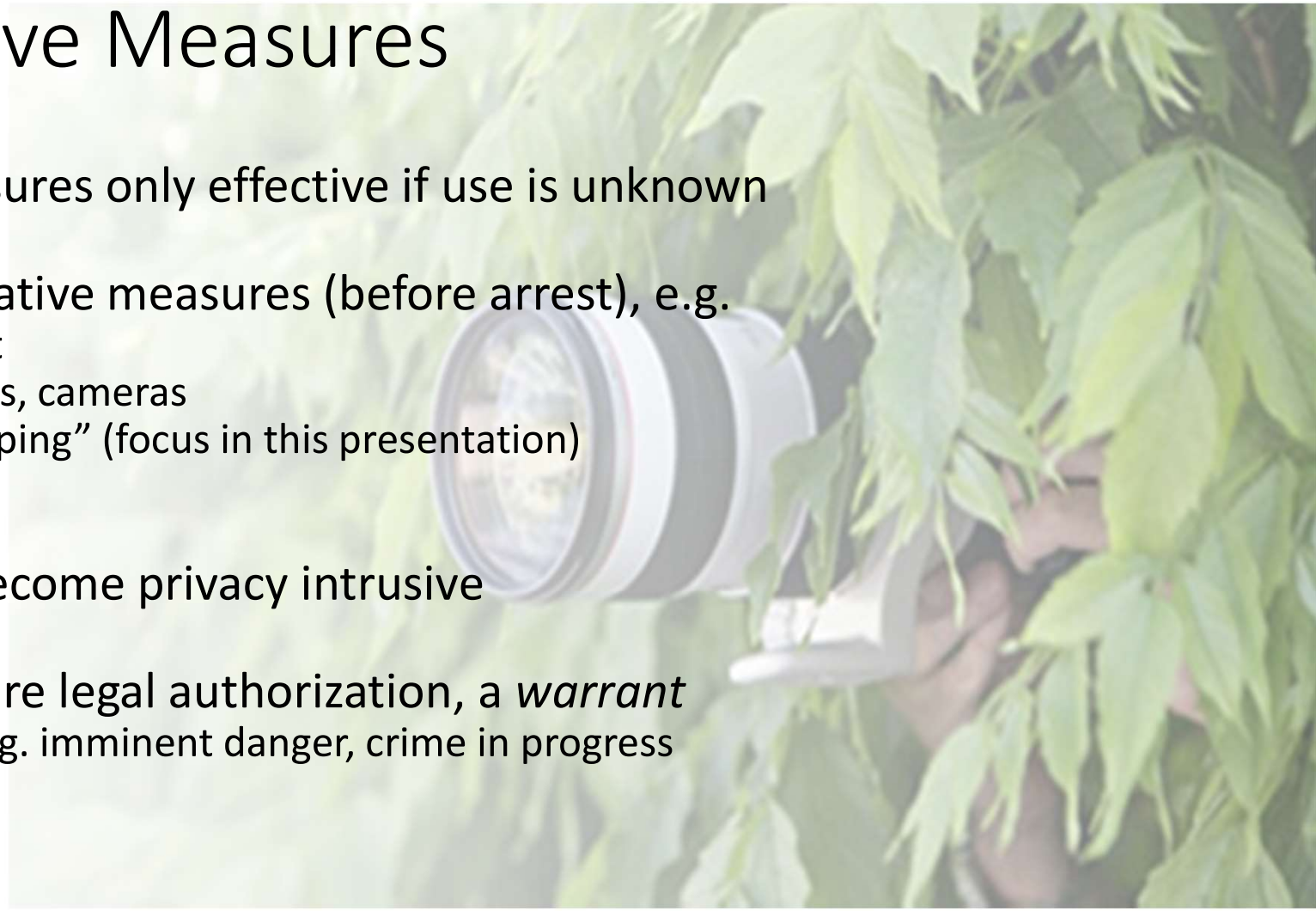
Motivation

Coercive measures

- Law enforcement based on voluntary co-operation from criminals is not feasible

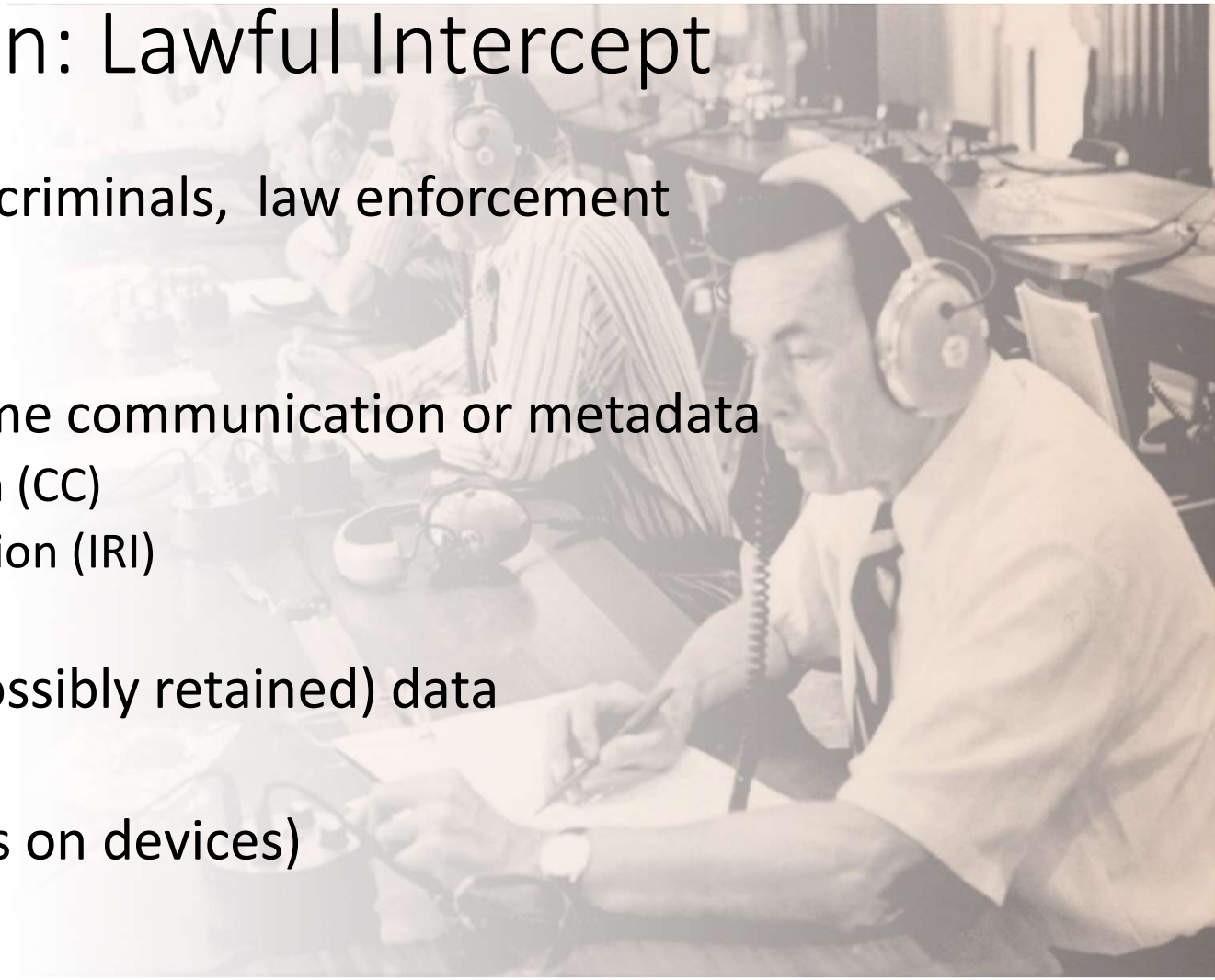
- Various *coercive measures* necessary
  - conducting on-premise searches (including private homes)
  - confiscating weapons and evidence
  - arresting suspects
  - etc

Secret Coercive Measures



- Some coercive measures only effective if use is unknown
- Particularly, investigative measures (before arrest), e.g.
  - Put a tail on suspect
  - Hidden microphones, cameras
  - Telephone ”wiretapping” (focus in this presentation)
  - …
- Measures tend to become privacy intrusive
- Rule of law $\Rightarrow$ require legal authorization, a *warrant*
  - some exceptions, e.g. imminent danger, crime in progress

Telecommunication: Lawful Intercept



Tele- and datacom used by criminals, law enforcement needs matching tools:

- Intercept of (near) real-time communication or metadata
  - Content of communication (CC)
  - Intercept-related information (IRI)
- Collection of historical (possibly retained) data
- Active measures (implants on devices)

Legal Aspects

Disclaimer:
- following slides focus on Sweden and only gives a high level summary
- some aspects may have been lost in translations into English

Legal Framework in Sweden

- Law regulating <u>which communication service providers</u> that are required to provide LI-related information,
  - "Law on electronic Communication" (2003:389)[1]

- Three frameworks regulating <u>when/how LI may be used</u>
  - "Code of judicial procedure" (1942:740)[2], the general LI framework
  - "Law on prevention of serious crime" (2007:979)[4], if imminent risk of committing serious crime
  - "Collection act" (2012:278)[3], to prevent/detect serious crime

- Recently also "Secret reading of data" (2020:62)[5]

1. Lagen om elektronisk kommunikation
2. Rättegångsbalken
3. Inhämtningslagen
4. "Prevlagen"
5. Lag om hemlig data-avläsning

General Prerequisites for LI Usage*

18 §, 19 §: crime under investigation must be *serious*

- a certain penal value (IRI: 6 months prison, CC: 2 years)
- some specifically listed crimes (espionage, terrorism, …)

20 §: a *specific suspect* is normally needed

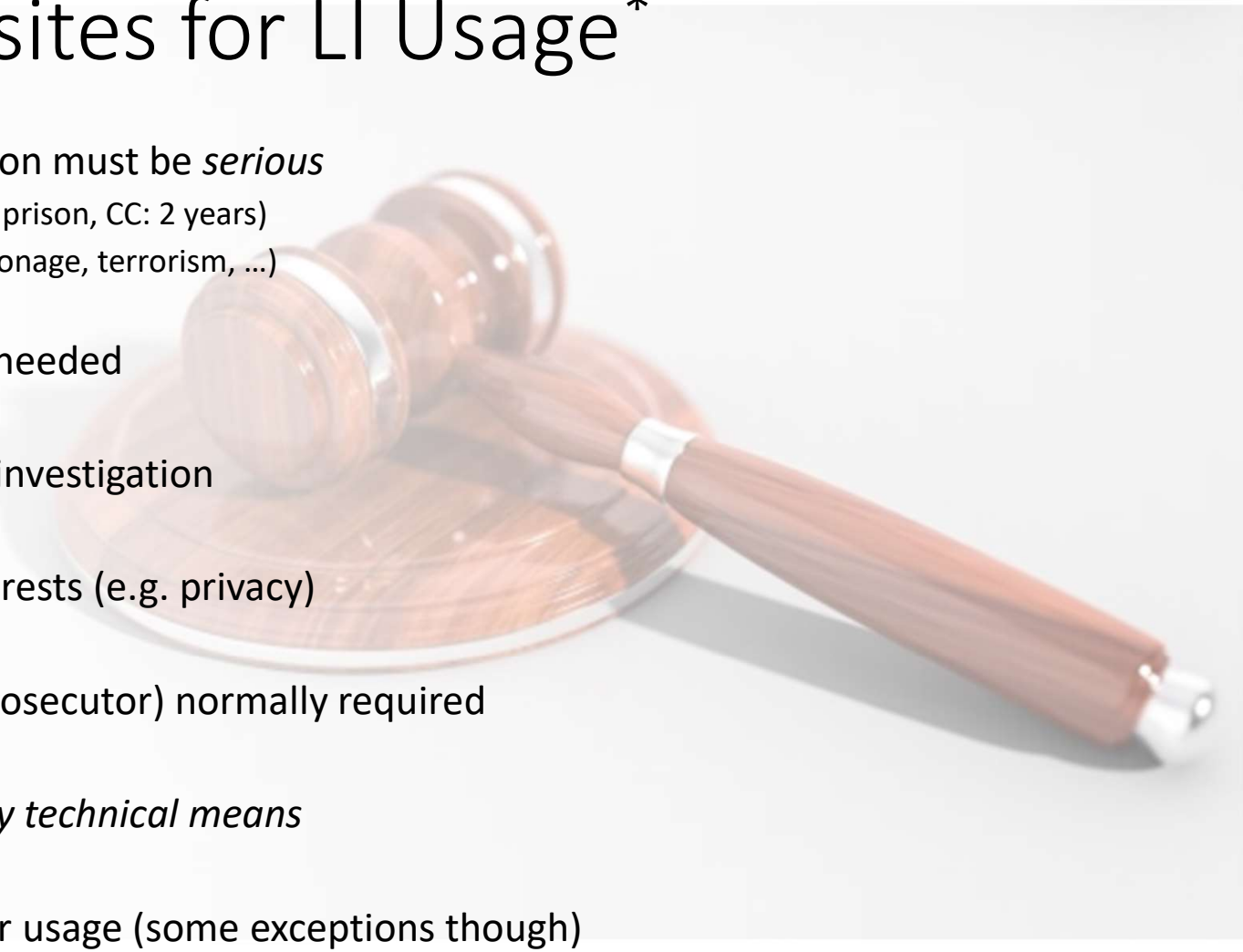
20 §: of *exceptional* importance to investigation

1 §: must *outweigh* conflicting interests (e.g. privacy)

21 §: *warrant* by court (or public prosecutor) normally required

25 §: authorization to use *necessary technical means*

33 §: *notification* to individual after usage (some exceptions though)



* (Law 1942:740, Ch 27)

Note on Data Retention

- EU Data Retention Directive 2006/24/EG
- Implemented in Sweden 2012
- Overturned: EU Court (2016), Swedish Court of Appeal (2017)
- This affected CSP:s obligation to retain data, but warrants still possible for historical data
  - e.g. presence of phones in a certain area at a certain time

Swedish Authorities with LI Mandate

Other Countries

- Finland's law (www.finlex.fi/sv/laki/ajantasa/2011/20110806)* similar, perhaps a bit "richer"
  - based mainly on length of text…
- EU: Council Resolution 17/1/1995 on Lawful Interception of Telecommunications
- USA: Omnibus Crime Control Act, CALEA, Patriot Act
- International: the Budapest Convention on Cybercrime (2001)
  - Accession by EU, Australia, Canada, Japan, USA and a few others

*) replace "sv" by "fi" to get version in finnish

Service Providers and Obligations

- CSP* = operator of: public communication network, public fixed telephony service, or public mobile communication service
  - proposed amendment (Dec 2020): interpersonal communication services based on number-plans

- Two main obligations
  - Non-disclosure of intercept activation
  - Facilitating information handover
    - could mean providing decryption keys, if available

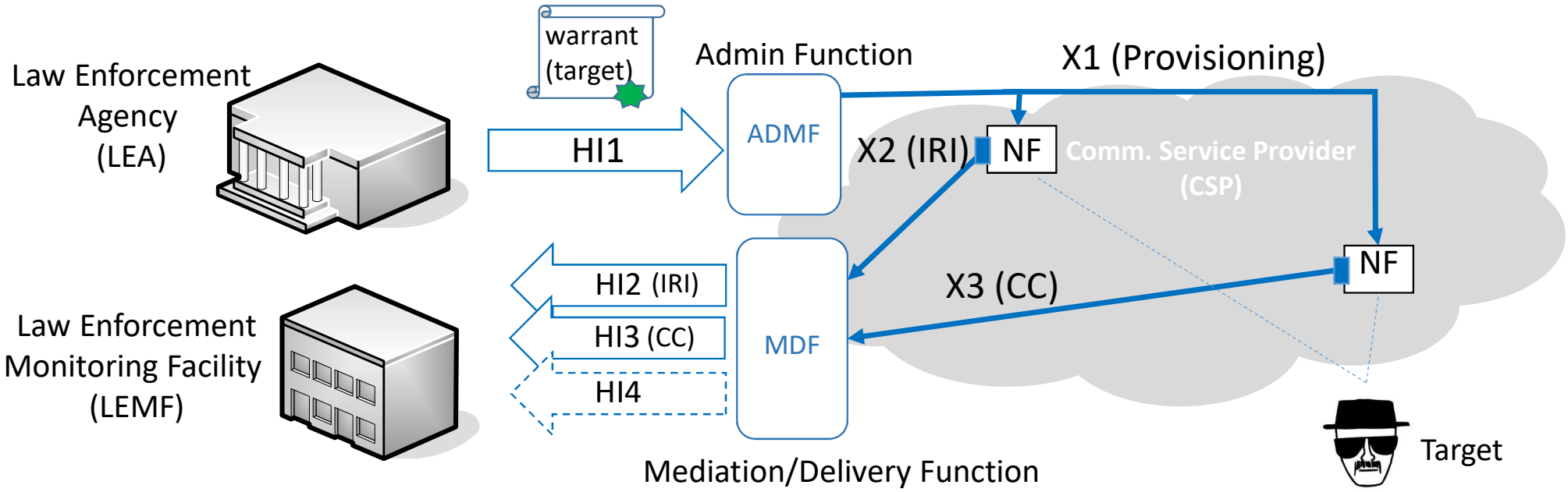
*) in Sweden

LI Standards and 5G Architecture

LI Standards

- Many vendors, many CSP:s, and many law enforcement agencies ⇒ need to standardize also LI functions and interfaces
- Interfaces between network and law enforcement are called *Handover Interfaces*
- Network-internal, LI-related interfaces called *X-interfaces*
- Standardized by ETSI TC LI (fixed) and 3GPP SA3LI (mobile)
  - For 5G LI, some dependencies to ETSI TC NFV
- (Also national and non-3GPP related standards)

HI and X Interfaces: High Level View



HI1, X1: Intercept management and provisioning
HI2, X2: IRI (e.g. comm. monitoring, metadata)
HI3, X3: CC (communication content)
HI4: LI status notification
▮ : Point-of-Intercept (POI)

5G LI Standards

Requirements

3GPP TS 33.126 V16.2.0 (2020-07)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security;
Lawful Interception requirements
(Release 16)

Architecture & Functions

3GPP TS 33.127 V16.5.0 (2020-09)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security;
Lawful Interception (LI) architecture and functions
(Release 16)

Protocols & Procedures

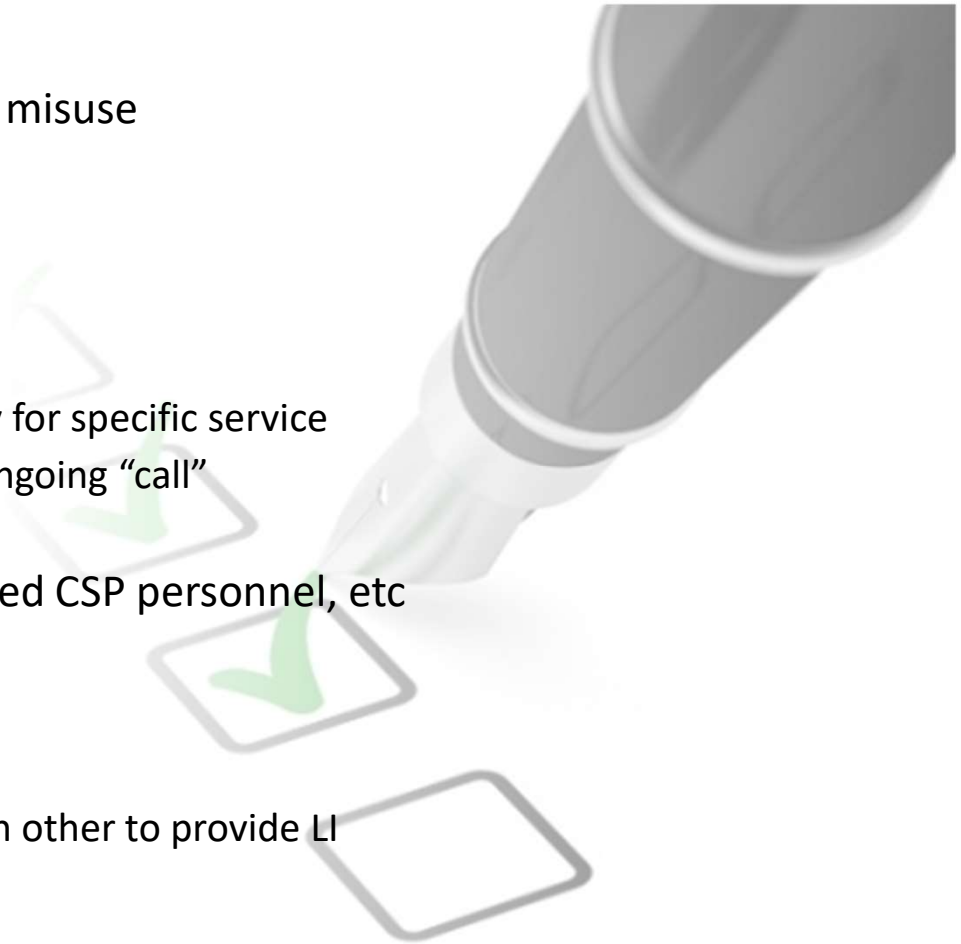
3GPP TS 33.128 V16.4.0 (2020-09)

Technical Specification

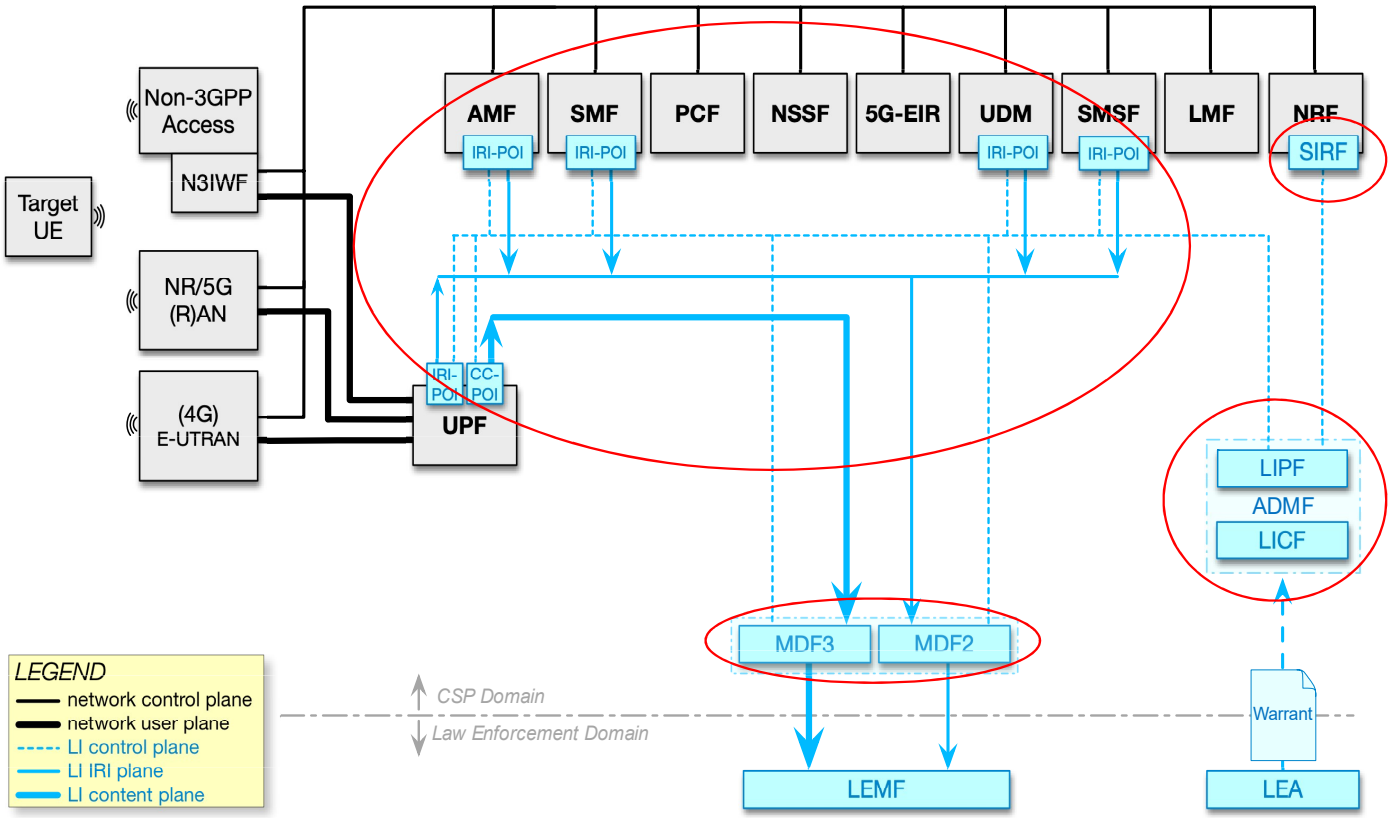
3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security;
Protocol and procedures for Lawful Interception (LI);
Stage 3
(Release 16)

Crucial Requirements

- The handover interfaces must be secure, avoiding misuse
- The intercept only done for the specified target
- Avoid both under-collection and over-collection
  - Warrant can be limited e.g. to only IRI, and/or only for specific service
  - Must be possible to activate/deactivate LI under ongoing “call”
- LI must not be detectable by: target, non-authorized CSP personnel, etc
  - E.g. activating LI must not affect the service
- Independence between jurisdictions
  - E.g. home/serving network cannot depend on each other to provide LI

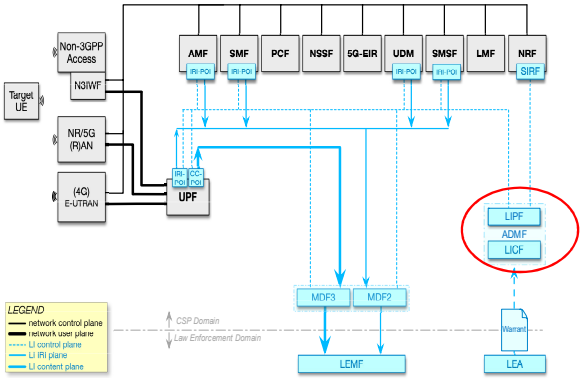


33.127 Architecture

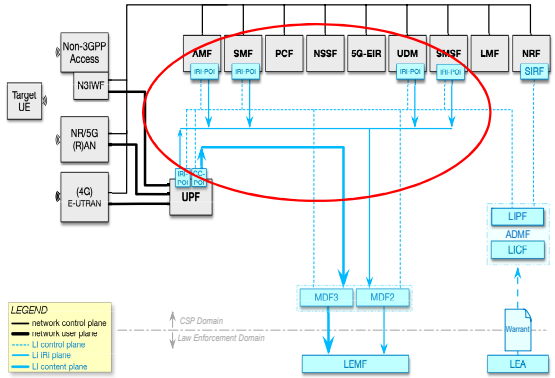


Administration Function

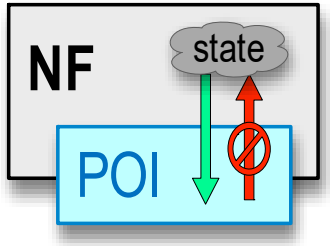
- Receives warrant from LEA
  - Often manual handling, e.g. over crypto-fax
- LI Control Function (LICF)
  - Master record of LI information (e.g. list of targets)
  - Authorizes LI-related operations (e.g. deploying new function with intercept capabilities)
  - Implemented on LI-specific Infrastructure
- LI Provisioning Function (LIPF)
  - Provisions functions to carry out intercept



Point-of-Intercept (POI)



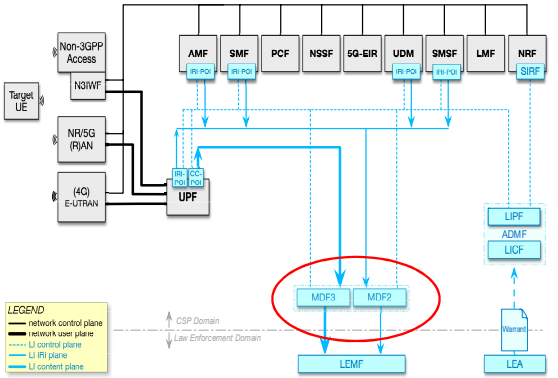
- Network Function (NF) that may have LI-relevant info has a Point-of-Intercept
  - IRI-POI or CC-POI depending e.g. on control plane or user plane
- POI normally pre-provisioned by LIPF to collect data associated with LI Target
- ”one-way” access into state machine of NF
  - to meet undetectability requirements



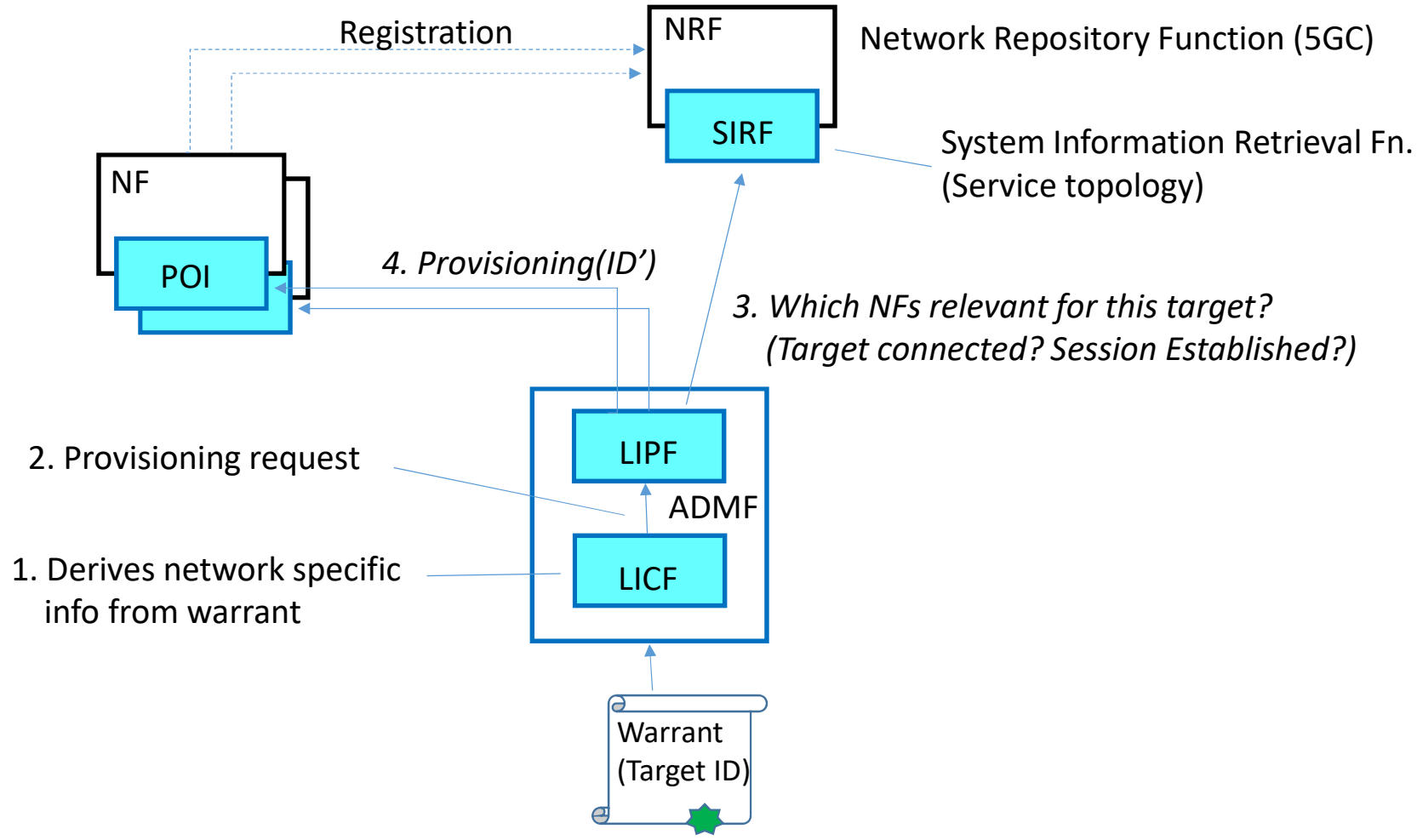
Mediation/Delivery Function

- Deliver “well-formatted” LI-product to LEMF

- Attaches LI specific metadata
  - LIID (Lawful Intercept ID)
  - Timestamp
  - Network ID
  - Other correlation information

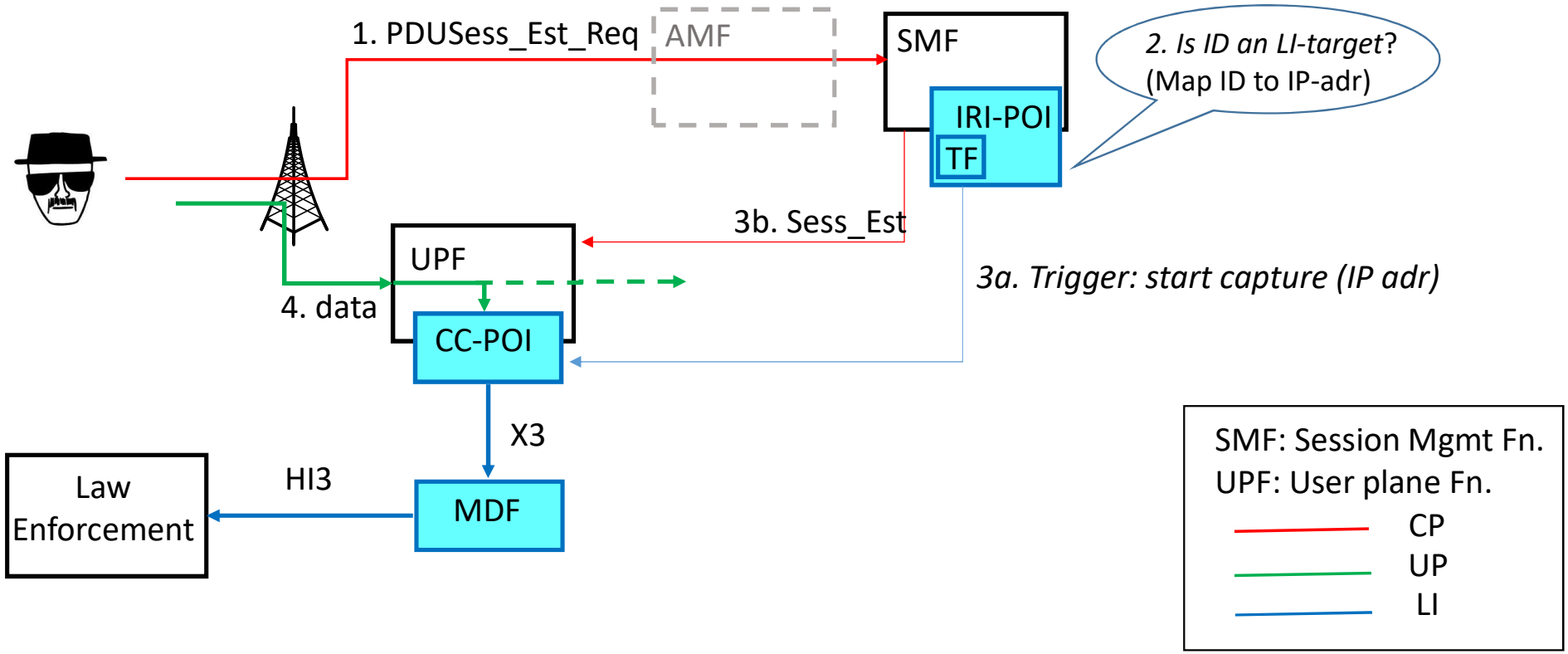


Intercept Control Flow



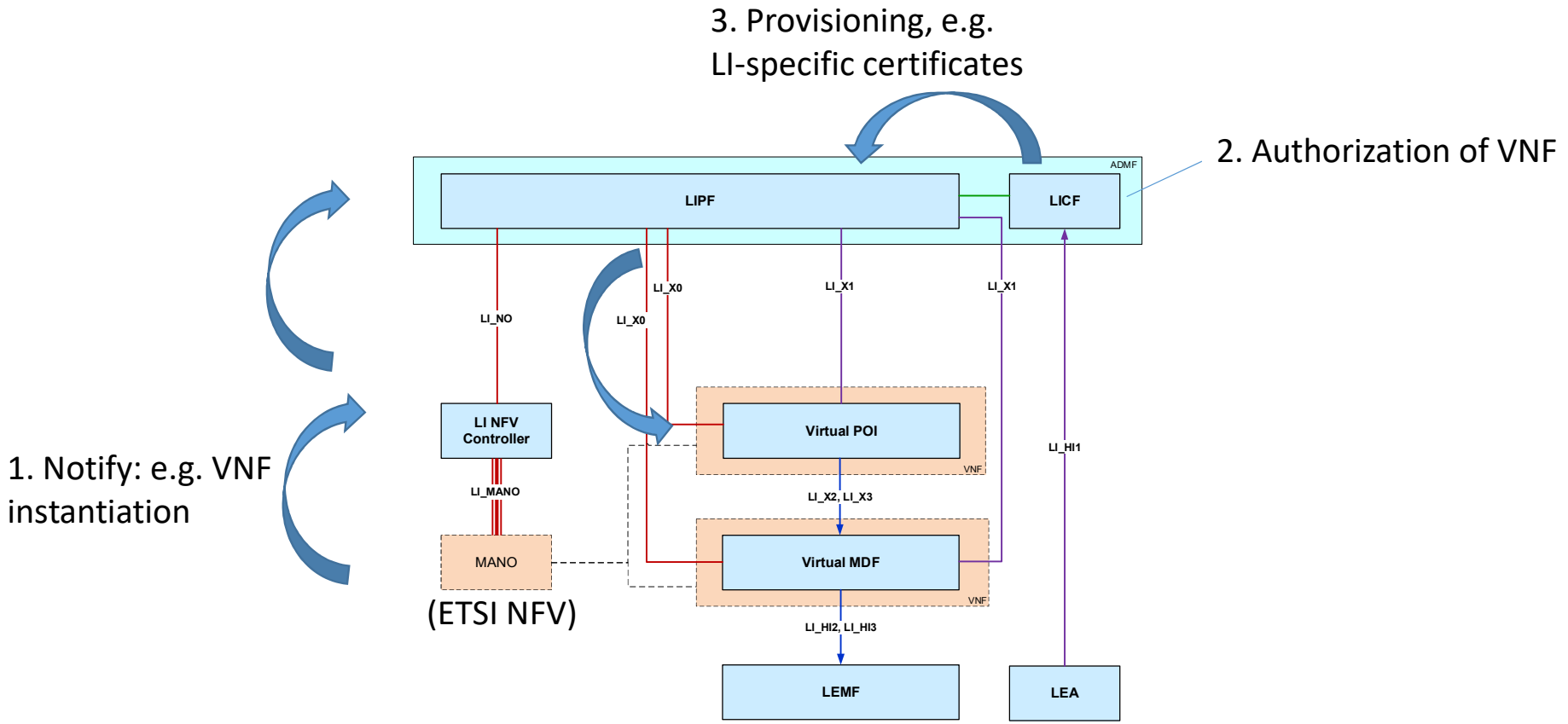
Triggered POIs and Triggering Functions

Control- and user-plane split

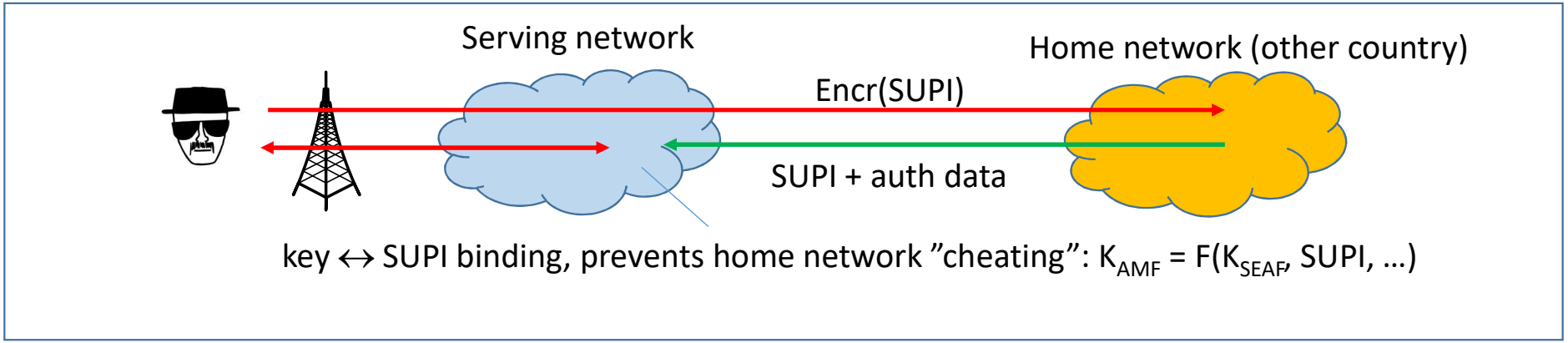


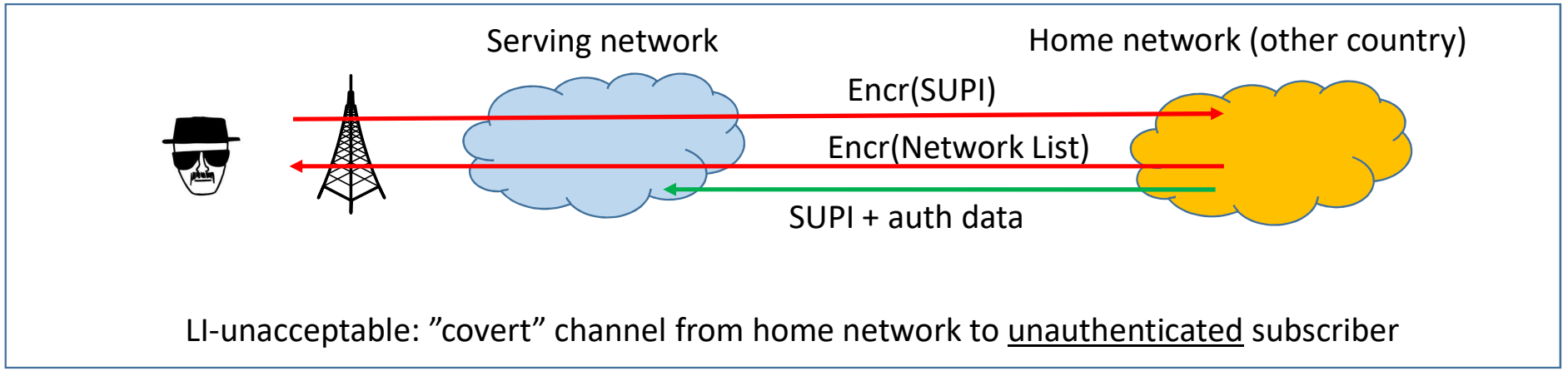
Examples of 5G LI Considerations

Virtualization – LI Interaction

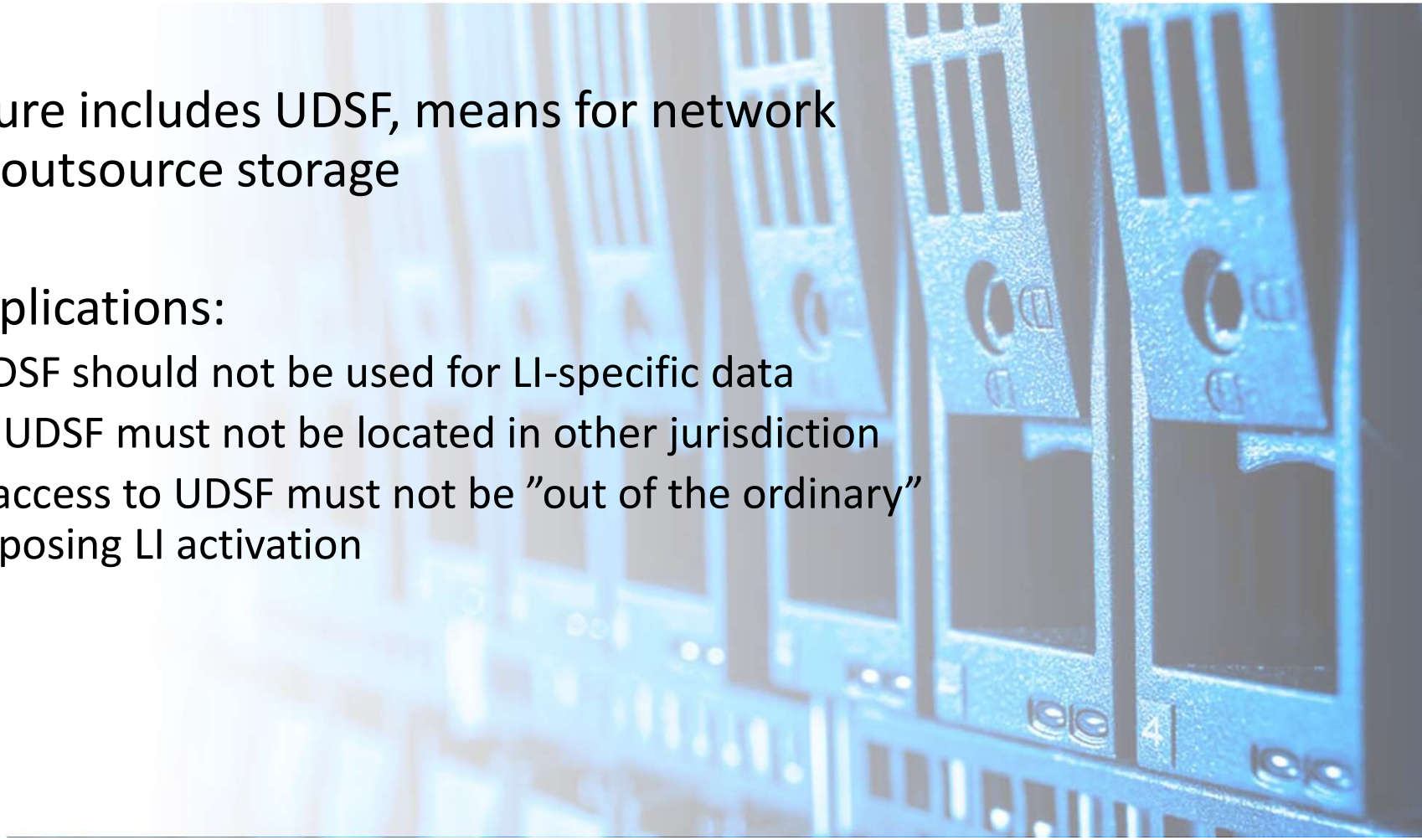


SUPI Encryption and Steering of Roaming





UDSF: Unstructured Data Storage Function



- 5G architecture includes UDSF, means for network functions to outsource storage

- Several LI implications:
  - (shared) UDSF should not be used for LI-specific data
  - Li-relevant UDSF must not be located in other jurisdiction
  - LI-specific access to UDSF must not be ”out of the ordinary” to avoid exposing LI activation

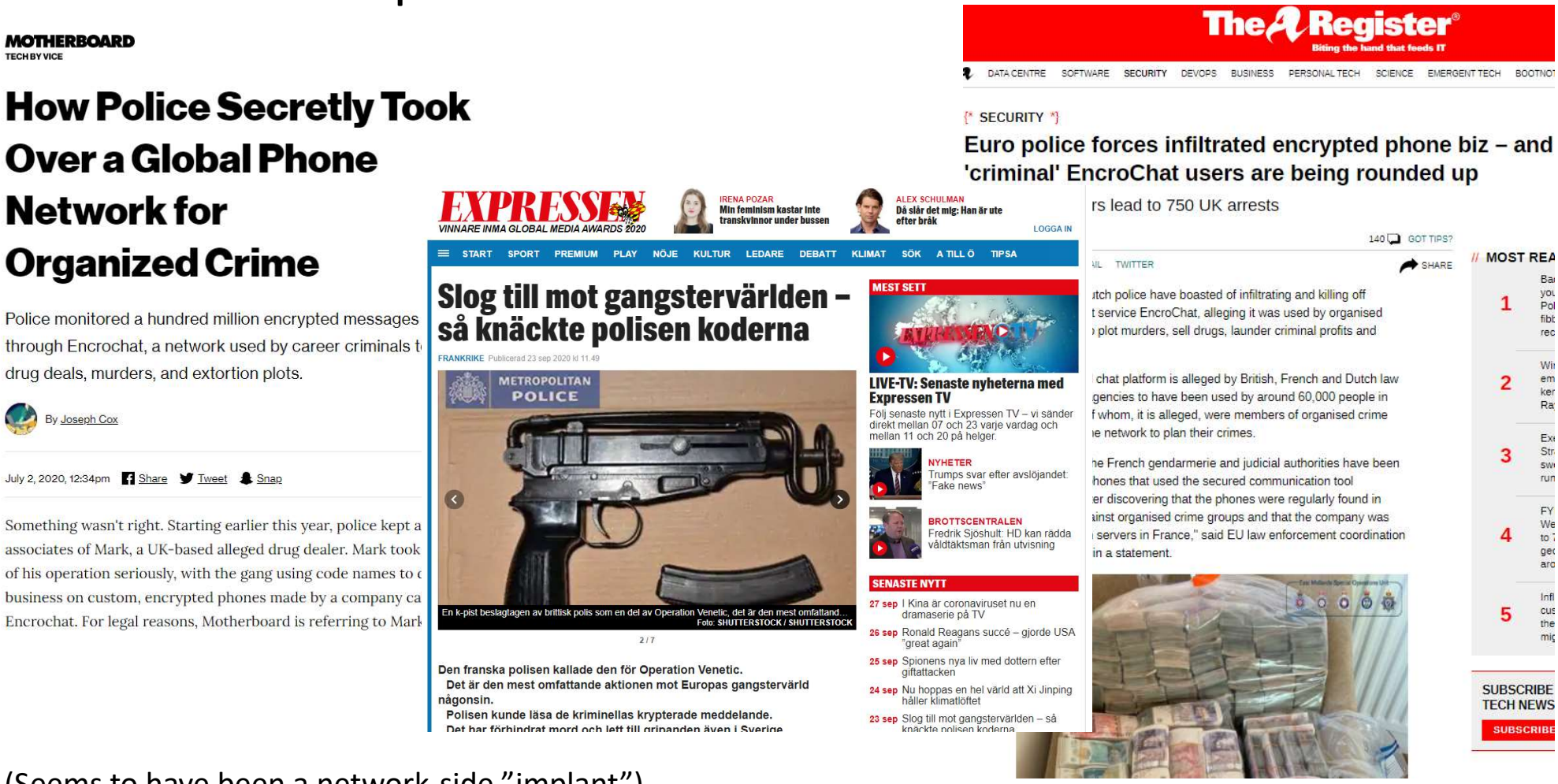
Some Challenges

Non-traditional Telecom Providers

- More and more user traffic moving to NTT messaging apps
- These apps almost always use end-to-end encryption
- May fall outside LI obligations and/or cannot aid in providing cleartext content
- A main motivation behind new Swedish law “secret reading of data” (2020:62)
  - crimes which give at least 2 years in prison (or other specifically listed crimes)
  - applies to information systems used by the suspect or which the suspect can reasonably be assumed to contact
  - cannot be used on system regularly in use by lawyer, doctor etc
  - allowed technical means include “circumventing security measures and exploiting vulnerabilities”
  - (Finnish legal framework in principle supports similar LI functionality*)

*) Lagrådsremiss: Hemlig dataavläsning, 24 oktober 2019

Recent Example of Active Measures



MOTHERBOARD
TECH BY VICE

How Police Secretly Took Over a Global Phone Network for Organized Crime

Police monitored a hundred million encrypted messages through Encrochat, a network used by career criminals t drug deals, murders, and extortion plots.

By Joseph Cox

July 2, 2020, 12:34pm Share Tweet Snap

Something wasn't right. Starting earlier this year, police kept a associates of Mark, a UK-based alleged drug dealer. Mark took of his operation seriously, with the gang using code names to c business on custom, encrypted phones made by a company ca Encrochat. For legal reasons, Motherboard is referring to Mark

The Register
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOT

{* SECURITY *}

Euro police forces infiltrated encrypted phone biz – and 'criminal' EncroChat users are being rounded up

rs lead to 750 UK arrests

140 GOT TIPS?

IL TWITTER SHARE

itch police have boasted of infiltrating and killing off t service EncroChat, alleging it was used by organised plot murders, sell drugs, launder criminal profits and

chat platform is alleged by British, French and Dutch law gencies to have been used by around 60,000 people in f whom, it is alleged, were members of organised crime e network to plan their crimes.

he French gendarmerie and judicial authorities have been hones that used the secured communication tool er discovering that the phones were regularly found in ainst organised crime groups and that the company was servers in France," said EU law enforcement coordination in a statement.

MOST REA
1 Ba you Pol fibt rec
2 Wi em ker Ra
3 Ex Str sw run
4 FY We to ge ard
5 Infl cus the mig

SUBSCRIBE TECH NEWS
SUBSCRIBE

EXPRESSEN
VINNARE INMA GLOBAL MEDIA AWARDS 2020

IRENA POZAR
Min feminism kastar inte transkvinnor under bussen

ALEX SCHULMAN
Då slår det mig: Han är ute efter bråk

LOGGA IN

START SPORT PREMIUM PLAY NÖJE KULTUR LEDARE DEBATT KLIMAT SÖK A TILL Ö TIPSA

Slog till mot gangstervärlden – så knäckte polisen koderna

FRANKRIKE Publicerad 23 sep 2020 kl 11.49

METROPOLITAN POLICE

En k-pist beslagtagen av brittisk polis som en del av Operation Venetic, det är den mest omfattand...
Foto: SHUTTERSTOCK / SHUTTERSTOCK

2 / 7

Den franska polisen kallade den för Operation Venetic.
Det är den mest omfattande aktionen mot Europas gangstervärld någonsin.
Polisen kunde läsa de kriminellas krypterade meddelande.
Det har förhindrat mord och lett till gripanden även i Sverige

MEST SETT

LIVE-TV: Senaste nyheterna med Expressen TV
Följ senaste nytt i Expressen TV – vi sänder direkt mellan 07 och 23 varje vardag och mellan 11 och 20 på helger.

NYHETER
Trumps svar efter avslöjandet: "Fake news"

BROTTSCENTRALEN
Fredrik Sjöshult: HD kan rädda våldtäktsman från utvisning

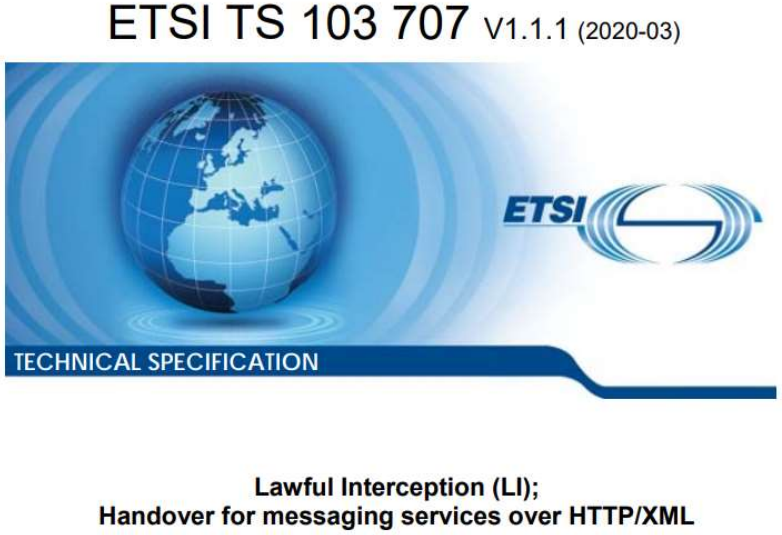
SENASTE NYTT

27 sep I Kina är coronaviruset nu en dramaserie på TV
26 sep Ronald Reagans succé – gjorde USA "great again"
25 sep Spionens nya liv med dottern efter giftattacken
24 sep Nu hoppas en hel värld att Xi Jinping håller klimatlöftet
23 sep Slog till mot gangstervärlden – så knäckte polisen koderna

(Seems to have been a network-side ”implant”)

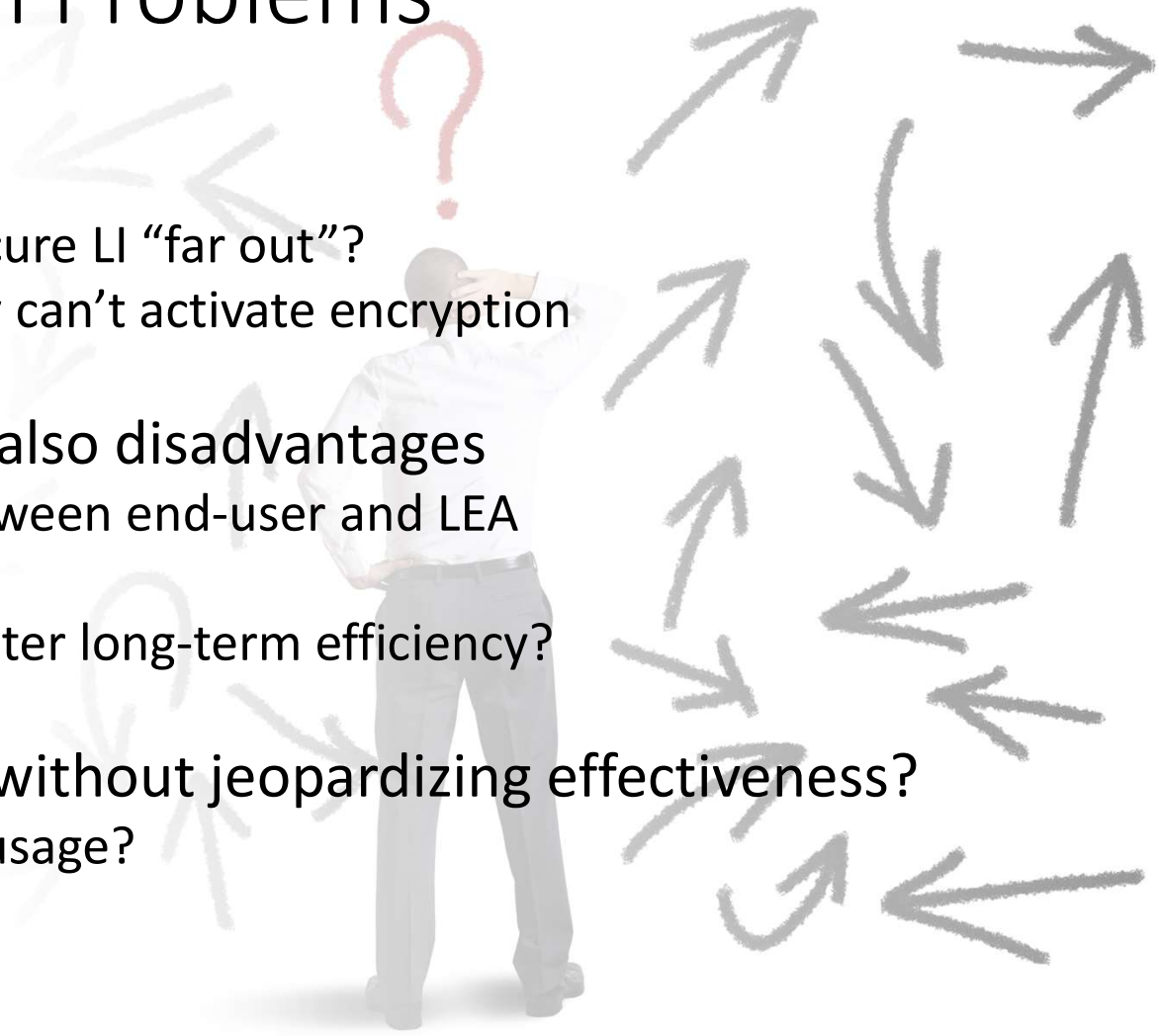
New Standard: ETSI TS 103 707

- LI standard for messaging services (March 2020)
- Based on HTTP/XML (instead of ASN.1)
- Several of the large NTT:s have been involved in standardization effort



Some (Difficult) Open Problems

- Further 5G developments
  - E.g. edge computing: how to secure LI “far out”?
  - Home-routed services: currently can’t activate encryption
- ”Active LI” has advantages but also disadvantages
  - A kind ”handover interface” between end-user and LEA
  - Impossible to standardize
  - Acceptable alternatives with better long-term efficiency?
- Can we improve transparency without jeopardizing effectiveness?
  - Technical means for auditing LI usage?



Summary

- Lawful Intercept: Important tool for law enforcement
  - Governed by law(s), authorized by warrants
  - Real-time or historical data
  - Metadata (IRI) or communication content (CC)
- Technical standards: ETSI and 3GPP
- 5G LI has specific technical considerations (virtualization etc)
- Encrypted services currently handled by “active LI”

Selected Q&A:s (1/3)

- Q: Are there any LI functions defined for the roaming interfaces?
- A: No, LI interfaces are only defined internal to the core network.

- Q: Can there be conflicts between GPDR and LI regulations?
- A: GDPR makes an exception to allow LI. There are however regulations stating how law enforcement needs to handle personal data after it has been handed over from the CSP, e.g. EU directive 2016/680.

Selected Q&A:s (2/3)

- Q: Does LI apply to SIM-specific functions such as OTA?
- A: The 3GPP standards do not cover things such as SIM OTA. Since OTA would be difficult to use for general purpose communication it is currently not seen as important to enable LI for it.

- Q: If a person is notified about having been a target for intercept, are also persons who have communicated with the target notified?
- A: The way the law is formulated, it seems to apply only to the target itself.

Selected Q&A:s (3/3)

- Q: How are the requirements on undetectability of LI handled, do the standards cover it or is it left to implementation?
- A: Both. The standards are written to avoid bad designs that would imply a risk that activation of LI can be noticed by users. For example, the standards avoid relying on LI-specific signalling taking place outside of the protected LI-domain. Then there will be some things left to implementation, e.g. the implementation has to be done to avoid that undesired extra delays imposed by LI functions could be detected outside the LI-domain.