Lawful Interception (LI) für IP-basierte Dienste

Standardisierung bei ETSI

Historisches

- Leitungsvermittelte Netze (PSTN, ISDN und GSM)
  - Überwachungsverordnung schreibt Implementierung von ES 201 671 in Version 2.1.1 vor.
  - ES 201 671 beschreibt (im Wesentlichen) die Schnittstelle zwischen Netzbetreiber und LEA (Law Enforcement Agency)
  - Bereitstellung dieser Schnittstelle mit 1. Jänner 2005
  - IP-basierte Dienste werden von ES 201 671 V2.1.1 nicht abgedeckt.

IPLI - Problematik

- Vermischung zwischen Dienst-Erbringung und Bereitstellung der Transportleistung.
  - Dienste sind für die darunterliegende Transportschicht transparent (horizontales Schichtenmodell).
- Überwachungsrelevante Informationen sind in der Regel nicht zentral erfassbar. Verschiedene Rollen sind zu betrachten:
  - NWO (Network Operator)
  - AP (Access Provider)
  - SvP (Service Provider)
- Identifikation der „richtigen“ IP-Pakete
  - Dynamische Vergabe von IP-Adressen
  - IP-Adressen sind daher nicht allein zur Identifikation des zu überwachenden Verkehrs ausreichend.

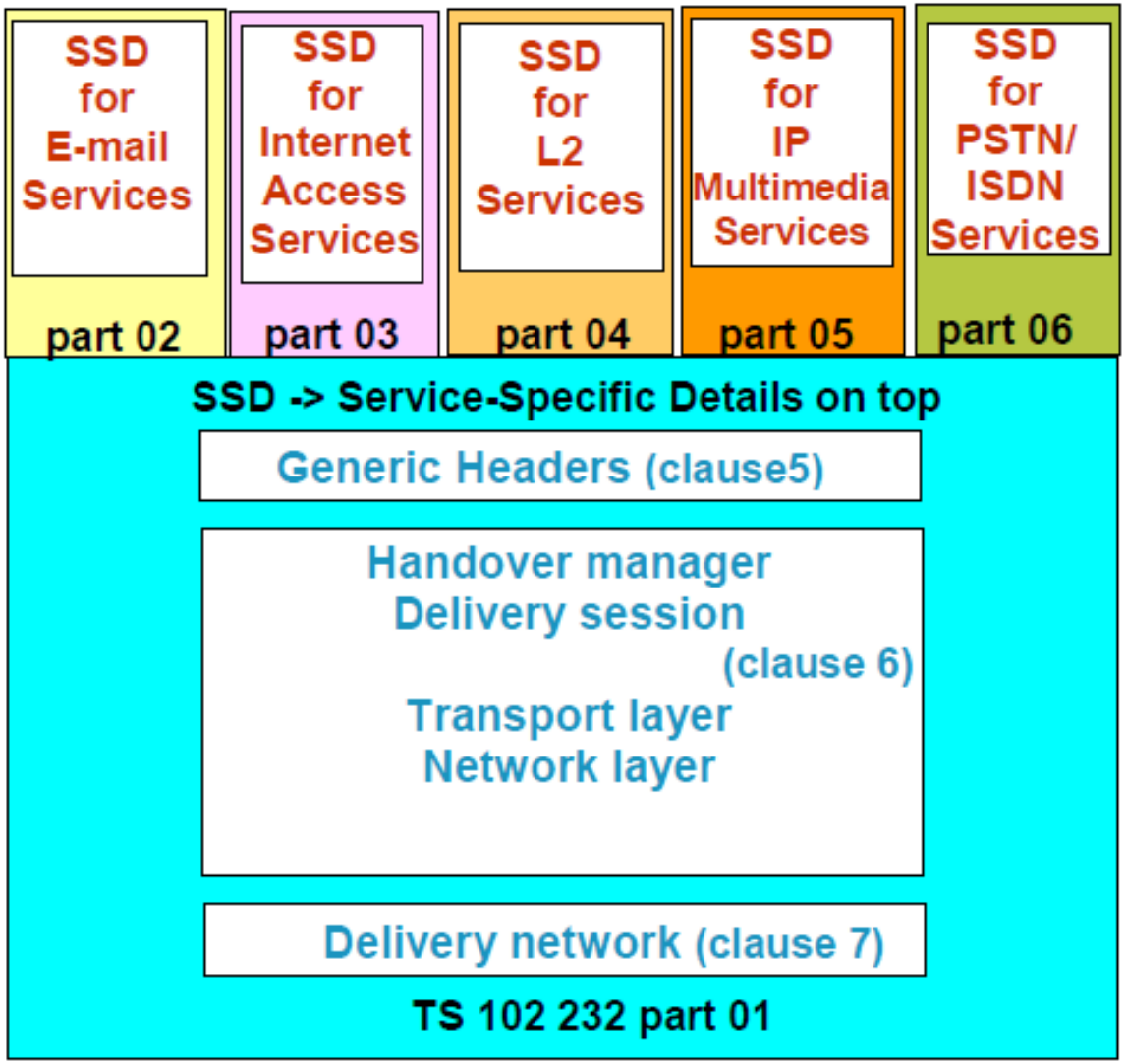
IPLI - Problematik

- Schlussfolgerung von ETSI
  - LI-Anforderungen sind selektiv unter Berücksichtigung der verschieden Rollen (NWO, AP, SvP) zu definieren.

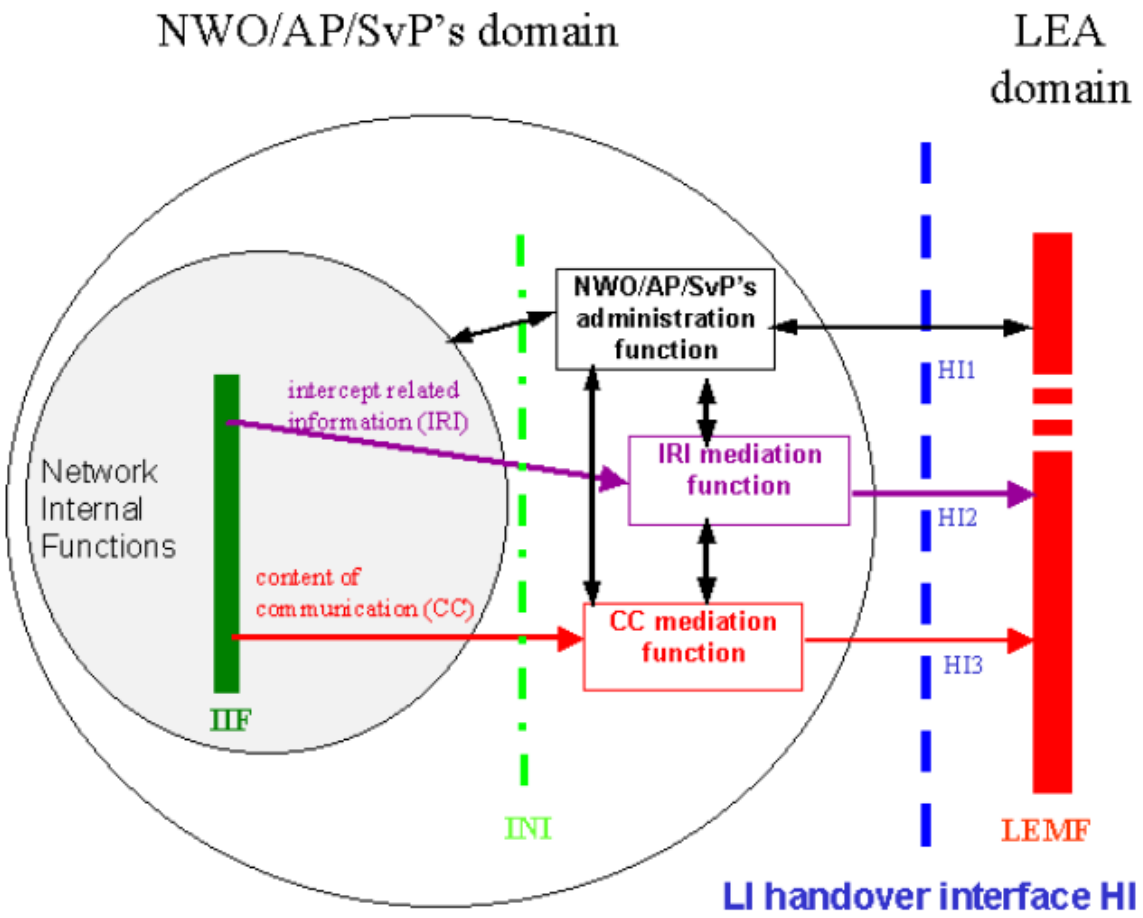
ETSI TS - Struktur

- ETSI wählt für die Beschreibung folgende Struktur:
  - TS 102 232-1
    umfasst die allgemeinen Teile des Handover Interface (HI)
  - TS 102 232-2 bis 6
    umfassen die servicespezifischen Details. Die Transportleistung wird dabei ebenfalls als „Service“ gesehen.

ETSI TS - Struktur



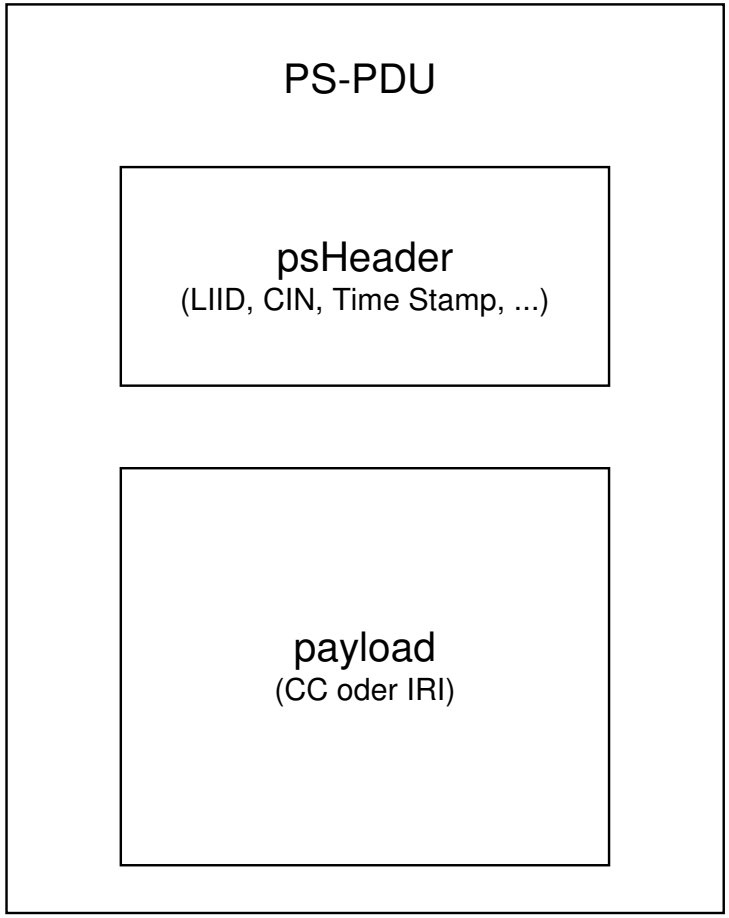
- Es werden 3 Handover Interfaces (HI) definiert:
  - HI 1: Administrative Schnittstelle
  - HI 2: Intercept Related Information (IRI)
  - HI 3: Content of Communication (CC)
- Anforderungen an netzinterne Überwachungsfunktionen werden indirekt definiert.



IIF: internal interception function
INI: internal network interface

HI1: administrative information
HI2: intercept related information
HI3: content of communication

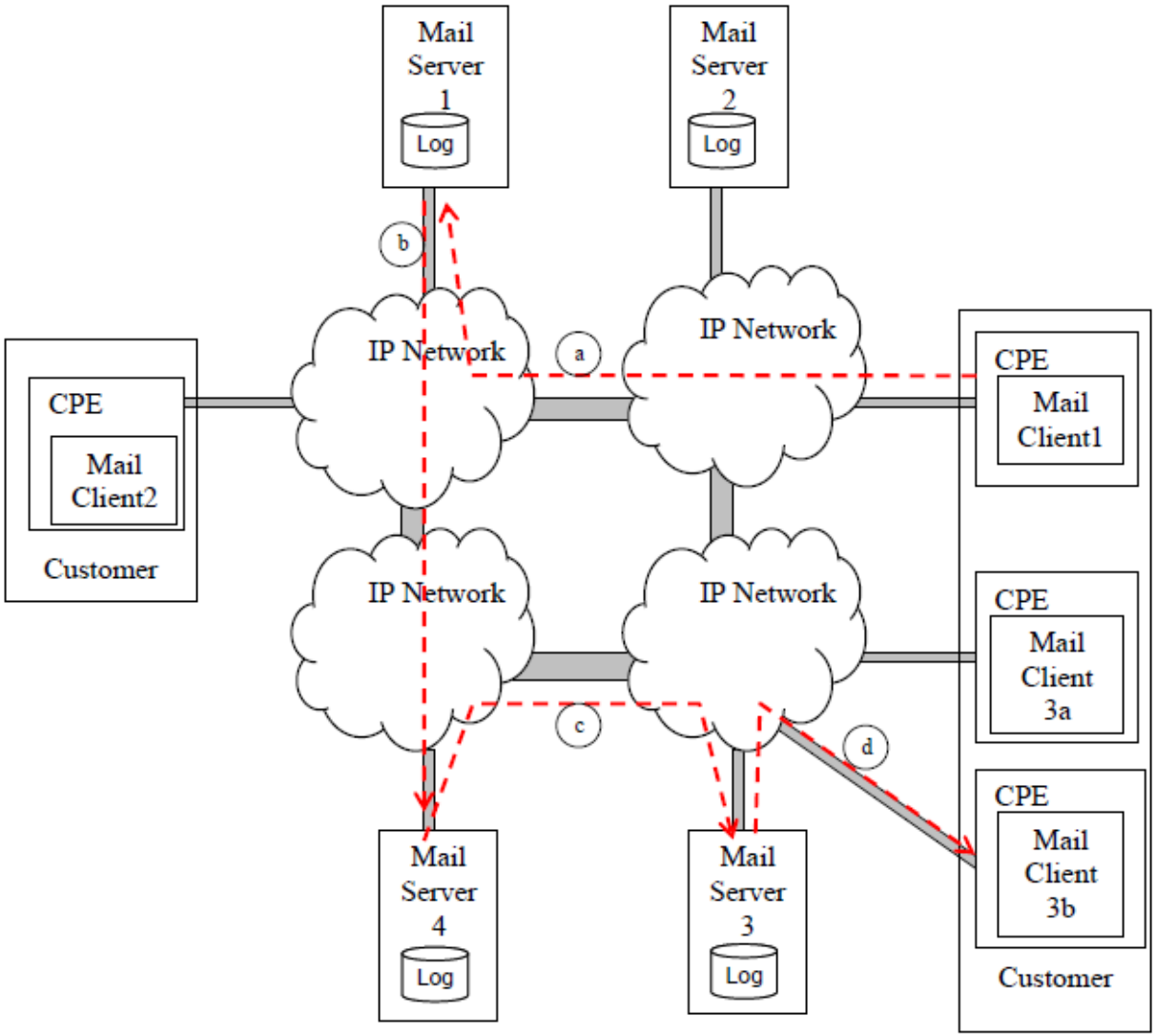
- HI 1
  - Wird nicht näher spezifiziert
- HI 2 und HI 3
  - Übergabe der Daten erfolgt in Protocol Data Units (PDU)
  - Diese PDU haben folgende Struktur:
    - Header
    - Payload


PS-PDU
psHeader
(LIID, CIN, Time Stamp, ...)
payload
(CC oder IRI)

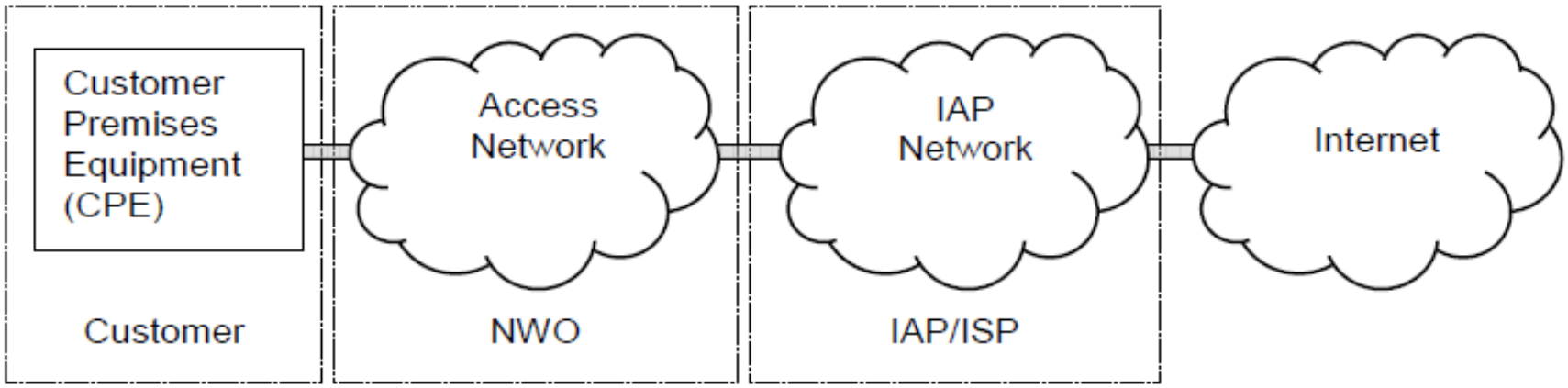
- Parameter im Header
  - LIID Lawful Interception Identifier
  - CIN Communication Identifier
  - Sequence number
  - Payload timestamp
  - Payload direction
  - Interception type
  - IRI type
  - ...

- Betrachtet werden „ARPANET Textnachrichten“
- Instant Messaging und Chat werden explizit ausgeschlossen.
- Es werden die relevanten Fälle und die zu übermittelnden Inhalte definiert.

E-Mail Services (TS 102 232-2)



- Unter einem Internet Access Service (IAS) wird die Bereitstellung eines Zugangs zum Internet für Endkunden verstanden.
- Die Teilnehmeranschaltung erfolgt über einen NWO, der die Hoheit über das Access Network hat.
- Mögliche Access Networks sind:
  - PSTN/ISDN Dial-up
  - xDSL
  - TV-Kabelnetze
  - Wireless LAN-Netze (WLAN)

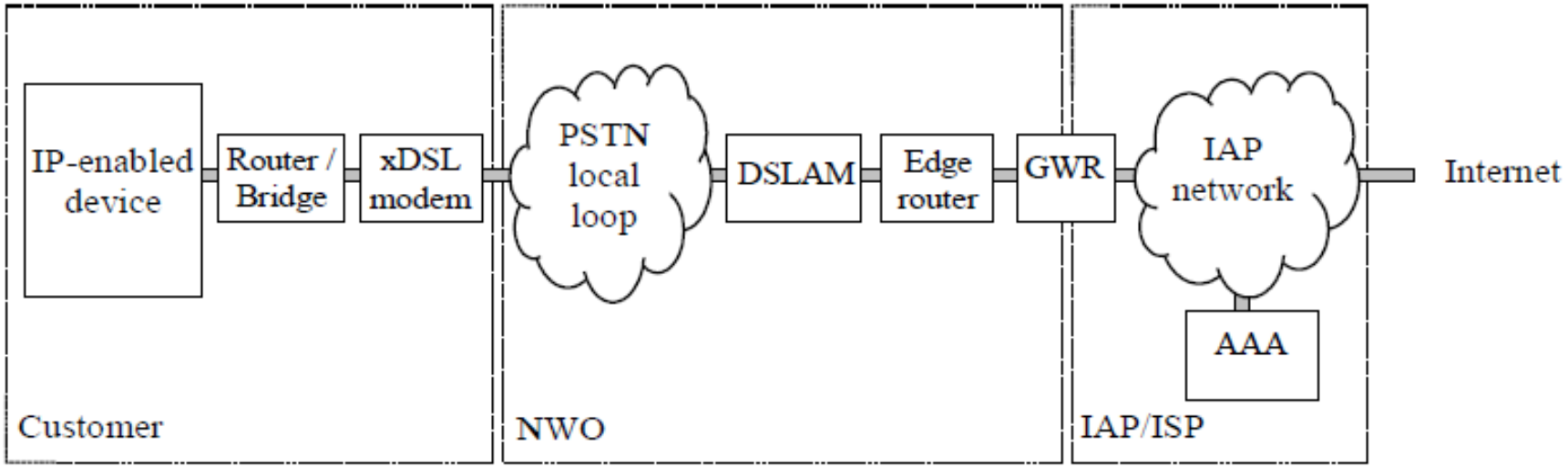

Customer Premises Equipment (CPE)
Customer
Access Network
NWO
IAP Network
IAP/ISP
Internet

- ETSI ist sich bewusst, dass die im Feld befindlichen Implementierungen heterogen sind. Es wird daher auf Begriffe nur in allgemeiner Form eingegangen.

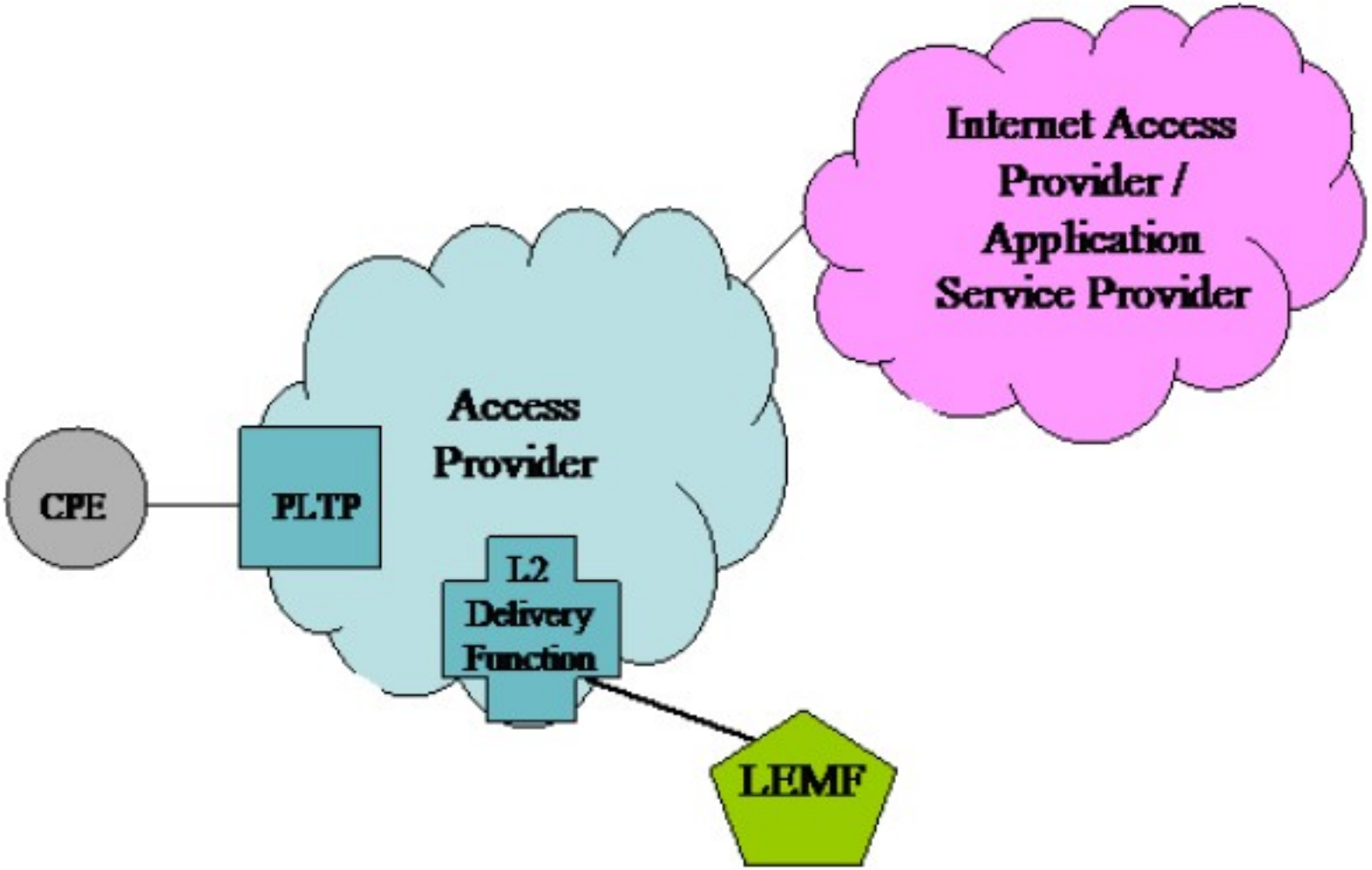
  Beispiele:
  - Target Identity
    - Bereitstellung einer IP-Adresse nach Authentifizierung, Autorisierung und Accounting (AAA)
    - User Name
    - Network Access Identifier
    - Ethernet-Adresse
    - Calling Line Identity (CLI)

- IRI-Records
  - Erzeugung bei Anmeldung und Statusänderung
  - Enthalten die jeweilige Target Identity
- Content of Communication
  - IP-Datagramm
  - Umfasst alle Protokollschichten über und inklusive Layer 3 (IP-Layer)

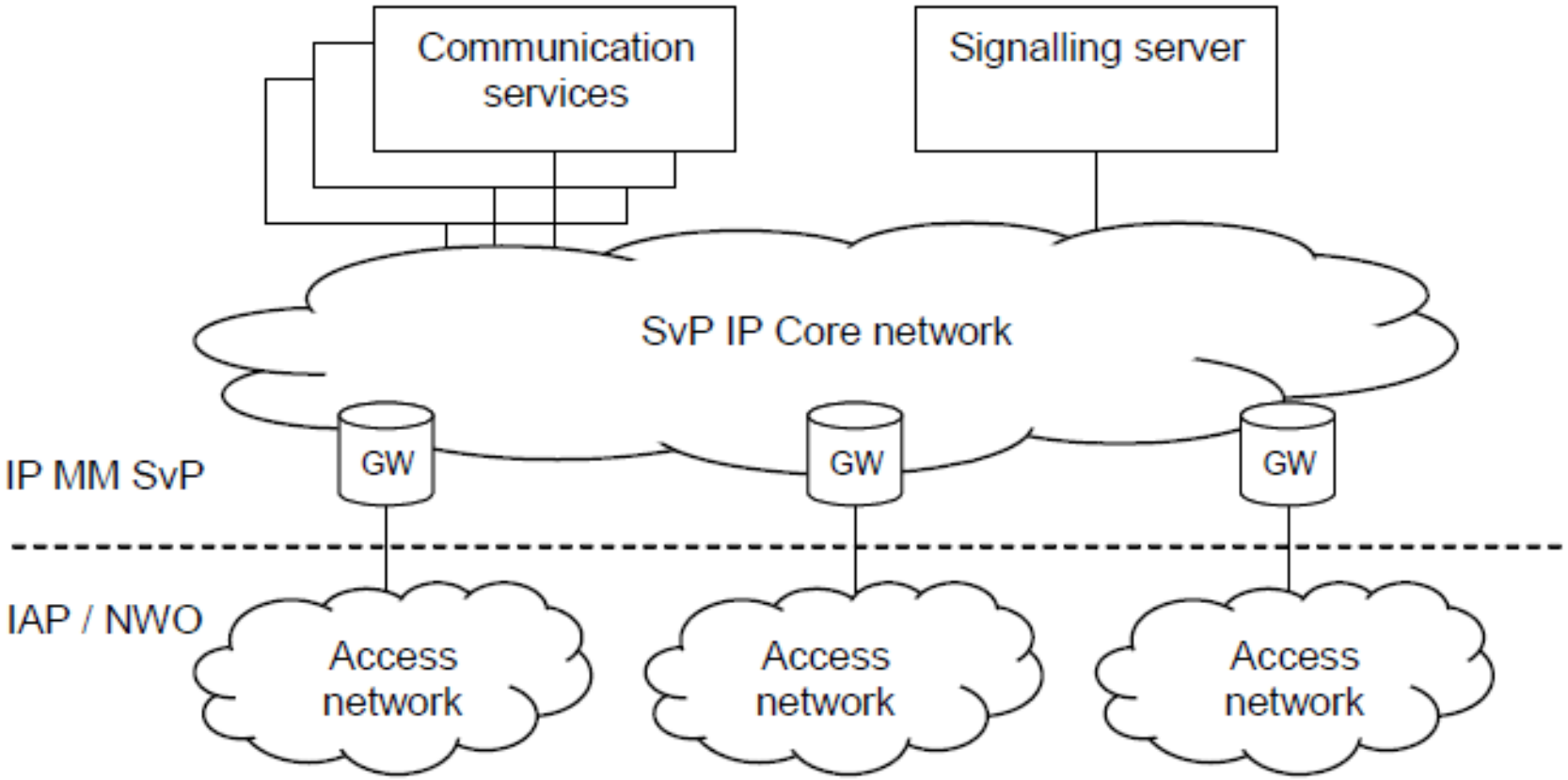
- Es werden verschiedene Netztopologien betrachtet
  - Beispiel xDSL (nächste Seite)


IP-enabled device
Router / Bridge
xDSL modem
PSTN local loop
DSLAM
Edge router
GWR
IAP network
AAA
Internet
Customer
NWO
IAP/ISP

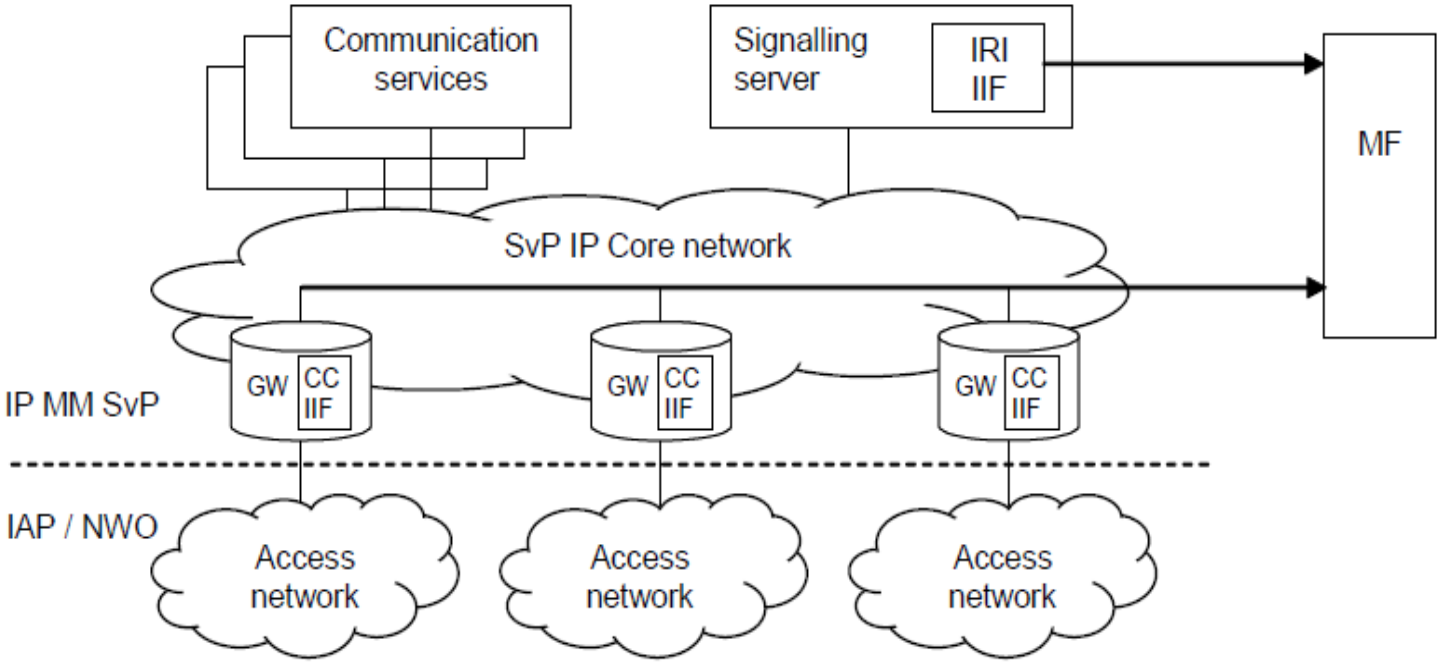
- Überwachung des IP-Verkehrs im Access Network
- Dem LEA wird eine exakte Kopie der Layer 2 Datagramme übergeben (Layer 2 Tunnel).


Internet Access Provider / Application Service Provider
Access Provider
CPE
PLTP
L2 Delivery Function
LEMF

- IP Multi Media (MM) Services werden auf gesonderten Plattformen erbracht.
- Diese Plattformen befinden sich in der Hoheit eines beliebigen IP MM Service Providers.
- Referenzmodell
  - Siehe nächste Seite:


Communication services
Signalling server
SvP IP Core network
GW
GW
GW
IP MM SvP
IAP / NWO
Access network
Access network
Access network

- ETSI unterscheidet in:
  - Network Layer Interception
  - Service Layer Interception



Teil 6 – PSTN/ISDN Services

- Dieser TS bezieht sich auf die Überwachung von emulierten PSTN/ISDN Services.
- Teil 6 verweist auf die relevanten Festlegungen in ES 201 671 V3.1.1.

Vielen Dank!