Lawful Interception of VoIP

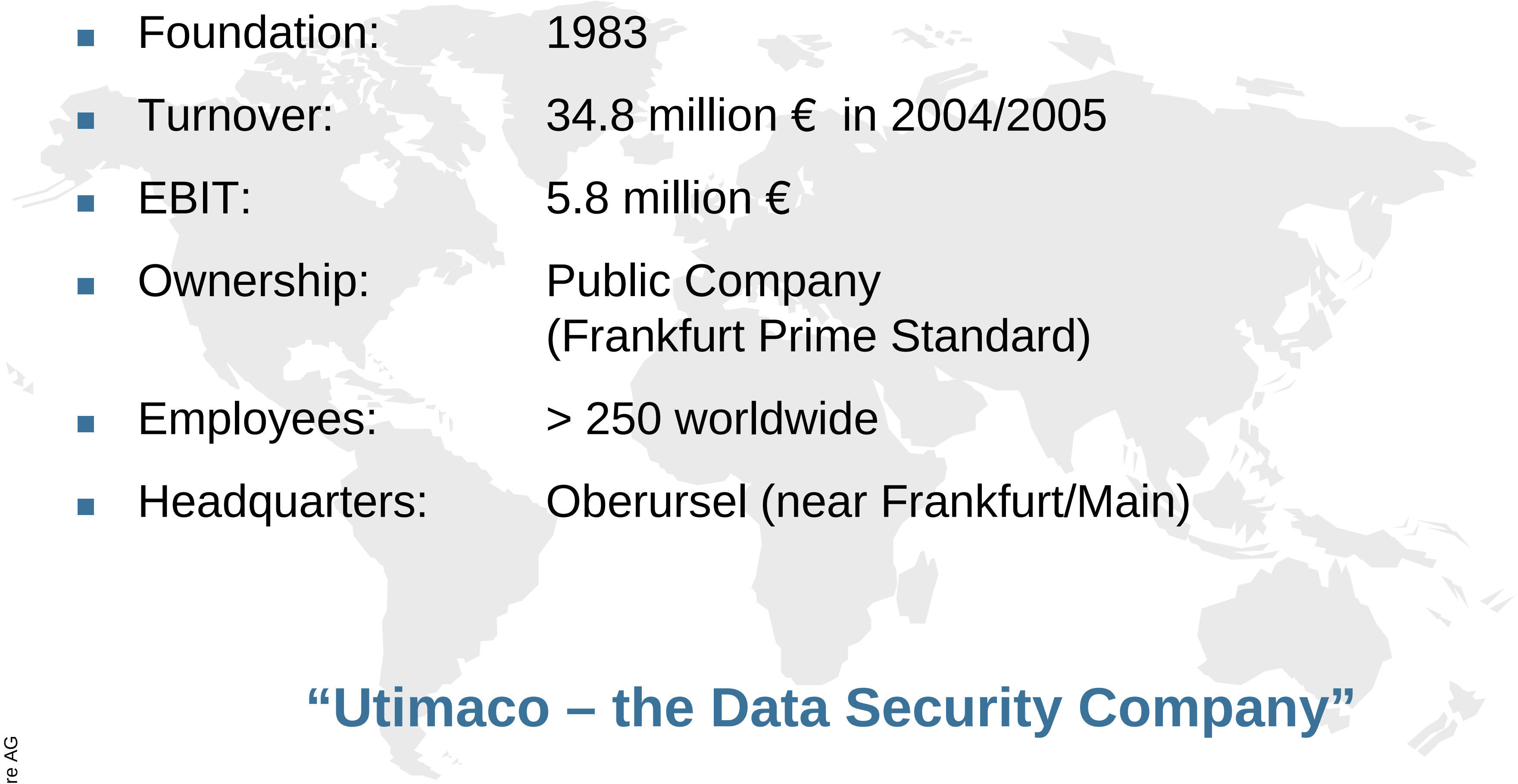
Rudolf Winschuh
Business Development
Transaction Security /
Telecommunications

utimaco®
safeware

Agenda

- Company Overview
- Lawful Interception
  - Definition and Terms
  - Legal Framework
  - Functional Overview
- LI for VoIP
  - LI solutions for VoIP
  - LI of peer-to-peer VoIP
  - Standards and Regulation
  - Open Issues
- LI for NGN/IMS

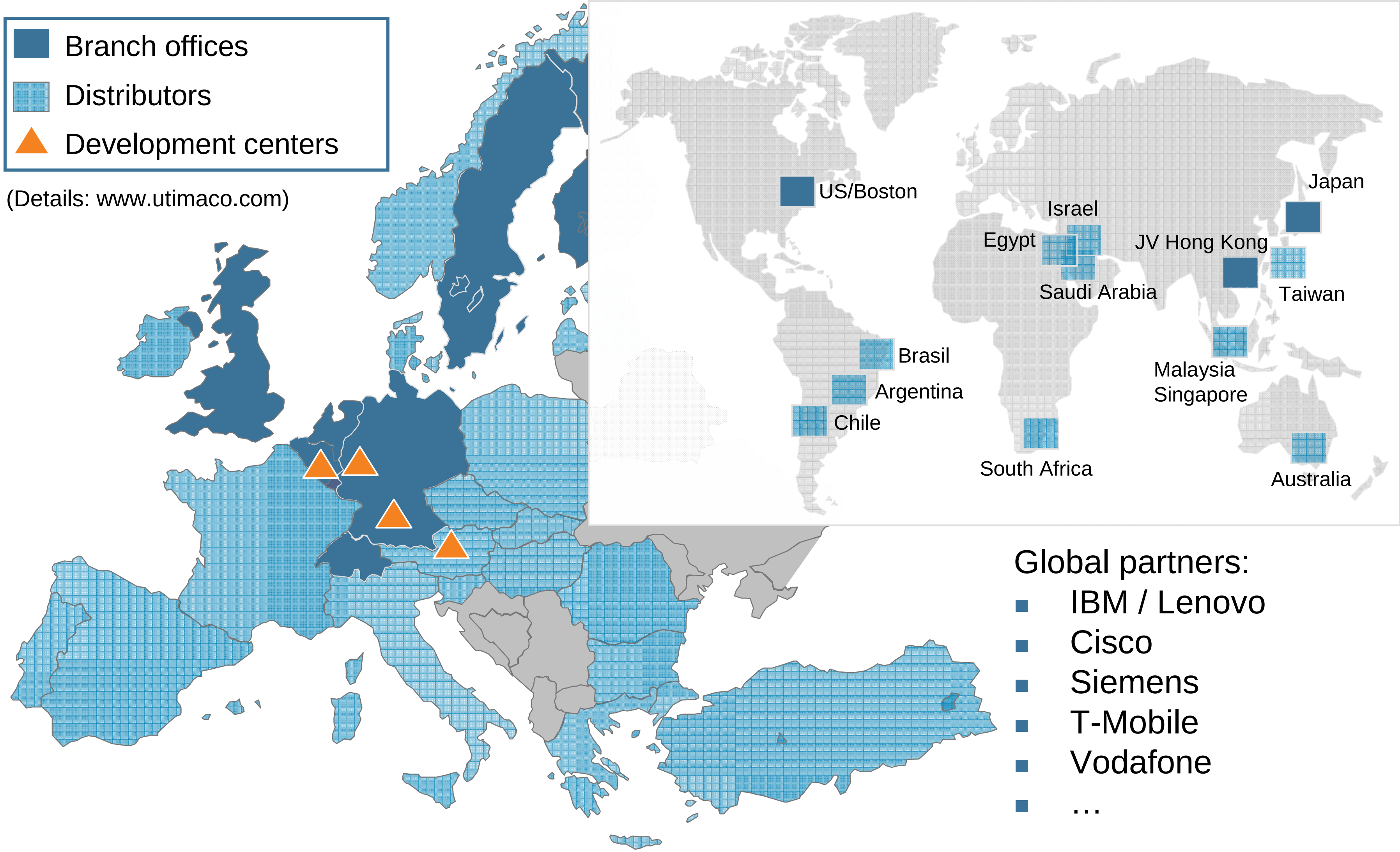
Company Profile



Foundation:	1983
Turnover:	34.8 million € in 2004/2005
EBIT:	5.8 million €
Ownership:	Public Company (Frankfurt Prime Standard)
Employees:	> 250 worldwide
Headquarters:	Oberursel (near Frankfurt/Main)

“Utimaco – the Data Security Company”

Presence



(Details: www.utimaco.com)

Global partners:

- IBM / Lenovo
- Cisco
- Siemens
- T-Mobile
- Vodafone
- …

Portfolio

- **Utimaco Product Portfolio:**

Personal Device Security

Innovative, trustworthy SafeGuard® solutions protect your data against misuse – on the terminals in private as well as public organizations (SafeGuard® Easy, - PrivateDisc, - LANCrypt, - PrivateCrypto, - Advanced Sec., - PDA).

Transaction Security

Focusing on innovative eBusiness and eGovernment solutions on the basis of Utimaco technologies (e-mail security, PKI, PKI-enabled applications, Hardware Security Module, Lawful Interception Management System).

- Hard disk encryption
- Virtual disk
- File security
- Management of rights
- PDA protection

- Sign - Verify
- Encrypt - Decrypt
- PKI - Infrastructure
- Time-Stamping
- Hardware Security Modules
- LI-Management

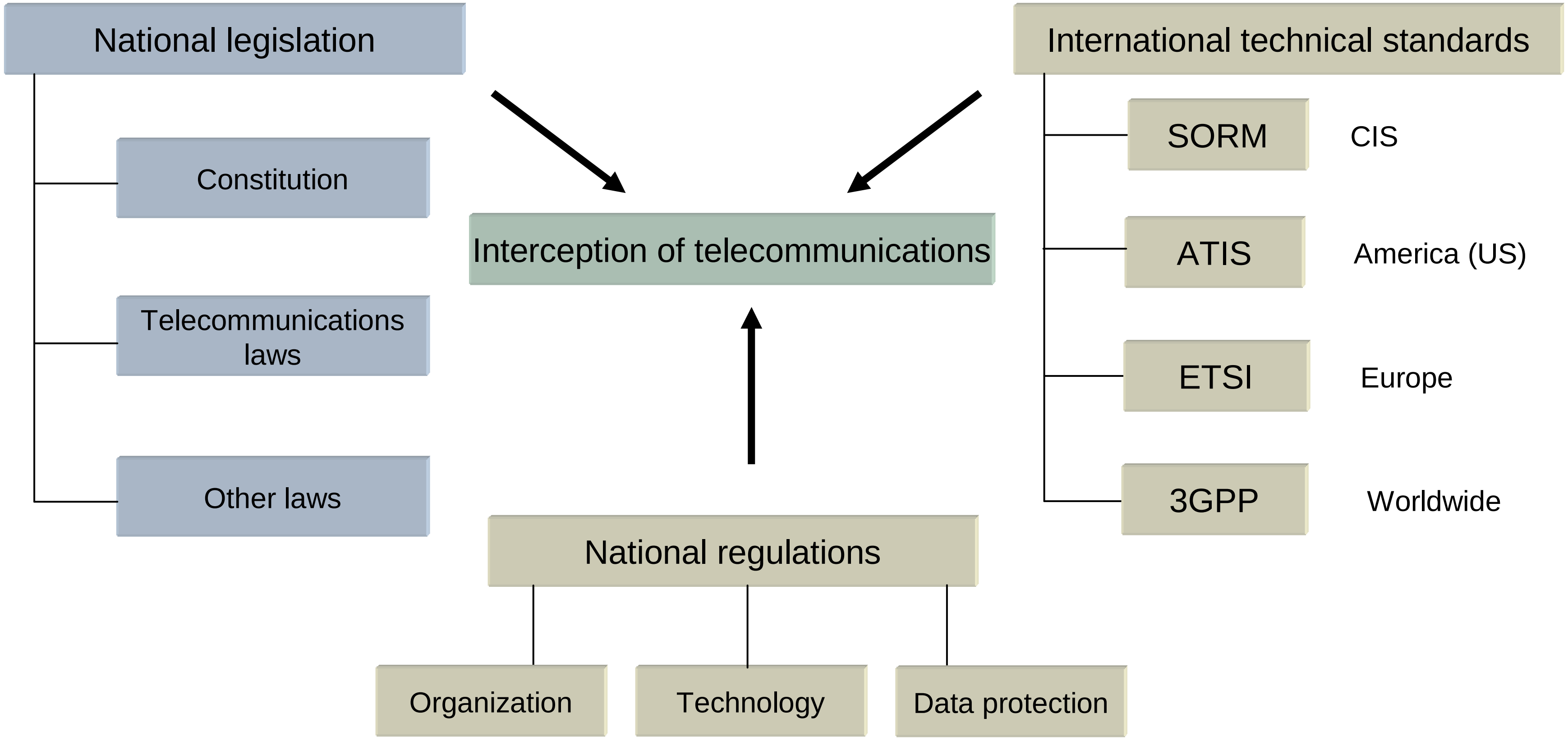
Lawful Interception – Definition and Terms

- Lawful Interception (LI)
  - Interception of telecommunications for purposes of law enforcement based on laws and other regulations
- Requirements for telecommunication service providers
- Law Enforcement Agency (LEA)
- Interception Related Information (IRI)
  - Information about intercepted communications (e.g. identifiers of participants, times, location information)
- Call Content (CC)
  - Content of intercepted data (e.g. speech, e-mail, data)
- Handover Interfaces (HI)

Legal Framework

LI is based on national laws and regulations

Implementation is often based on standards

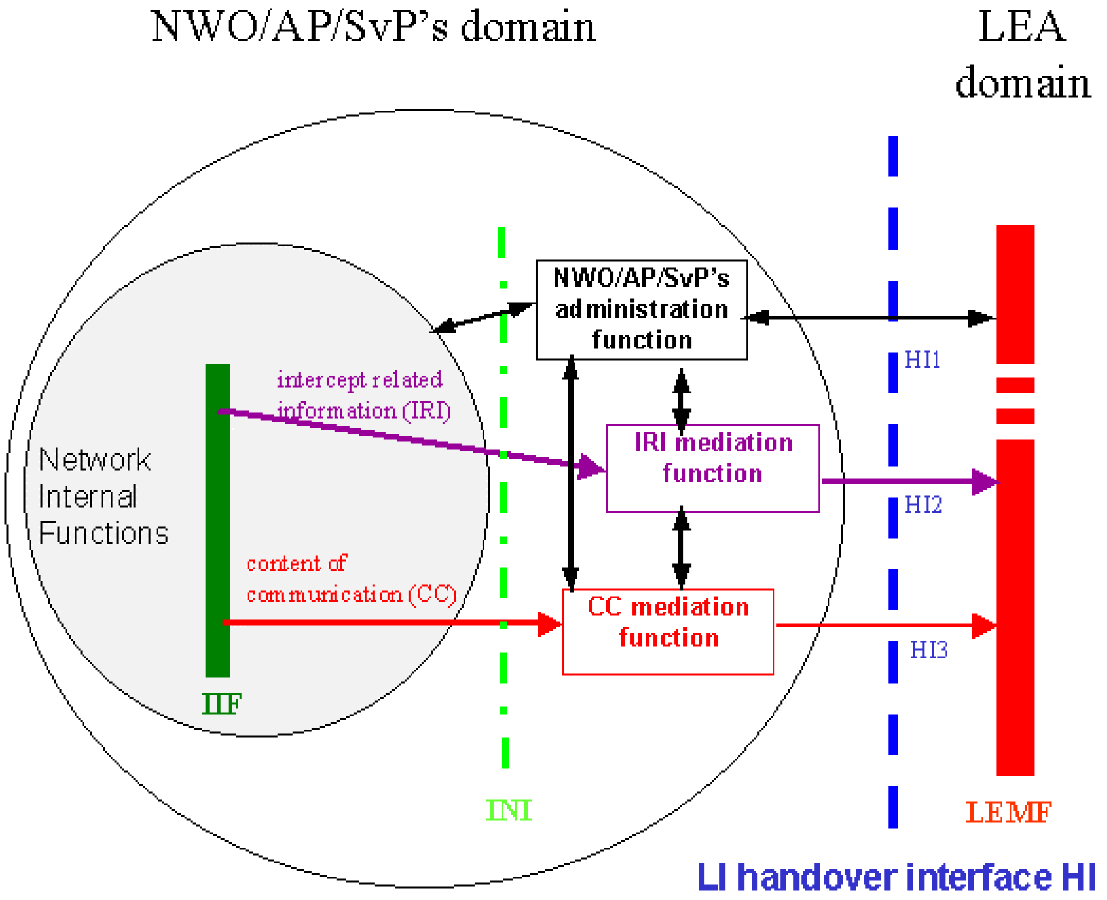


© Utimaco Safeware AG

Generic Requirements

- All communication of a target and service must be intercepted
- Integrity and confidentiality of Information must be ensured
- Only authorized personnel must be able to use the LI equipment
- All information must only be accessible to authorized personnel
  - ➔ Every use of LI equipment must be logged
- Intercepted subject must never be able to detect the interception
  - ➔ Active interception measures must never influence the telecommunication service
- Provider only required to provide accessible data
  - ➔ Network-intrinsic encryption must be removed

Functional Overview


NWO/AP/SvP's domain
LEA domain
Network Internal Functions
intercept related information (IRI)
content of communication (CC)
IIF
INI
NWO/AP/SvP's administration function
IRI mediation function
CC mediation function
HI1
HI2
HI3
LEMF
LI handover interface HI

IIF: internal interception function

INI:internal network interface

HI1: administrative information

HI2: intercept related information

HI3: content of communication

Functions of LI Solutions

- Administration Function
  - GUI to administrate LI components and interception measures
- Mediation (Delivery) Function
  - Communication between administration system and access functions
  - Delivery Function (DF) transmits IRI and CC to LEA
- Access Function
  - Accesses data to be intercepted in telecommunication network
  - Active: Internal Interception Function (IIF) integrated in network node
  - Passive: Probe/Sniffer, filtering to be intercepted communications out of whole network traffic

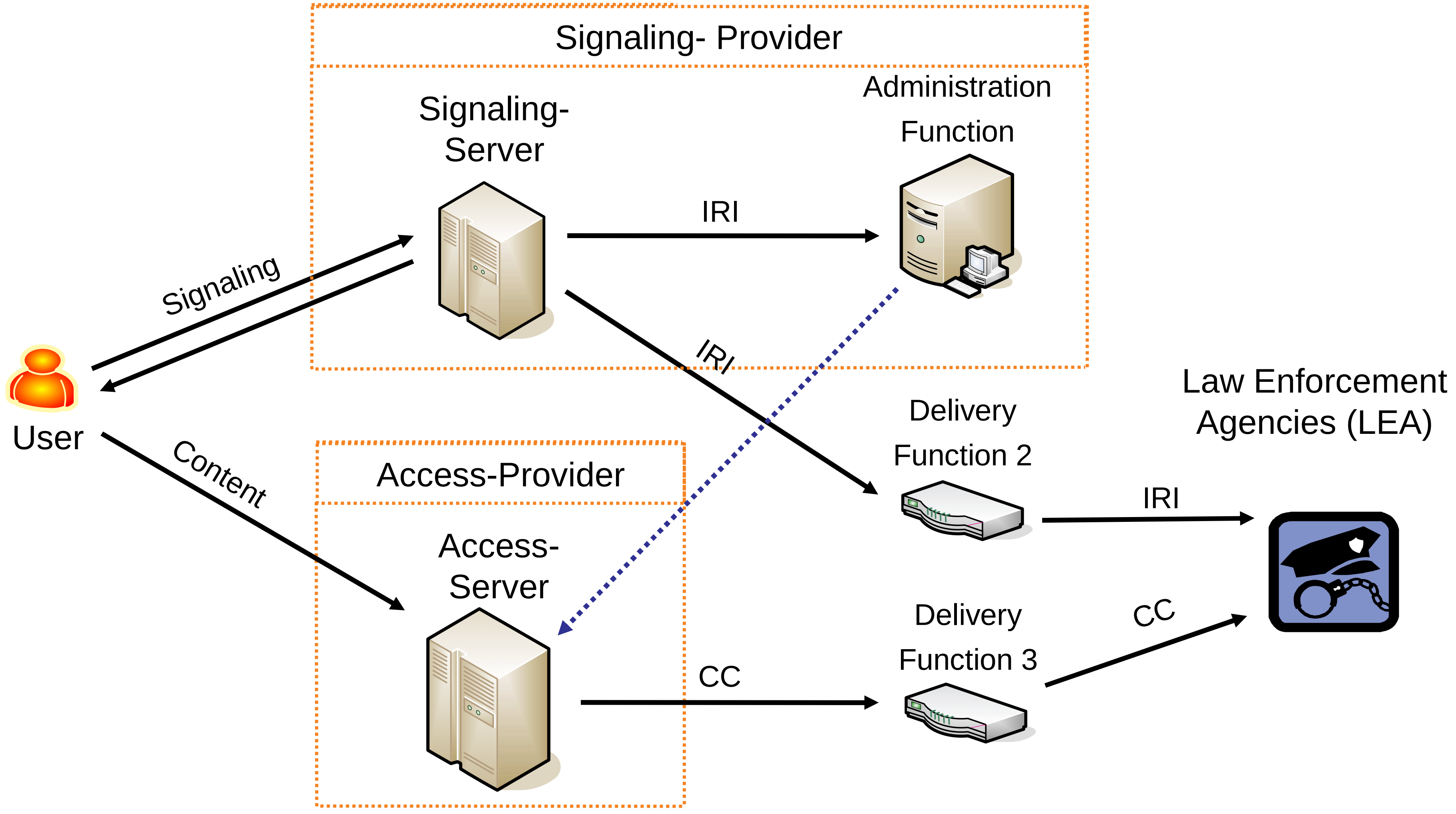
Functions of LI Solutions for VoIP

- Delivery Function
  - IP
  - PSTN
- Access Function
  - Active/IIF:
    - Signaling Server (e.g. SIP Server)
    - Access Router
    - Session Border Controller
    - Application Server
  - Passive:
    - Probes (SIP, H.323, RTP, …)

Valuation of LI Solutions for VoIP

	Pros	**Cons**
Active	+ no additional hardware	- security
Signaling Server	+ scales good + minimal effort for provider	- IIF integrated in server - performance
Access Router	+ access to all media + sometimes only alternative	- correlation of IRI and CC difficult - LI functions at multiple points
Session Border Controller	+ reuse of SBCs + easy correlation of IRI and CC	- calls to PSTN not covered - additional hardware
Application Server	+ centralized solution + easy correlation of IRI and CC	- rerouting could be necessary - application dependent
Passive	+ very secure	- additional hardware
Probes	+ indepent of vendor (in theory)	- scaling can become an issue - possibility of packet losses

LI of peer-to-peer VoIP



LI-Standards for VoIP

- ATIS T1.678
  - US
- ETSI WI 00024
  - Europe
  - Canada, Australia, Asia?
- 3GPP 33 108
  - 3rd generation mobile network operators
- CableLabs PacketCable
  - (Broadband) Cable operators
- ETSI TS 101 671
  - Originally for PSTN networks
  - Possible solution for PSTN and VoIP operators

Status of Regulation

- US
  - Based on CALEA
  - Second order of FCC from 12 May 2006
  - Interconnected VoIP services
  - Providers must be compliant by 14 May 2007
- Europe
  - Different from country to country
  - Germany: Interim solution until ETSI standard is finalized
  - Netherlands: LI of VoIP already active

Open Issues

- IRI
  - Forwarding of signalling information e.g. SIP messages

  vs.

  - Mapping of SIP messages to defined structures
- CC
  - Some providers cannot access the content

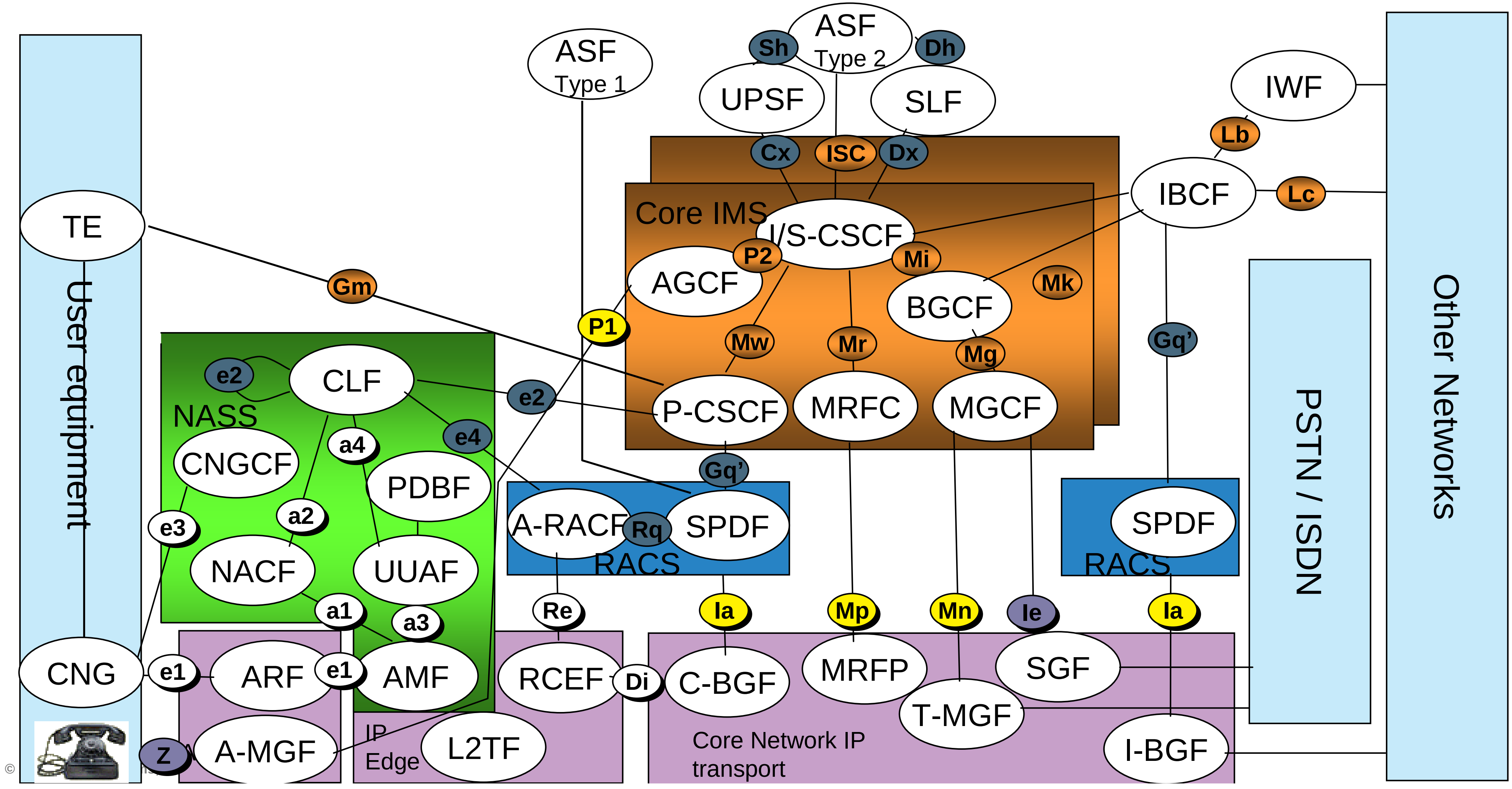
  ➔ Possible ban of business models
- Application/service specific data
- Encryption is a hard problem for LEAs

  ➔ Blocking of encrypted traffic?

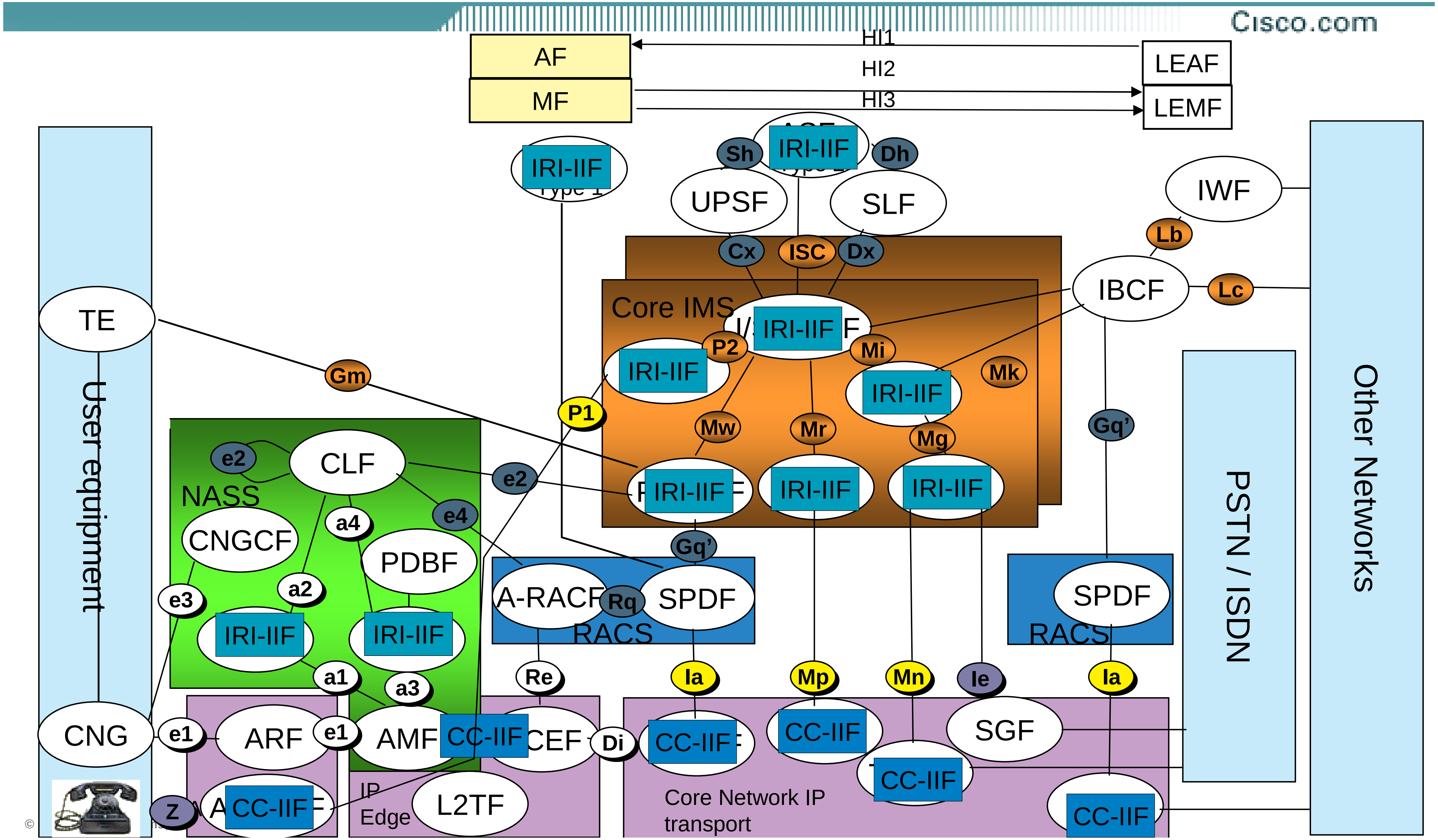
LI for NGN/IMS

- Next Generation Networks (NGNs) standardized by ETSI TISPAN
- Based on 3GPP approach
- Core component: IP Multimedia Subsytem (IMS)
- Goals:
  - Independent of underlying network architectures
  - Services in networks independent of access type (PSTN, mobile, DSL, …)
  - Terminal and user mobility
  - Easy deployment of new services

TISPAN R1NGN IMS architecture (ES 282 0001)



TISPAN R1NGN architecture with IMS LI reference points



Questions?

www.utimaco.com

Rudolf Winschuh
rudolf.winschuh@aachen.utimaco.de
Tel.: + 49 (0)241 1696 248