



Legal Interception in Telecommunications from a technical perspective

Possibilities and Restrictions of Legal Interception
Dr. Christian W. Schaumann LL.M., T-Mobile Austria GmbH



Agenda

- 1.0 **Functionality of a mobile network****
- 1.1 Legal Interception in Detail (mobile and fixed)
- 1.2 Call Content and Interception Related Information
- 1.3 Example of decoded S-Record Files

- 2.0 **Information about traffic data****
- 2.1 IMEI / IMSI / MSISDN

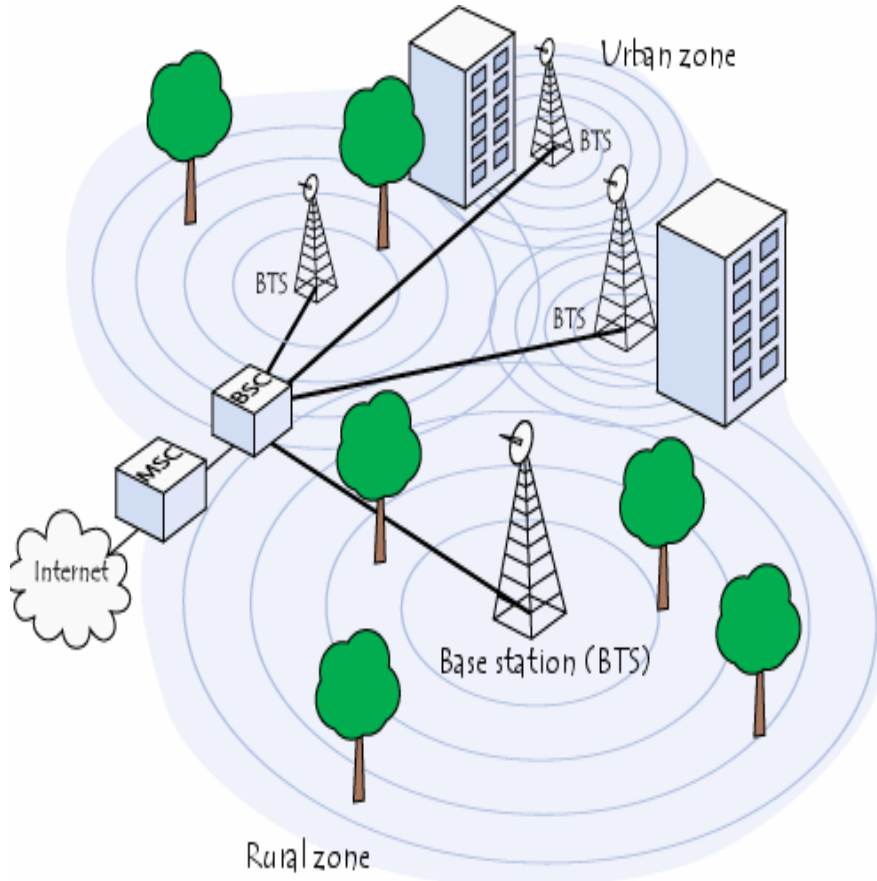
- 3.0 **Online-Localisation****
- 3.1 Radio Cells
- 3.2 Localisation / Results

- 4.0 **Restriction of Legal Interception****

- 5.0 **Developments and future aspects****



1.0 Functionality of a mobile network



BTS = Base Transceiver Station
(Mobile Site with varying number of Cells)



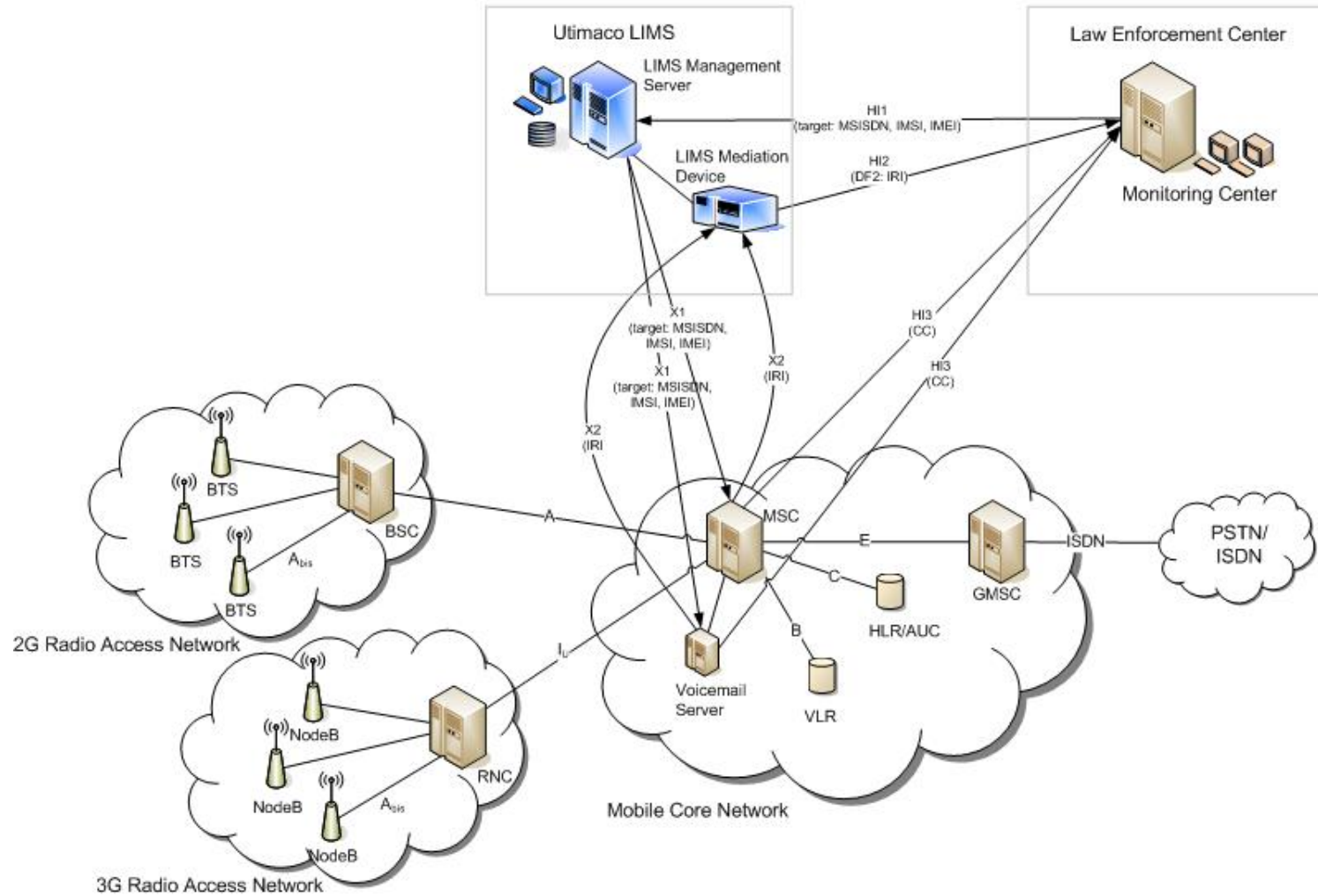
BSC = Base Station Controller



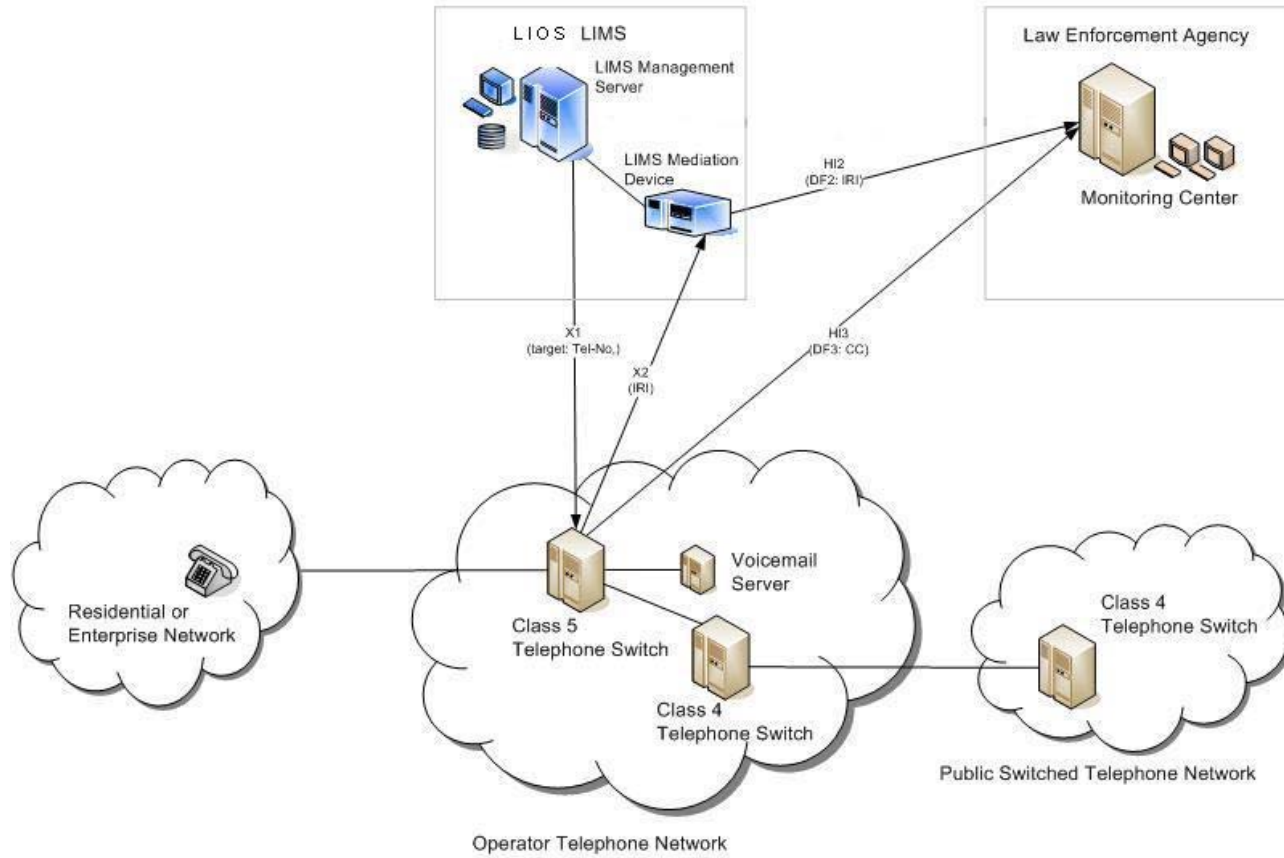
MSC = Mobile Switching Center



1.1 Legal Interception in mobile networks (e.g. one MSC)



1.1 Legal Interception in fixed networks



1.2 Call Content and Interception Related Information

Call Content (CC): Content Data (Voice)

§ 134 Z. 3 StPO „Überwachung von Nachrichten“

- are forwarded via HI3-Interfaces to the Law Enforcement Center of the law enforcement agency

Interception Related Information (IRI/S-Records): call related data (CDR)

(called party number, calling party number, location information, etc.)

§ 134 Z. 2 StPO „Auskunft über Daten einer Nachrichtenübermittlung“

- concerning these data, the forwarded information depends on the respective request of the law enforcement agency
- are forwarded via HI2-Interfaces to the Law Enforcement Center of the law enforcement agency

Content Voice Data (CC) and call related data (IRI/S-Records) are forwarded separately via highly secured lines in standardized form (national selection of options out of ETSI ES 201 671 Version 2.1.1 according to the interception regulation) to the receiving interface of the Federal Ministry of Interior - there, the decoding takes place



1.3 Example of a decoded S-Record Files

```

IRI_Continue_record [ 3] ::= (size = 227)
  iriVersion [23] ::= version2 ( 2, 0x2 )
  lawfulInterceptionIdentifier [ 1] ::= '436764014xxx' (size = 12)
  communicationIdentifier [ 2] ::= (size = 22)
  communication_Identity_Number [ 0] ::= (size = 3)
  10 66 96 .f.
  network_Identifier [ 1] ::= (size = 15)
  operator_Identifier [ 0] ::= 'TMA' (size = 3)
  network_Element_Identifier [ 1] ::= (size = 8)
  x25_Format [ 2] ::= '100011' (size = 6)
  31 30 30 30 31 31 100011
  timeStamp [ 3] ::= (size = 21)
  localTime [ 0] ::= (size = 19)
  generalizedTime [ 0] ::= 20070927171811
  winterSummerIndication [ 1] ::= notProvided ( 0, 0x0 )
  intercepted_Call_Direct [ 4] ::= originating_Target ( 1, 0x1 )
  intercepted_Call_State [ 5] ::= setUpInProgress ( 2, 0x2 )
  ringingDuration [ 6] ::= 000037
  locationOfTheTarget [ 8] ::= (size = 29)
  gsmLocation [ 5] ::= (size = 27)
  geoCoordinates [ 1] ::= (size = 25)
  latitude [ 1] ::= 'N481113.00' (size = 10)
  longitude [ 2] ::= 'E0162415.00' (size = 11)
  partyInformation [ 9] ::= (size = 116)
  PartyInformation [16] ::= (size = 56)
  party_Identifier [ 0] ::= originating_Party ( 0, 0x0 )
  party_Identifier [ 1] ::= (size = 19)
  imei [ 1] ::= '357968003704xxx'
  msISDN [ 6] ::= '436764014xxx'
  Nature of address : (0x01) 'international number'
  Numbering plan : (0x01) 'ISDN/Telephony Numbering Plan (CCITT Rec E.164)'
  supplementary_Services_Information [ 3] ::= (size = 30)
  non_Standard_Supplement_Services [ 2] ::= (size = 3)
  simpleIndication [ 1] ::= answer_Indication ( 6, 0x6 )
  other_Services [ 3] ::= (size = 23)
  otherServices [16] ::= (size = 19)
  specificationVersion [ 0] ::= 2, 0x2
  gsm_Parameters [ 1] ::= (size = 14)
  teleServiceCode [ 2] ::= telephony (17, 0x0011)
  ss_Code [ 3] ::= (size = 9)
  11 12 29 2a 2b 41 42 51 f3 ..)*+ABQ.
  PartyInformation [16] ::= (size = 16)
  party_Identifier [ 0] ::= terminating_Party ( 1, 0x1 )
  party_Identifier [ 1] ::= (size = 11)
  calledPartyNumber [ 5] ::= (size = 9)
  mAP_Format [ 2] ::= '436763174xxx'
  Nature of address : (0x01) 'international number'
  Numbering plan : (0x01) 'ISDN/Telephony Numbering Plan (CCITT Rec E.164)'
  PartyInformation [16] ::= (size = 20)
  party_Identifier [ 0] ::= terminating_Party ( 1, 0x1 )
  party_Identifier [ 1] ::= (size = 15)
  calledPartyNumber [ 4] ::= (size = 13)
  mAP_Format [ 2] ::= '43c200b3306763174xxx'
  Nature of address : (0x01) 'international number'
  Numbering plan : (0x01) 'ISDN/Telephony Numbering Plan (CCITT Rec E.164)'
  PartyInformation [16] ::= (size = 16)
  party_Identifier [ 0] ::= terminating_Party ( 1, 0x1 )
  party_Identifier [ 1] ::= (size = 11)
  calledPartyNumber [ 5] ::= (size = 9)
  mAP_Format [ 2] ::= '676223174xxx'
  Nature of address : (0x02) 'national significant number'
  Numbering plan : (0x01) 'ISDN/Telephony Numbering Plan (CCITT Rec E.164)'
  nature_of_The_intercepted_call [12] ::= gsm_ISDN_PSTN_circuit_call ( 0, 0x0 )

```

Example of an IRI_Continue_Records

During a call, several different IRI-Records with partly differing contents are generated:

- IRI_Begin_Record
- IRI_Continue_Record
- IRI_End_Record)

* These data are decoded by the Federal Ministry of Interior and combined with the separately forwarded Voice call content data



2.0 Information about traffic data (historical CDRs)

Possibilities:

- Mobile originating/terminating wrt MSISDN
- Mobile originating/terminating wrt IMEI
- Date/Duration/used service
- Location information (MSISDN)
- Location information (IMEI)
- Analysis on used IMSI-number
- Analysis on used IMEI-Nummer
- Used MSISDN
- Cell analysis

Restrictions:

- Data older than 6 months
- Call attempts
- Movements in network without radio contact

Example (wrt MSISDN):

Rufnummer	Datum	Zeit	Dauer	Gesprächspartner	Anrufer bei RU	Rufart	Standort	Plz	Ort	Straße	IMSI	IMEI
436766113xxx	05.07.2008	11:10:42	145	4318886xxx		MTC	WI10_Laaer_Berg_Str_Sued	1100	Wien	Laaer Berg Straße 172/1	232033520639xxx	35612901195xxx



IMEI / IMSI / MSISDN

- An **IMSI** (*International Mobile Subscriber Identity*) is a number programmed on the SIM-card, is usually 15 digits long, but can be shorter. The first 3 digits are the Mobile Country Code (MCC), and is followed by the Mobile National Code (MNC), either 2 digits (European standard) or 3 digits (North American standard). The remaining digits are the mobile subscriber identification number (MSIN) within the network's customer base.

IMSI	MCC	MNC	MSIN
	232	03	XXXXXXXXXX
	Österreich	TMA	

- The **IMEI** (*International Mobile Equipment Identity*) is usually 14 to 15 digits long and includes information on the origin, model, and serial number of the device. It consists of the Type Approval Code (TAC), the Final Assembly Code (FAC), the Serial Number (SNR) and the Spare (SP).
- The **MSISDN** (*Mobile Subscriber ISDN Number*) is the dial number of a mobile network customer. It includes the Country Code (CC), the National Destination Code (NDC) and the Subscriber Number (SN).



3.0 Online - Localisation

Functionality/Purpose:

If a customer does not have active/passive radio network contact (e.g. via calls, SMS, etc) and has therefore not generated data in the network, the localisation can only analyse the latest network contact.

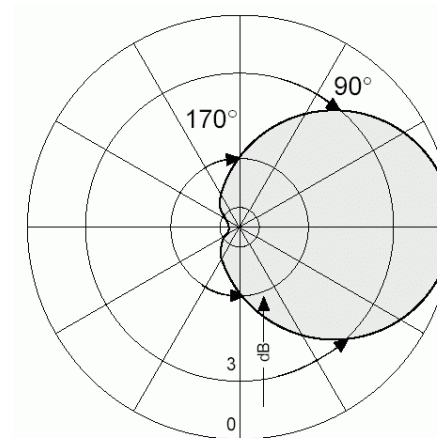
To deal with this issue, the following service is offered by the network operator (precondition: handset is activated):

- Creation of a network contact (without knowledge of the respective customer)
- Analysis of this network contact on basis of the used Cell ID
- Analysis of Cell ID with regard to location based center point information

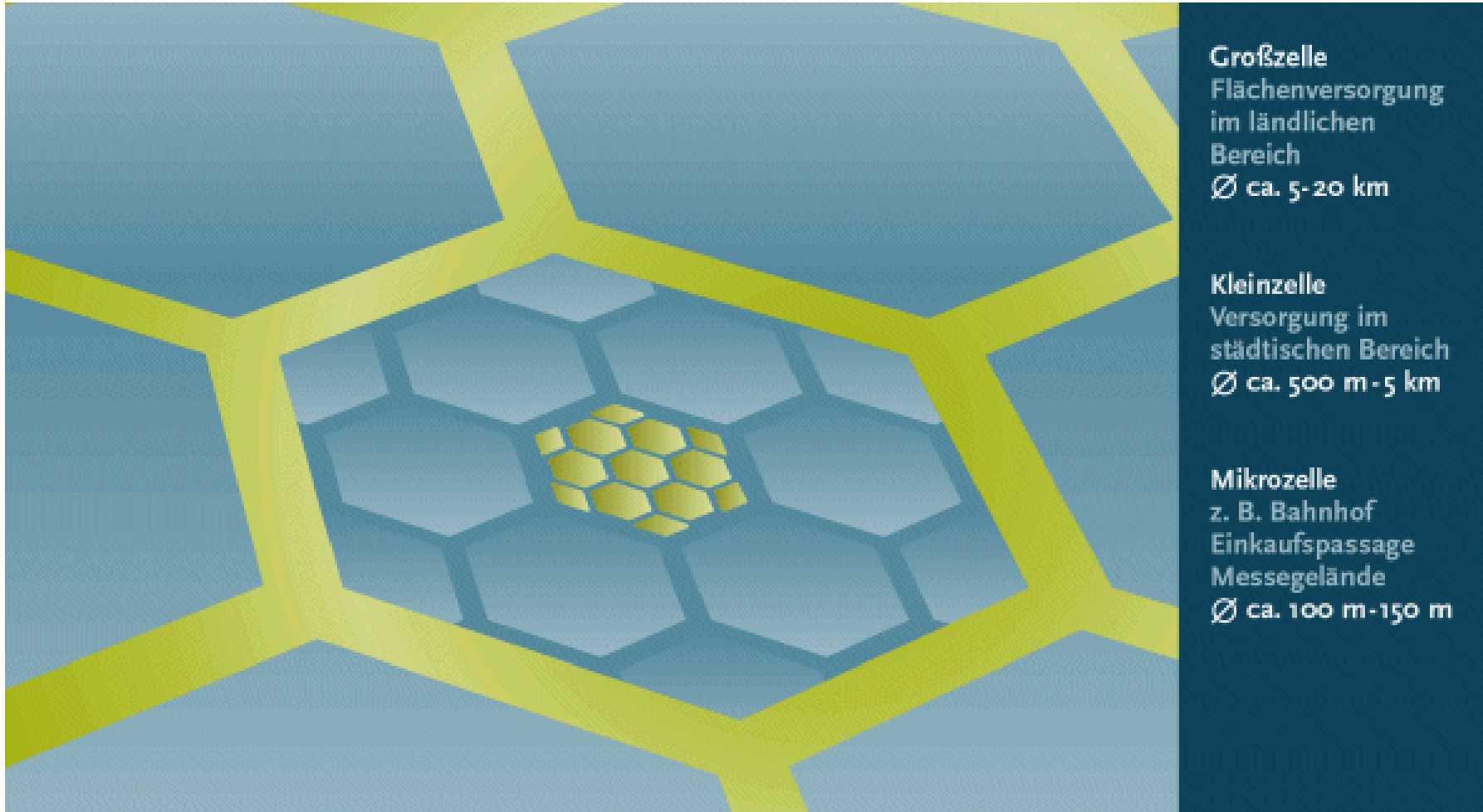


Cell_ID (CI)

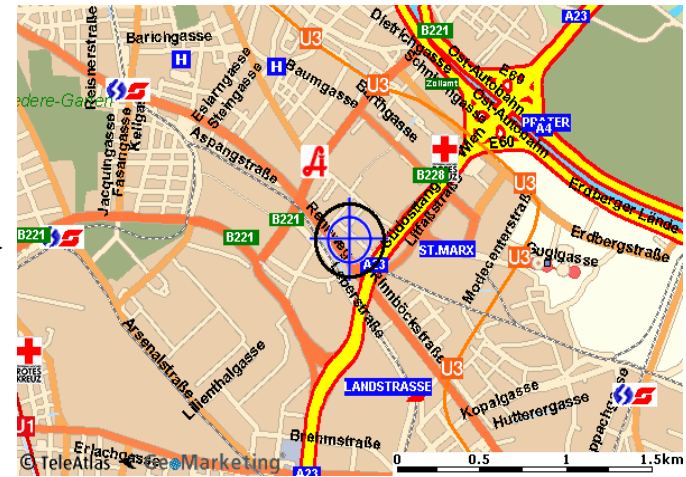
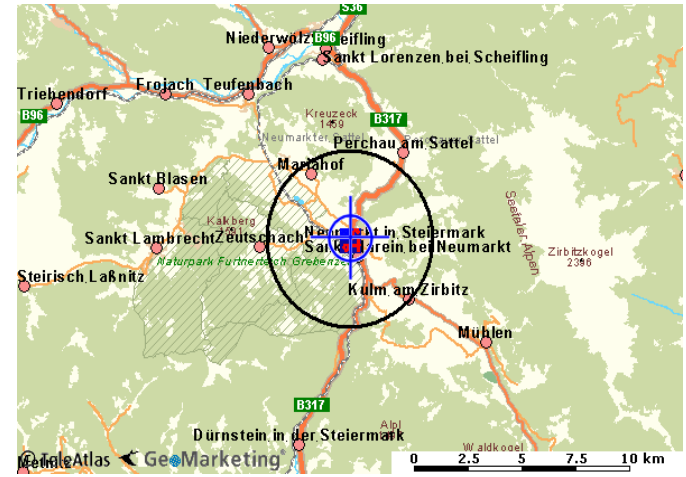
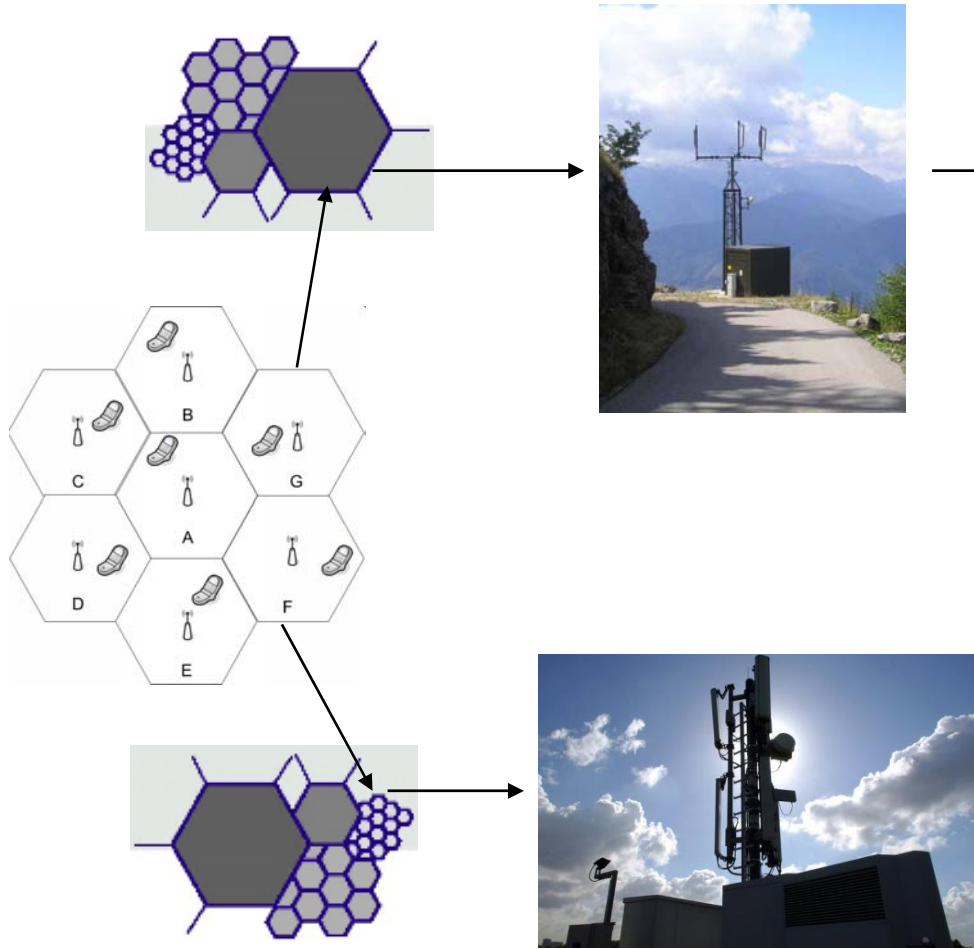
BTS
(Localisation)



3.1 Radio Cells



3.2 Localisation / Results



4.0 Restriction on Legal Interception

- Handsets which are switched off cannot be intercepted
- Handsets which are switched off cannot be activated by the network operator
- Movements in network (without radio contact) are not stored by the network operator
- Call attempts are not stored
- Data older than 6 months are deleted
- The link between temporarily used IP-adresses to a MSISDN is in the most cases due to technical reasons not possible
- The Interception of IP-based services is not possible (the interception standard ES 201 671 Version 2.1.1 does not include IP-based services)



5.0 Developments and future aspects

Next Generation Networks (NGN):

- The upcoming major changes in network core elements (all IP Core Networks) require a complete redesign of the configuration and the connectivity of lawful interception systems (call content interception and data providing)

Data Retention:

- It is expected that the implementation of the EC Data Retention Directive in Austria will have major impact on storing/data providing systems. The effects on the systems are regulated by the extent of data retention obligations which are still under discussion.



Thank you for your attention!

