# MIKEY-IBAKE and LI Requirements

# Introduction

SA WG3 is discussing MIKEY-IBAKE key management protocol for inclusion in TR 33.829 Extended IMS media plane security features

This contribution discusses LI approaches for MIKEY-IBAKE and compares these approaches against LI requirements for encrypted services as specified in TS 33.106.


All Rights Reserved © 2010 Alcatel-Lucent

# MIKEY-IBAKE Basic Operation

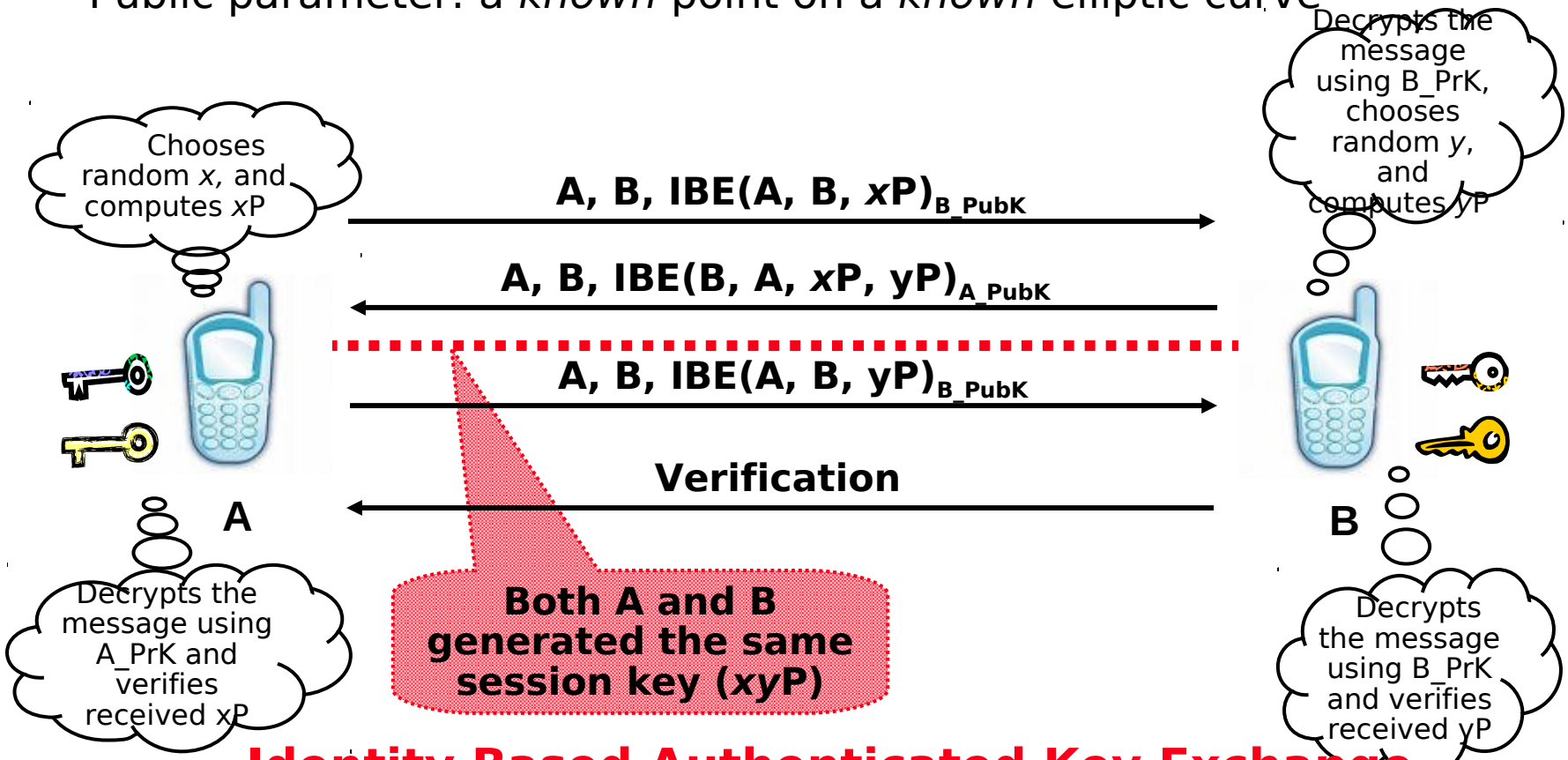
A's public key (A_PubK)

A's private key (A_PrK)

B's public key (B_PubK)

B's private key (B_PrK)

Public parameter: a *known* point on a *known* elliptic curve




**Identity Based Authenticated Key Exchange**



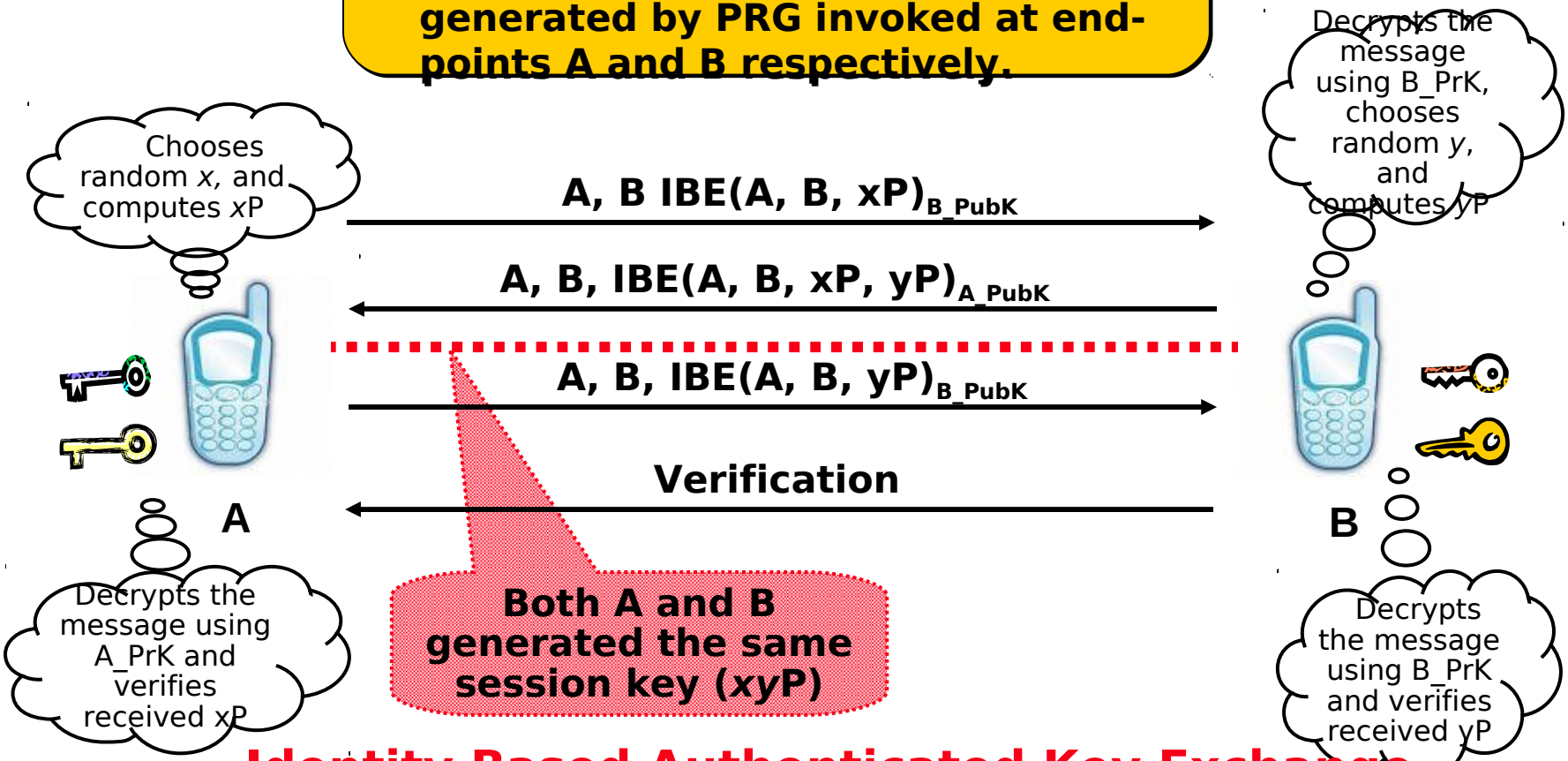
All Rights Reserved © 2010 Alcatel-Lucent

Alcatel·Lucent

# MIKEY-IBAKE Security

**Security is based on:**

1. **Secrecy of Private Keys A_PrK and B_PrK**
2. **Secrecy of pseudo-random $x$ and $y$ generated by PRG invoked at end-points A and B respectively.**




**Identity Based Authenticated Key Exchange**



All Rights Reserved © 2010 Alcatel-Lucent

# Discovery of MIKEY-IBAKE Session Keys

MIKEY-IBAKE session key

- SK = *xy*P
  - P is known point on a known elliptic curve
  - *x* and *y* are output of a Pseudo-Random Generator (PRG) invoked at A and B

Multiple ways to obtain *x* and/or *y*

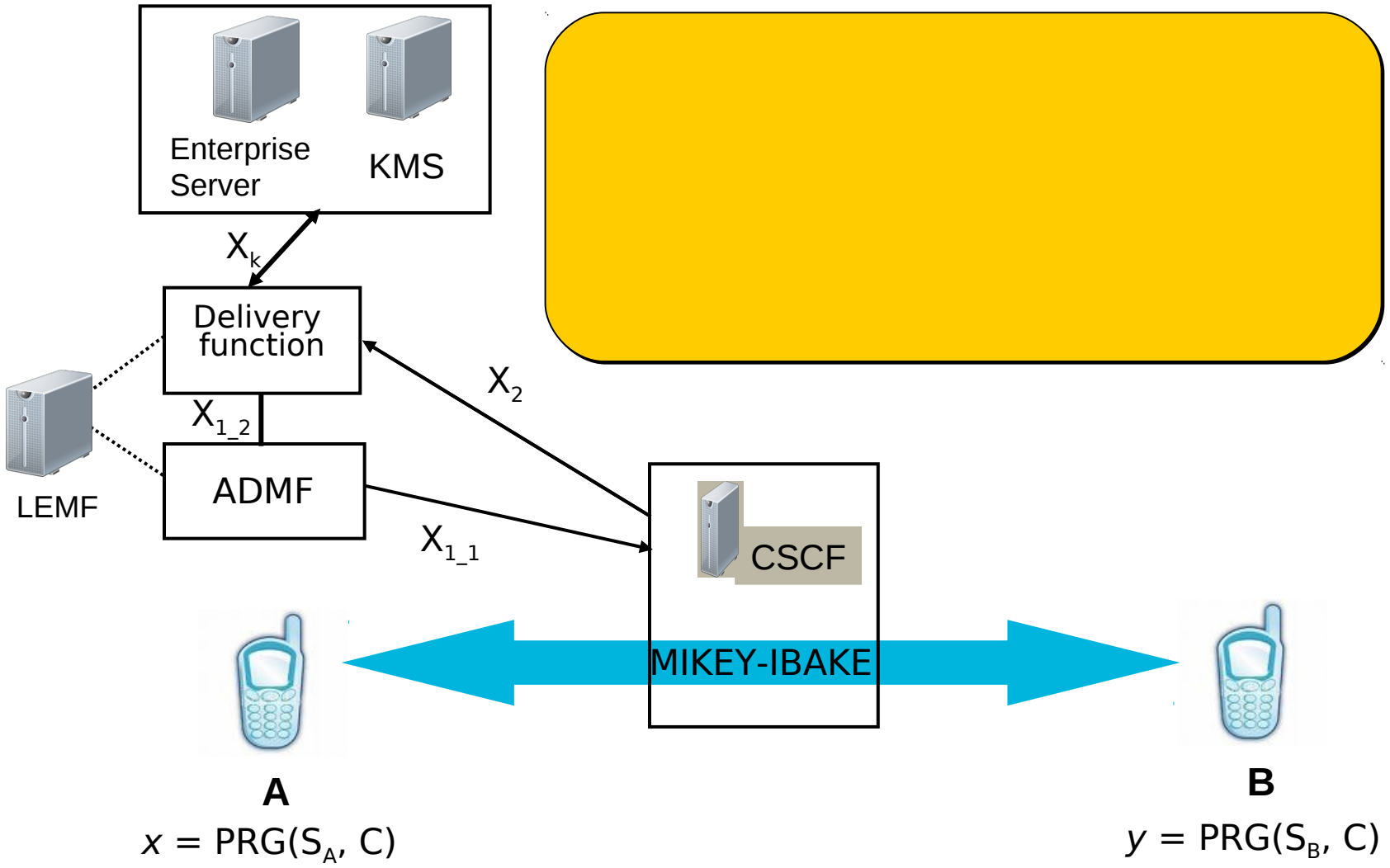
Re-generate *x* and/or *y*

1. Re-generate *x* and/or *y*
2. Exchange encrypted *x/y* during MIKEY-IBAKE exchange
3. A/B communicate *x/y* with KMS



All Rights Reserved © 2010 Alcatel-Lucent

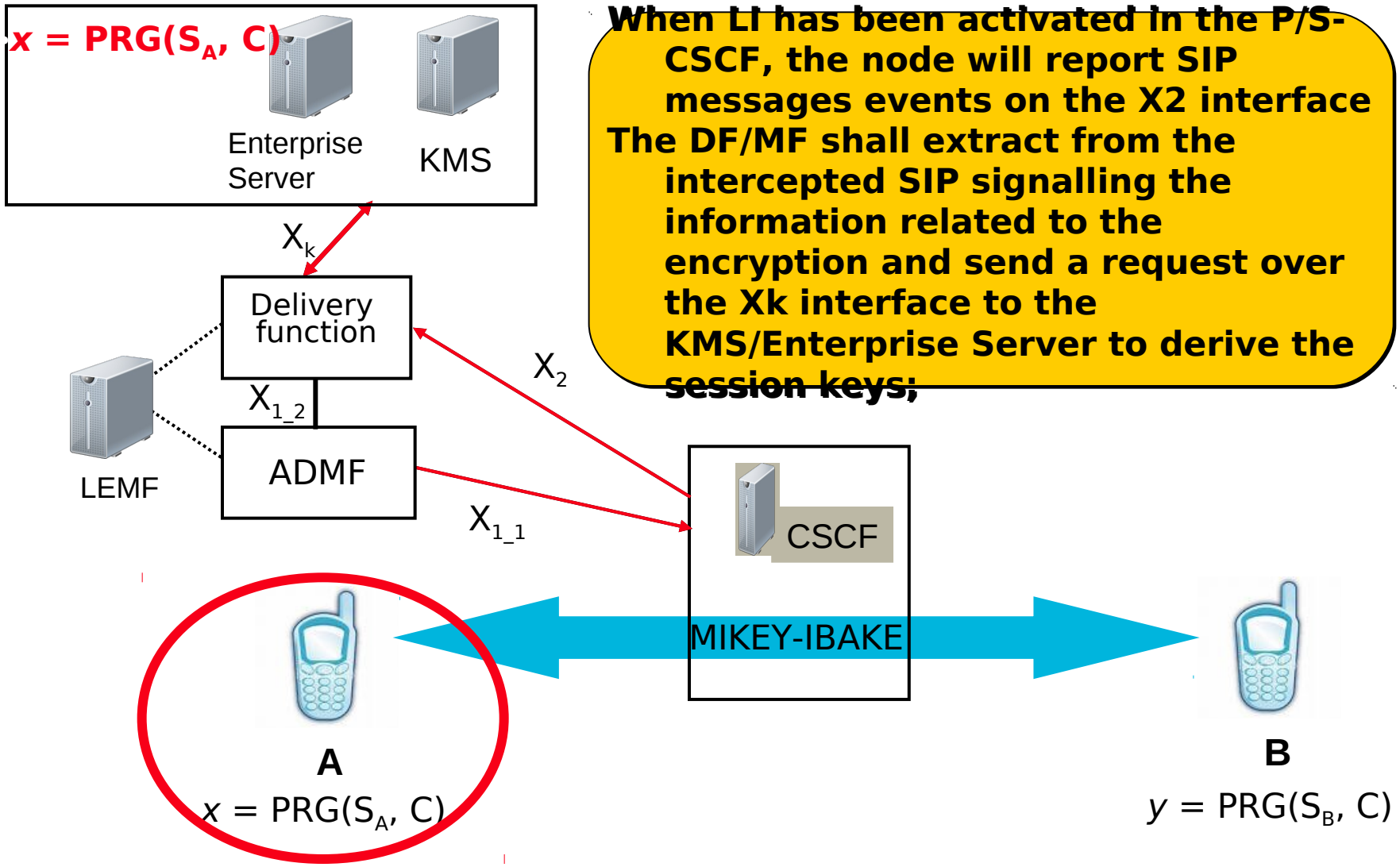
# Discovery of Session Key with Re-Generation of Secret






All Rights Reserved © 2010 Alcatel-Lucent

# Discovery of Session Key with Re-Generation of Secret




**When LI has been activated in the P/S-CSCF, the node will report SIP messages events on the X2 interface**

**The DF/MF shall extract from the intercepted SIP signalling the information related to the encryption and send a request over the Xk interface to the KMS/Enterprise Server to derive the session keys;**



All Rights Reserved © 2010 Alcatel-Lucent

# Discovery of Session Key Summary

- Session set-up the same for the case of intercepted and non-intercepted traffic
- Same session key used at both ends
  - No decryption/encryption of the traffic
- Non-detectable way to provide LI for MIKEY-IBAKE key management protocol
- Once LI is activated, just private keys and secret of the LI target need to be obtained
  - i.e. no need to obtain private keys and secret of the other party involved in communication


All Rights Reserved © 2010 Alcatel-Lucent

# LI Requirements for Encrypted Services (1/5)

1. When an encryption service is provided by the PLMN, lawful interception shall take place as for a non encrypted communications.

a. In addition encrypted communications shall be decrypted, or the decryption keys and any required associated information (e.g. roll over counters) shall be provided to the LEMF.

b. For the specific case where a key server based solution is used, it is a national option for the operator to make keys and any associated information (e.g. roll over counters) directly available to the LEMF for the decryption of communications

**MIKEY-IBAKE:** Lawful interception takes place as for a non encrypted communications. In addition keys and any associated information are available to the LEMF.


All Rights Reserved © 2010 Alcatel-Lucent

# LI Requirements for Encrypted Services (2/5)

2. Interception shall be performed in such a manner as to avoid detectability by the Target or others. In particular:

a. There shall be **no significant difference in latency** during call setup or during communications compared to a non intercepted communications.

**MIKEY-IBAKE:** Call setup is exactly the same for intercepted and non intercepted communications.

b. Interception of a Target shall not prevent the use of key exchange applications which provide a **user key confirmation mechanism**.

**MIKEY-IBAKE:** Interception does not prevent the use of key exchange applications which provide a user key confirmation mechanism.

c. Should **interception fail** during a call (or during call setup), the call shall be unaffected

**MIKEY-IBAKE:** Failure of interception does not affect the communication.


All Rights Reserved © 2010 Alcatel-Lucent

# LI Requirements for Encrypted Services (3/5)

3. Where the PLMN operator provides decryption of the communication, it is the operator's choice where in the network this decryption is performed. However, following decryption, all IRI and CC shall be provided to the LEMF using handover mechanisms as per a non encrypted communication.

**MIKEY-IBAKE:** When regenerating the secret, operator can choose where in the network to perform the decryption. Following decryption, all IRI and CC is provided to the LEMF using handover mechanisms as per a non encrypted communication.


All Rights Reserved © 2010 Alcatel-Lucent

# LI Requirements for Encrypted Services (4/5)

4. An encryption solution shall not prohibit **commencement of Interception and decryption** of an existing communication.

**MIKEY-IBAKE:** This requirement is supported by regenerating the secret. Alternative way is network-initiated re-keying feature of MIKEY-IBAKE.


All Rights Reserved © 2010 Alcatel-Lucent

# LI Requirements for Encrypted Services (5/5)

5. If key material and any associated information are available, it shall be possible to **retrospectively decrypt** encrypted communications.

**MIKEY-IBAKE:** If all encrypted communication content and associated key material are retained, encrypted communications can be decrypted.


All Rights Reserved © 2010 Alcatel-Lucent

www.alcatel-lucent.com