2 G Architecture– GSM, GPRS and Others

Lesson 10

Security in GSM Services

GSM NETWORKS VARIOUS SECURITY FEATURES

- A wireless radio based network system quite sensitive to unauthorized use of resources
- Design must protect subscriber privacy
- Secured network against misuse of resources by unregistered users

GSM NETWORKS VARIOUS SECURITY FEATURES

- Controlled access to the network by Mobile station
- Required to use a PIN before it can access the network through U_m interface

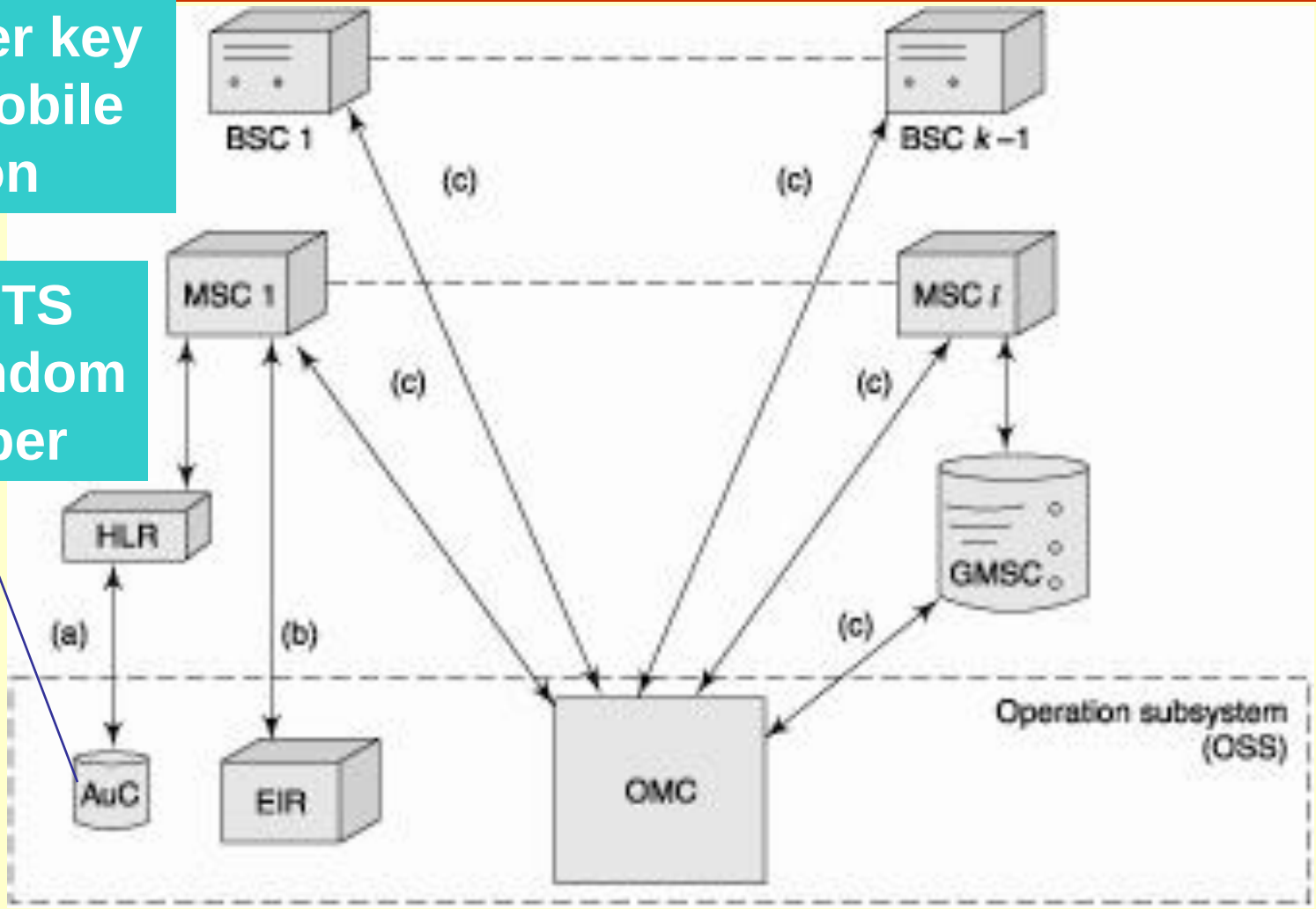
Authentication

- An AuC (authentication centre) for the operation and maintenance subsystem of the GSM network
- Authentication of the Mobile station
- The AuC first authenticates the subscriber Mobile station and only then does the MSC provide the switching service to another terminal TE, which is also authenticated in case it is a Mobile station)

AuC sending random number for BTS and BTS sending cipher key for encryption

Cipher key for Mobile station

For BTS a Random Number



Authentication algorithm

- Use a random number sent by the AuC during the connection set up
- An authentication key which is already saved in the SIM
- Authentication algorithm used differs for different mobile service providers

IMSI and TMSI of the Mobile station

- Its public identity
- TMSI is the identity granted on moving to a particular location
- When a Mobile station moves to a new location area, the VLR (visitor location register) assigns a TMSI which is stored in the SIM of the Mobile station

TMSI

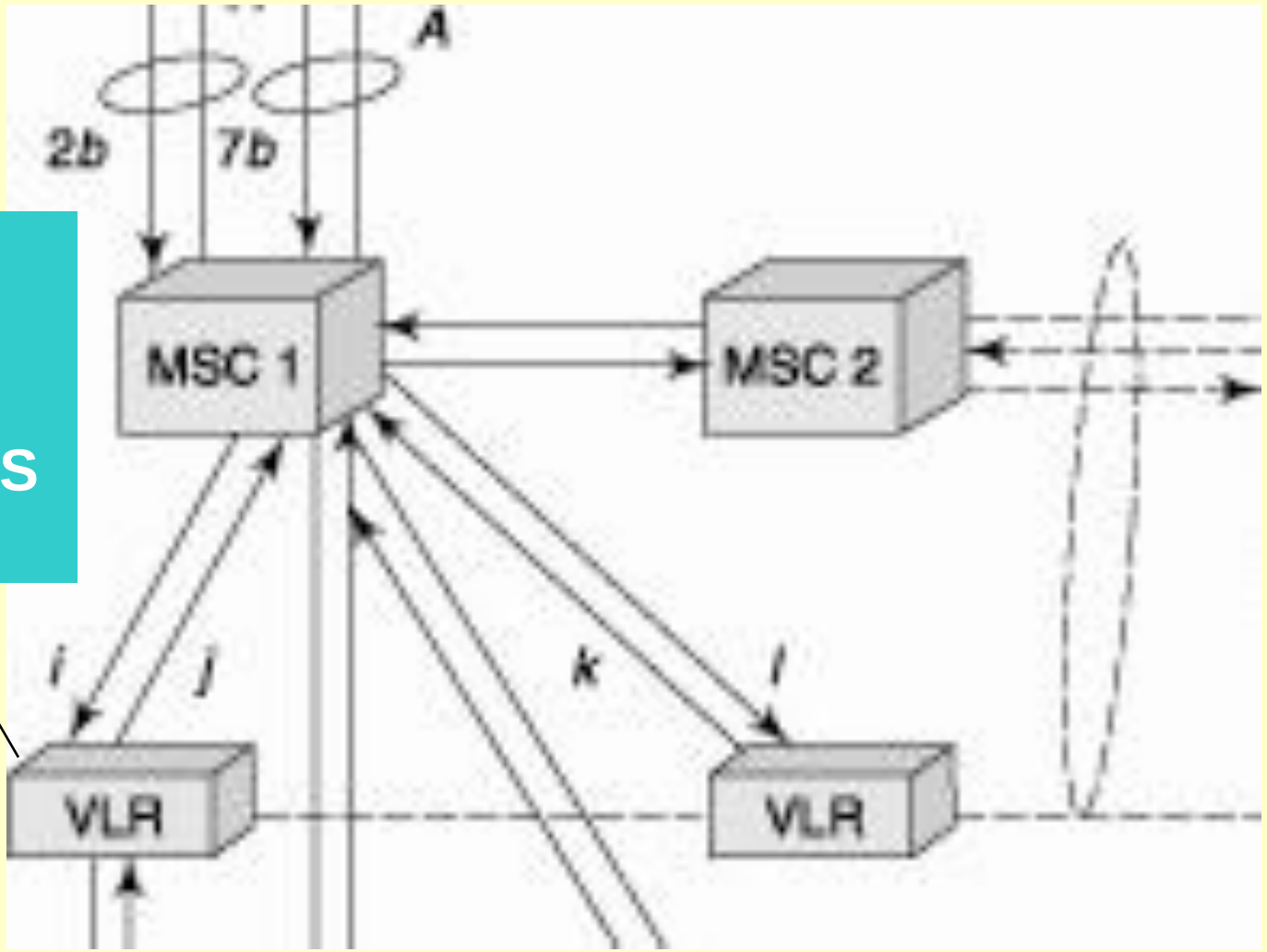
- The identification of the subscriber during communication done not using the IMSI but the TMSI
- Ensures anonymous call number identity transmission over the radio channels

Use of TMSI

- The VLR assigned TMSI generates that ID
- This protects the Mobile station against eavesdropping from external sources
- Caller line identification provision is a supplementary service

VLR for sending TMSI for BTS and Mobile station through MSC and BSC

For Mobile station and BTS a TMSI



Encryption

- The BTS and the Mobile station perform ciphering before call initiation or before connecting for receiving a call
- The Mobile station uses a cipher (encryption key) for encryption
- Only encrypted voice and data traffic and control channel data transmit to the BTS

The cipher

- A result of performing mathematical operations on (a) the cipher key saved in the SIM and (b) the cipher number received from the BTS when the call setup is initiated
- The BTS transmits the cipher number before a call is set up or transmitted

Secured wireless communication between the Mobile station and BTS

- The encryption algorithm identical for all mobile service providers
- This ensures compatibility of the BTS, BSC, and MSC units made by different manufacturers
- The BTS deciphers the voice and data channel data by running a deciphering algorithm before communicating over the wired PCM (pulse code modulation) lines

Challenge

- Random numbers used in authentication and ciphering processes
- Challenge to the mobile station to generate the results (responses) of the algorithms
- If these results are correct only then BTS and other units grant access to the challenged Mobile station

Summary

- Controlled access to the network by Mobile station
- PIN before Mobile station can access the network through U_m interface
- VLR generated TMSI
- Random number generation and then encryption algorithm for cipher key generation
- Challenge

End of Lesson 10

Security in GSM Services