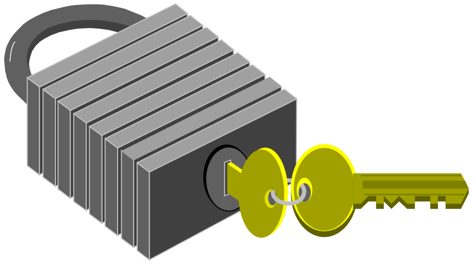
Security, Authentication and Access Control for Mobile Communications



Vijaya Chandran Ramasami
EECS 865

Overview

- Introduction.
- Requirements.
- Introduction to Cryptography.
- Common Techniques.
- GSM Security.
- 3GPP-UMTS Security.

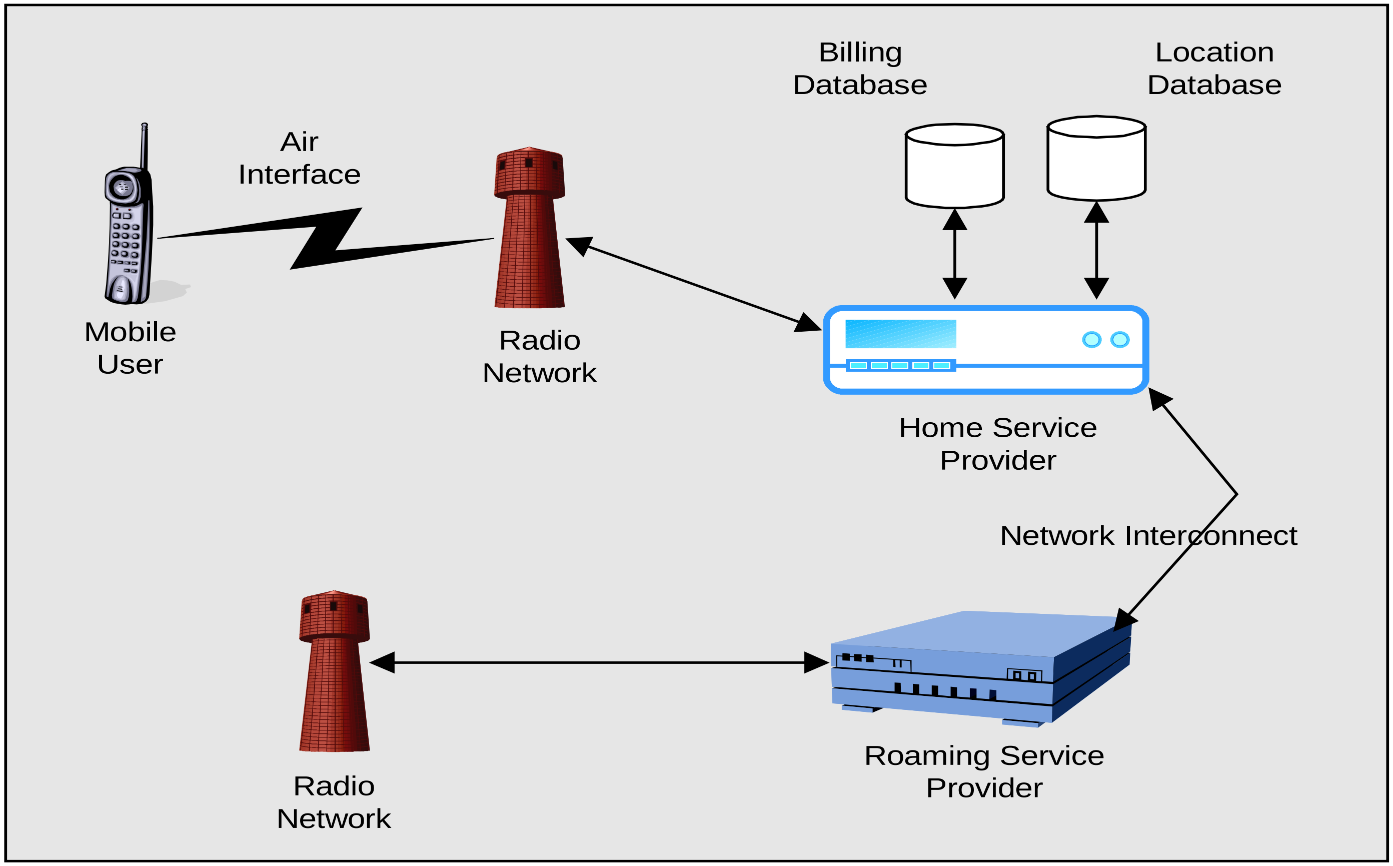
Introduction

- Security
  - Implies the protection of “Subscriber” Assets.
- Authentication And Access Control
  - Implies the protection of “Network” Assets.

Security - Wired Vs Wireless

- Wireless Medium is a ubiquitous shared one.
  - Eaves-dropping cannot be prevented.
  - Presence of communication does not uniquely identify its originator.
  - Eaves-dropping cannot even be detected !

General Architecture of a Mobile Communication System



Security Requirements

- Requirements for End User Privacy.
  - Privacy of Call-Setup Information.
  - Privacy of Speech.
  - Privacy of Data.
  - Privacy of Location.
  - Privacy of User-ID.
  - Privacy of Financial Transactions.

Requirements (Contd…)

- Support for Roaming.
- Data Integrity.
- Theft of Service or Equipment.
  - “Cloning” of Equipment.
  - User-ID’s and provisioning.
  - Equipment Identifiers.

Requirements (Contd...)

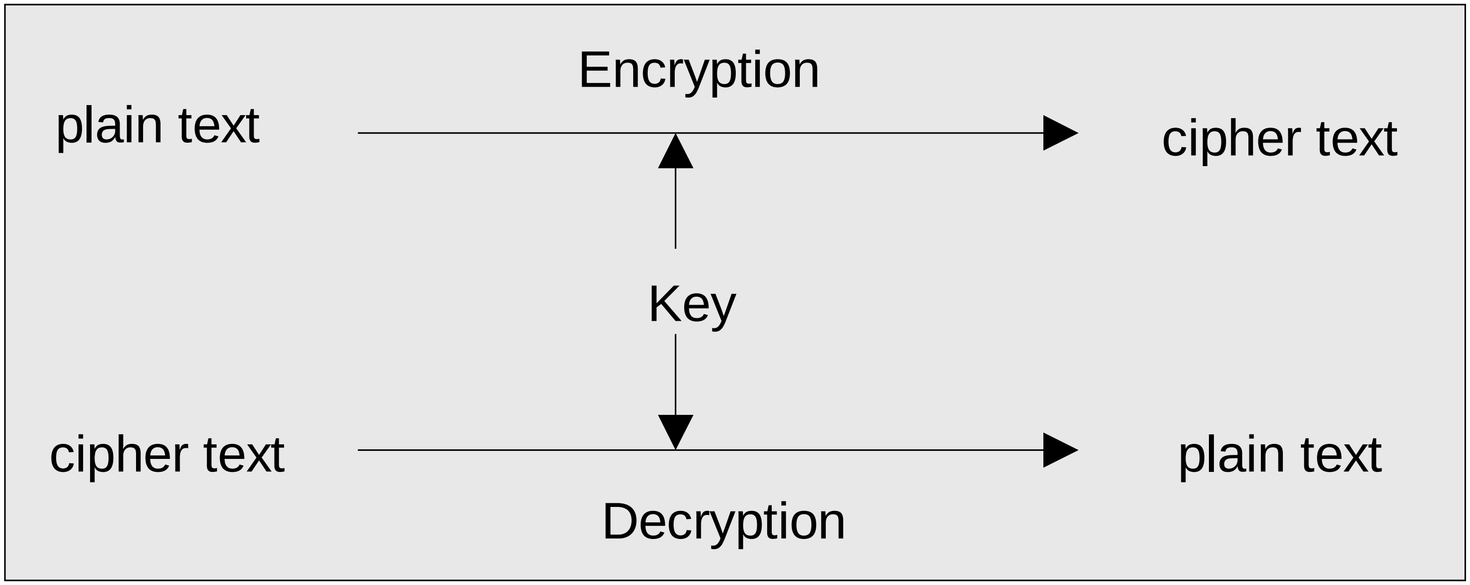
- Power/Bandwidth/Computational Usage.
  - Limited Computational Complexity.
  - Limited Outputs.
  - Limited number of transactions (for Authentication).
- System Lifetime.
- Export Control Requirements.
  - Export License Approval.
- Law Enforcement Requirements.

Cryptography

- A Cryptographic subsystem is required to satisfy the security requirements.
- Two major categories:
  - Secret Key Systems.
  - Public Key Systems.

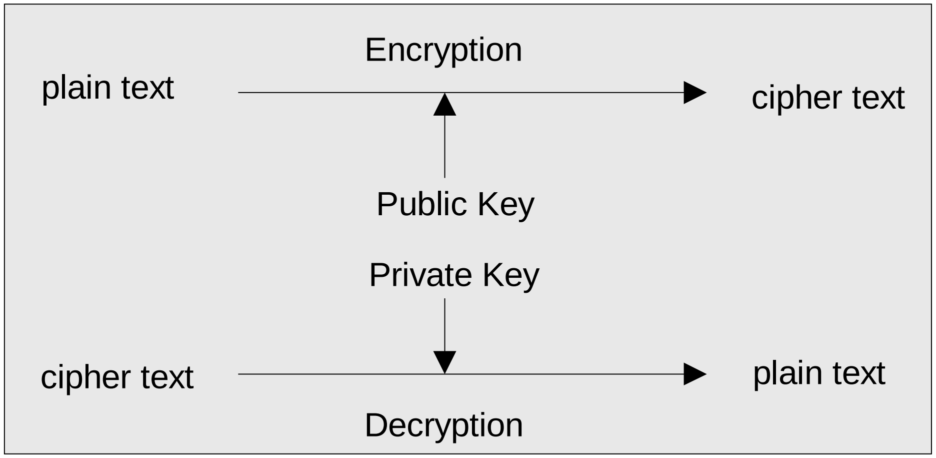
Secret Key Systems

- A Single (Shared) Secret Key between entities



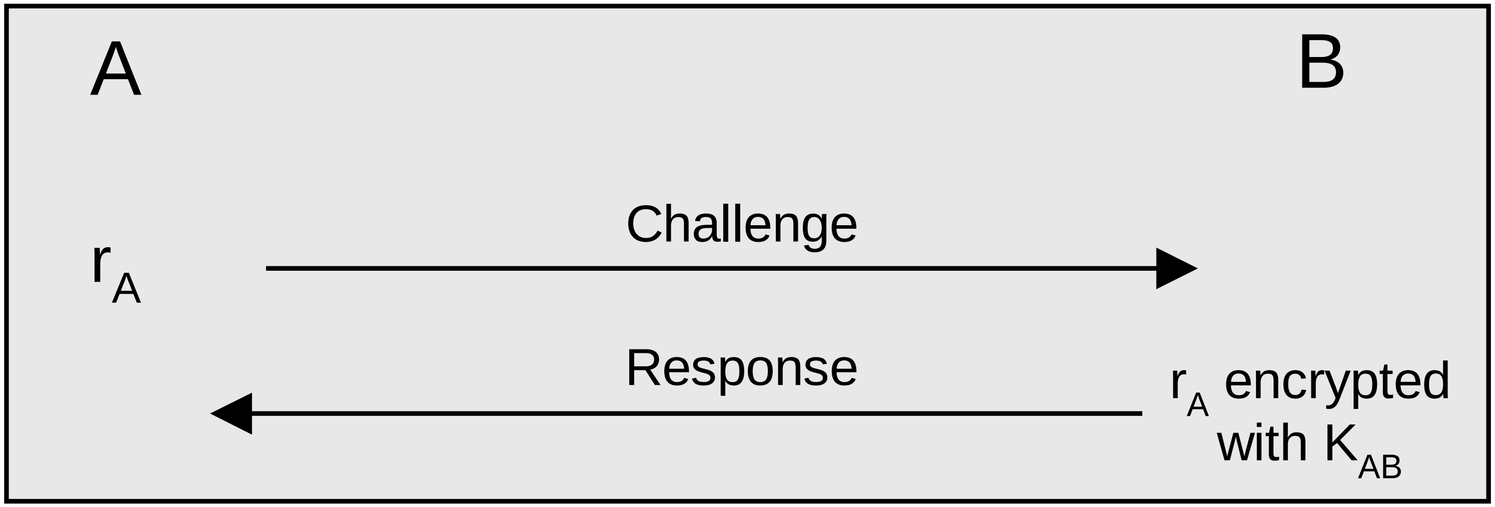
Public Key Systems

- Two Keys
  - Public Key -> known to everyone.
  - Private Key -> known only to the respective entity.

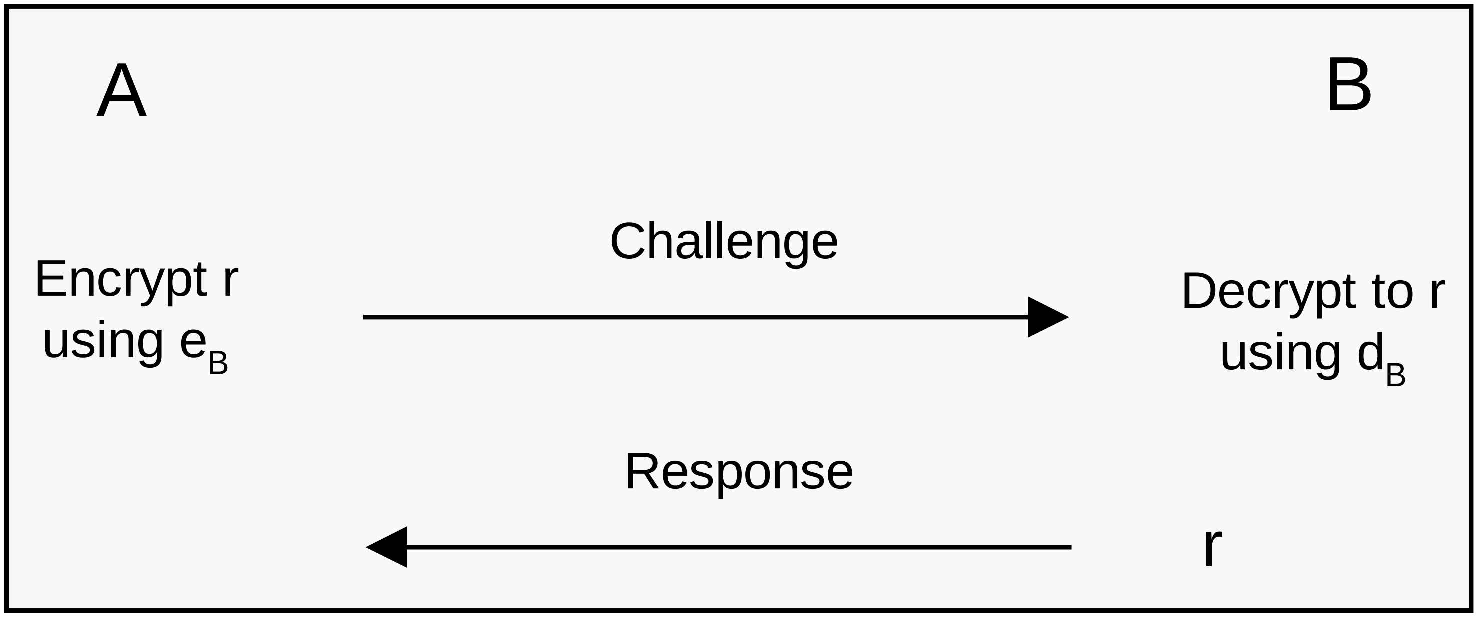


Authentication (Secret Key Systems)

- Challenge Response Mechanism.



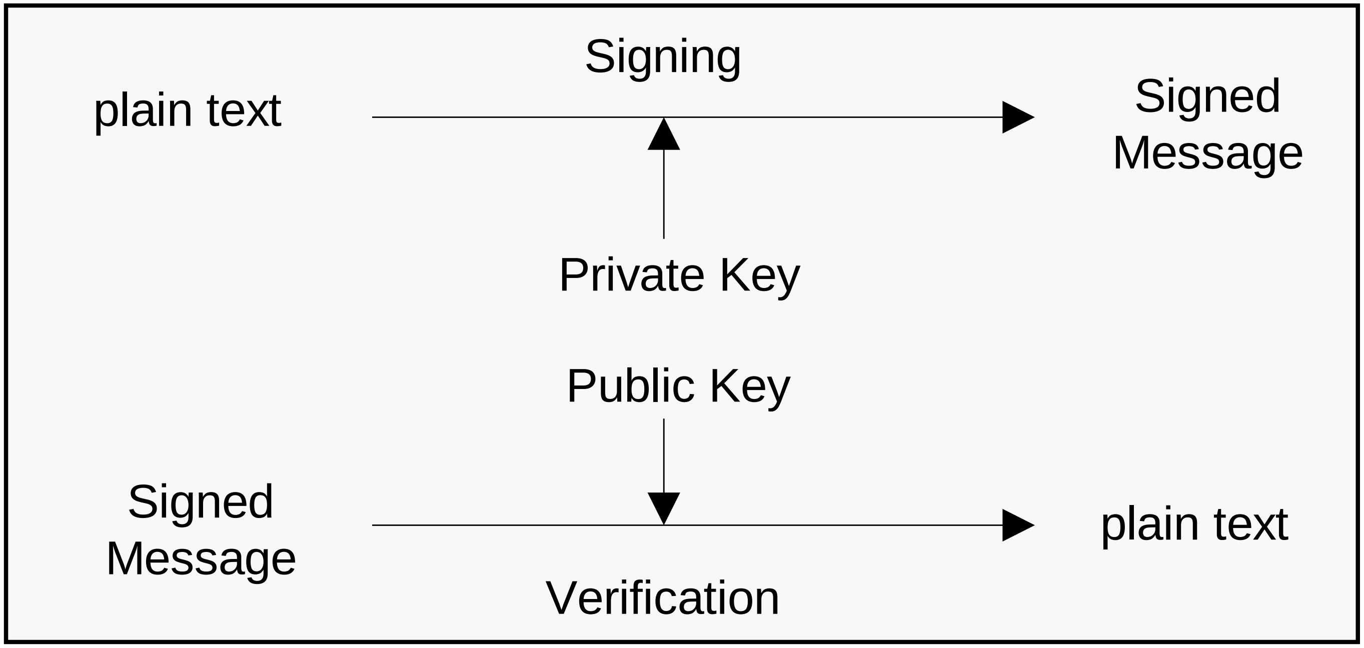
Authentication (Public Key Systems)



- No need to share secret Keys with others.

Digital Signatures

- Used for Verification Purposes.

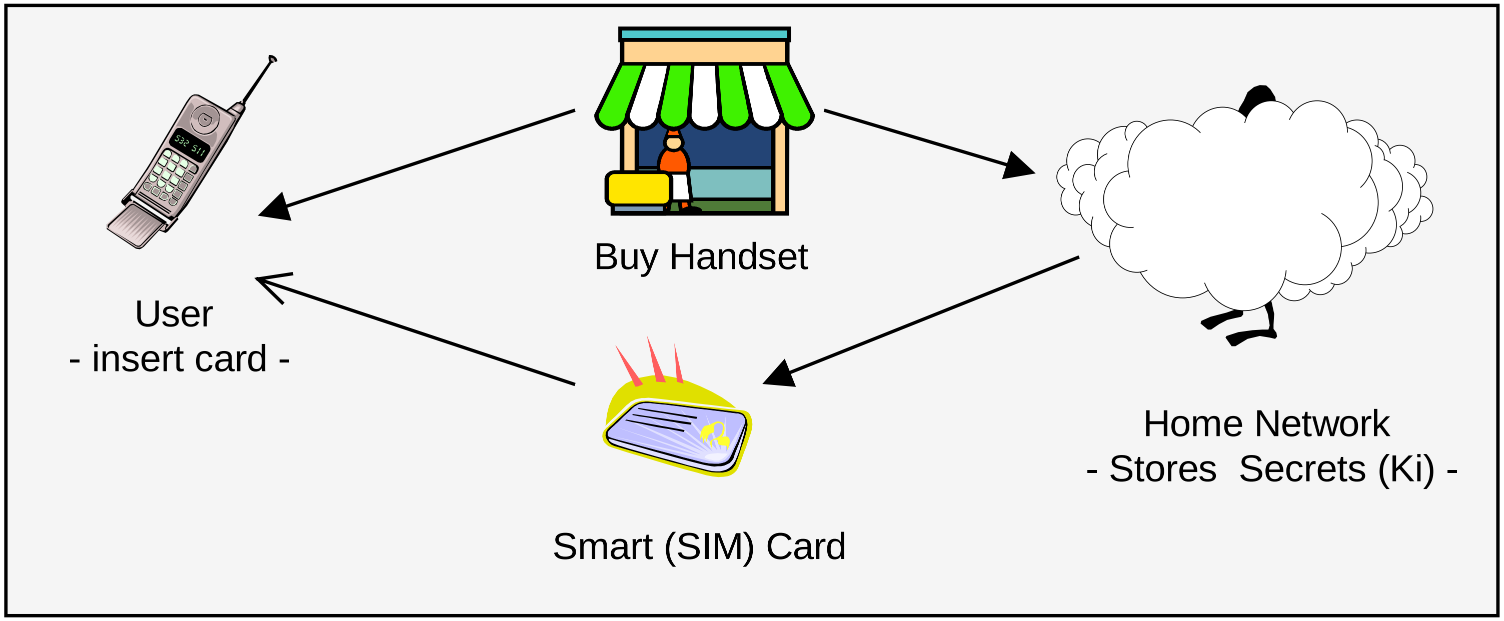


Commonly Used Techniques

- Authentication and Key Agreement (AKA).
  - Provisioning.
  - Roaming Support.
  - Verification and Cipher Key Generation.
- Encryption for Privacy.
  - Encryption of user traffic using the previously generated cipher key.

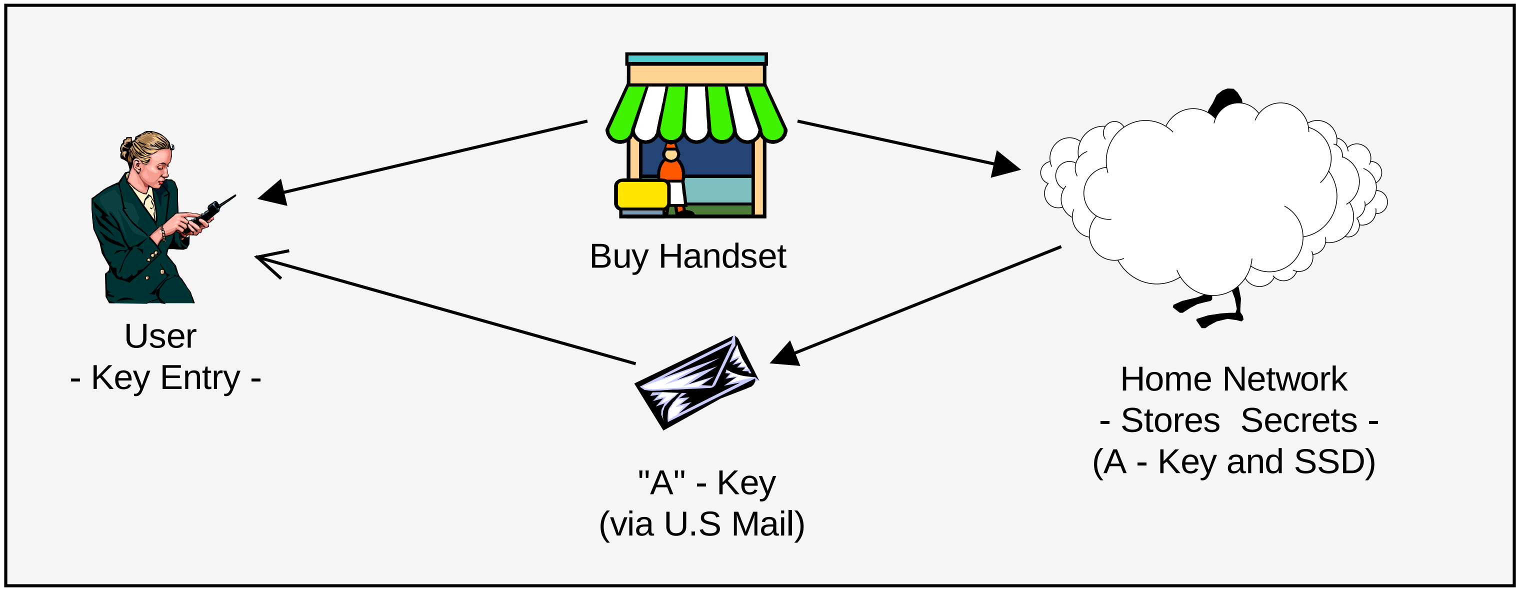
Secret Key Systems - Provisioning

- GSM - SIM (Subscriber Identity Module) cards. (Ki - Secret Key).

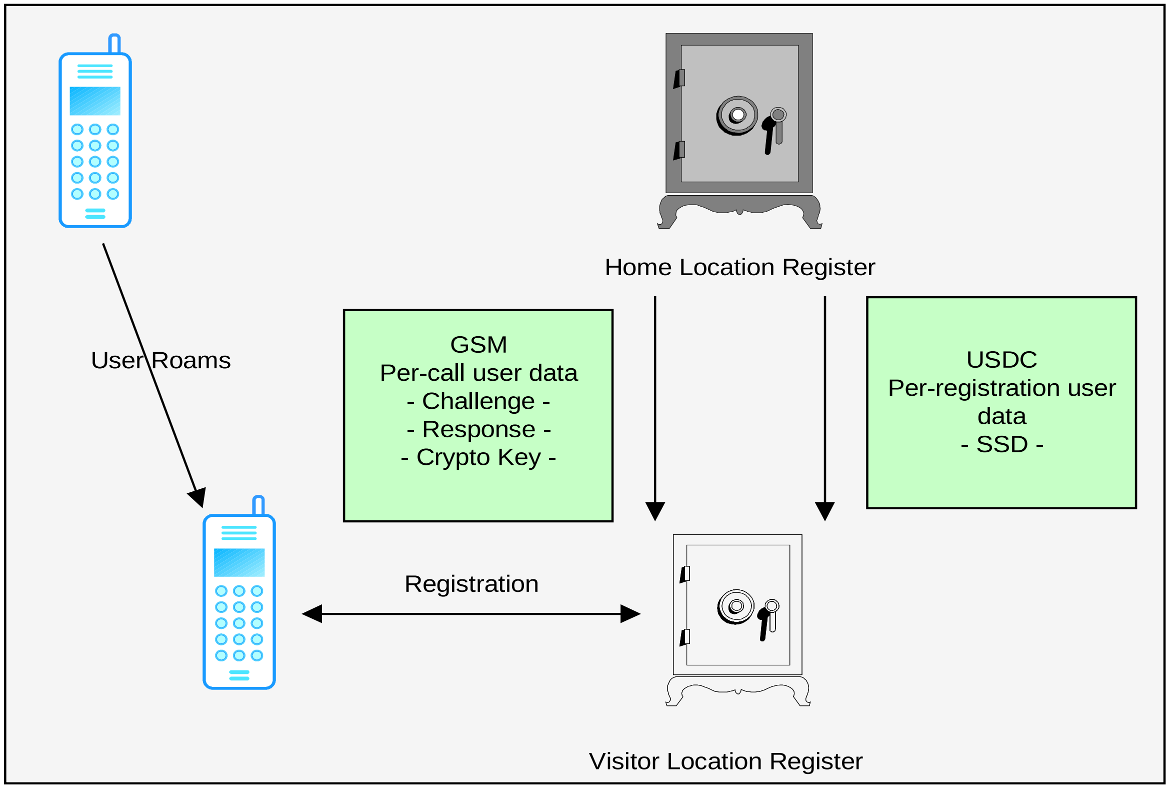


Secret Key Systems - Provisioning

- USDC - “A” Key and SSD (Shared Secret Data).



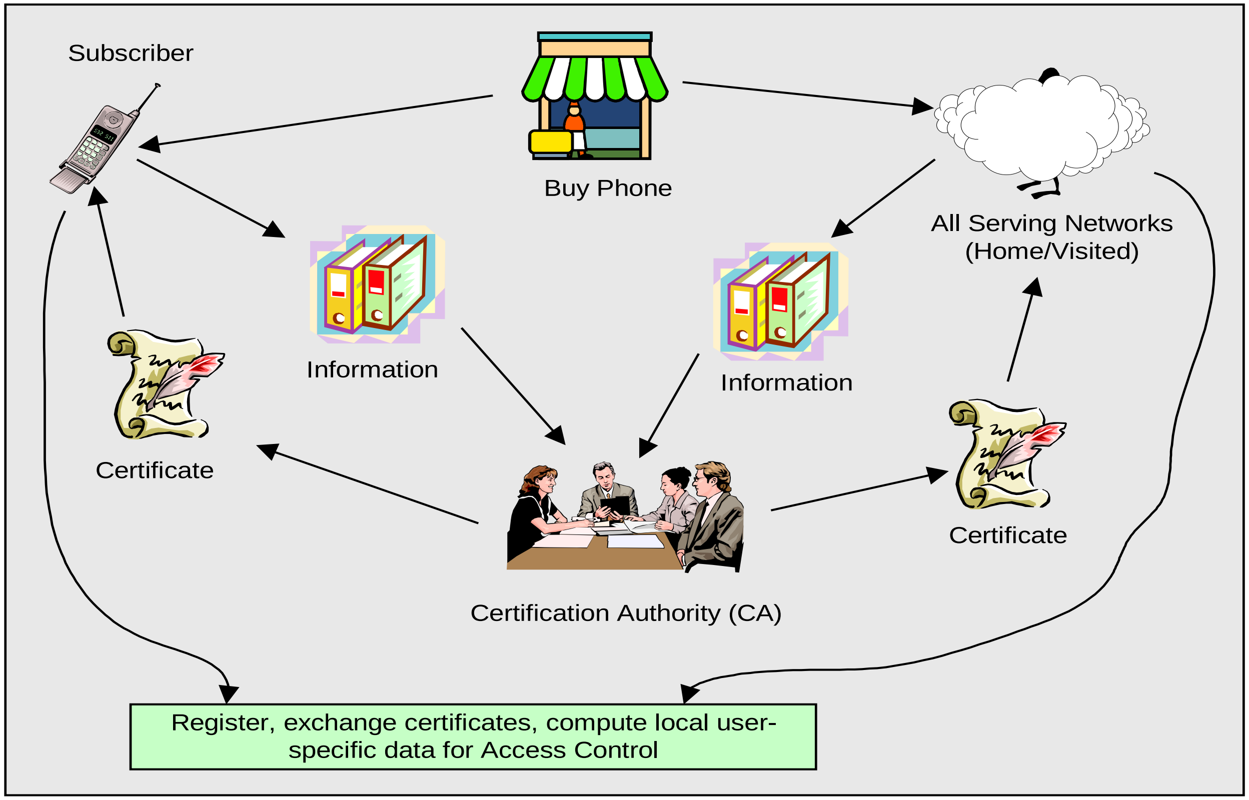
Secret Key Systems - Roaming Support



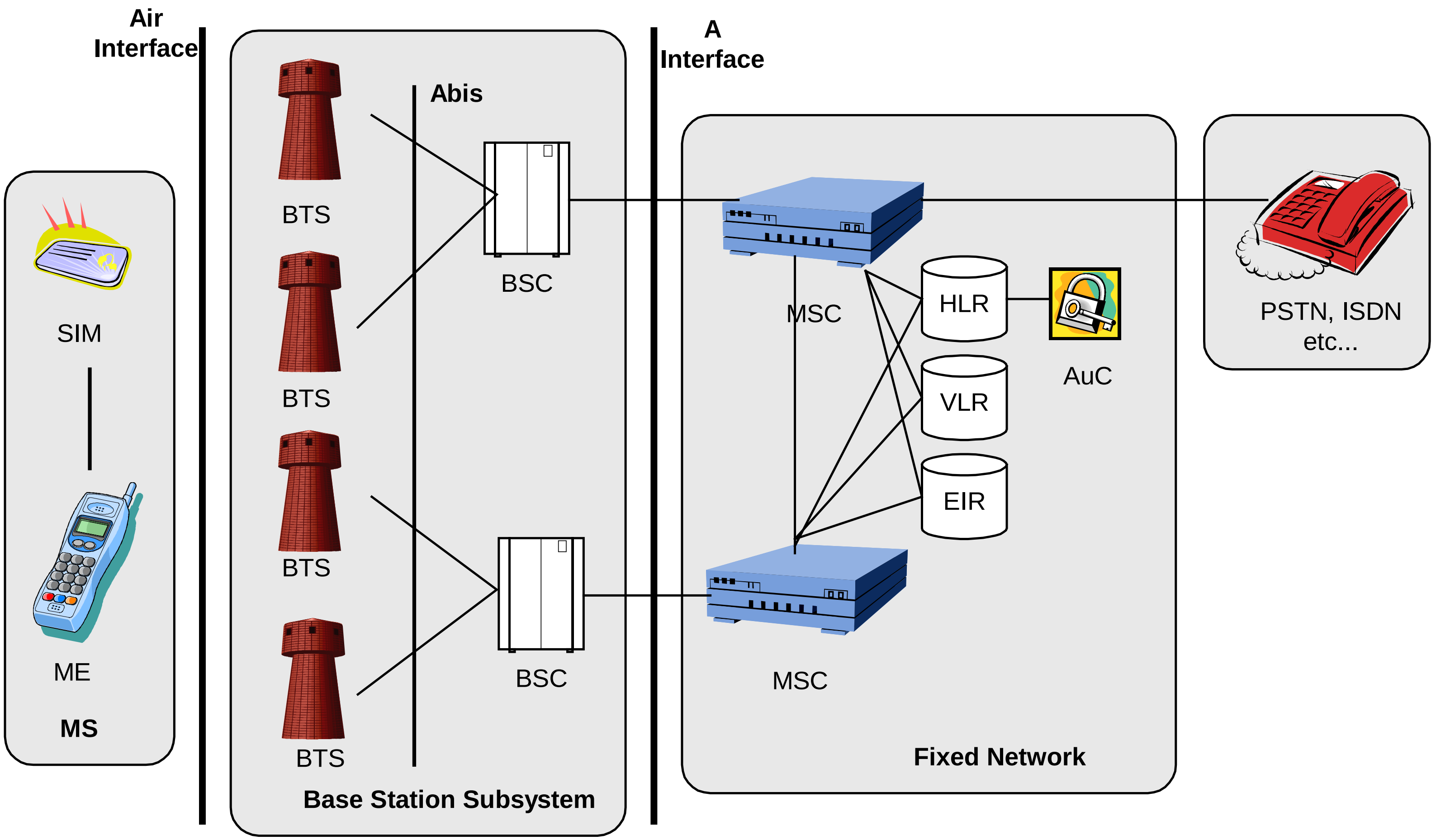
Verification and Session Key Establishment

- Challenge - Response Mechanism.
- USDC
  - 32 bit broadcast global challenge.
  - Mobile - (response + call-setup information).
  - Verification by Serving Network using SSD.
  - Cipher Key Generation.

Public Key Systems


Subscriber
Buy Phone
All Serving Networks
(Home/Visited)
Information
Information
Certificate
Certificate
Certification Authority (CA)
Register, exchange certificates, compute local user-specific data for Access Control

GSM Security



GSM Security...

- SIM - Subscriber Identity Module.
  - Permanent - IMSI, Ki, A3, A8.
  - Temporary - TMSI, LAI, Kc.
- HLR - Home Location Register.
  - Subscriber specific parameters (Ki, IMSI, ...).
- AuC - Authentication Center.
  - Calculation of Authentication Related Parameters.
- VLR - Visitor Location Register.
  - Roaming Users. (TMSI, Kx, LAI, …)
- EIR - Equipment Identity Register.

GSM Security Features

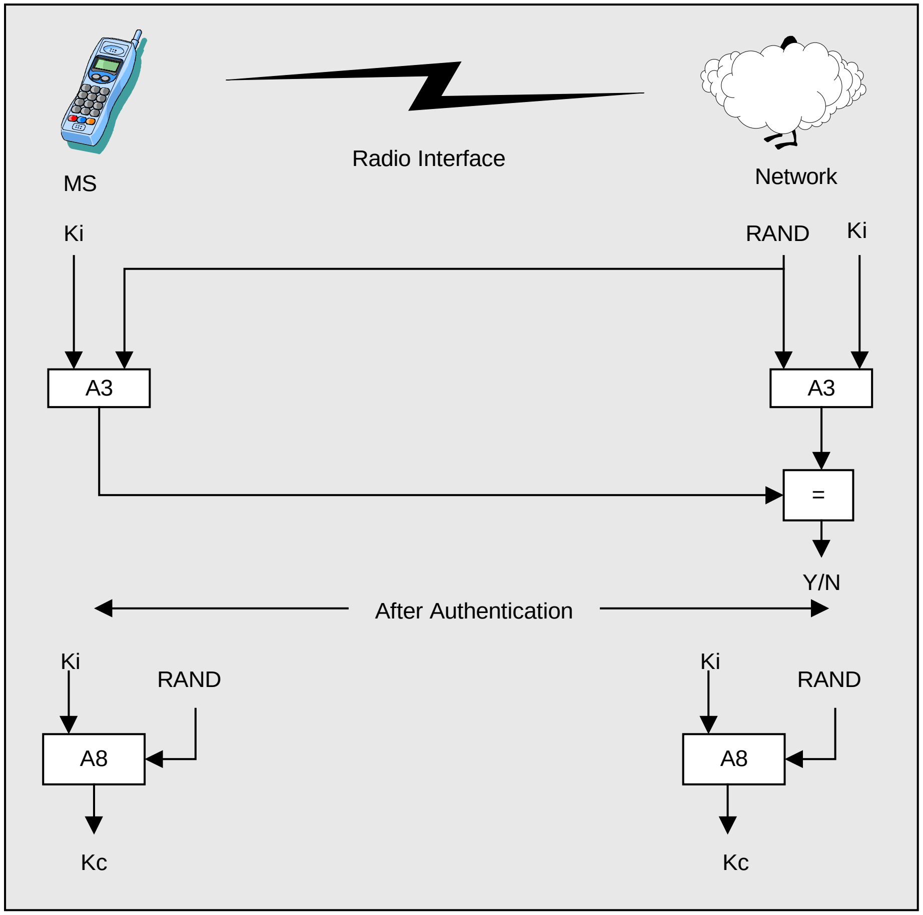
- Subscriber Identity Confidentiality.
  - Protection of subscriber ID.
- Subscriber Identity Authentication.
  - Protection of Network Assets from unauthorized use.
- User Data Confidentiality on Physical Connection.
  - Protection of User Speech data.
- Connectionless User Data Confidentiality.
  - Protection of L3 connectionless User data.
- Signaling Information Element Confidentiality.
  - Protects sensitive signaling information.

Subscriber Identity Confidentiality

- Implemented using Temporary Identities (TMSI).
- Prevents long-term impersonation.
- TMSI - local significance only.
- (TMSI, LAI) - identifies a mobile.
- TMSI - allocated during each location update.
- HLR must be notified of the update.

Subscriber Identity Authentication

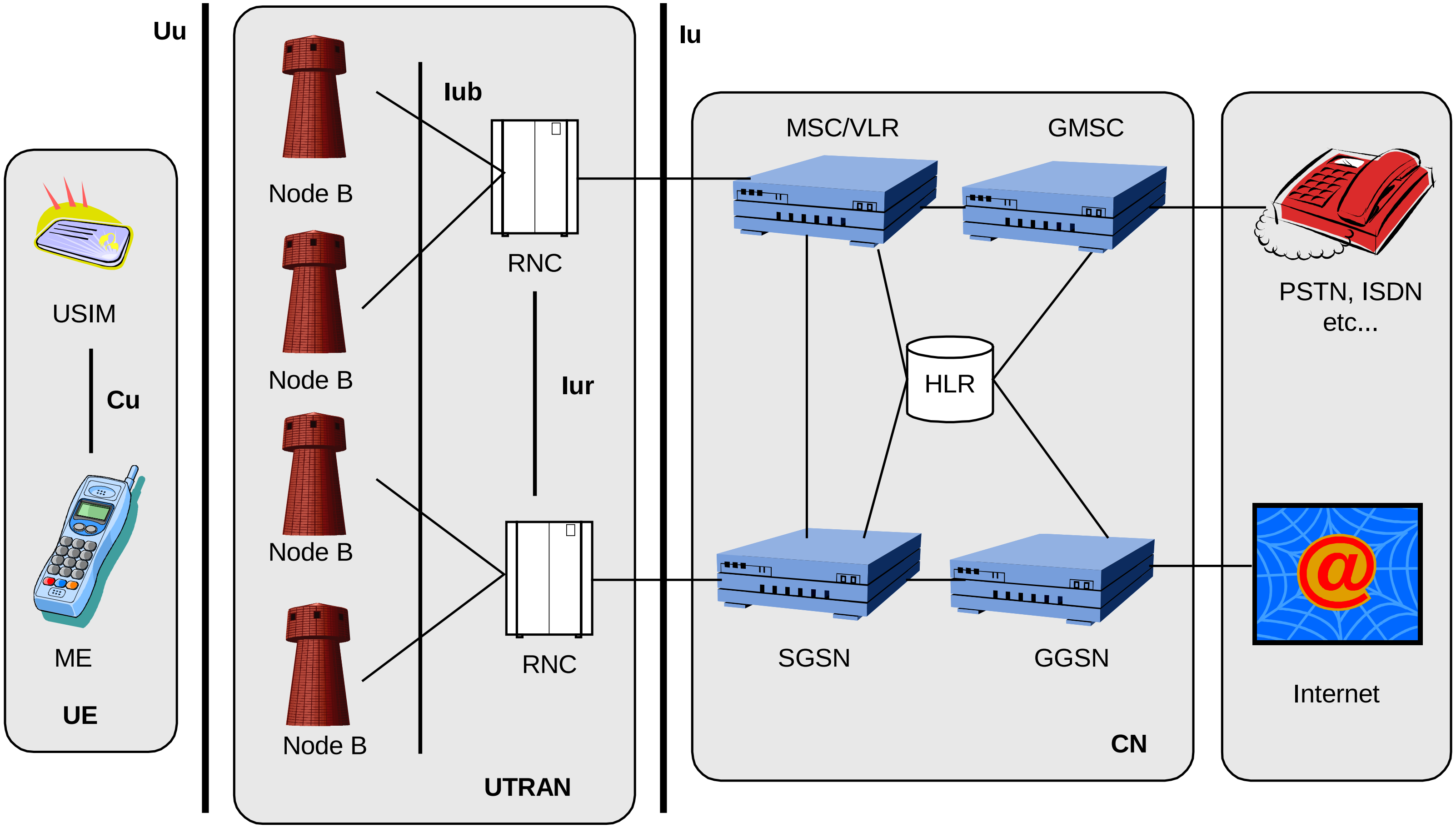
- Secret-Key Authentication (Challenge-Response Mechanism)
- HLR -> Authentication Vectors -> VLR.
- Authentication Vector (Triplet)
  - Challenge (RAND).
  - Response (SRES).
  - Crypto-Key (Kc).



2G (GSM) Security Weaknesses

- Attacks using a false BTS is possible.
- Transmission of cipher keys in clear within networks.
- Absence of data integrity.
- Lack of scalability and flexibility.

3GPP-UMTS Security



3G Security Architecture

- Network Access Security.
- Network Domain Security.
- User Domain Security.
- Application Domain Security.
- Visibility and Configurability of Security.

Network Access Security

- User Identity Confidentiality.
  - Using TMUIs (like GSM).
- Authentication of Users.
  - Additional paramter ‘AUTN’ to verify the BTS.
- User Data Confidentiality.
  - Cipher Key (Kc).
- Data Integrity
  - Using a Integrity Key (IK) and an integrity Algorithm.
- Mobile Equipment Identification.
  - IMEI (International Mobile Equipment Identifier).

3G Security Architecture…

- Network Domain Security.
  - 3-Layered Security Architecture.
  - Provides for,
    - Network element authentication.
    - Signaling Data Confidentiality (between Networks).
    - Data Integrity.
    - Fraud Information Gathering System.
- User Domain Security.
  - Secret shared between User and USIM.
  - Secret shared between Terminal and USIM.

3G Security Architecture ...

- Application Domain Security
  - USIM Application Toolkit.
  - Provides for Application level authentication.
- Security Visibility and Configurability.
  - Indication of Security features to the user.
  - Configuration of Security.
    - Enabling/Diabling User-USIM Authentication.
    - Accepting/Rejecting incoming non-ciphered calls.
    - Setting up/not Setting up non-ciphered calls.
    - Accepting/Rejecting the use of certain ciphering algorithms.

Conclusion

- The issue of Security in Wireless Networks has been addressed right from its infancy.
- Security in Public Wired Networks is just a patch-work effect to uncover discovered security holes.
- Conclusion ??
  - *In the near future, Wired Networks can never be as secure as Wireless Networks !!*

References/Additional Reading

- Charlie Khaufman, Radia Pearlman, Mike Speciner, "*Network Security - PRIVATE Communication in a PUBLIC World*", Prentice Hall.
- *IEEE Personal Communications Magazine*, Aug 1995 issue.
- GSM Documents (http://webapp.etsi.org/pda/QueryForm.asp)
  - GSM 02.09 - Security Aspects.
  - GSM 03.20 - Security Related Network Functions.
  - GSM 02.17 - SIM.
- 3GPP Documents (http://www.3gpp.org/ftp/Specs/December_99/)
  - Overview - Harri Holma, Antti Toskala, *"WCDMA over UMTS"*, John Wiley & Sons
  - 3G TS 33.102 - Security Architecture.
  - 3G TS 21.133 - Security Threats and Requirements.
  - 3G TS 33.120 - Security Principles and Objectives.
  - 3G TS 33 900 - A Guide to 3rd Generation Security.

Any Questions ?