SIM, USIM/CSIM and ISIM Overview

James Ni

04/22/2013
SIM

• Subscriber Identification Module (SIM)
  – An integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices
  – Initially introduced in GSM (TS 11.11)

• Key Information Stored in SIM
  – unique serial number (ICCID) – up to 20 digits
  – international mobile subscriber identity (IMSI) – MCC + MNC + MSIN
  – security authentication and ciphering information
    • Authentication Key (Ki) - 128-bit unique key for each SIM, also stored in AuC/HSS
  – temporary information related to the local network
    • Local Area Identity (LAI) – received from local carrier
  – a list of the services the user has access to
    • Operator-Specific Emergency Number
    • SMSC (Short Message Service Center) number
    • Service Provider Name (SPN)
    • Service Dialing Numbers (SDN)
    • Advice-Of-Charge parameters
    • Value Added Service (VAS) applications
  – two passwords:
    • a personal identification number (PIN) for ordinary use and
    • a personal unblocking code (PUK) for PIN unlocking
USIM

• UMTS SIM

• Similar to GSM SIM
  – More capabilities – allowing 3G UMTS services
  – Stronger Authentication and Security capabilities
  – Larger and securer phone book
  – Key information stored
    • similar to GSM SIM
    • Additional information to support UMTS services
CSIM

• CDMA SIM
• Similar to GSM SIM
  – runs on a UICC
  – file structure derived from the R-UIM card
  – For cdmaOne/CDMA2000

• Key parameters
  – Identifications
    • MIN+ESN prior to introduction of IMSI, MIN for identifying the subscriber and MIN+ESN for registration and authentication
    • IMSI (international mobile subscriber identifier).
    • TMSI (temporary mobile subscriber identifier, for position security).
    • UIMID (hardware identifier) - a pseudo value if EUIMID is in use.
    • EUIMID Either short form (based on MEID) or long form (based on ICCID).
    • ICCID Present even if it is not used as EUIMID
    • MEID (hardware identifier).
  – Encryption keys
  – Phone Number
  – List of services available
    • Call Control
    • SMS
    • BCMCS Broadcast
    • IP Location
  – CDMA2000 Parameters
  – Stats
  – Misc.
**ISIM**

- **IP Multimedia Service Identity Module (IMS SIM)**
  - An application residing on the UICC
  - Contains parameters for identifying and authenticating the user to IMS
  - ISIM can co-exist with (U)SIM and/or CSIM on the same UICC

- **ISIM Application Dedicated File (ADF) Contains multiple Elementary Files (EFs)**
  - IST (ISIM Service Table): Lists available optional services:
    - P-CSCF address
    - Generic Bootstrapping Architecture (GBA),
    - HTTP Digest
    - GBA-based Local Key Establishment Mechanism,
    - Support of P-CSCF discovery for IMS local break out
  - DOMAIN (Home Network Domain Name)
    - For 3GPP systems without ISMI, UE derives DOMAIN from IMSI
  - IMPI (IMS Private User Identity)
    - Every IMS user has one or more IMPIs – assigned by the home network operator
    - Used for Registration, Authorization, Administration and Accounting purposes
    - an ISIM stores ONE IMPI – not modifiable on UE
    - Identifies the subscription, NOT the user
    - Is used to identify the user’s information (e.g. authentication info) stored in HSS (e.g. for Registration)
    - HSS needs to store the IMPI
    - S-CSCF needs to obtain and store the IMPI upon registration
    - For 3GPP systems without ISIM, IMPI can be derived from IMSI
ISIM

• ISIM Application Dedicated File (ADF) Contains multiple Elementary Files (EFs)
  – IMPU (IMS Public User Identity – one or more)
    • Every IMS user has one or more IMPUs
    • IMPUs are used by users for requesting communications to other users
    • IMPU takes the form of either
      – SIP URI (RFC 3261): sip:username@domain or
      – TEL URI (RFC 3966): tel:<E.164 number>
    • Both formats can be used to address users
    • At least one IMPU is stored in ISIM – cannot be modified on UE
    • An IMPU must be registered (explicitly or implicitly) before use for IMS procedures
    • Implicit registration allows registering a user with multiple IMPUs through one registration
    • IMPUs are not authenticated during registration
    • IMPUs MAY be used to identify the user’s information in HSS (for mobile terminated sessions)
    • Alias IMPUs can be grouped and used to identify the same user - stored in HSS
    • IMPUs MAY be shared across multiple IMPIs within the same IMS subscription
    • For 3GPP systems without ISIM, Temporary IMPU is derived from the IMSI
  – AD (Administrative Data): UE operation mode – normal or type approval
  – ARR (Access Rule Reference): access rules for files located under the ISIM ADF
  – P-CSCF: P-CSCF Address (one or more)
  – GBABP (GBA Bootstrapping parameters):
    • RAND (AKA Random Challenge
    • Bootstrapping Transaction Identifier (B-TID) associated to a GBA NAF derivation procedure
  – NAFKCA (NAF Key Centre Address – one or more)
MSISDN/MDN and MSRN/TLDN

• MSISDN/MDN are Public Mobile Telephone Numbers
  – MSISDN: GSM/UMTS Networks
  – MDN: CDMA Networks

• MSRN/TLDN are mobile routing numbers
  – MSRN: GSM/UMTS Networks
    • Calling party dials MSISDN of the called mobile station
    • HLR maps MSISDN to IMSI
    • VLR maps IMSI to MSRN
    • MSRN is used to route the call to called mobile station
  – TLDN: CDMA Networks
    • Calling party dials MDN of the called mobile station
    • In non-roaming case
      – HLR returns registration status
      – MDN is used to route the call
    • In roaming case
      – Serving MSC/VLR and HLR returns TLDN
      – TLDN is used to route the call
CAVE Authentication

• CDMA Authentication
  – HLR/AuC:
    • (SSD RAND, ESN, A-key) → SSD
    • SSD RAND, MIN, ESN deliver to Serving MSC and Mobile
  – Mobile Station:
    • (SSD RAND, ESN, A-key) → SSD
  – Authentication
    • Global challenge: to all mobile stations using a particular radio channel
    • Unique challenge: to a individual mobile station
    • Done at location updates time or service originating time
    • Authentication results are compared at
      – Either the serving MSC (when SSD is shared)
      – Or the HLR/AuC (when SSD is not shared)
AKA Authentication

• IMS Authentication
  – HSS:
    • Generates and passes (RAND, AUTN, XRES, CK, IK) to S-CSCF via MAA
  – S-CSCF:
    • Relays (RAND, AUTN, CK, IK) to P-CSCF via 401(REGISTER), keeps XRES
  – P-CSCF:
    • Relays (RAND, AUTN) to Mobile Station via 401(REGISTER)
  – Mobile Station:
    • Calculates RES and send with REGISTER to IMS core
  – S-CSCF:
    • Compare RES and XRES to complete the authentication

• Notes:
  – Random number (RAND)
  – Authentication token (AUTN)
  – Signed/expected result (XRES)
  – Cipher key (CK)
  – Integrity Key (IK)
  – Result (RES)
IMS Registration (TS.23.228)

• What are registered?
  – Public User Identity:
    • It shall be possible to register multiple public identities via single IMS registration
    • It shall be possible to register a Public User Identity that is simultaneously shared across multiple contact addresses
    • Registration of a Public User Identity shall not affect the status of already registered Public User Identity(s)
    • When multiple UEs share the same public identity(s), each UE shall be able to register its contact address(es) with IMS.
  – Private User Identity
  – Home network domain name
  – UE IP address
  – Instance Identifier
  – GRUU Support Indication
IMS Registration(TS.23.228)

• What is sent from S-CSCF to HSS
  – Public User Identity
  – Private User Identity
  – S-CSCF name

• What is passed on from HSS to S-CSCF
  – one or more names_ADDRESSES information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF.
  – the names_ADDRESSES information,
  – security information.
  – etc.
MDN/MSISDN+IMSI as Temporary IMPU

• When ISIM is not available (for legacy non-IMS access devices)
  – IMSI + MDN/MSISDN is used as temporary IMPU for registration and authentication
  – This is only for early IMS deployment and can only be a temporary solution

• The definition of IMPU can be carrier specific, MDN can be used in either one of the following IMPU format
  – sip:MDN@network-domain
  – tel: MDN