S3-030450

Joint Meeting 3GPP / 3GPP2

Michael Marcovici
Lucent Technologies Inc.

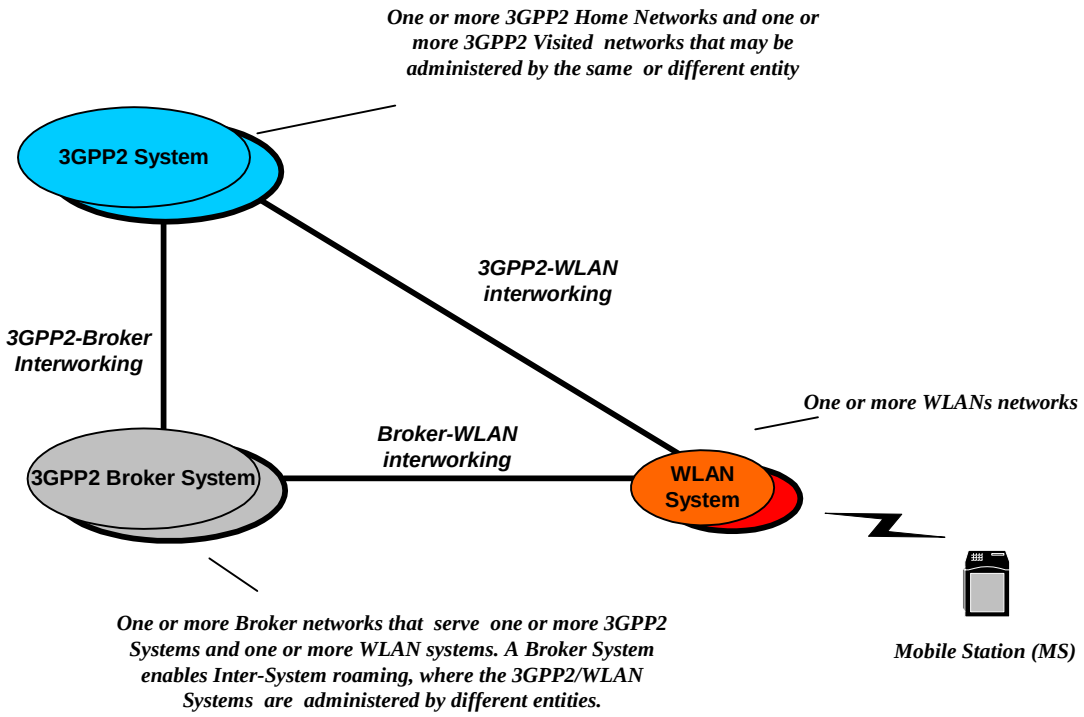
WLAN-3GPP2 Interworking 3GPP2 S.P0087 (Draft)

WLAN-3GPP2

Service interworking between 3GPP2 systems and WLAN systems should reuse the existing WLANs, i.e. transportation of IP packets, with minimum modifications for both the 3GPP2 system and the WLAN system. Any change to the WLAN system should be minimized and there should be no changes to IEEE 802.11 specifications.

3GPP2 - WLAN interworking shall not be limited to any specific WLAN technology.

Interworking Model



Trust Model

- **The WLAN system may be completely un-trusted by the MS and the 3GPP2 system.**
- **The WLAN system contains elements that may be trusted by the MS and the 3GPP2 system. For example, the WLAN system may include trusted servers that look after aspects of security and authentication interworking with the 3GPP2 systems (e.g. 802.1x). However, other elements of the WLAN system may be un-trusted.**
- **All of the elements of the WLAN system may be fully trusted by the MS and the 3GPP2 system.**

WLAN-3GPP2
Sample Requirements

Conn-01: The 3GPP2-WLAN system interworking shall support IPv4 and should support IPv6 based connectivity.

Conn-02: It shall be possible for the MS to establish connectivity to the Internet through the WLAN System directly, or through the WLAN and 3GPP2 Systems. .

ACC-1: Accounting records shall be generated by either the WLAN system or 3GPP2 system or both.

ACC-2: The accounting information for the user's WLAN access shall be made available to the home 3GPP2 system.

ACC-3: To assist billing, it shall be possible for the home operator to receive Accounting records associated with WLAN system usage, to support online (i.e., prepaid) and offline (i.e., postpaid) accounting by the 3GPP2 system.

Roam-1: While roaming to a WLAN system, it shall be possible for the MS to obtain all access independent IP services provided by the 3GPP2 Home System.

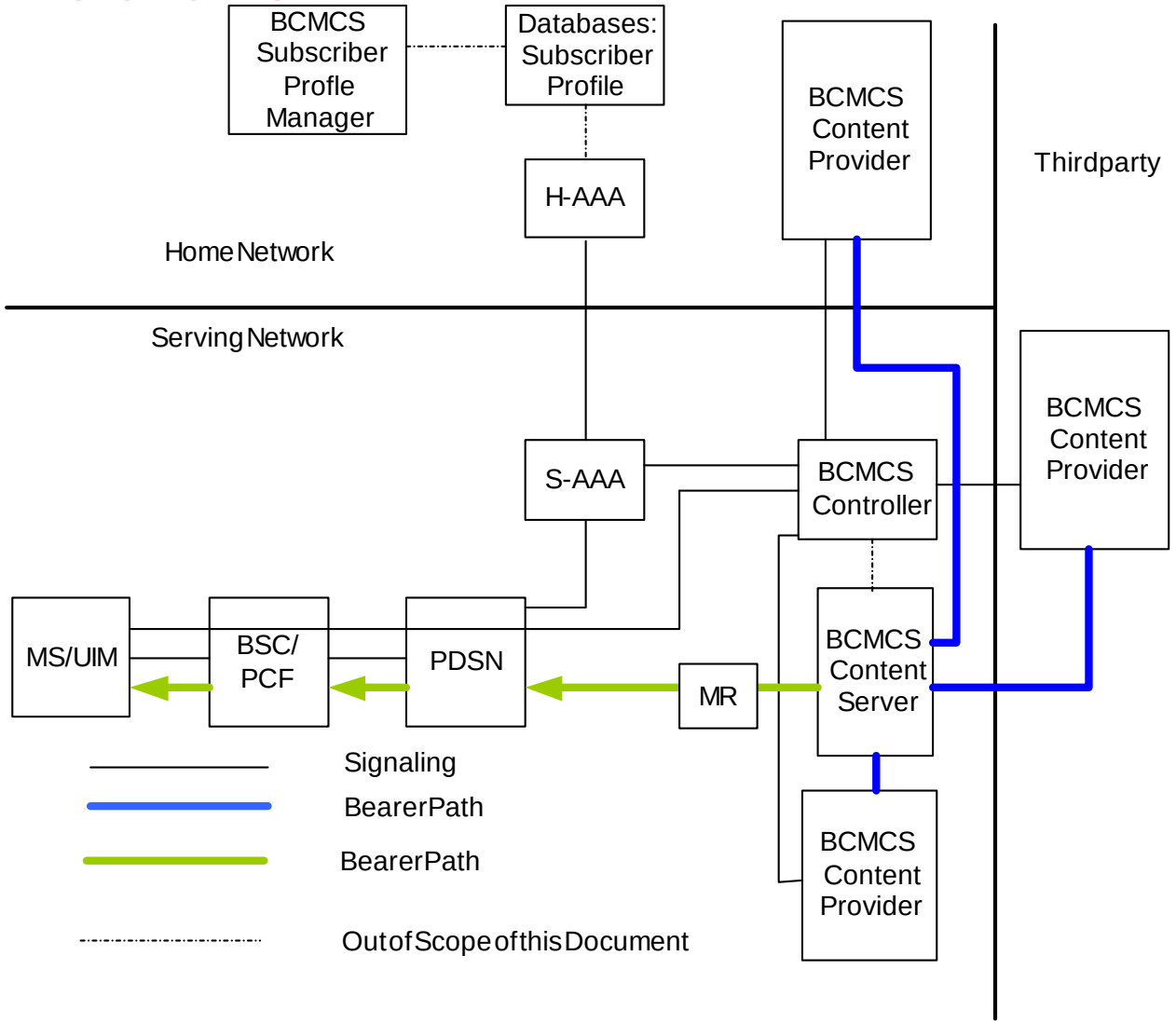
Roam-2: It shall be possible for a dual mode MS to revert to the 3GPP2 system to access a desired service if it is unable to access a desired 3GPP2 service through the WLAN system.

Broadcast/Multicast

3GPP2 S.P0083

Broadcast-Multicast Service Security Framework

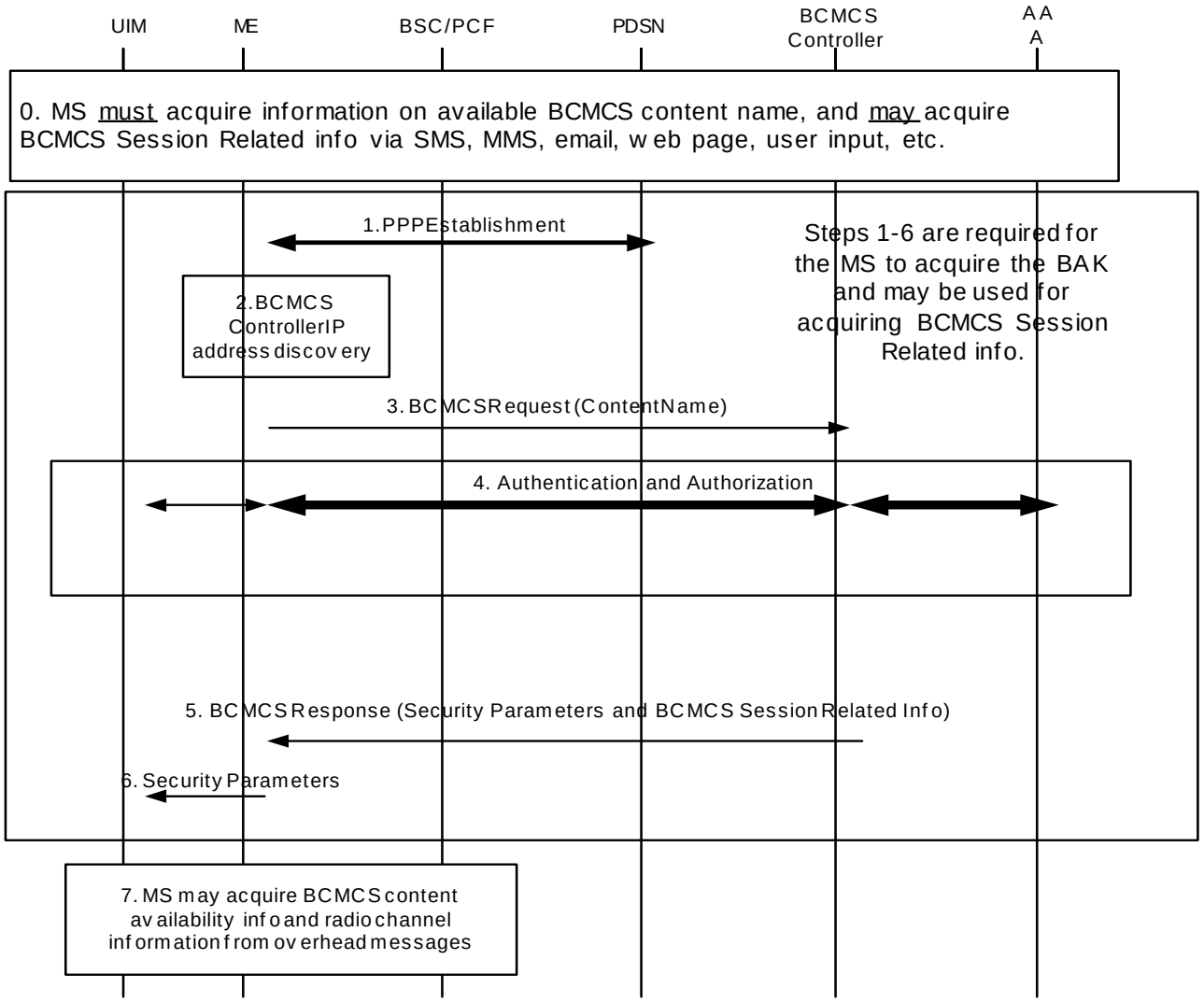
Architecture



Architecture

- BCMCS Controller:
  - Communicates with the mobile to provide detailed information necessary to choose and receive a BCMCS program. May also provide lists of available programs.
  - Communicates with the BCMCS Content Provider to control the ability of a Content Provider to send BCMCS programs to a BCMCS Content Server.
  - Generates and distributes BCMCS Access Keys (BAKs) to encrypt BCMCS program content.
  - Communicates via the AAA with the PDSN to provide IP multicast addressing and flow treatment information to the PDSN.

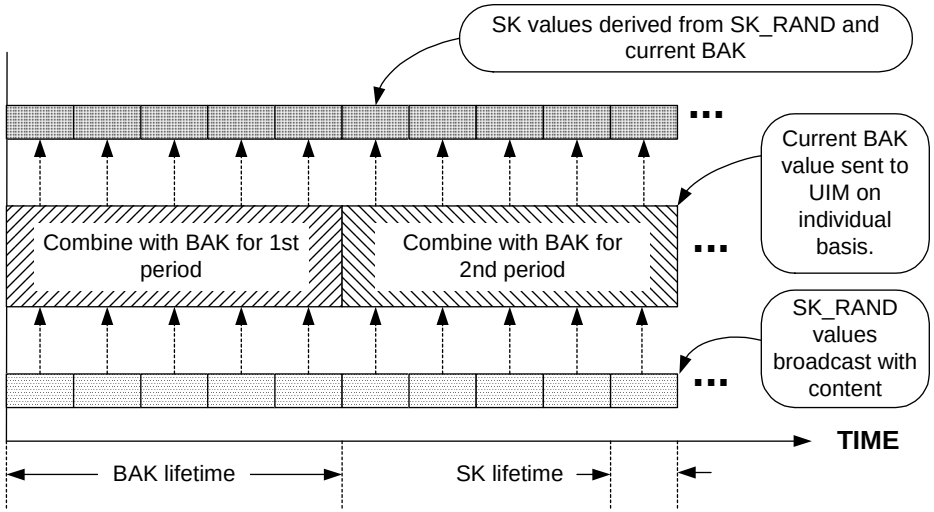
Sample Scenarios - Service Discovery, Information Acquisition



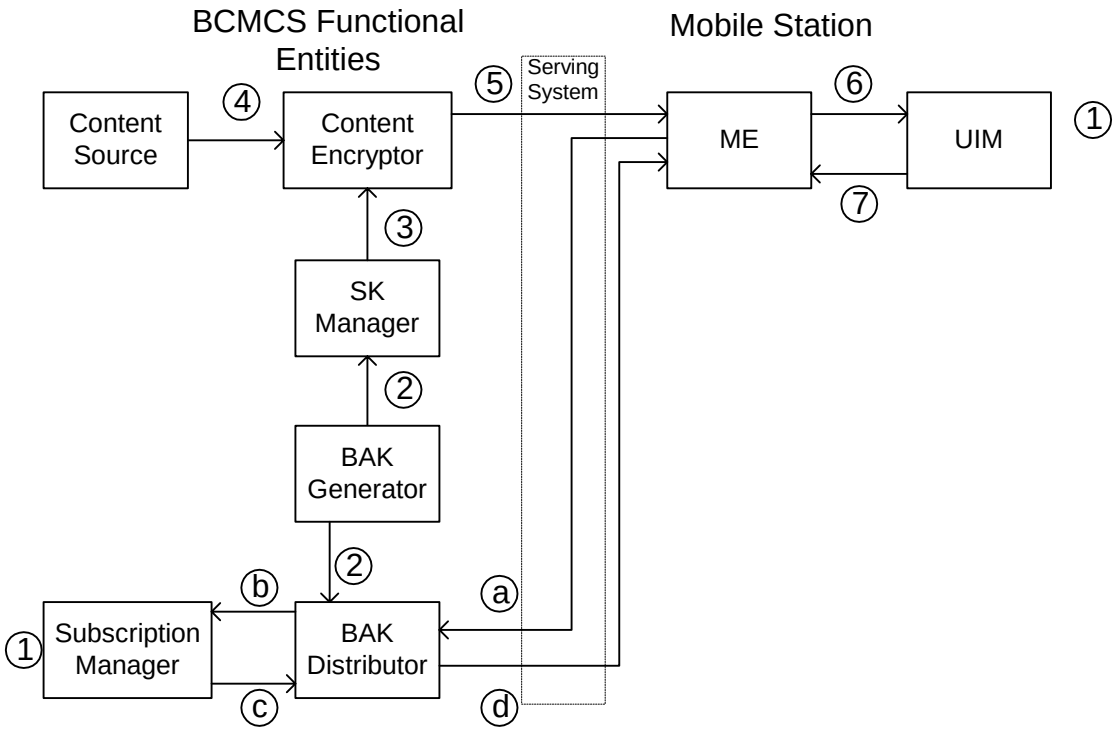
Security Keys

- BAK (BCMCS Access Key) – Generated in the network for each BCMCS Program.
- SK (Session Key) – Generated from the BAK and a random value (SK-Rand) and used to encrypt the content of a multimedia IP flow.
- RK (Root Key) – Contained in the UIM logical component of the mobile device. Used to generate temporary keys (TK).
- TK (Temporary Key) – Generated from the RK and a random value (TK-Rand) and used to encrypt the BAK for transmission to the mobile.

Key Management

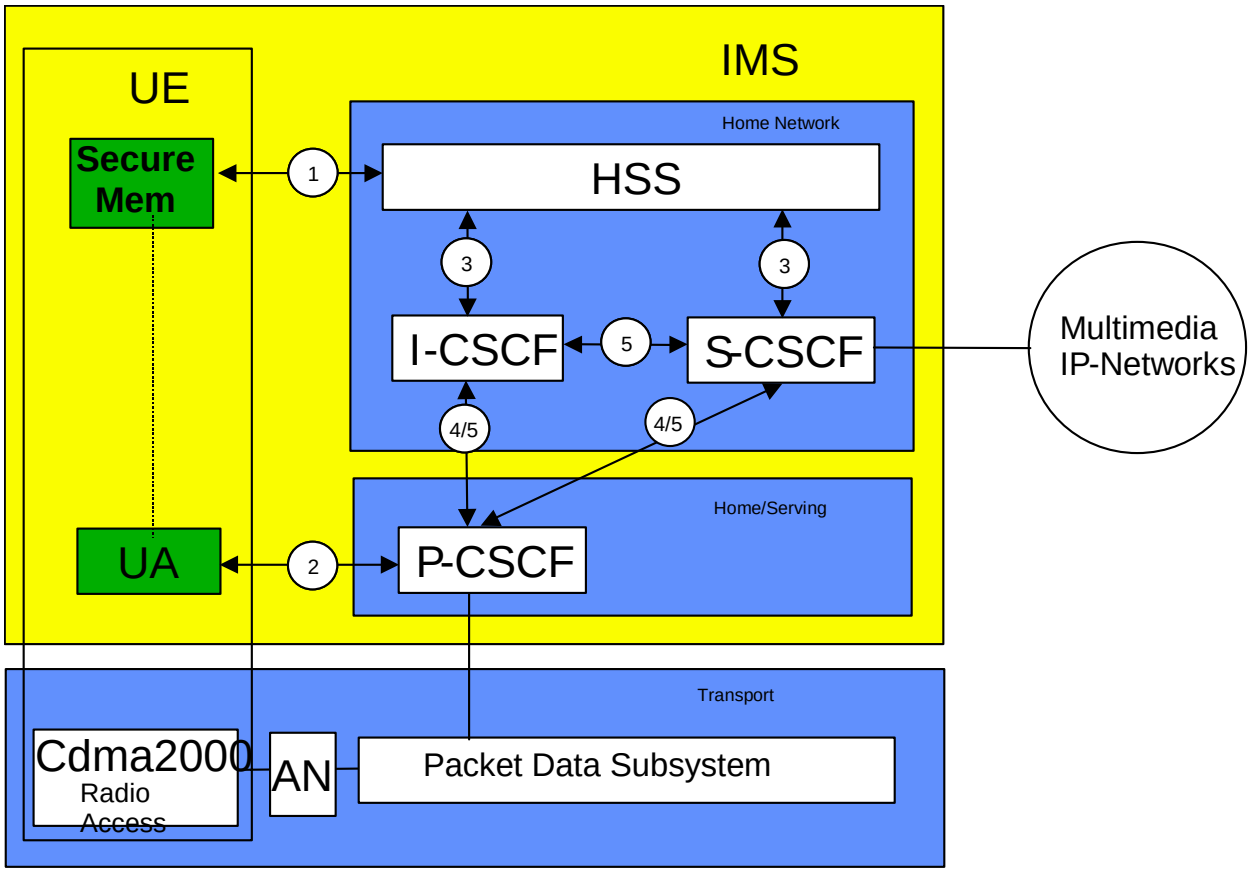


Logical Architecture



IMS Security Framework
3GPP2 S.P0086

IMS Security Architecture



Full Support for Sip-Sec-Agree (RFC 3329)

- The user's subscription is authenticated by the S-CSCF (home service provider). The security association between the UE and the first access point into the operator's network (P-CSCF) is negotiated based on the protocol defined in RFC 3329 [22]. The options supported by [22] are: tls, digest, ipsec-ike, ipsec-man, and ipsec-3gpp. **When the negotiated protocol is not ipsec-3gpp, sections 5 through 8 do not apply, and the appropriate RFC e.g. the SIP RFC [6] security mechanism shall be applied.**

Network Security

- **Inter-domain Security**

  Referring to Figure 1, interface 4 provides security between different networks for SIP capable nodes. The involved nodes shall be capable of IPsec [14]. Privacy protection shall be applied with cryptographic strength greater than DES. Integrity protection shall be applied. IPsec may be used in either transport mode or tunnel mode; when used in tunnel mode, one or both of the network security domains may use Security Gateways. Security associations between nodes in different networks shall be negotiated using IPsec/IKE [25].

Intra-domain Security

The interfaces labeled 3 and 5 in Figure 1 are between SIP-capable nodes in the same network security domain. As this interface exists entirely within one network security domain, the administrative authority may choose any mechanism to secure this interface, including physical security where appropriate. Cryptographic methods of security, if applied, shall include both privacy and integrity protection, and be at least equivalent to IPsec [14] using triple-DES and HMAC-MD5.

AKA in 3GPP2
3GPP2 X.P0006

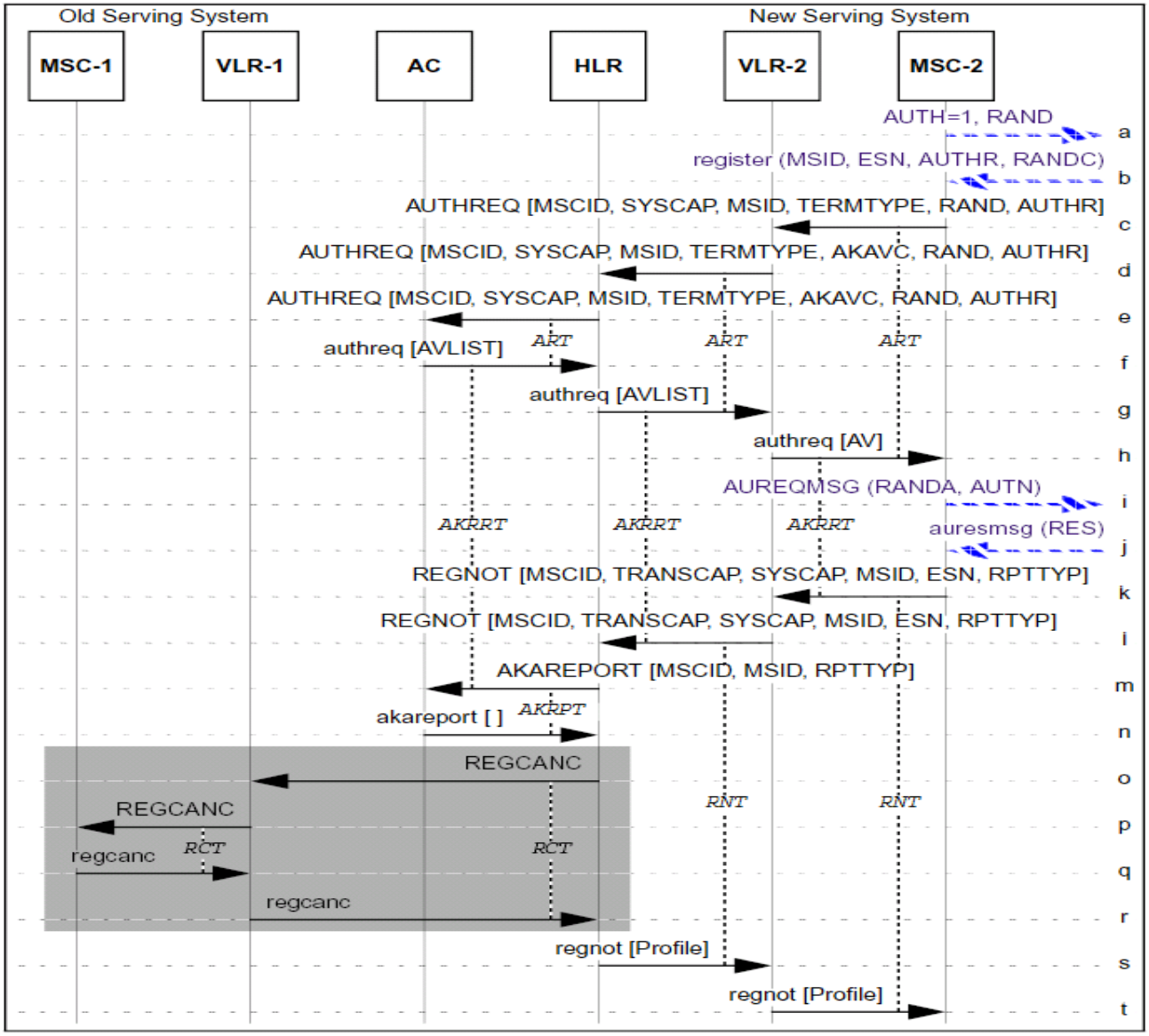


Figure 1 **Successful AKA on Initial Registration**

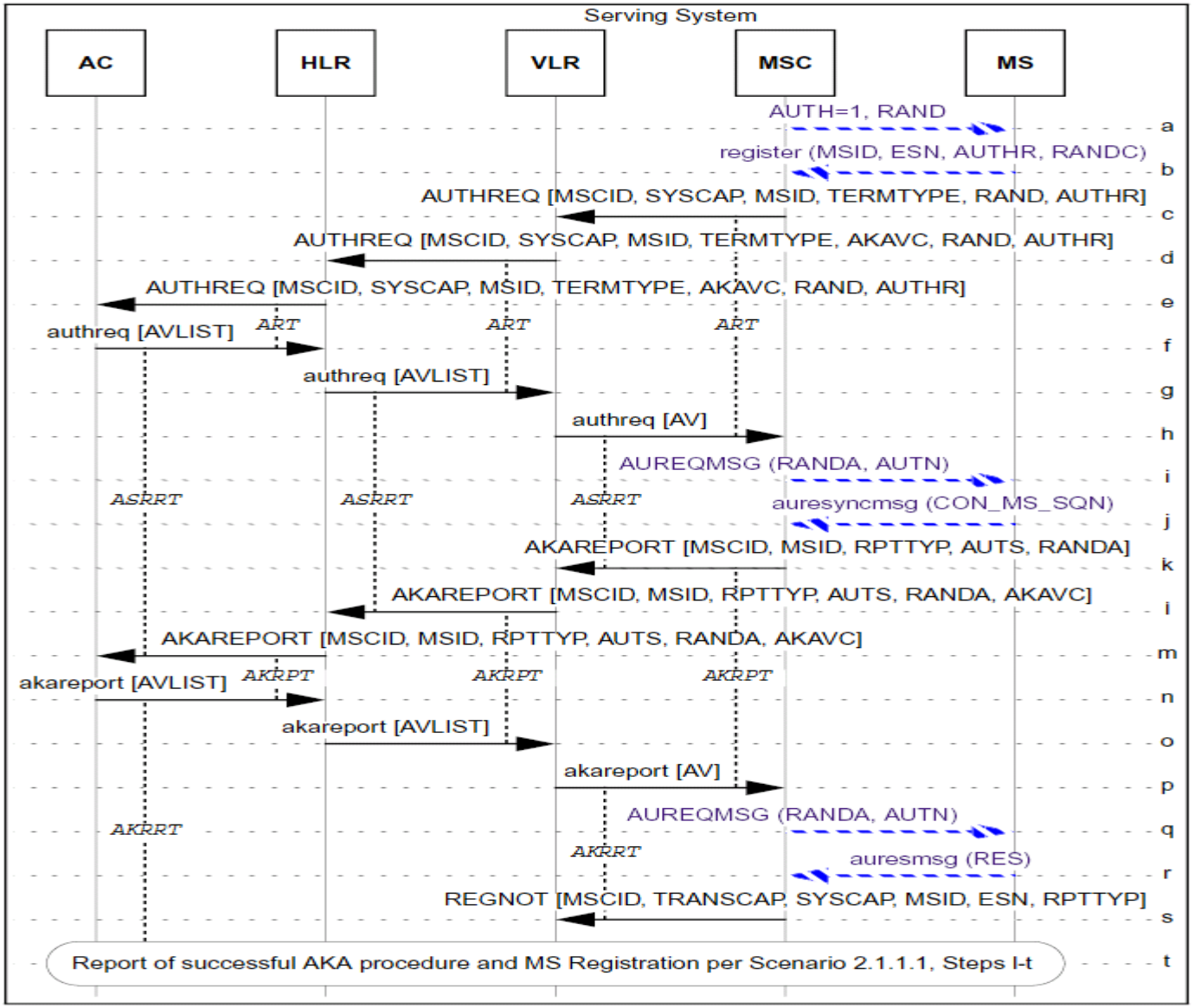


Figure 3 **AKA Synchronization Failure on Initial Registration**

Security Algorithm
3GPP2 S.S0053,54,55 and S.S0078

S.S0053 - ***Common Cryptographic Algorithms*** **(legacy)**

S.S0054 - ***Interface Specification for Common Cryptographic Algorithms***

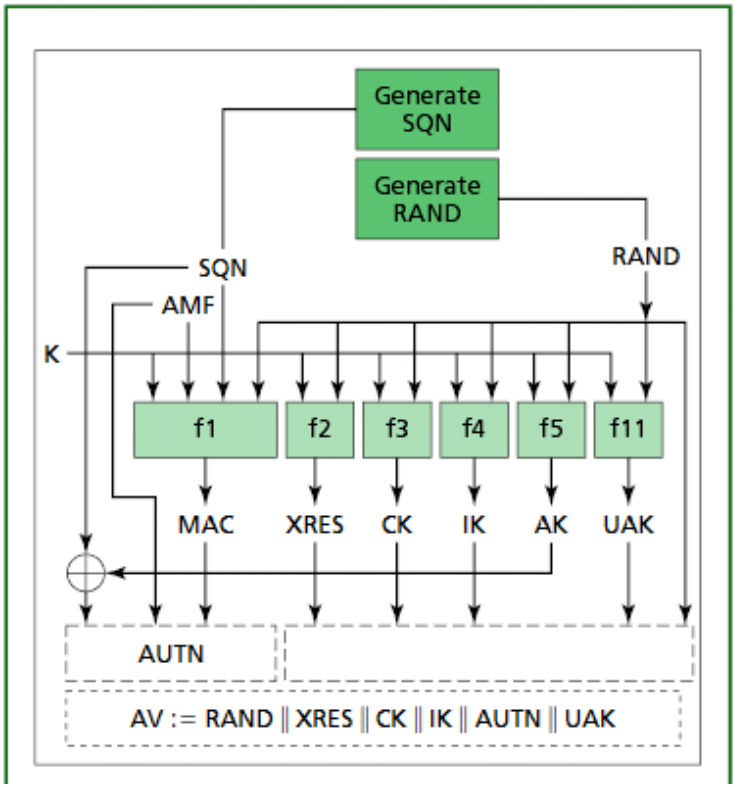
S.S0055 - ***Enhanced Cryptographic Algorithms***

S.S0078 - ***Common Security Algorithms***

The documents can be downloaded from
ftp://ftp.3gpp2.org/TSGS/Working/security_algorithms/

Security Algorithms

- All functions are specified and standardized, including the key generation functions
- The USIM is authenticated to the TE to protect against rogue shell attacks, i.e., USIM has to be plugged into the terminal at all times, and the UAK (known to the USIM and to the AN only) is used to sign messages. This is an optional key for the network, mandatory for a CDMA2000 (3G) compliant MS.



Local USIM Authentication

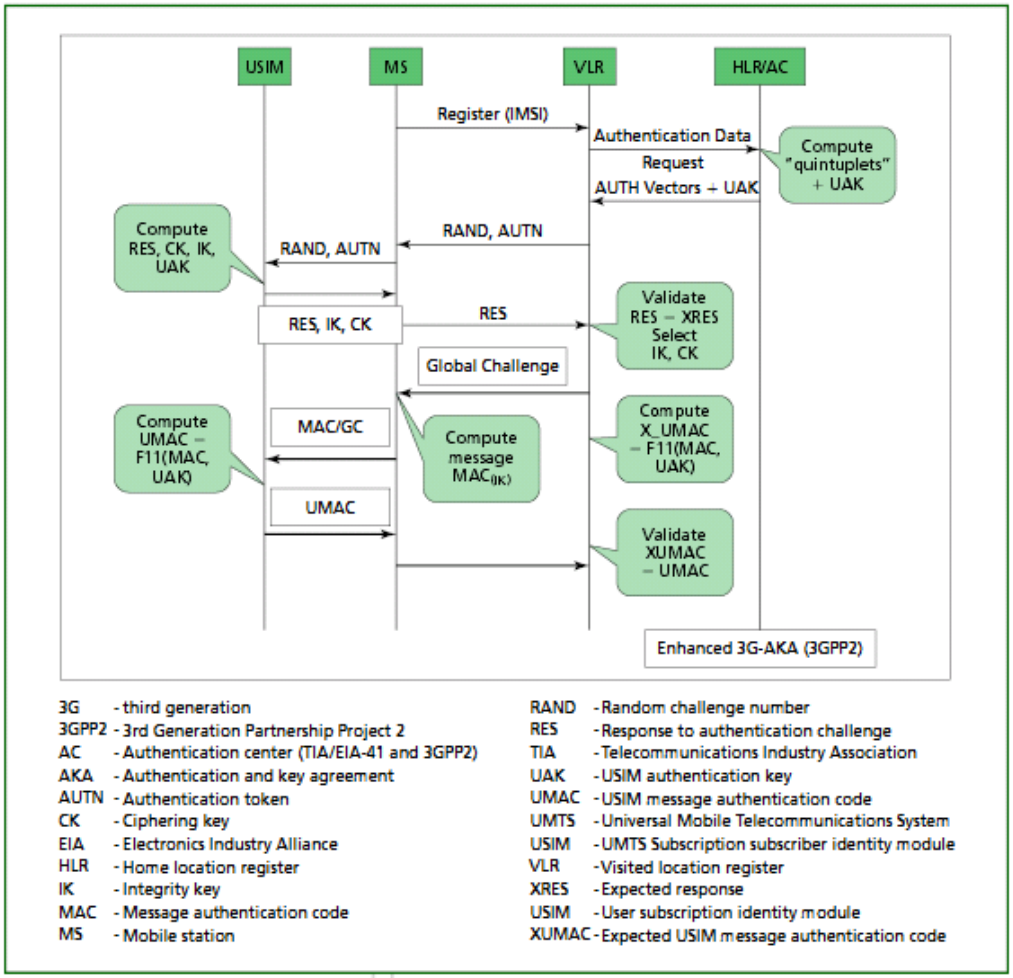


Figure 6.
Local and USIM authentication.

3GPP2 S.S0055

3GPP2 S.S0078