Security Architecture Standardization and Services in UMTS

Christos Xenakis and Lazaros Merakos

Communication Networks Laboratory
Department of Informatics & Telecommunications
University of Athens, 15784 Athens, Greece.
{xenakis,merakos}@di.uoa.gr

Abstract
Security is a primary concern in mobile communication systems. Wireless access is inherently less secure, and mobility implies higher security risks than static operation. The security framework for 3G mobile systems is considered, and its principles and security requirements are discussed. Furthermore, the security features that are currently being standardized in 3GPP, as well as the emerging 3G-security architecture are elaborated. The focus is on the various mechanisms and protocols, which are employed to provide security at different levels, and on their effect on network operation.

1 Introduction

The deployment of mobile systems is changing the telecommunication landscape. Along with a variety of new perspectives and possibilities, third-generation (3G) mobile systems impose serious security threats to the communicating parties.

Wireless access is inherently less secure, and mobility implies higher security risks than static operation. The advanced network infrastructure, which supports higher access rates, and the complex network topologies, which enable "anywhere-anytime" connectivity, may increase the number and the ferocity of potential attacks. Furthermore, the introduction of IP the layer in the network domain, for both signaling and user data transport, shifts towards open and easily accessible networks.

This paper considers the security framework in advanced 3G mobile systems. The principles that should be followed in the security architecture design are presented, and the potential attacks as well as the intruders that may threaten network operation are outlined. The security requirements imposed by the different types of traffic, and by the different players involved (mobile users, serving network and service providers) are investigated. The security architecture for the Universal Mobile Telecommunication System (UMTS), as it is developing in 3GPP [23], is presented with focus on the various mechanisms and protocols employed to provide security at different levels, and their effect on network operations.

The rest of this paper is organized as follows. Section 2 outlines the UMTS architecture. Section 3 presents an analysis of the security issues in 3G mobile systems focusing on the security requirements. Section 4 elaborates on the UMTS security architecture. Finally, section 5 contains the conclusions.

2 UMTS

UMTS refers to the European standardization efforts towards a new generation of mobile communication systems, where personal communication services will be supported independent of location, terminal equipment, means of transmission (wired or wireless), and underlying network capabilities. UMTS is intended to establish a single integrated system, in which users have seamless access to a wide range of new and sophisticated telecommunication services, such as high data rate transmission for high-speed Internet/Intranet applications, electronic multimedia mail, full-motion video, and electronic commerce.

UMTS is a realization of 3G mobile systems, which is compatible with the evolved Global System for Mobile communications (GSM) network [1]. The fundamental difference between GSM/GPRS (General Packet Radio Services) [27] and UMTS release '99 is that the latter supports higher bit rates (up to 2Mbps) [9, 10]. This is achieved through a new WCDMA (Wideband Code Division Multiple Access) radio interface for the land based communications system, named UMTS Terrestrial network Access Network (UTRAN) [12]. UTRAN consists of two distinct elements: a) Node B, which converts the data flows between the lu-b and Uu interfaces, and participates in radio resource management, and b) the Radio Network Controller (RNC), which owns and controls the radio resources of the Nodes B connected to it. The RNC is the service access point for all the services UTRAN provides to the core network. Fig. 1 depicts the UMTS release '99 network architecture.

While UMTS release '99 is a logical evolution

from the 2G+ system architecture, UMTS release 4 and release 5 (R4, R5) are revolutionary, introducing new concepts and advanced features [21, 22]. A major point of differentiation is the shift towards an all-IP network architecture that eventually replaces the circuit switched transport technologies, which are still used in UMTS release '99, by packet switched transport technologies. Another difference is the incorporation of an Open Service Architecture (OSA), which mandates that network operators provide third party access to their UMTS service architecture, thus, liberalizing the telecommunication service market. Furthermore, the multimedia support is built-in to the UMTS core network.

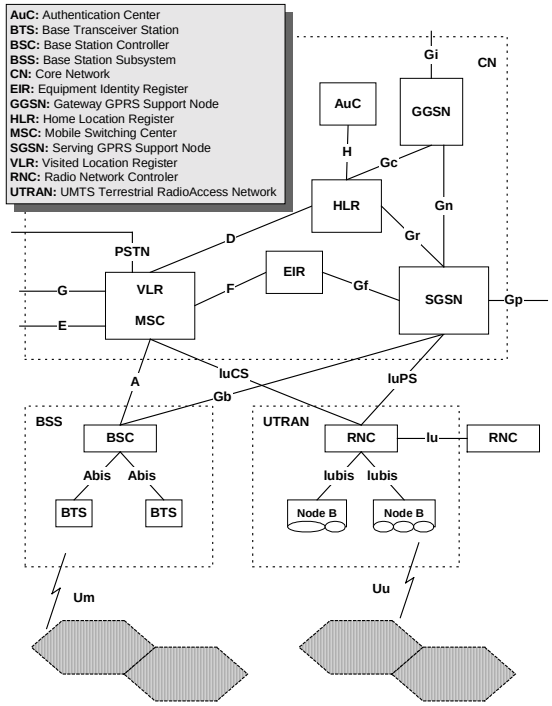

Fig. 1: UMTS release '99 system architecture

The UMTS network architecture evolution signifies not only a shift towards a common IP-based platform, which guarantees interworking with existing and forthcoming data networks, but also a shift towards an open and easily accessible network architecture. Consequently, from a security point of view, a whole new set of threats and risks must be faced.

3. Security Issues in 3G Mobile Systems

Security design in 3G mobile networks is a complex task, which requires the consideration of different parameters, such as the end-user mobility, the particular security threats, the type of information to be protected, and the network architecture. A brief description of the most important constituents of the mobile networks security context is given below.

3.1 Security principles

Although 3G mobile networks differ in nature from fixed terrestrial networks, its security measures should also support the following principles defined for traditional IP networking [13].

- **Confidentiality** ensures that certain information is never disclosed to unauthorized entities. Confidentiality is protected by the use of encryption and the enforcing of an access policy.
- **Integrity** guarantees that undetected modifications to the content of a packet in transit is not possible. A message could be corrupted due to radio propagation impairments, or due to malicious attacks on the network.
- **Authentication** enables a node to ensure the identity of the peer node with which it is communicating. Without authentication, an adversary could masquerade as a node, thus gaining unauthorized access to resources and sensitive information.
- **Availability** means that data or services are accessible to authorized subscribers when needed and without unnecessary delay. Availability can be compromised by any Denial of Service (DoS) attack, which aims at hampering a service.
- **Authorization** determines what the users are allowed to do. It allows network managers to determine which network services are available to different users, as well as permit user mobility.
- **Accounting** tracks what the users did and when they did it. It can be used for an audit trail or for billing for the connection time or the resources used.

3.2 Threats

Presently, a number of security threats to the mobile systems [15, 18] have been listed, such as unauthorized access to data and services, threats to integrity, DoS attacks, and repudiation. These attacks, which can also be classified into active or passive, might be attempted by individual "crackers", mobile network subscribers, or even network operator personnel. The term crackers refers to persons trying to break into the network from external IP-networks. Their intention is to cause harm to the mobile network, or steal information. Network subscribers may also present a threat to the network when, for example, are using a malfunctioning MS. Finally, statistics reveal that the operator's own personnel cause at least three fourths of system breakings. This does not mean that employees should not be trusted in general, but care has to be taken when allowing access rights to devices or applications.

3.3 Information classes

Different types of data require different types and levels of protection [15].

- **User data** comprise data content transmitted over end-to-end traffic channels. The security of this traffic type within the mobile network is the operator's responsibility.
- **Charging and Billing data** comprise data relating to charges incurred by users whilst using network resources and services.
- **Customer Information data** comprise the user location data, data relating to the user addressing, data determining the user identity, and data referring to the user profile.
- **Network Management data** comprise data relevant to the physical access of a mobile user to the network, data relating to the security management, such as encryption keys and message authentication, data referring to the network routing, and finally data needed to set up, maintain and release calls.

3.4 Security requirements

The main components in the communication model of 3G mobile systems are the mobile users, the Serving Network (SN), and the cooperative Service Providers (SPs). Particular security requirements are identified based on this discrimination.

A mobile user connected to a mobile network requires to be able to verify that the SN is authorized to offer services on behalf of the user's Home Environment (HE) at the start of, and during, the service delivery. All data exchange occurring between the mobile user and the SN or the SP must be protected against unauthorized modification. Moreover, the mobile user should be able to check whether data traffic and call-related info is confidentially protected. The end-user has also to be assured that no personal information, such as user identity or user location, is revealed to other individuals. From the SN point of view, any potential intruder should be prevented from obtaining unauthorized access to services by masquerading as an authorized user. It must be possible for the HE to immediately terminate all services provided to a certain user or group of users, if the latter brakes the service offering rules. The SN has to be able to authenticate the origin of user traffic, signaling, and control data, especially over the vulnerable radio interface. Moreover, the network has to protect the confidentiality as well as the unauthorized modification of user data, signaling and control data, which either reside in the network, or travel through it.

Finally, the SP has to authenticate the users at the start of, and during the service delivery, in order to prevent intruders from obtaining unauthorized access. Furthermore, the SP must be able to detect and prevent the fraudulent use of services (e.g., unauthorized access to data while being downloaded to an authorized user).

4. UMTS Security

3G-security is built on the security principles of 2G systems, with improvements and enhancements in certain points in order to provide advanced security services. The elementary security features employed in 2G, such as subscriber authentication, radio interface encryption, subscriber identity confidentiality, are retained and enhanced where needed. The main objective of 3G-security is to ensure that all information generated by or relating to a user, as well as the resources and services provided by the SN and the HE, are adequately protected against misuse or misappropriation. The level of protection will be better than that provided in the contemporary fixed and mobile networks. The security features shall be adequately standardized to ensure worldwide availability, interoperability, and roaming between different SNs. Furthermore, 3G-security features and mechanisms can be extended and enhanced as required by new threats and services. Fig. 2 gives an overview of the complete 3G-security architecture, illustrating five major security classes [24]:

- Network access security (I)
- Network domain security (II)
- User domain security (III)
- Application domain security (IV)
- Visibility and configurability of security (V)

In the sequel, we elaborate on these security classes.

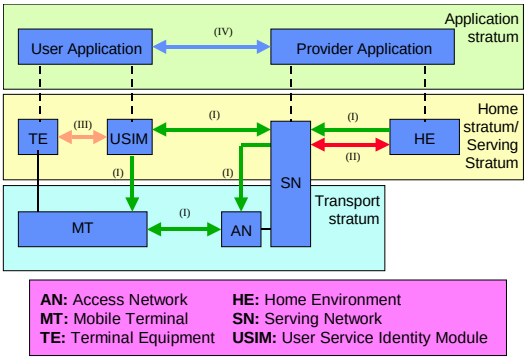

Fig. 2: UMTS security architecture

4.1 Network access security

This security class deals with the set of security features that provide users with secure access to 3G services, as well as protect against attacks on the radio interface [24]. Network access security takes place independently in each service domain.

User Identity confidentiality.
This mechanism allows the identification of a user on the radio access link by means of a Temporary Mobile Subscriber Identity (TMSI). A TMSI has a local significance only in the location area or the routing area, in which the user is registered. The association between the permanent and temporary user identities is stored in the Visited Location Register/Service GPRS Support Node (VLR/SGSN), in which the user is registered. To avoid user traceability, which may lead to the compromise of user identity confidentiality as well as to the user location tracking, the user should not be identified for a long period by means of the same temporary identity. Additionally, any signaling or user data that might reveal the user's identity are ciphered on the radio access link.

Authentication and key agreement
This mechanism achieves mutual authentication between the mobile user and the SN showing knowledge of a secret key K. The authentication method is composed of a challenge/response protocol (see Fig. 3), and was chosen in such a way as to achieve maximum compatibility with the GSM/GPRS security architecture facilitating the migration from GSM/GPRS to UMTS. Furthermore, the User Service Identity Module (USIM) [5] and the HE keep track of counters SQN_{MS} and SQN_{HE}, respectively, to support the network authentication. The sequence number SQN_{HE} is an individual counter for each user, while the SQN_{MS} denotes the highest sequence number that the USIM has accepted.

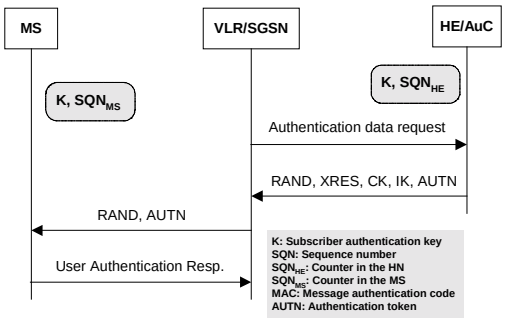

Fig. 3: 3G authentication and key aggrement

Upon receipt of a request from the VLR/SGSN, the HE Authentication Center (HE/AuC) forwards an ordered array of Authentication Vectors (AV) to the VLR/SGSN. Each AV, which is used in the authentication and key agreement procedure between the VLR/SGSN and the USIM, consists of a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK, and an authentication token AUTN.

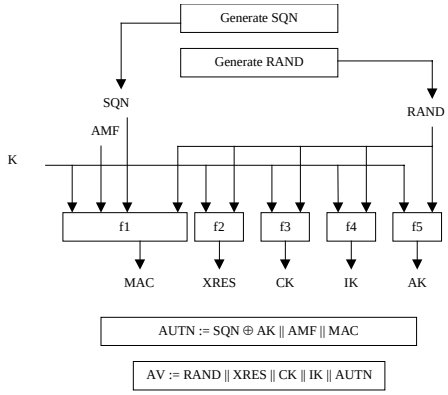

Fig. 4: Generation of authentication vectors

Fig. 4 shows an AV generation by the HE/AuC. The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND. Then, computes:

- The Message Authentication Code $MAC = f1_k (SQN \,||^1\, RAND \,||\, AMF)$, where f1 is a message authentication function, and the Authentication and key Management Field (AMF) is used to fine tune the performance, or bring a mew authentication key stored in the USIM into use [24, 26].
- The expected response $XRES = f2_k (RAND)$ where f2 is a (possibly truncated) message authentication function.
- The Cipher Key $CK = f3_k (RAND)$,
- the Integrity Key $IK = f4_K (RAND)$,
- and the Anonymity Key $AK = f5_K (RAND)$ where f3, f4 and f5 are key generating functions.
- Finally, the HE/AuC assembles the authentication token $AUTN = SQN \oplus^2 AK \,||\, AMF \,||\, MAC$.

When the VLR/SGSN initiates an authentication and key agreement procedure, it selects the next AV from the ordered array, and forwards the parameters RAND and AUTN to the user. The USIM first computes the AK

$AK = f5_K (RAND)$,

and retrieves the SQN

$SQN = (SQN \oplus AK) \oplus AK$.

Then, it computes $XMAC = f1_K (SQN \,||\, RAND \,||\, AMF)$, and checks whether the received AUTN and the retrieved SQN values can be accepted [24].

If so, the USIM computes the $RES = f2_K (RAND)$, and triggers the MS to send back a user authentication response. Afterwards, the USIM computes the CK

$CK = f3_K (RAND)$

[1] || Concatenation

[2] ⊕ Exclusive or

and the IK

$IK = f4_K\ (RAND)$.

The VLR/SGSN compares the received RES with the XRES field of the AV. If they match, it considers that the authentication and key agreement exchange has been successfully completed. Finally, the USIM and the VLR/SGSN transfer the established keys, CK and IK, to the entities that perform ciphering and integrity functions.

Integrity protection of signaling messages

The radio access interface in 3G mobile systems has been carefully designed to support integrity protection on the signaling channels, which enables the receiving entity (MS or SN) to be able to verify that the signaling data have not been modified in an unauthorized way since was sent. Furthermore, it ensures that the origin of the signaling data received is indeed the one claimed. The integrity mechanism also protects against network impersonation attacks, and prevents potential intruders to attempt to hijack connections where ciphering is not applied [18].

The function f9 is used to authenticate the integrity and the origin of signaling data between the MS and the RNC in UMTS. It computes a 32-bit Message Authentication Code (MAC) (see Fig. 5), which is appended to the frame, and is checked by the receiver. The main inputs to the algorithm are a 128-bit secret Integrity key IK, and the variable-length frame content MESSAGE. Additional inputs, which are used to ensure that MACs for two frames with identical content are different, are a 32-bit value COUNT, a 32-bit value FRESH and a 1-bit value DIRECTION. For the UMTS release '99, the f9 is based on the Kasumi algorithm [25, 17].

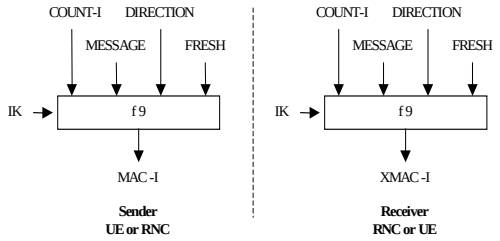

Fig. 5: Derivation of MAC on a signaling message.

Data confidentiality

User and signaling data, which are sent over the radio interface, are also subjected to ciphering using the function f8. The f8 is a symmetric synchronous stream cipher algorithm that is used to encrypt frames of variable length. The main input to the f8 is a 128-bit secret Cipher Key CK. Additional inputs, which are used to ensure that two frames are encrypted using different keystream, are a 32-bit value COUNT, a 5-bit value BEARER and a 1-bit value DIRECTION (see Fig. 6). The output is a sequence of bits (the 'keystream') of the same length as the frame. The frame is encrypted by XORing the data with the keystream. For UMTS release '99, f8 is based on the Kasumi algorithm [25, 17].

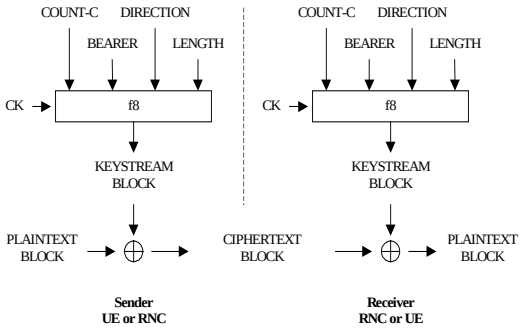

Fig.6: Ciphering over the radio access link.

4.2 Network domain security

Network domain security (NDS) [16] features ensure that signaling exchange within the UMTS core, as well as within the whole wireline network will be protected. Various protocols and interfaces are used for the control plane signaling inside, and between core networks, such as the protocols MAP (Mobile Application Part) [8], and GTP (GPRS Tunneling Protocol) [11], and the interfaces Iu and Iur (IuPS, IuCS) [9]. These will be protected by standard procedures based on the existing cryptographic techniques. Specifically, the IP–based protocols shall be protected at network level by means of IPsec [13], while the realization of protection for the SS7-based protocols and the lu and Iur interfaces shall be accomplished at the application layer. In the following, the NDS context for IP-based [16, 7] and SS7-based protocols [16] is presented. It is worth mentioning that the NDS has not been fully specified, while the security features for the lu and lur interfaces have not been specified at all.

IP-based protocol

The UMTS network domain control plane is sectioned into security domains, which typically coincide with the operator borders. Security Gateways (SEGs) are entities at the borders of the IP security domains used for securing native IP-based protocols. It is noted that the NDS does not extend to the user plane, which means that packet flows over the Gi [9] interface will not be protected by the SEGs. The key management functionality is logically separate from the SEG. Key Administration Centers (KACs) negotiate the IPsec Security Associations (SAs) [13] by using the Internet Key Exchange (IKE) protocol [14] in a client mode, on behalf of the Network Entities

(NEs) and the SEGs. The KACs also distribute SAs parameters to the NEs or the SEGs through standard interfaces. In Fig. 7 the UMTS NDS architecture for IP-based protocols is depicted.

To secure the IP traffic between two NEs, either a hop-by-hop or an end-to-end scheme may be applied. The first requires from the originating NE to establish an IPsec tunnel to the appropriate SEG in the same security domain and forward the data to it. The SEG terminates this tunnel and sends the data through another IPsec tunnel to the receiving network. The second tunnel is terminated by the SEG in the receiving domain, which in turn uses IPsec to pass the data to its final destination (path (a) in Fig. 7). The end-to-end scheme implies that an IPsec SA is established between the two NEs (path (b) in Fig. 7). This scheme can also be employed in case that the two parties belong to the same security domain.

Node authentication can be accomplished using either pre-shared symmetric keys or public keys [14]. Using pre-shared symmetric keys means that the KACs or the NEs do not have to perform public key operations, as well as that there is no need for establishing a public key infrastructure. The IPsec protocol can be configured either in transport mode or in tunnel mode [13]. Whenever at least one endpoint is a gateway, then the tunnel mode should be used. However, the tunnel mode provides source and destination address confidentiality, which is incompatible with the use of NAT [19]. This can be a problem in IPv4 networks, since address space is scarce and NAT is a common way of solving the address space problem. Finally, the IPsec protocol shall always be Encapsulation Security Payload (ESP) [20], given that it can provide confidentiality and integrity protection as well.

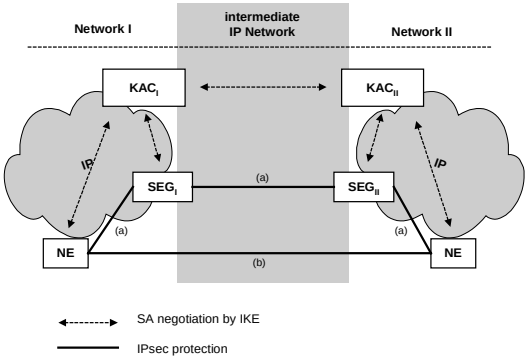

Fig. 7: NDS architecture for IP-based protocols

SS7-based protocols

This section describes the NDS architecture for SS7-based protocols, which are also referred as legacy protocols. Security mechanisms for these protocols are mainly found at the application layer. Specifically, in case that the transport for a legacy protocol is based on SS7, or on a combination of SS7 and IP then, the security shall be provided at the application layer. On the contrary, whenever the transport is based on IP only, then, security may be provided at the network layer exclusively, or in addition to the application layer security, by using IPsec [13]. For signaling data protection at the application layer the necessary SAs will be network-wide and they are negotiated by KAC, similarly to the IP-based architecture (see Fig. 8). End-to-end protected data will be indistinguishable to unprotected traffic, to all parties except for the sending and receiving sides.

It is worth mentioning that in R4 the only legacy protocol that is to be protected is the MAP [8]. The complete set of enhancements and extensions that facilitate the MAP security is termed MAPsec [6]. The MAPsec covers the transport security of the protocol itself, as well as the security management procedures. The MAPsec security services include: data integrity, data origin authentication, anti-reply protection and confidentiality. Finally, for IKE adaptation a specific Domain of Interpretation (DoI) is required.

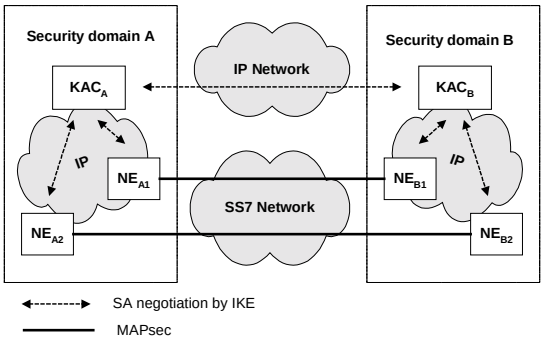

Fig. 8: NDS architecture for SS7 and mixed SS7/IP-based protocols

4.3 User domain security

User domain security [24] ensures secure access to the MS. It is based on a physical device called UMTS Integrated Circuit Card (UICC), which can be easily inserted and removed from terminal equipment, containing security applications such as the USIM [5]. The USIM represents and identifies a user and his association with a HE. It is responsible for performing subscriber and network authentication, as well as key agreement, when 3G services are accessed. It may also contain a copy of the user's profile.

The USIM access is restricted to an authorised user, or to a number of authorised users. To accomplish this feature, the user and the USIM must share a secret (e.g., a PIN). The user gets access to the USIM only if he proves knowledge of the secret.

Furthermore, access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret. If a USIM fails to prove its knowledge of the secret, then, access to the terminal is denied.

4.4 Application domain security

Application domain security [24] deals with secure messaging between the MS and the SN or the SP. USIM Application Toolkit, as specified in [4], provides the capability for operators or third party providers to create applications that are resident on the USIM. This requires secure message exchange over the network with the level of security chosen by the network operator or the application provider. USIM Application Toolkit security is implemented by means of mechanisms described in [3] and supports entity authentication, message authentication, replay detection, sequence integrity, confidentiality assurance and proof of receipt. Although these mechanisms address the security requirements identified in [2], further work is required to identify potential enhancements such key management support, increase flexibility in algorithm choice, etc. [24]

4.5 Security visibility and configurability

Although the security measures provided by the SN should be transparent to the end user, for certain events and according to the user's concern visibility of the security operation as well as the supported security features should be provided. This may include: a) indication of access network encryption; b) indication of network wide encryption; and c) indication of the level of security (e.g., when a user moves from 3G to 2G).

Configurability is the property that enables the mobile user and the HE to configure whether a service provision should depend on the activation of certain security features. A service can only be used when all the relevant to it security features are in operation. The configurability features that are suggested include: a) enabling/disabling user-USIM authentication for certain services; b) accepting/rejecting incoming non-ciphered calls; c) setting up or not setting-up non-ciphered calls; and d) accepting/rejecting the use of certain ciphering algorithms.

4.6 Network-wide confidentiality

Network-wide confidentiality is an option that provides a protected mode of transmission of user traffic across the entire network. It assures that users data are protected against eavesdropping on every link within the network, and not only on the vulnerable radio links. When network-wide confidentiality is applied then, access link confidentiality on user traffic between the UE and the RNC is disabled avoiding replication. However, the access link confidentiality for signaling information as well as user identity retains to facilitate the encryption establishment. Network-wide confidentiality uses a synchronous stream cipher similar to the access link encryption algorithm. In Fig. 9, the network-wide encryption deployment is depicted.

Initially, a data channel is established between the communicating peers indicating also the intention for network-wide encryption. VLRa and VLRb exchange cipher keys (Ka and Kb) for user a and b correspondingly using cross boundaries signaling protection and then, pass them to the MSs over protected signaling channels. When each MS has received the other party's key, the end-to-end session key, Ks, is calculated as a function of Ka and Kb. Alternatively, The VLRs can mutually agree on the Ks using an appropriate key agreement protocol. Both key management schemes satisfy the lawful interception requirement, since Ks can be generated by the VLRs.

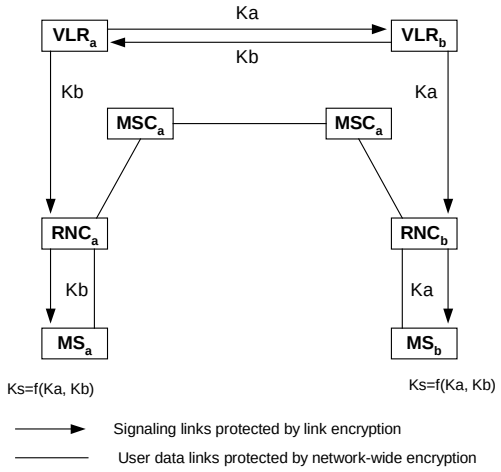

Fig. 9: Network-wide encryption deployment

4.7 Future work

Although the major points in the UMTS security architecture have been adequately outlined in the context of 3GPP, there are some security features that have not been standardized yet, and there are some others that are in a preliminary stage. Specifically, the NDS for legacy protocols, which currently supports only the MAP protocol, should be enhanced to address security for the entire set of the employed protocols and interfaces. The user identity confidentiality has to be upgraded with a mechanism that protects the user identity against active attacks on the radio interface. The network wide confidentiality feature needs to be standardized and incorporated in a specific UMTS release. Furthermore, special attention has to be considered in the security interopera-

tion in cases that a mobile user roams between UMTS and GSM/GPRS.

Eventually, regardless of the security level that a UMTS network supports, the evolution, and the standardization activities for the UMTS security architecture will continue towards the provision of advanced security features that will address the enhanced service requirements, and will confront the new emerging security threats.

5. Conclusions

Security is a primary concern in the evolving mobile communication systems. In this paper, we have overviewed the UMTS security framework. The principles that should be followed in the security architecture design have been presented, and the potential attacks as well as the intruders that may threaten network operation have been outlined. The security requirements imposed by the different types of traffic, and by the different players involved (mobile users, SN and SPs) have been investigated. Furthermore, the UMTS security architecture, as it is developing in 3GPP, have been elaborated with emphasis on the various security mechanisms and protocols.

The UMTS is being designed to provide higher level of protection than that provided by contemporary fixed and mobile networks. The security architecture supports a high degree of granularity, which facilitates continuous evolution of the security functionality to deal with the new emerging threats and services. It comprises five individual security classes: a) access network security, b) network domain security, c) user domain security, c) application domain security, and e) visibility and configurability of security. Additionally, a network-wide encryption/confidentiality is a potential option that will provide end-to-end protection on the user traffic channel between the communicating MSs.

References

[1] M. Mouly and M.B. Pautet, The GSM System for Mobile Communications, 1992.

[2] GSM 02.048, Security mechanisms for the SIM Application Toolkit; Stage 2, 1999.

[3] 3GPP TS 23.048 (v4.2.0) “Security Mechanisms for the (U)SIM application toolkit; Stage 2”, release 4, Dec 2001.

[4] 3GPP TS 31.111 (v3.7.0) “USIM Application Toolkit (USAT)”, release ‘99, Dec 2001.

[5] 3GPP TS 21.111 (v3.3.0) “USIM and IC card requirements”, release ‘99, Oct 2000.

[6] 3GPP TS 33.200 (v4.2.0) 3G Security; Network Domain Security; “MAP application layer security”, release 4, Dec 2001.

[7] 3GPP TS 33.210 (v1.0.0) “3G Security; Network Domain Security: IP network layer security”, release 5, Dec 2001.

[8] TS 29.002: "Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification".

[9] 3GPP TS 23.002 (v3.5.0) “Network Architecture”, release ’99, Jan 2002.

[10] 3GPP TS 22.100 (v3.7.0) “UMTS phase 1 Release 99”, release ’99, Oct 2001.

[11] GSM 09.60 GPRS, GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface, 1998.

[12] 3GPP TS 25.401 (v3.8.0) “UTRAN Overall Description”, release ’99, Sept 2001.

[13] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 2401, Nov. 1998.

[14] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, Nov 1998.

[15] 3GPP TS 21.133 (v3.2.0) 3G Security “Security Threats and Requirements”, release ’99, Dec 2001.

[16] 3GPP TR 33.800 “3G Security; Principles for Network Domain Security”, release 4/5 Oct 2000.

[17] 3GPP TR 33.908 (v3.0.0) “3G Security; General report on the Design, Specification and Evaluation of 3GPP Standards Confidentiality and Integrity Algorithms”, release ’99 March 2000”.

[18] 3GPP TR 33.900 (v1.2.0) A Guide to 3G Security; Jan 2000.

[19] Phifer, L., "The Trouble with NAT" Cisco, The Internet Protocol Journal, Vol 3, No 4 Dec 2000.

[20] S. Kent and R. Atkinson, “IP Encapsulation Security Payload (ESP)” RFC 2404, Nov. 1998.

[21] 3GPP TS 23.002 (v4.4.0) “Network Architecture”, release 4, Jan 2002.

[22] 3GPP TS 23.002 (v5.5.0) “Network Architecture”, release 5, Jan 2002

[23] 3GPP TS 23.101 (v3.1.0) General UMTS Architecture, Dec 2000.

[24] 3GPP TS 33.102 (v3.10.0) 3G Security Security Architecture”, release ‘99, Dec 2001.

[25] Steve Babbage, “Design of Security Algorithms for Third Generation Mobile Telephony” Elsevier Science, Information Security Technical Report, Vol.5, No. 3, 2000

[26] Colin Blanchard, “Security for Third Generation (3G) Mobile Systems” Elsevier Science, Information Security Technical Report, Vol.5, No. 3, 2000

[27] GSM 03.60, GPRS, Service Description, Stage 2, 1998