Annales UMCS Informatica AI XI, 3 (2011)
141–153; DOI: 10.2478/v10065-011-0016-5

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI
http://www.annales.umcs.lublin.pl/

Mobile identity management system in heterogeneous wireless networks

Łukasz Kucharzewski*, Zbigniew Kotulski†

Institute of Telecomunications, Faculty of Electronics and Information Technology, Warsaw University of Technology, Nowowiejska 15/19, 00-665 Warsaw, Poland

Abstract

Heterogeneous wireless networks increasingly encroach on our lives. Various technologies and mobile applications more often than usual are now used by mobile users. Intensive development of mobile networks not only sets new standards for radio, but increasingly focuses on providing security for traffic transmitted in wireless networks. Security in wireless networks has never been the primary objective of the designers of new network standards. The reason for this fact were both low hardware resources of equipment, but also lack of awareness of users about the potential vulnerabilities. Creating a secure, independent of network architecture solutions effectively raising the level of security of transmitted data between end users is the main priority of our research. Current wireless security solutions do not provide sufficient protection of the integrity, confidentiality of data, are not designed to operate in heterogeneous networks, or are too complex to implement. Both networks WiMAX, LTE and WiFi, there are methods that protect the resources in these networks, but they are not consistent with each other. The proposed security system requires the use of mobile version of the PKI to verify the identity of mobile users. Mobile PKI center is an innovative solution, not yet introduced for casual use. Such a solution in heterogeneous wireless networks is a fast, secure and transparent to transmission medium. Designing secure and efficient authentication protocols to enable

*E-mail address: l.kucharzewski@tele.pw.edu.pl
†E-mail address: zkotulski@tele.pw.edu.pl

fast connections to the heterogeneous network is challenging. In the proposed system in this paper, the users authenticate their identity digital certificates that are issued by a trusted third party (CA). PKI uses the algorithms based on elliptic curves. Advantages of elliptic curves in mobile environment will be particularly evident. This ensures adequate protection of data in a heterogeneous networks. In this system, it is possible to implement many new secure services for end users secure email, secure chat, secure remote access.

1. Mobile Access Networks

Currently, nearly 4 billion active subscribers using mobile services, constitute 85% . Mobile networks development introduced more new services and solutions. The main determinant of the development of such networks, has become the speed of data transfer. The first generation of wireless (1G) was focused primarily on analog voice transmission. Digital Networks second generation (2G) increased bandwidth to offer a better quality of voice transmission. Developing some standards also allowed to use the phone while roaming abroad. 2G networks became popular in the two standards: GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access). Both standards were developed primarily for voice transmission. In the subsequent amendment of the systems data transmission were extended. In the early stages transmission was at the level of dial-up connections. The next steps of the evolution of mobile communications were directed to the transition to 3G. However, the first standards do not provide a system of assumptions about the data. Actual data transfer speed was much lower than that previously expected. Only for the project 3GPP2 HRPD system (High Rate Packet Data) [1] the presented sophisticated method of optimizing the radio channel aimed at increasing the transmission speed (CDMS2000-1xEVDO (Evolution Data Only)). In parallel, 3GPP introduced a draft standard for HSPA (High Speed Packet Access) [2] based on WCDMA. Standard HSPA contained an almost identical list of fixes in a radio channel with HRPD. Allowing for the simultaneous transmission of voice and data in a common transmission channel with a width of 5 MHz. Both of these standards have become commonplace and are used in wireless access. During the further development and implementation of standards and HRPD HSPA, IEEE 802 committee LMSC (LAN / MAN Standard Committee) presented the IEEE 802.16e [3]. This standard was the development of the current 802.16 standard already nomadic. Standard 802.16e assumed different OFDMA modulation methods (Orthogonal Frequency Division Multiple Access). Frequency division access by multiple users is implemented by assigning different users different subchannels. Compared with HSPA and HRPD the networks offer greater speed incoming data and spectral efficiency. Although the

IEEE 802.16 standard is officially called WirelessMAN IEEE, WiMAX Forum group changed its name to WiMAX (Worldwide Interoperability for Microwave Access). Simultaneously with the development of WiMAX network, another 'future' standard mobile network is being developed. LTE (Long-Term Evolution) is presented as the successor to the standard of WCDMA / HSPA. Current radio technology provides, inter alia, much higher speed data transfer, low latency and greater number of services offered.

2. Authentication process in mobile networks

In order to protect communications data in the telecommunication networks from unauthorized access, we have to use multiple advanced access methods. In addition to firewalls and IDS (Intrusion Prevention System) systems, the processes of authentication, authorization, and accounting are very important. They are often called AAA (Authentication, Authorization, Accounting). They are closely linked. One of the most critical elements of the system is the authentication process. Authentication is an ability for communicationg parties, including network operators and users, to validate each other's authentic identity. In the following chapter I the authentication methods in the mobile networks: WiMAX and LTE are presented.

2.1. Authentication in WiMAX.

Reffering to the ISO/OSI model,
WiMAX standard is located in the first two layers: the physical layer and the medium access layer MAC transmission. Advanced radio techniques have been implemented at the physical layer [5]. The WiMAX security architecture has been defined in a special sublayer - Security Sublayer. Already at the stage of its design, it focuses on avoiding the mistakes that were committed in another mobile standard - 802.11. This layer focuses on specific mechanisms responsible for authentication, integrity and confidentiality of transmitted data sites involved in the transmission. Parties involved in the transmission are the SS -Subscriber Station and BS - Base Station. Information necessary for safe data transmission is implemented in the Security Association. The security aspect in 802.16 standard is based primarily on the PKM protocol [9]. This protocol is used in the process of logging equipment for the network and authenticates the client. The modified version of PKM protocol version of the second stage of authentication uses EAP (Extensible Authentication Protocol). PKM protocol operates in the client/server system where the terminal sends a request to the base station allocation of keys, or update them. Among the keys used by the PKM protocol, there can be distinguished:

- **Terminal Public Key:** the key system is used by the subscriber station SS during the initial authorization process. The base station BS uses it to encrypt the authorization AK key. Most keys are generated using the RSA algorithm.
- **AK - Authorization Key:** Key used for authentication. It activates the base station for each SS and sends an authenticated secure channel to the SS (160 bits). Lifetime between 1 and 70 days.
- **KEK - Key Encryption Key:** This 3-DES key is derived from the AK and is used to encrypt the transmission of TEK encryption keys (128 bits).
- **Keys HMAC_KEY_U and HMAC_KEY_D:** These keys are derived from the AK and the key is used to verify the authenticity of the message system (downlink and uplink direction) (160 bits).
- **TEK - Traffic Encryption Key:** The key is used to encrypt the data on the network (128 bits). Lifetime between 30 min and 7 days.

The authorization process is initiated by the subscriber station SS. Each such device has a unique X.509 digital certificate, generated during the production phase of the terminal. The certificate consists of the RSA public key and MAC address. After identifying the network and making preliminary procedures, the terminal starts the process of authentication to the network. This process involves authenticating the terminal base station certified by its authenticity and delivered to the authorization key AK. The authorization process begins from the base station using two consecutive messages:

(1) **Authentication Information:** This is a message containing only pure X.509 digital certificate of the terminal.
(2) **Authorization Request:** This is a request to the base station for an authorization terminal. This message contains a digital certificate, but also information on the cryptographic algorithms that can operate the terminal.

Upon receiving the second message by the base station, it is checked whether the terminal has the right to use the network. For this purpose, it is used for X.509 certificate sent in Authorization Request. If the terminal is authorized to use the network, the base station sets to the terminal algorithms which will be used to encrypt the traffic, generate the AK key and send this information to the terminal in an Authorization Request message. When the terminal receives this message it is authorized to the network. The authorization process must be periodically renewed. Renewal of the authorization process itself is almost identical, differ only in that the terminal does not send Authentication Information messages any more. The exchange of these messages does not allow full use of

the network. The authorizes only terminal in the network. After this process, the terminal, holding a AK key, must apply to the base station for it to activate the encryption TEK key. This process is done by sending the Key Request message to the base station. After receiving it, the base station checks again whether the terminal is authorized to the network, and then activates the TEK key for terminal and encrypts the key using the KEK key derived from AK. It then sends the key TEK to the terminal in the Key Reply message feedback. Only after receiving this message and obtaining the encryption transmission key it has the right to use network resources. Like the key AK, the TEK key must also be renewed. The TEK key is used for encryption. The encryption algorithm in the basic version is DES in the CBS mode. It is also possible to use AES in the CCM mode, but this algorithm is not typically implemented on devices. Only MAC PDU (Pocket Data Unit) is encrypted. Their headers are not encrypted. The process of authentication in the WiMAX networks is implemented using public key infrastructure. In this way, they also generate encryption keys. The extended version of the PKM protocol is defined in the 802.16e standard (Privacy Key Management v2). PKMv2 defines the following types of authentication:

- Authentication protocol based on RSA (Rivest-Shamir-Adleman). In this model, the base station BS, authenticates the client workstation SS, using X.509 digital certificates assigned to the mobile terminal at the manufacturing stage. This certificate contains the public key of SS and the MAC address. To get the AK key, SS sends the certificate to the base station, which after checking it encrypts the AK key and sends back to the device. All mobile devices (SS's) must be uploaded of a pair of keys and X.509 certificates, generated by the SS manufacturer.
- Authentication based on EAP (Extensible Authentication Protocol). In this model, the mobile terminal is authenticated using the additional, unique information defined by the operator (SIM card, X.509 certificate, etc.). Among them there can be distinguished:
  (1) EAP-AKA (Authentication and Key Agreement) for the methods of using the smart card (SIM / USIM)
  (2) EAP-TLS (Transport Layer Security)for the methods of using X.509 digital certificates
  (3) EAP-TTLS (Tunnelled Transport Layer Security) for the authentication method SS-CHAPv2 (Microsoft-Challenge Handshake Authentication Protocol)
- Authentication based on EAP, preceded by the RSA authentication protocol

2.2. Authentication in LTE.

LTE standard is called the system "almost 4th generation", which is the successor to UMTS / HSPA. LTE is not the 4G system because it does not meet all requirements set by the ITU (International Communications Union) 4G/IMT-Advanced technology [21]. 3GPP Group (Third Generation Partnership Project) has created certain requirements of the LTE standard, which should be fulfilled. By creating an LTE system it focuses primarily on reducing the cost of a single bit rate, the implementation of new mobile services and better use of radio bandwidth, while minimizing the level of energy consumed by the device. Its implementation, e.g. in the WiMAX networks, will completely switch to packet traffic based on IP in the mobile networks. LTE introduces an entirely new architecture, and security key management hierarchy, resigns from their present SIM (Subscriber Identity Module in English), and introduces a USIM (Universal Subscriber Identity Module) card. They use 128-bit key, expandable to 256 bits. The extended hierarchy keys used in the LTE allow for faster generation and in the process of refreshing keys to switch between broadcasting stations, included in the 2G/3G network. The following figure illustrates these structure keys (Fig. 1).

The user authentication process is done using the AKA mechanism (Authentication and Key Agreement) between the UE (User Equipment) and MME (Mobility Managemnet Entity) [21]. The additional module ASME (Access Security Management Entity), deployed with the MME is responsible for protecting the signalling NAS (Network Access Server or Nonaccess Stratum).The process of encryption and data integrity checking is done using AES and SNOW 3G. The keys used to protect the NAS are located separately and are in the eNB (E-UTRAN nodeB) and EPC (Evolved Packet Core). ASME module receives a K_{ASME} key necessary in the process of authentication with the UE. ASME forwards the key to the MME, and sends the generated keys obtained from K_{ASME} to the eNB. The keys K_{NAS} and K_{eNB} obtained from K_{ASME}, do not leave the EPC. The keys K_{eNB-UP} and $K_{eNB-RRC}$ are obtained from K_{eNB}, eNB and the UE. When the UE enters into the sleep mode, these keys are removed. The K_{NAS} keys are used to protect NAS communications and encryption. K_{eNB-UP} key is used to secure communications U-Plane, the key $K_{eNB-RRC}$ is only used to protect traffic RRC (Radio Resource Controller). If the keys are corrupt (damaged), the UE carries out a re-negotiation.

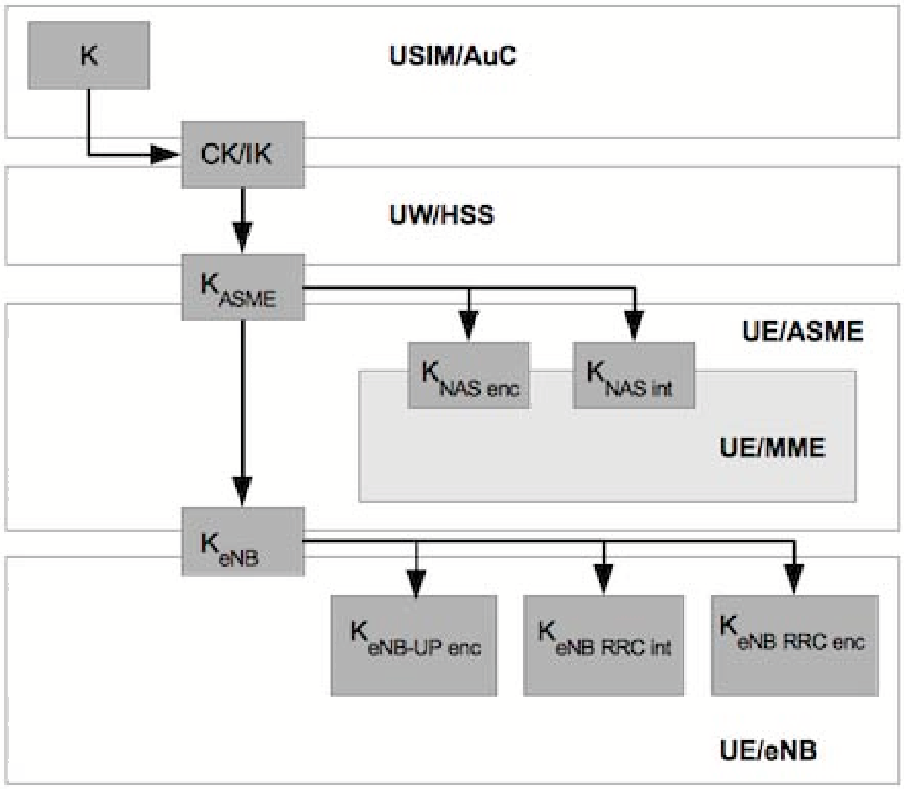

FIGURE 1. Keys structure in the LTE networks

3. The proposed Authentication system using mobile PKI

In connection with the influx of new services (eCommerce, eVoting, eTicketing, stock trading, gambling..etc) in mobile networks, there is a need to implement additional security mechanisms. There are many possibilities to implement authentication mechanism and digital signatures, including a static user ID and password, smart cards and cryptographic tokens (two-factor authentication). The quality of solutions is identified not only by the implemented mechanisms but also by the ease of use for the end user. The proposed additional security in communication between users of mobile, heterogeneous system is based on the mobile PKI [25]. Mobile PKI is a technology that shows great potential in its ability to authenticate users of mobile systems. It provides the high level of security and relatively user-friendly manner. In the proposed system, the mobile PKI may use the SIM /USIM cryptographic modules, which are

commonly used by telecommunication operators to store confidential information or use the internal, secured resources of the terminal. A great advantage of Mobile PKI is that almost everyone used the mobile terminal and that almost all of these mobile devices are suited for Mobile PKI. A second advantage is that Mobile PKI is a standardized technology, which benefits both the security and the interoperability. Currently, there are a few isolated mobile solutions using the mobile PKI [18, 19]. They work, however in a limited, closed environment. The system model presented here is independent of network architecture. It is designed for each user in the mobile system, regardless of the radio system and OS. It assumes the use of an external trusted CA and presents the private key distribution model to the end user (SS) and secure storage of those digital certificates on the mobile terminals. The system is designed to operate on mobile devices, regardless of the network and radio technology they work. Mobile terminals can be used in this system, both in authentication and digital signing process. All end user need is a digital certificate. This certificate can be stored on the USIM card (Java Cryptographic Cards) or on another internal, encrypted disk resource. Access in both cases is additionally protected by a PIN code. The private key is stored on the end user side (SS) and the digital certificate is stored on the external, trusted directory server. Certificates stored in the external directory server contain only a public part of the user's certificate. Public and private keys are strictly dependent on each other. The main challenge here is to secure distribution of private key to the end user (only during generation of keys outside the mobile terminal). The system assumes that the mobile PKI will be independent of the operator. Then the problem of verification and access to certificates for the users of different radio systems does not occur. However, it will work and cooperate with mobile operators.
The system can distinguish two ways of obtaining a digital certificate:

- The certificate is loaded on the USIM card in the external distribution centers. The process of key generation and verification is done by using an external point of registration and verification of the DP (Distributed Point).
- There is also the possibility of generating a certificate directly from the device. The mobile subscriber using the secure communication channel (SSL) logs in on the external mobile CA website. Next digital certificate typing all required information (personal data, MSISDN) starts. The keys are generated on the device. During this process the user defines a personal PIN. The private key never leaves the device. The user sends the generated public key (using the special application) to a trusted CA for signing. The CA public key is signed by the user

and returns to the DP. After the successful verification and authorization process in DP the user receives a signed public certificate. Next DP sends information to CA about the finished enrollment process. CA updates the external certification repository.

The enrollment process is initiated by the external security operator (same which holds External Mobile CA)(Fig. 2). The operator service for mobile certificate enrollment is available at Distributed Point. Authorization to use the enrollment service is based on the external Distributed Point of a valid certificate issued by the external trust centre service (CA). These authentication certificates will be issued in advance to Distributed Points. Those certificates will be in the form of software tokens. External Operator CA generates random PINs in advance and prints them in the PIN letters. Envelopes will be distributed to the DP. PINs will be have limited validity for security reasons. All PINs have unique labels. All PINs and labels are registered at the External Mobile CA. Each user, who wants to use his mobile terminal as a device

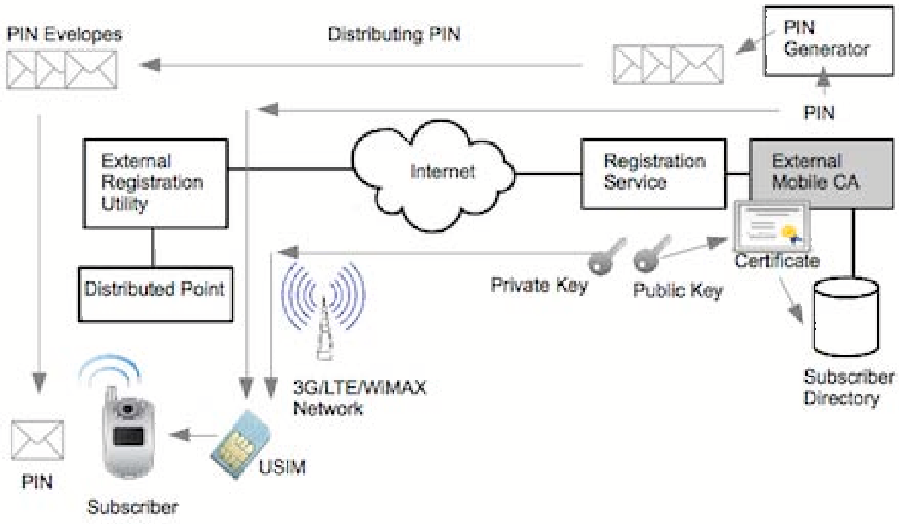

FIGURE 2. Enrolment scenario for the trust worthy enrolment of mobile PKI credentials

for authentication and digital signing needs to visit certified DP for the enrollment procedure. A worker in DP logs on using the software token. Security is guaranteed by the challenge-response authentication process. A worker in DP randomly selects a PIN envelope from stock and enters the identity data of a new user and the label of the envelope in the External Registration Utility (ERU). ERU generates an asymmetric key pair and requests a certificate from

the External Mobile CA. CA generates the certificates with all identity data included. CA returns the PIN associated with the label on the PIN envelope to the DP. This PIN will never be visible by the DP workers. Next the DP worker connects the USIM card to the ERU using a special terminal. Next ERU writes a private key to the USIM and sets PIN, which protects the private key from unauthorized use. The USIM card and the selected PIN envelope will be handed over to the end user to complete this process. Only the subscriber in possession of the envelope is the only person who knows the PIN. At he end, ERU confirms the enrollment process to the CA, which publishes the certificate in an external directory. From now on the mobile subscriber can use his mobile phone in a secure way for services and transactions that require authentication or a digital signature. Secure transaction using the mobile terminal can now be performed in the following way (Fig. 3). The user connects to the requested service over the mobile network using mobile application installed on the device. The server connects to a validation server to authenticate the mobile user. A challenge response protocol will be performed between the validation server and the mobile device. The server sends a random challenge number to the phone, which activates the SIM card's signature function. The user confirms operation typing his private PIN number. Then the mobile device signs the challenge number using the private key. The signature and the subscriber's certificate will be returned to the validation server. The server checks the revocation status with the external mobile CA. If validation is OK, the server sends confirmation to the service. The service grants access to the mobile subscriber. Commitment signatures can be handled in a very similar way. Challenge is replaced by the data to be signed. The validation server can be located in the mobile network operator or the service provider. In Fig. 4 the mobile terminal can be

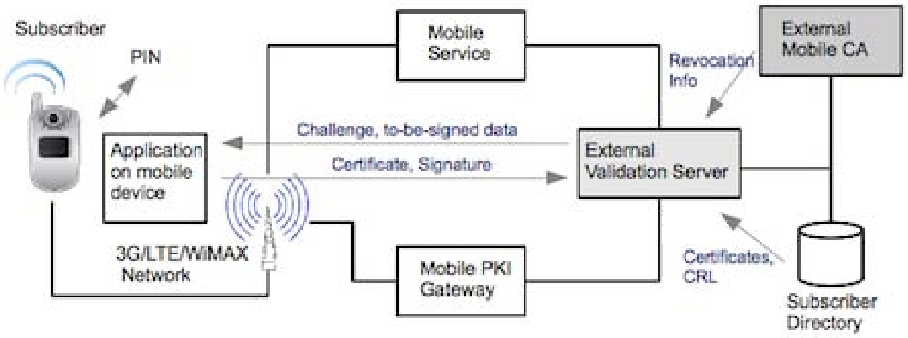

FIGURE 3. Validation scenario for the mobile PKI-based authentication by a smart phone application

used as a secure signature creation device for authentication and digital signing process performed on a PC. The user using PC connects to a service provider's application. The application requests to perform authentication process using a mobile terminal.Challenge-response authentication is then performed between the validation server and the mobile terminal. Afer successful validation, the user's identity is passed to the application. Then the user can enter the service.

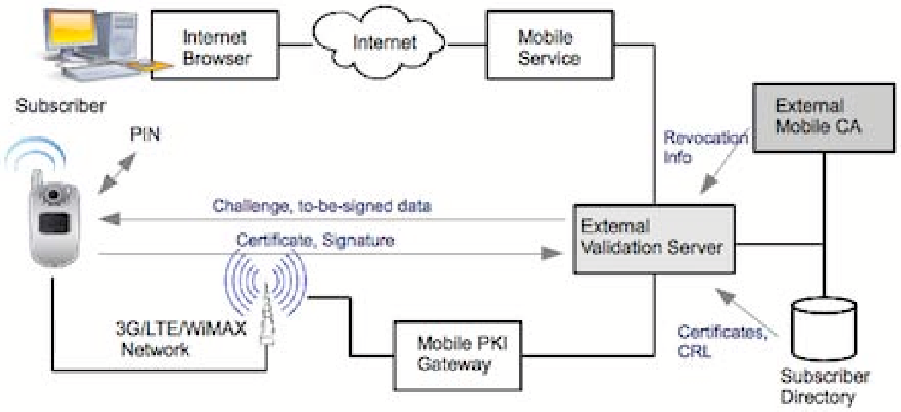

FIGURE 4. Mobile terminal as a secure signature creation device

3.1. Cryptography.

Mobile PKI presented in this paper (Chapter 3) uses Elliptic Curve Cryptography (ECC) [20]. The encryption algorithm that uses elliptic curves is increasingly used, but has never been presented with the mobile PKI in the heterogeneous wireless networks. The importance of such an application of cryptography as it grows with the same key length, is more security (the fracture requires more calculations) in comparison with RSA. Implementation of encryption algorithms based on the elliptic curves is well suited for the use in mobile solutions (smart cards, mobile terminals) where the issue of energy management and the speed of encryption are very important. ECC is much more efficient compared to the traditional method based on the RSA protocol, has a lower demand for resources (memory, energy), and the encrypted data blocks with ECC are smaller than RSA, by which transmission of such data in the network is faster.

4. Conclusions

Enormous development of telecommunication networks that we are witnessing, leads to the development of new technologies and services provided by this route. More and more people use mobile access devices that encrease its functionality and capabilities similar to desktops. In this paper we have presented an overview of authentication methods and key management solutions in the WiMAX and LTE networks. We also proposed a draft for a secure system based on mobile PKI and Eliptic Curve Cryptography. Mobile PKI using public key cryptography with ECC tries to solve the problem of security mobile devices in the heterogeneous wireless networks (WiMAX, LTE, UMTS). This solution seems to be appropriate, where power consumption and bandwidth are limited.

Acknowledgement: Research reported in this paper was partially supported by the 7FP NoE EuroNF project.

References

[1] 3GPP2 TSG C.S0024-0 v2.0, cdma2000 High Rate Packet Data Air Interface Specification
[2] 3GPP TSG RAN TR 25.848 v4.0.0, Physical Layer Aspects of UTRA High Speed Downlink Packet Access.
[3] IEEE Std 802.16e-2005,Air Interface for Fixed and Mobile Broadband Wireless Access Systems
[4] Li H., Fan G., Qiu J., Lin X., GDKA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security, Department of Electronic Engineering, Tsinghua University, Beijing, China, Intel China Research Center, Beijing, China, Graduate School at Shenzhen, Tsinghua University, Shenzhen, Guangdong, China
[5] IEEE 802.16e-2005, IEEE Standard for Local and metropolitan area networks-Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands (2005).
[6] Shon T., Choi W., An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, NBiS'07, (2007): 88-97
[7] Andrews J., Ghosh A., Muhamed R., Fundamentals of WiMAX Understanding Broadband Wireless Networking, Prentice Hall (2007).
[8] Zhang Y., Handbook of Research on Wireless Security, Idea Group Publishing (2008).
[9] Ahson S., Ilyas M., WiMAX Standards and Security, Aurebach Publications, Taylor & Francis Group (2008).
[10] Ergen M., Mobile Broadband Including WiMAX and LTE, Springer (2009).
[11] Huijie L., Guangbin F., Jigang Q., Xiaokang L., GDKA: A Group-Based Key Distribution Algorithm for WiMAX MBS Security, Springer-Verlag, Berlin (2006).
[12] Hasan J., Security Issues of IEEE 802.16 (WiMAX), School of Computer and Information Science, Edith Cowan University, Australia.
[13] Zhang Y., Handbook of Research on Wireless Security, Idea Group Publishing (2008).

[14] Kucharzewski Ł., Kotulski Z., Sieci WiMAX – architektura i bezpieczeństwo danych, Konferencja IBIZA (2009).
[15] Taeshik S., Wook C., An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions, Springer-Verlag, Berlin (2007).
[16] Zawadzki P, Podsystem bezpieczeństwa sieci WiMAX, Przeglład Telekomunikacyjny (2-3) (2007): 67-72.
[17] Mobile PKI Security Potential, Challenges and Prospects, Technology Nexus AB, January (2010).
[18] http://www.peak-solution.de/
[19] http://www.corisecio.com/
[20] Hankerson, Darrel, Menezes, Alfred J., Vanstone, Scott, Guide to Elliptic Curve Cryptography, Springer Professional Computing (2004).
[21] Khan F., LTE for 4G Mobile Broadband, Air Interface Technologies and Performance, Cambridge university Press (2009).
[22] Chen J-C., Zhang T., IP-based Next-Generation Wireless Networks, System, Architectures, and Protocols, Wiley-Interscience, John Wiley & Sons (2004).
[23] Jeffrey Hoffstein J., Pipher J., J.H. Silverman, An Introduction to Mathematical Cryptography, Springer (2000).
[24] Kucharzewski Ł., Kotulski Z., Mobilne sieci przyszłości - architektura i bezpieczeństwo WiMAX i LTE, Przegład Telekomunikacyjny i Wiadomości Telekomunikacyjny, Tom LXXXIII, Numer 8-9, (2010): 919 - 928.
[25] Lee Y., Lee J., Song J., Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce, Computer Communications, Volume 30 Issue 4, Elsevier Science Publishers, Amsterdam (2007).
[26] Schneier B., Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Copernicus Books (2003).
[27] Whitman M., Mattord H., Principles of Information Security, Thomson Course Technology, Canada (2003).