A protocol for incorporating biometrics in 3G with respect to privacy

Christos K. Dimitriadis, Despina Polemi

University of Piraeus, 80 A. Dimitriou, 18534 Piraeus, Greece

Abstract: This paper proposes a protocol, called BIO3G, for embedding biometrics in 3G security. BIO3G is an enhanced alternative to the common practice of utilizing biometrics locally, for gaining access to the device. BIO3G provides real end-to-end strong user authentication to the mobile operator, requiring no storing or transferring of biometric data and eliminating the need for biometric enrolment and administration procedures, which are time-consuming for the user and expensive for the mobile operator.

1 Introduction

Security in 3G is designed in order to address the main weaknesses of previous generation systems [1]. The Universal Mobile Telecommunications System Authentication and Key Agreement (UMTS-AKA) mechanism is the core component of the 3GPP specifications for implementing network access security [2], through mutual authentication between the user and the node of the mobile operator. End-to-end network security is implemented by the deployment of security mechanisms at the network layer, such as the Internet Protocol Security protocol (IPSEC)[3,4], while application security is implemented by a combination of mechanisms, including cryptographic technologies [5]. A common parameter in most of these security mechanisms is user authentication, which is usually implemented by the use of a Personal Identification Number (PIN) or a password [6]. The rest of the process relies on the authentication of pre-stored secrets, such as cryptographic keys, or identifiers such as the International Mobile Subscriber Identity (IMSI), but not actually the user. Furthermore, knowledge as well as the possession of an item, does not distinguish a person uniquely, revealing an inherent security weakness of password and token-based authentication mechanisms. Moreover, PIN stealing, guessing or cracking have become very popular, with software tools implementing relevant attacks and research papers describing sophisticated techniques for invading PIN security [7].

Modern biometric technologies provide enhanced security levels by introducing a new dimension in the authentication process called “proof by property”. Biometrics are defined as “the automatic use of human physiological or behavioral characteristics to determine or verify an identity” [8]. However, the design and deployment of a security architecture incorporating biometric technologies hides many pitfalls, which when underestimated can lead to major security weaknesses and privacy threats [9].

K. Dimitriadis C. and Polemi D. (2005).
A protocol for incorporating biometrics in 3G with respect to privacy.
In *Proceedings of the 3rd International Workshop on Security in Information Systems*, pages 123-135
DOI: 10.5220/0002560701230135

This paper studies the incorporation of biometrics in the security architecture of 3G mobile systems, with respect to user privacy. The paper proposes a secure protocol, called BIO3G, which is differentiated from the common practice of utilizing biometrics locally, for gaining access to the device, providing real end-to-end user strong authentication. BIO3G was created by following the complete life cycle of a system development procedure.

The paper consists of five main sections: the "requirements and specifications" section, which analyzes various security and privacy issues regarding the incorporation of biometrics in 3G security, identifies specific requirements and defines the corresponding specifications, the "biometric transformation related work" section, presenting several research results related to the objectives of the paper, the "UMTS network access security summary" section, presenting the basics of the UMTS network access security in order to elaborate the protocol description in the homonym section and the "protocol assessment" section, evaluating BIO3G in terms of security, privacy, performance, usability and implementation complexity.

2 Requirements and specifications

Biometric systems and data are twofold as far as security and privacy in concerned. Biometrics enhance security and privacy, by implementing strong authentication mechanisms towards the protection of private data that may be exchanged over a 3G application. On the other hand, biometrics may threaten the overall security of the system, because incorrect and immature implementations may lead to even greater security weaknesses [10]. Furthermore, privacy may be ventured by the unintended usage of private information that could be derived from biometric measurements, such as genetic or medical data that may become criteria for discriminating human population into segments [11]. Privacy may also be invaded, in terms of identity disclosure and position or services tracking, because of the strong binding between a user and a user identity. Privacy concerns become even greater if we take into account that most biometric features cannot be hidden in everyday life, with face recognition being the most indicative example.

Legislation is a principal countermeasure for enforcing privacy in biometric applications. Forward to that, privacy is practically implemented by designing and deploying biometric architectures that incorporate the appropriate technical features for privacy protection [12]. Studying in more detail the incorporation of biometrics in a 3G environment, we conclude to the following categories of requirements and specifications towards a maximum level of security and privacy.

2.1 Biometric data storage

Biometric data are considered as private data [13], due to the strong binding with a property of the human physiology or behavior. According to the relevant legislation analysis, biometric data should be stored only for justified purposes, after ensuring

the free and informed consent of the user, obligations that complicate the situation and create concerns regarding the collection and storage of biometric data.

The biometric data that are captured by a sensor during a sampling procedure, before being processed by another component of the biometric device are called “raw biometric data” [8]. After their processing from the feature extractor, the biometric data are encoded to non-invertible “biometric templates” [8]. Raw data are very sensitive, because private information such as genetic or medical data, could be derived from them and because they are the key for creating biometric templates. Raw data should not be stored permanently at any form in the 3G device or the mobile operator and it must be ensured that temporary stores are securely erased.

The biometric templates should be stored in secure mediums. Server based architectures, where the biometric templates are stored centrally, are generally avoided due to the increased risk of the system [9], or implemented in complex structures that uncouple the direct relationship of the biometric data with real identities. Template storage in smart cards is considered as more secure [10]. Smart cards however, are not free of vulnerabilities. Capturing the power consumption of a chip can reveal the software code running on the chip, even the actual command. The application of Simple Power Analysis and Differential Power Analysis [14] techniques is possible to break the matching mechanism of the biometric system or reveal the biometric template. Timing Analysis attacks are similar, measuring the processing time instead of the power consumption. These types of attacks belong to a category of attacks against microcontrollers that may bypass local biometric authentication. Countermeasures for microcontrollers include noise generators, low power consumption chips and time-neutral software design.

We conclude that the most secure solution would be never to store biometric data (raw or templates) permanently in any sort of storage medium.

2.2 Biometric data transfer

We distinguish two categories of communication channels. The 3G network and the communication channels within the 3G user equipment and between the user equipment and the UMTS Subscriber Identity Module (USIM).

Regarding the first category, the sensitivity of biometric data, as explained in the previous paragraph, imposes significant security and privacy needs for their submission over a 3G network. The transfer of raw biometric data over communication networks should be strongly avoided. The transfer of biometric templates also introduces high risk and if realized, strong security measures should be deployed. Forward to the above, the most secure solution would be to avoid any submission of any form of biometric data.

Regarding the second category, data could be captured in order to be replayed at a future time for gaining access to the system, realizing replay and man-in-the-middle attacks. These types of attacks should be addressed for preserving the security of the biometric component of the system. Confidentiality and integrity should be implemented for all transmitted data in both categories towards communicational security.

2.3 System operations, enrolment and administration

Several attacks can be realized to operations of the biometric component of the system. A possible attack can be realized with a Trojan Horse on the feature extractor, the matching algorithm or the decision algorithm of the biometric system, acting as a manipulator of each component's output [9]. Spoofing attacks, where human artifacts or mimic techniques are deployed are also very effective [15]. Brute force attacks are also applicable and are implemented by attempting continuously to enter the system, by sending incrementally increased matching data to the matching function until a successful matching score is accomplished [10].

These attacks are addressed by several countermeasures including vitality detection (an extra measurement of properties such as skin elasticity, the relative dielectric constant, the conductivity, eye movement), mutual authentication between the components of the system, reduction of the local functions (for example template matching) and implementation of the functions by a trusted component of the system (such as the USIM).

Poor enrolment and biometric data administration procedures expose system to serious threats. During the enrolment phase, raw biometric data and biometric templates can be compromised and databases can be altered or filled with imprecise user data. Moreover, the enrolment and administration overload for preserving security and privacy is very demanding for the entity that manages the relevant services [12], which is the mobile operator in the current application. The most secure and cost-effective solution would be to minimize and if possible eliminate these procedures.

2.4 Summary of protocol specifications

One of the targets of BIO3G is to implement real end-to-end user strong authentication to the mobile operator, achieving at the same time a maximum level of security and privacy. The following list summarizes the specifications of BIO3G, as derived from the security and privacy analysis for introducing biometrics in 3G security:

- Biometric data (raw data or templates) should not be stored, neither in a central database on the mobile operator, or the USIM.
- Biometric data (raw data or templates) should not be transmitted over the 3G network.
- The biometric data should be protected from replay and man-in-the-middle attacks, while being processed by the various components of the system.
- Any transmitted data over the 3G network should be protected in terms of confidentiality and integrity.
- The biometric component of the 3G user equipment should embed vitality detection features, implement mutual authentication between its components, reduce the local biometric functions such as template matching and implementation as many functions as possible within the USIM.
- The need for enrolment and biometric data administration procedures should be minimized or if possible eliminated.

- The user must be informed about the use of biometrics during the process, in order to avoid system operation without the users consent (for example face image capturing and authentication, without the users will).

Furthermore, the incorporation of biometrics in 3G security, should respect the existing infrastructure of the mobile operator, take into account the capabilities of the terminal devices and take into account usability issues. Forward to the above, additional specifications include:

There should be no alteration of the existing subscriber registration procedure – the subscribers should be able to purchase devices and USIMs and quickly connect to the mobile network.

The protocol should utilize the main existing algorithms and functions of the USIM.

The protocol should be lightweight.

The protocol must be user-friendly.

3 Biometric transformation related work

A core component for addressing the BIO3G security and privacy specifications, regards the transformation of the biometric data into other forms of secrets. Instead of storing or transferring any form of biometric data, a more secure solution to use them as generators of non-invertible random secrets that are embedded in an end-to-end user authentication mechanism and which are disassociated with real identities for ensuring privacy. The main obstacle towards this target is that two biometric measurements of the same person are never the same, due to a number of reasons, such as the interaction of the user with the sensor, the small but existent changes of the user's characteristic through time or the environmental conditions. This fact creates the requirement for error correction codes (Hamming Distance, Set Difference and Edit Distance), in order to be able to calculate the same secret by slightly different inputs.

Towards that direction Davida et al. [16] proposed that instead of storing the biometric template, to store its one-way digest. During verification the acquired biometric template is reduced to its canonical representation (original template) using error correction codes. Towards error correction Juels et al. [17] proposed a "fuzzy commitment" and later [18] constructed a "fuzzy vault" scheme utilizing the Set Difference metric. Very similar approaches to fuzzy extractors where proposed by Linnartz et al. [19] and Verbitskiy et al. [20], who assumed a multivariate Gaussian input distribution. Csirmaz et al. [21] proposed the different approach of quantization for correcting errors in physical random functions. Frykholm et al. [22], as well as Dodis et al. [23], extended these ideas and created an enhanced solution. More specifically, Dodis et al., created a semantically-secure key encapsulation mechanism for generating random values that can be utilized for key generation, from different inputs, by deploying error correction codes. The mechanism is called fuzzy extractor and allows the generation of randomness R from w and then successfully the reproduction of R from any string $w`$ that is close to w, with the help of a public string P produced during the initial extraction. Regarding the generation of random numbers in similar problem, research is also focused on ordinary extractors [24].

4 UMTS network access security summary

The UMTS-AKA mechanism is based on a 128-bit secret key (K), which is pre-shared between the mobile operator and the USIM. The USIM is a cryptography-enabled smart card identified by a 15 digit number, called IMSI. The USIM authenticates the user, by the use of a PIN. Mutual authentication between the USIM and the mobile operator is realized by a challenge and response mechanism. A random number (RAND) is calculated by the mobile operator and submitted to the USIM, along with a value (AUTN) derived by the combination of RAND and K with a number of parameters, including a sequence number. The USIM authenticates the mobile operator by analyzing and verifying AUTN. The USIM computes a value (RES), by applying RAND and K to a function (f2), and submits it to the mobile operator for verification (comparison with similarly computed XRES), realizing the authentication of the USIM.

Regarding confidentiality, the USIM is using the UMTS ciphering algorithm (f8), which produces a keystream block (*KSB*) using a 128-bit Cipher Key (CK) and a number of parameters. Integrity protection is implemented by the deployment of a 128-bit Integrity Key (IK), which is used for the calculation of Message Authentication Codes (MAC). The CK and IK are computed by the USIM and the mobile operator, by applying the pre-shared K and RAND to key generation functions (f3 and f4 respectively). The CK, IK, AUTN, RAND and XRES compose a group of UMTS-AKA authentication elements, called Authentication Vector (AV).

To summarize, according to the specifications of 3GPP, the user is authenticated only locally in the USIM, by the provision of a PIN. The USIM utilizes two pre-stored values, IMSI for identifying and K for authenticating the user to the mobile operator, residing the whole security infrastructure to a simple PIN mechanism

5 Protocol description

BIO3G implements end-to-end strong authentication of the user to the mobile operator, by introducing a biometric process to the core of UMTS-AKA. Figure 1 presents a sequence chart of BIO3G, based on the Message Sequence Charts (MSC) graphical language,[1]. There are three entities present: the User (U), the USIM connected to the User Equipment (USIM/UE) and the Mobile Operator (MO).

[1] http://www.sdl-forum.org/MSC/index.htm

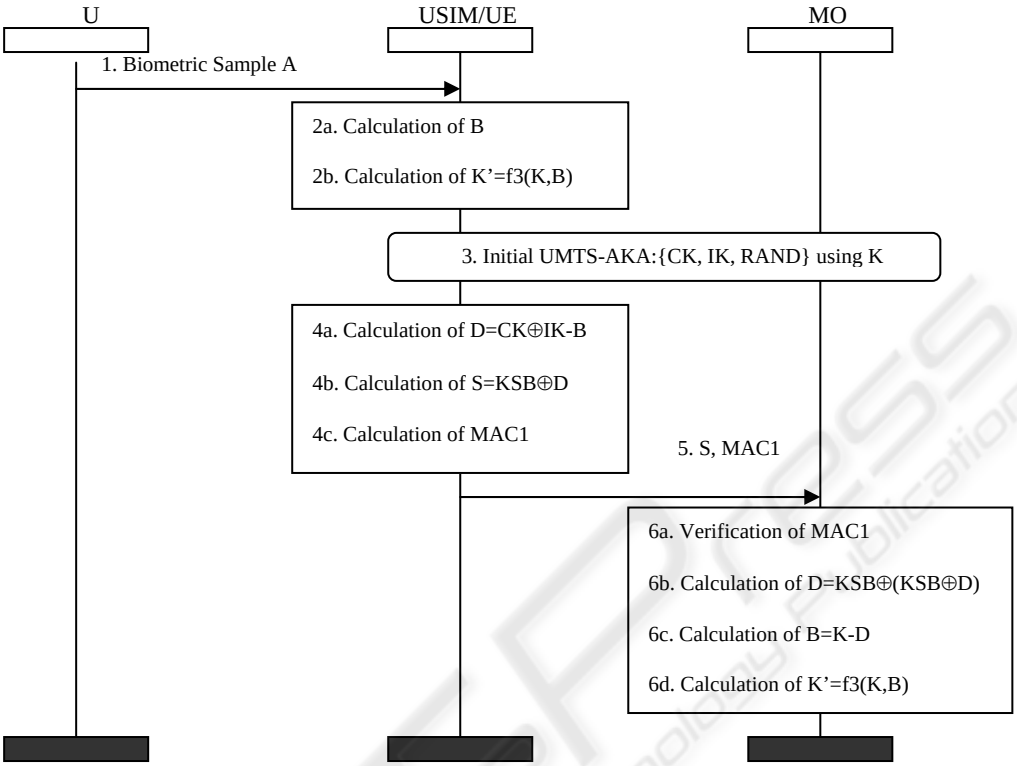

Fig. 1. BIO3G Overview

The protocol initiates when the User attempts to access the mobile device. The protocol consists of the following steps:

1. The User provides a biometric sample *A* - after being clearly requested to do so, by the UE - by utilizing the biometric sensor, which is embedded on the UE. The sensor should embed vitality detection features, depending on the biometric method deployed.
2. During this step:

2a. The UE receives the biometric sample and calculates a random, non-invertible 128-bit secret B. Error correction codes are deployed for ensuring the reproduction of B, by a biometric measurement m` that is sufficiently and securely close to the initial measurement m. Mutual authentication between the sensor and the other components of the UE should be deployed during communication, while replay attacks should be addressed by the introduction of random numbers in the exchanged signals, complemented by signal integrity protection (hash values).

2b. The value B, is passed to the USIM. Mutual authentication between the USIM and UE is possible by implementing a mechanism based on a shared secret, according to a specification by 3GPP [25]. A new secret key K` is

calculated by the USIM utilizing the f3 function of UMTS-AKA. This function produces a 128-bit key, by combining two 128-bit values - K and RAND in normal UMTS-AKA operation. The following calculation is realized:

$$K`=f3(K,B) \quad (1)$$

3. The UMTS-AKA mechanism is deployed for mutual authentication between the USIM and the MO using the initial key K. According to the 3GPP specifications, during this phase the random value RAND is being submitted to the USIM by the MO, while the CK (for data encryption) and IK (for integrity protection) are calculated by the USIM and the MO.
4. During this step:

4a. In order to avoid the direct submission of *B*, an offset *(D)* from the combination of two pre-established secret values (*CK* and *IK*) is calculated by the USIM, according to the following equation:

$$D=CK\oplus IK-B \quad (2)$$

4b. D is encrypted by the USIM using the UMTS ciphering algorithm (f8), which produces a keystream block (KSB) by the introduction of CK and a number of parameters. Encryption is realized by the following equation according to the 3GPP specifications:

$$S=KSB\oplus D \quad (3)$$

4c. A Message Authentication Code (MAC1) is also computed by the USIM, according to the UMTS-AKA algorithms, for the preservation of message integrity. MAC1 calculation takes into account RAND for replay protection.

5. The values S and MAC1 are submitted to the MO.
6. During this step:

6a. MAC1 is verified.

6b. D is calculated by the following equation:

$$D=KSB\oplus(KSB\oplus S) \quad (4)$$

6c. B is calculated by the following equation:

$$B=CK\oplus IK-D \quad (5)$$

6d. The new shared key K` is calculated using equation (1) and stored on the MO, instead of K, while B is deleted from any permanent memory units.

These protocol steps are realized only during the first interaction of the user with the mobile operator. After their completion, K` is shared between the USIM and MO and can replace K, for the deployment of UMTS-AKA in the future, authenticating the user end-to-end to the MO, only by implementing steps 1, 2 and 3. It must be highlighted that in step 2, K' is calculated on the fly, using B (which is not stored on the USIM/UE nor the MO).

6 Protocol assessment

6.1 Security and privacy analysis

BIO3G implements end-to-end biometric authentication, avoiding local template matching, as well as storing and submission over the 3G network of any type of biometric data. In more detail:

Identity privacy support protects the privacy of the subscriber identity against passive eavesdropping, which can result user location tracking and delivered services tracking, as well as the binding of any information captured with a specific user identity. The biometric data are automatically transformed to random secrets that embed no data that could reveal the real identity of the user. These secrets (B) are used for the generation of new secrets (K`) that implement end-to-end authentication with the MO and negotiate user access to the network. Furthermore, the random secret B, is not stored permanently in any storage medium and is only used for the generation of K' in the USIM/UE (every time the user is trying to access the network) and in the MO only during first interaction. It must be highlighted that the random secret B, which is a one-way transformation of the biometric data, is only transmitted once from the UE/USIM to the MO, transformed and encrypted. So even in the worst case scenario of being able to revert-engineer the random number B to biometric data (which is not possible according to the state of the art), the attacker must capture S the only time it is submitted, decrypt it for revealing D (by breaking the encryption algorithm) and calculate B, after possessing CK and IK. We conclude that this operation is much more difficult than attacking a single cryptographic algorithm, during a common security architecture, where biometric templates are transmitted encrypted between two entities.

Mutual authentication is established between the entities of the protocol. The UE/USIM and the MO are mutually authenticated via the UMTS AKA mechanism. The User is authenticated end-to-end with the MO through BIO3G. Mutual authentication between the USIM and UE is realized by implementing a mechanism based on a shared secret [25]. Mutual authentication between the various components of the UE is also provisioned in the operation of BIO3G.

Confidentiality is established through symmetric encryption using function f8 of the UMTS-AKA mechanism. The strength of the encryption mechanism is inherited from the UMTS-AKA specifications of 3GPP. More specifically symmetric encryption is utilized for encrypting D, which is an offset of B.

Integrity protection is realized through the deployment of Message Authentication Codes based on UMTS-AKA algorithms. A MAC is calculated, during the exchange of messages between the MO and the UE/USIM.

Replay protection in the 3G network is established by two factors. The first is the alternation of the Authentication Vectors on every full authentication procedure of the UMTS-AKA, as specified by 3GPP, causing the modification of the CK and IK. The second factor is the alternation of the TMSI, as specified by the UMTS-AKA mechanism. Replay protection regarding the various components of the UE/USIM is provisioned by the protocol operation, through the deployment of random numbers and signal integrity protection.

Man-in-the-middle attacks, session hijacking attacks and entity impersonation, are addressed through the establishment of integrity, confidentiality, replay protection and mutual authentication, as described above.

Common brute- force and dictionary attacks are not applicable since BIO3G is not a password protocol. Brute force attacks in biometrics are usually realized by the monitoring of the matching results of a template comparison, which is not realized in BIO3G. The submission of random biometric data, without the monitoring stage is almost impossible to produce the random number B [23].

The most applicable Denial of Service (DoS) attacks, are those realized by the submission of false error messages to the involved entities. The current level of protocol description does not include the specification of error cases and the corresponding error messages. This is one of the issues scheduled for future work.

6.2 Risk assessment results

Risk analysis was conducted, according to a methodology (Biometric Knowledgebase –BK) [26] that is specifically targeted to the development and implementation of biometric systems. BK considers vulnerabilities that take into account the specifications of the Biometric Evaluation Methodology (BEM) [27], which is a supplement to the Common Evaluation Methodology (CEM) of the Common Criteria (CC) [28] for product and system security evaluation, specialized for biometric systems. Furthermore, BK also considers the vulnerabilities, which are incorporated in the protection profiles [29,30] that are created for evaluating biometrics, according to the Common Criteria. In that sense, improving BIO3G through BK, contributes to its compatibility with the CC towards security certification.

BIO3G was evaluated in terms of security and privacy according to BK. The results of risk analysis indicated that the following vulnerabilities were not applicable:

- Spoofing: since vitality detection features are present. Furthermore, no local matching of any kind (especially template) is implemented by the device or the USIM. Most of the functions are implemented by the USIM, utilizing its existing functions (generation of K`, simple functions such as the offset calculation, encryption and MAC calculation). The generation of the random number B is implemented by the UE on the fly.
- Fake templates: Since no templates or other forms of biometric data are permanently stored.
- Replay: Since the appropriate countermeasures were included BIO3G.
- Cross system: since the key K` is derived from a unique key K and a random number B.
- Component alteration: Since the appropriate countermeasures were included BIO3G.
- Enrolment and administration: Since no enrolment and administration procedures are required.
- Noise and power loss: Since presenting noise or attacking the power input of the device is unable to create the random number B.

- Residual characteristic: Since modern biometrics are resistant to these types of attacks in combination with vitality detection. However, certified biometric components should be deployed for ensuring the appropriate security level.
- Similar template - Similar characteristics: Since modern biometric algorithms are resistant to these types of attacks, having adequate performance levels. However, certified algorithms should be deployed for ensuring the appropriate security level.
- Brute force (verification applications): Since BIO3G is resistant to these types of attacks according to the security and privacy analysis
- Identity management implementation: Since BIO3G implements identity privacy in combination to UMTS-AKA

The only vulnerability that is in doubt regards power and timing analysis. These types of attacks are very effective and can be realized against any microcontroller of the device or the USIM. Countermeasures such as noise generators, low consumption chips and time neutral code design should be implemented for eliminating the residual risk level of 3% that was the final result of the risk analysis process. However, this vulnerability regarding mobile equipment in general and is not specifically introduced by BIO3G. The risk level is an indicative percentage for presenting the security level of the system and is not related to biometric error rates.

6.3 Performance, usability and implementation issues

BIO3G requires no administration procedures for the mobile operator and no additional features for the USIM. In more detail, there is no need for enrolment and biometric data administration procedures that would increase the operational cost of the mobile operator and the complexity of the subscriber registration procedure, in contradiction to other approaches that may require template storage in central databases. Through BIO3G, the subscribers are able to purchase devices and USIMs and quickly and transparently connect to the mobile network, without the need to collect and remember PINs.

From a technical perspective, the incorporation of biometrics in 3G security, introduces no changes to the existing infrastructure of the mobile operators. BIO3G takes into account the capabilities of the 3G mobile devices and the USIM. More specifically, BIO3G utilizes the existing functions of the USIM, implementing simple subtractions and “exclusive or” functions, as well as key generation procedures by utilizing the facilities of UMST-AKA. The only additional software component needed for the mobile device, regards the generation of a random number B from a biometric input.

In terms of communicational load, BIO3G exchanges only one message between the USIM/UE and the MO and only during its first operation. In normal authentication mode (after the first interaction of the USIM/UE with the MO), the protocol does not add any messages, while UMTS-AKA is deployed with a new secret key K’.

7 Conclusions

Due to the increased sensitivity of biometric data, the introduction of biometrics in 3G security is a very demanding process as far as security and privacy is concerned. BIO3G was created by following a design approach that identified the necessary requirements and defined the corresponding specifications, through the detailed study of biometric technologies within the framework of their incorporation in a 3G environment. BIO3G is a lightweight and user-friendly protocol that implements real end-to-end strong authentication of the user to the mobile operator, though a mechanism that is integrated to the existing components of 3G security, requiring no storing or transferring of biometric data and eliminating at the same time any biometric enrolment and administration procedure, which are time-consuming for the user and expensive for the mobile operator. BIO3G went through a security and privacy evaluation process, including a risk assessment procedure, taking into account the security objectives of the Biometric Evaluation Methodology and the relevant Common Criteria protection profiles, making its implementation capable of CC certification.

Part of this work is the author's contribution to the European Commission (EC) project IST-2002-001766 Biometrics and Security – BIOSEC[2]. The authors would like to thank the EC for funding BIOSEC.

References

1. Neimi, V., Nyberg, K.: UMTS Security. John Wiley & Sons (2003)
2. 3rd Generation Partnership Project: TS 33.102 - 3G Security; Security architecture (2004)
3. 3rd Generation Partnership Project: TS 33.210 - 3G Security; IP network layer security (2004)
4. Wisely, D., Eardley, P., Burness, L.: IP for 3G—Networking Technologies for Mobile Communications. John Wiley & Sons (2002)
5. Mitchell, C., J.: Security for Mobility. IEE Telecommunication Series 51 (2004)
6. 3rd Generation Partnership Project: TS 31.101 - UICC terminal interface; physical and logical characteristics (2005)
7. Benoit, O., Dabbous, N., Gauteron, L., Girard, P., Handschuh, H., Naccache, D., Socile, S., Whelan, C.:Mobile Terminal Security. Cryptology ePrint Archive: Report 2004/158 (2004)
8. ISO/IEC JTC1, SC37/SG1: Biometric vocabulary corpus (2004)
9. Dimitriadis, C., Polemi, D.: Biometrics –Risks and Controls. Information Systems Control Journal (ISACA), vol.4 (2004) 41-43
10. IST-1999-20078 Business environment of biometrics involved in e-commerce – BEE: Deliverable D7.1 Conclusions and Recommendations. http://expertnet.net.gr/bee (2002)
11. Prabhakar, S., Pankanti, S., Jain, A.,K.: Biometric Recognition Security and Privacy Concerns. IEEE Security and Privacy, vol. 1, no. 2 (2003) 33-42
12. IST – 2002 –001766 Biometrics and Security (BIOSEC): Deliverable D3.3 – Security recommendations: biometric systems integration, basic research on security, network protocols and PKI. Biosec consortium (2005)
13. Atricle 29 – EC data protection working party: Working document on biometrics (2003)

[2] http://www.biosec.org

14. Gandolfi, K., Mourtel, C., Olivier, F.: Electromagnetic Analysis: Concrete Results. Lecture Notes in Computer Science, Vol. 2162. Springer-Verlag (2001) 251-261
15. Matsumoto, T.: Gummy finger and paper iris – an update. Proceeding of workshop on information security research, Japan (2004)
16. Davida, G. I., Frankel, Y., Matt, B.:On enabling secure applications through off-line biometric. In Symposium on Security and Privacy (1998)
17. Juels, A., Wattenberg, M.: A Fuzzy Commitment Scheme. In Proc. ACM Conf. Computer and Communications Security (1999) 28–36
18. Juels, A., Sudan, M.: A fuzzy vault scheme. In Conference on Computer and Communications Security (2002)
19. Linnartz, J.-P.,. Tuyls, P.:New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. In AVBPA (2003) 393–402.
20. Verbitskiy, E., Tuyls, P., Denteneer, D., Linnartz, J.-P.: Reliable Biometric Authentication with Privacy Protection. In Proc. 24th Benelux Symposium on Information theory (2003)
21. Csirmaz, L., Katona, G.O.H.: Geometrical Cryptography. In Proc. International Workshop on Coding and Cryptography (2003)
22. Frykholm, N., Juels, A.: Error-Tolerant Password Recovery. In Proc. ACM Conf. Computer and Communications Security (2001) 1–8
23. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy Extractors: How to generate strong keys from biometrics and other noisy data. Advances in Cryptology -- Eurocrypt 2004, Lecture Notes in Computer Science 3027, Springer-Verlag (2004) 523-540
24. Shaltiel, R.: Recent developments in Explicit Constructions of Extractors. Bulletin of the EATCS, 77 (2002) 67–95
25. 3rd Generation Partnership Project: TS 22.022 - Personalisation of Mobile Equipment (ME); Mobile functionality specification (2005)
26. Dimitriadis, C., Polemi, D.: Risk Analysis of Biometric Systems. - Proceeding of the 2nd International Workshop on Security in Information Systems, WOSIS 2004, International Conference on Enterprise Information Systems ICEIS 2004, INSTICC Press (ISBN: 972-8865-07-4), Porto, Portugal (2004) 23-33
27. Common Criteria Biometric Evaluation Methodology Working Group: Biometric Evaluation Methodology (2002)
28. ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security (1999)
29. CC-Protection Profile: US Government biometric verification mode protection – profile for medium robusness environment (2003)
30. CC-Protection Profile: UK Biometric Device – Draft (2002)