Strong password authentication with AKA authentication mechanism

Libor Dostalek
Department of Computer Science and Engineering
University of West Bohemia
Pilsen, Czech Republic
dostalek@kiv.zcu.cz

Jiri Safarik
Department of Computer Science and Engineering
University of West Bohemia
Pilsen, Czech Republic
safarikj@kiv.zcu.cz

Abstract – **This contribution discusses algorithms for strong authentication of applications in mobile devices. The current LTE and IMS networks provide strong authentication using USIM smart cards based on AKA algorithm. The problem of this authentication is that this authentication is under the sole control of Telco operators. We can expect that more applications will be placed into the IMS environment in the future. These applications will be based either on SIP (video on demand etc.) or HTTP-based protocols (e.g. as government applications or banking applications etc.). They will be provided not only by Telco operators, but also especially by independent third parties - application (content) providers (e.g. government, banks etc.). This contribution proposes new authentication algorithms that combine AKA algorithm with other authentication algorithms. Therefore, the authentication is not under the sole control of Telco operators, still using strong authentication AKA protocol.**

Keywords - Authentication, AKA, Mobile Application, IMS, Robust Two-factor Authentication, Mobile authentication

I. INTRODUCTION

At present, mobile applications use a number of authentication methods, e.g.:

1. Native authentication methods in 3G/4G networks based on AKA mechanism [1]. This authentication is undoubtedly a cryptographically strong authentication. Its disadvantage is that it is used for authenticating of mobile device to the network (often called equipment authentication).
2. Password authentication is typical user authentication. Generally, this authentication method is unfortunately considered weak, so applications such as home banking or eGov seek other mechanisms.
3. Strong password authentication are more sophisticated password authentication methods resistant against known attacks (sniffing or elicitation of password, password-file compromise attack, guessing attack, forgery attack, impersonation attack, stolen-verifier attack, replay attack etc.).
4. Authentication based on public key certificates (PKI). The problem is, where the mobile device securely stores the private keys.
5. External devices such as authentication calculators generating one-time passwords. The main disadvantage of this solution is that a user must take care about an additional device, what he/she can find disagreeable.

Using multiple authentication method independently does not increase security. Our idea is to combine (to breed) methods 1 and 3 in a common multifactor authentication. The first factor is an equipment authentication based on AKA mechanisms and the second factor is strong password authentication.

II. USIM AND ISIM

In the 4th generation of mobile networks (Figure 1), LTE (Network Long Term Evolution) provides communication between the mobile device and base station (eNB) at the link layer. The base stations (eNB) are connected to the core network EPC (Evolved Packet Core) that will ensure that mobile devices can communicate through the Mobility Management Entity (MME) to IP networks. At the application layer, the mobile device communicates with IMS network which provides multimedia services.

The client authenticates towards LTE/EPC using the shared secret K, which he/she has stored in the Universal Subscriber Identity Module (USIM) application on his/her Universal Integrated Circuit Card (UICC)by AKA mechanism. The network has the shared secrets stored in the Authentication Center (AuC) of LTE/EPC networks. The AKA authentication mechanism is used.

At the application layer, the client authenticates towards IMS using the shared secret K that has stored in IP Multimedia Services Identity Module (ISIM) application to his/her Universal Integrated Circuit Card (UICC). The network has it stored in the AuC of IMS network. The authentication is also used AKA mechanism, however be encapsulated into another protocol.

AuC is jointly operated with subscriber database by the Home Subscriber Server (HSS).

ISBN 978-80-261-0641-8,

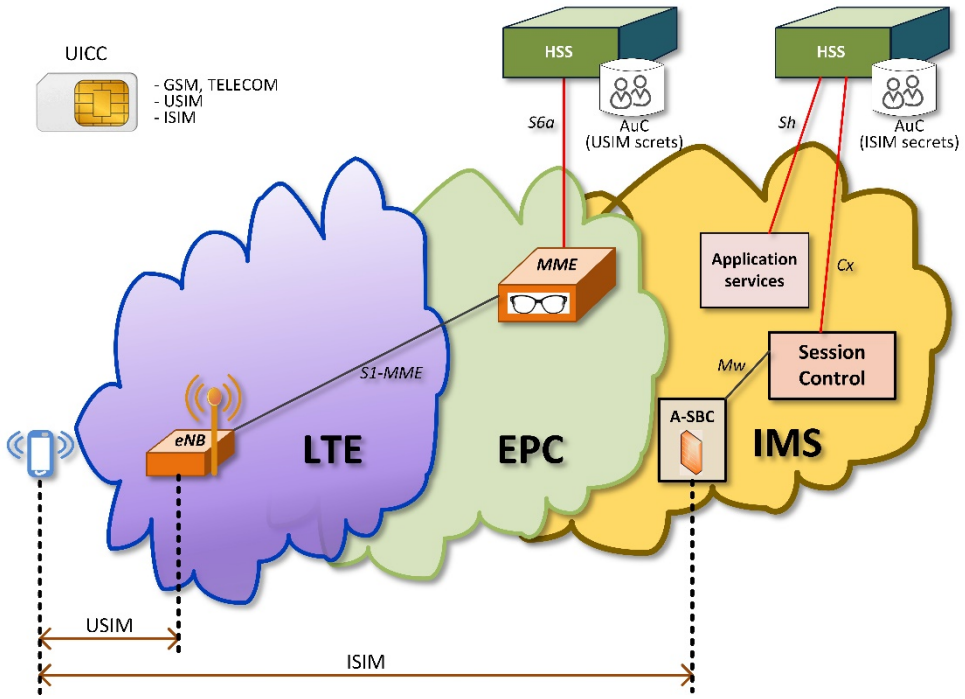

Figure 1 Authentication in mobile networks

Generally, the shared secret K for LTE/EPC is other than the IMS network. In practice, however client's smart card often contains only application USIM and ISIM application do not, so they use the same shared secret for LTE/EPS and for the IMS network too. In that case, on the Telco side AuC is common for LTE/EPC and for IMS.

III. AKA MECHANISM

AKA (Authentication and Key Agreement) mechanism is a security protocol used in 3G/4G mobile networks for mutual authentication and cryptographic material agreement (Figure 2).

There are three communication parties:

- A(mobile), mobile equipment usually equipped with USIM/ISIM containing shared secret K.
- B (network), usually A-SBC in IMS.
- Authentication center (part of a Home Subscriber Server - HSS).

Parties A (mobile) and Authentication center (AuC):

- share a secret K (shared secret) different for each smart card,
- maintain sequence number SEQ of authentication.
- Both parties support the AKA mechanism using one way functions $f1, f2, f3, f4$ and $f5$ (Figure 3).

AKA mechanism (Figure 2) is the following:

AKA-1: A (mobile) will grant access (sends its identity to B).

AKA-2: B (network) sends identification of A to Authentication center.

AKA-3: Authentication center on behalf of B:

- Generates random number $RAND$.
- Generates next sequence number SEQ of authentication.
- Runs Authentication functions $f1-f5$. (Figure 3) and generates Authentication vector $AV=(RAND,\ RES,\ CK, IK,\ SQN \oplus AK, AMF, MAC)$. While RES is one time password for authentication of A and MAC is one time password for authentication of B.
- Sends AV to B.

AKA-4: B cut and sore RES form Authentication vector AV. Next, $RAND,\ SQN \oplus AK,\ AMF$ and MAC sends to A.

Symbol	Meaning
K	Shared secret
AMF	Well known string
SQN	Sequence number of authentication
RAND	Random number
MAC	One time password for network authentication
RES	One time password for user equipment authentication
CK	Cyphering key
IK	Integrity key
AK	Anonymization key for SEQ anonymization
f 1-f 5	One way functions

TABLE 1 Notation of AKA mechanisms

AKA-5: Through the function $f5$, A computes SQN. A runs the rest of authentication functions and:

- If MAC, computed by A, is equal to MAC from AV, than B (network) is authenticated.

– Generates *RES* and sends it to *B*.

AKA-6: *B* compares the *RES*, obtained from *A*, with saved *RES* from *AV* (step *AKA-4*). If equal, *A* is authenticated.

IV. RELATED WORK

Method combining Secure Hash-Based Password Authentication Protocol Using Smartcards [3] and AKA mechanism [1] was introduced in [2] This method supports:

1. Multi-factor security - the security of the scheme is guaranteed when either the user's password or his data bearer token or USIM/ISIM is compromised, but not all.
2. Content provider keeps control over authentication to its applications.
3. Authentication is associated with USIM/ISIM i.e. AKA mechanisms used.
4. Roaming support - authentication is possible both in a home network and in a visited network.
5. Password change - a user can freely update his/her password.
6. Password change without communication with a server
   - a user can freely update his/her password without any interaction with a server.
7. Mutual authentication - a user and a server are sure about the identity of each other. Both the server and the user can verify the legality of its counterpart.
8. No time synchronization - The scheme does not require additional clock synchronization mechanisms
9. Anti-desynchronization both a user and a server cannot be desynchronized against their shared secrets or values, which could result in the user's denial of any future access to the server.
10. Data bearer revocation. In the case of data bearer token loss, invalidating the further use of the lost data bearer token should be provided to prevent an adversary from

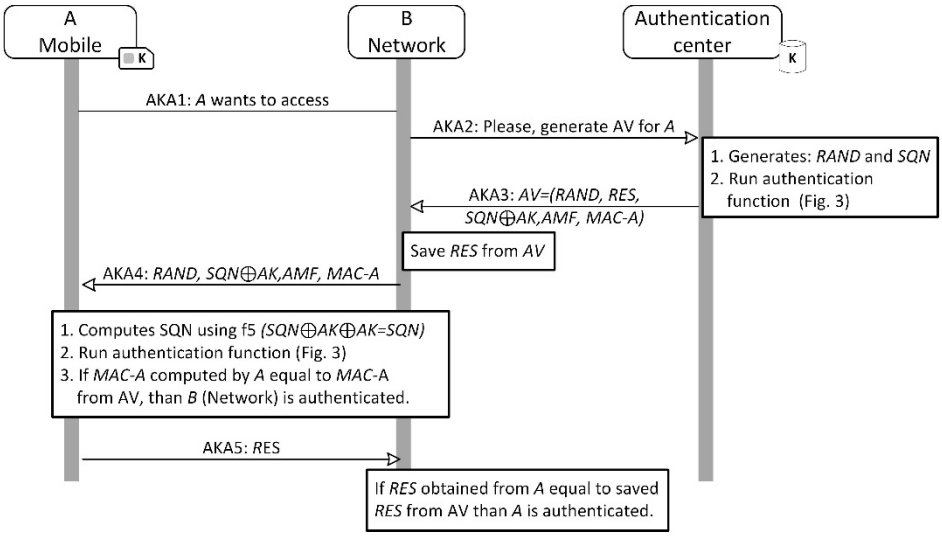

Figure 2 AKA mechanism

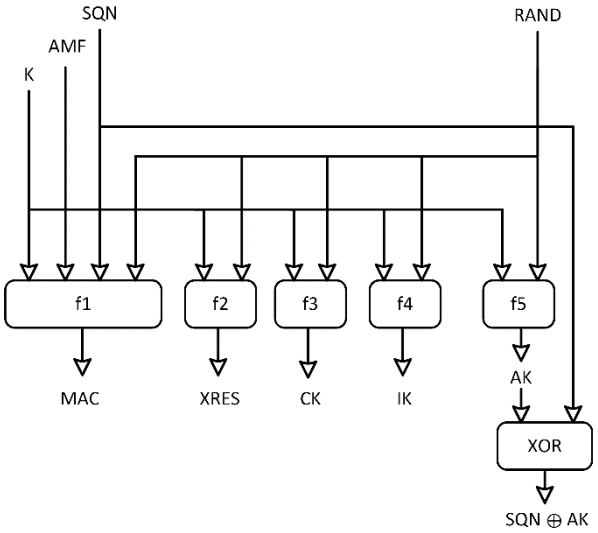

Figure 3 AKA Authentication function *f1-f5*

impersonating the registered user with the lost s data bearer token.

11. Password protection (eavesdropping, elicitation etc.) - except the user, no another party can get any information of the user's password. More specially, the user's password will not be revealed to the server during registration, and there are no variation tables such as plain text or hashed passwords stored in the server.

Method described in [2] has some disadvantages. The method does not supports:

12. Session key agreement - A session key is established between the user and the server during the authentication process, which is known only to the user and the server. Then, the session key is used to create a secure communication channel between the user and the server.
13. Perfect forward secrecy - a potential attacker cannot know any information about previously established session key, even when the long-term keys of the server and the user are disclosed.
14. Forward and backward secrecy - Forward secrecy means, that even though for some reason some session keys are exposed, the secrecy of any previous session key will be still maintained. Backward secrecy means, that even though some previous session keys are exposed, the secrecy of any future session key will be still maintained.
15. Key freshness. Neither party can guess the next shared session key.

V. THE PROPOSED SOLUTION

The proposed solution (**Figure** 4) creates multifactor authentication by merging AKA authentication mechanism [1] and Robust Two-factor Authentication [4]. Assume that the user is registered:

- In terms of Robust Two-factor Authentication: Parameter Generation phase was done. Mobile user *U* and Application function **S** (server) exchange messages R1 and R2.
- In terms of AKA mechanism [1]: A user equipped with USIM shares the secret K with Authentication Center (AuC).

In the proposed solution, the mobile user *U* and the Application function *S* during authentication exchange three messages Y1, Y2 and Y3:

Step Y1: *U* inserts its data bearer token with parameters IM_0 and *V* into its equipment and inputs its password *PW*. Next, a random integer r_C from $[1, n-1]$ is generated and $G_C=r_C \times G$ is computed. Then it continues to compute $V'=V-H(PW)=H(ID\|K_S)$ and $G'_C=G_C+V'$. At the end, *U* sends its identity (for AKA mechanisms) and $\{IM_0, G'_C\}$ to S.

Step Y2: This step consists of the step A1 (Robust Two-factor Authentication) and the steps AKA1, AKA2 and AKA3. Upon receiving message Y1, *S* asks AuC for AV generation for the user *U*. AuC sends AV to *S*. **S** cuts off RES from AV and stores it.

In the meantime, *S* handles message $\{IM_0, G'_C\}$, *S* decrypts the parameter IM_0 with K_S and obtains the value $ID\|r$. Then, *S* verifies whether the identifier *ID* is valid. If the verification fails, *S* terminates the session. Otherwise, *S* computes $V'=H(ID\|K_S)$ and recovers $G_C=G'_C-V'$.

After that, *S* generates $G_C=G'_C-V'$, where r_S is a random integer within range $[1, n-1]$, and then computes $IM_1=E_{Ks}(ID\|r')$, $K_{SU}=h_1(H(ID\|K_S)(r_S \times G_C))$, $IM'_1=h(K_{SU}) \oplus IM_1$ and $M_S=h_2(K_{SU}\|G_C\|G_S\|IM'_1\|MAC\text{-}A)$.

S sends to U: M_S, G_S, IM'_1, *RAND*, $SQN \oplus AK$ and AMF .

Step Y3: First, *U*'s equipment runs function f5 and obtains SEQ. Subsequently, it runs function f1, f2, f3 and f4 and obtains MAC, RES and cryptographic material IK, CK.

Upon receiving $\{M_S, G_S, IM'_1\}$, the U's equipment computes the session key $K_{SU}=h_1(V'\|(r_C \times G_S))$ and then, it checks whether the value M_S is equal to $h_2(K_{SU}\|G_C\|G_S\|IM'_1\|MAC\text{-}A)$. If it is not, it terminates this session. Otherwise, it computes $IM_1=h(K_{SU}) \oplus IM'_1$ and replaces IM_0 by IM_1, then, it computes $M_U=h_2(K_{SU}\|G_S\|RES)$ and sends $\{M_U\}$ to *S*.

Step Y4: Upon receiving $\{M_U\}$, *S* checks whether the value M_U is equal to $h_2(K_{SU}\|G_S\|XRES)$. If yes, *U* and *S* successfully authenticate each other and share the session key. Otherwise, *S* terminates this session.

TABLE 2 Notation of Robust Two-factor Authentication

Symbol	Meaning
p	A large prime
E	An elliptic curve equation over Z_p
F_p	Finite field with notions of addition (+), subtraction (-), multiplication (x) and division
G	A generator point of a large order
S	Server
U	User
ID	Login ID of U
PW	PW Password of U
Ekey(m)	Encryption of message m with key
Dkey(m)	Decryption of message m with key
h1(); h2(); h3()	Cryptographic hash function
H()	Cryptographic map-to-point (on elliptic curve) hash function, e.g. [5]
$\oplus$	Denotes the bitwise XOR operation
$\|$	Denotes concatenation

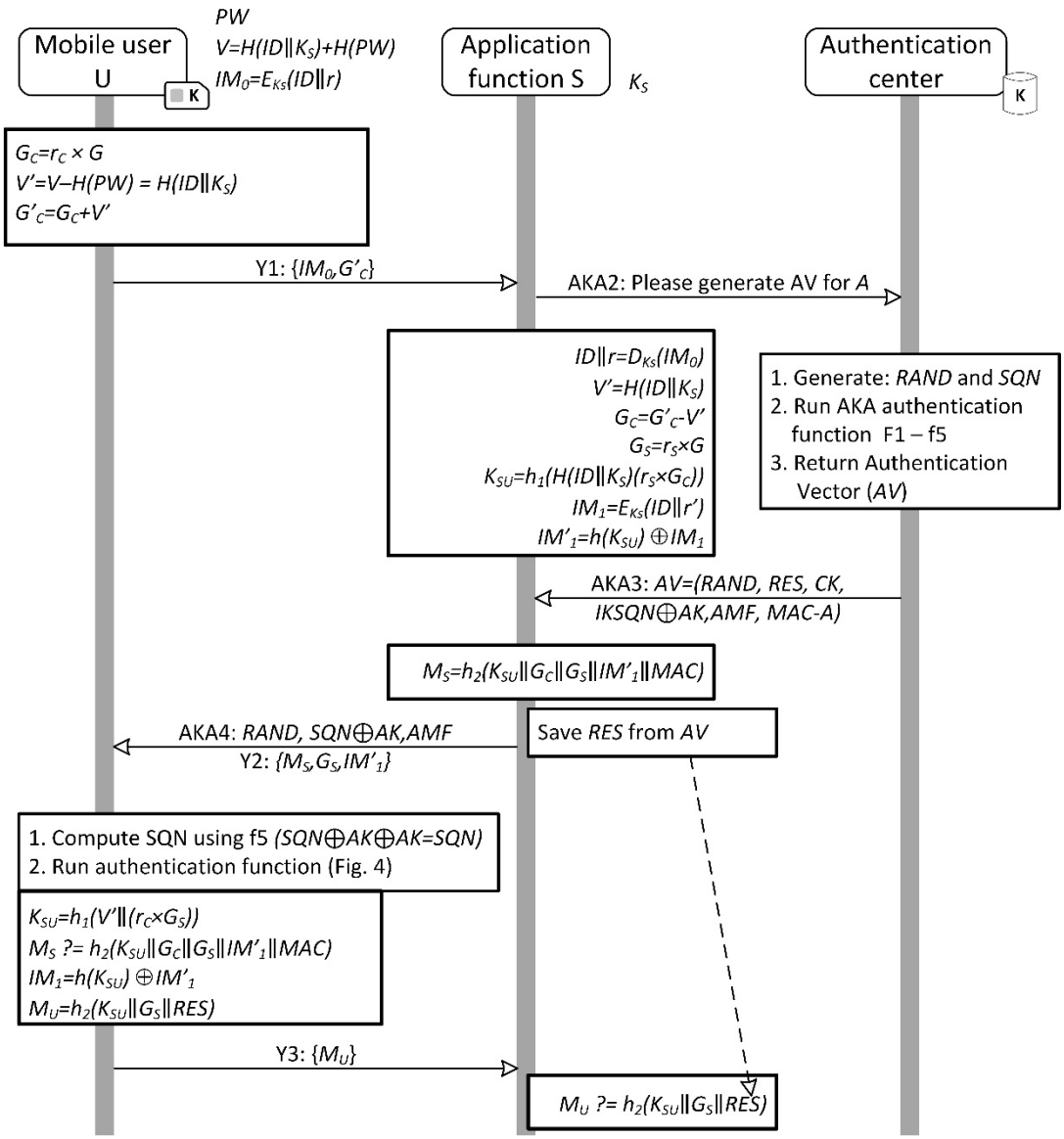

Figure 4 Proposed solution

VI. ANALYSIS

Table 3 compares properties of the described algorithm. Table 4 summarizes the computation costs comparison between our scheme and the previous schemes (in authentication phase).

TABLE 3 Properties of the described algorithms

		AKA [1]	Secure Hash-Based Password Authentication Protocol [3]	Robust Two-factor Authentication [4]	Strong authentication for mobile application [2]	Proposed solution
1	Multi-factor security	Yes	Yes	Yes	Yes	Yes
2	Content provider maintains control over authentication to its applications	No	Yes	Yes	Yes	Yes
3	Authentication is associated with USIM/ISIM	Yes	No	No	Yes	Yes
4	Roaming support	Yes	Yes	Yes	Yes	Yes
5	Password change	n/a	Yes	Yes	Yes	Yes
6	Password change without any interaction with the server	n/a	No	Yes	No	Yes
7	Mutual authentication	Yes	Yes	Yes	Yes	Yes
8	No time synchronization	Yes	Yes	Yes	Yes	Yes
9	Anti de-synchronization	Yes	Yes	Yes	Yes	Yes
10	Data bearer revocation	n/a	Yes	Yes	Yes	Yes
11	Password protection (eavesdropping, elicitation etc.)	n/a	Yes	Yes	Yes	Yes
12	Session key agreement	Yes	No	Yes	No	Yes
13	Perfect forward secrecy	n/a	n/a	Yes	No	Yes
14	Forward and backward secrecy	n/a	n/a	Yes	No	Yes
15	Key freshness	n/a	n/a	Yes	No	Yes

TABLE 4 Computation costs

	Secure Hash-Based Password Authentication Protocol [3]	Robust Two-factor Authentication [4]	Strong authentication for mobile application [2]	Proposed solution
Computation costs of the user	4h, 1A	3h, 1H, 2PM	4h, 1A, AKA	3h, 1H, 2PM, AKA
Computation costs of the server	4h, 2A	4h, 1H, 2S, 2PM	4h,2A, AKA	4h, 1H, 2S, 2PM, AKA
Communication round between the user and server	3	3	3	3

- h is defined as the time complexity of the hash computation;
- H is defined as the map-to-point hash computation;
- S is defined as the time complexity of the symmetric encryption/decryption;
- PM is defined as the time complexity of the EC point multiplication;
- A is defined as the time complexity of the asymmetric (e.g. RSA) encryption/decryption.
- AKA is defined as the time complexity of the AKA algorithm

VII. CONCLUSION

The proposed solution enables applications, running on IMS environments to use authentication, which brings:

- Evidence that the user is authenticated in the device that he/she uses, with the particular USIM (proof of ownership).
- Evidence that a concrete person who knows the password performed the authentication.
- Generating cryptographic material for securing subsequent communication

---

This work was supported by project SGS-2016-018

VIII. REFERENCES

[1] „3G security; Security architecture; 3GPP TS 33.102; 3GPP TS 33.102," 3GPP TS 33.102, September 2016. [Online]. Available: http://www.3gpp.org.

[2] L. Dostalek a J. Ledvina, „Strong Authentication for Mobile Application," *International Conference of Applied Elecronics,* č. IEEE CFP1569A-PRT, pp. 23-26, September 2015.

[3] H. Jung, H. S. Kim, B. Murgante, O. Gervasi a A. Iglesias, „Secure Hash-Based Password Authentication Protocol Using Smartcards," v *11th International Conference on Computational Science and Its Applications (ICCSA), PT V Book Series: Lecture Notes in Computer Science, Volume: 6786, Pages: 593-606*, 2011.

[4] Q. Jiang, J. Ma, G. Li a L. Yang, „ Robust Two-Factor Authentication and Key Agreement Preserving User Privacy," *IJ Network Security, 16(4),* pp. 321-332, 2014.

[5] T. Icart, „How to hash into elliptic curves," v *CRYPTO 2009*, Santa Barbara, California, USA, 2009.

[6] „Universal Subscriber Identity Module (USIM) application; 3GPP TS 31.102 V14.1.0," 2017. [Online]. Available: http://www.3gpp.org.