New Design of Generic Authentication Architecture Using ID-based Cryptosystem in 3GPP

Kyusuk Han, Chan Yeob Yeun, and Kwangjo Kim
Information and Communications University
Munjiro 119, Yuseong Gu, Daejeon, Korea
Tel. +82-2-866-6236 / Fax. +82-2-866-6273
E-mail: hankyusuk@icu.ac.kr, chanyeun@gmail.com, kkj@icu.ac.kr

Abstract

At present, the symmetric key cryptosystem is more commonly used than the asymmetric key cryptosystem in the 3GPP Generic Authentication Architecture (GAA). However, the 3GPP GAA with asymmetric key architecture has the public key management problem. Thus, we propose a novel GAA by using ID based cryptosystems that enables the easier key management.

1. INTRODUCTION

Generic Authentication Architecture (GAA) is described in [1] by 3GPP. The Generic Bootstrapping Architecture (GBA) is used to make the secure connection between the mobile device and various network applications such as mobile banking, ticketing services and *etc.*

For the GAA, symmetric and asymmetric cryptosystem based architecture are specified in [2] and [3]. The symmetric cryptosystem based architecture is commonly used, while the asymmetric cryptosystem based architecture is specified for the request on the capability of public key cryptosystems.

However, the public key cryptosystems have the several public key management problems. For example, how to authenticate the public keys, and how to store the public key pair are issued. For such storage problem, *Annex A* of [3] claims the weaker strength of storing public key pairs in the terminal.

Also, the symmetric cryptosystem based architecture use the same key for the authentication and the key exchange with the key used in the security architecture for the mobile network [4,5,6].

Our motivation is to overcome such a key management problem mentioned above. We applied ID-based cryptosystem (IDBC) that has the benefit due to the efficiency of public key invocation in our design. IDBC is the cryptosystem based on the properties of the pairing over the elliptic curve. IDBC uses the identities of the entities as the public keys, which reduces the additional cost for the public key management. However the computational overhead over the IDBC is rather high for the USIM that has less computational power.

Moreover, we propose a new way to provide cryptographic computation in the terminal without leaking the private key stored in USIM. Also, our design is compatible with existing GAA.

2. Issues on The Previous Architectures

2.1. Generic Authentication Architectures

Generic Authentication Architectures (GAA) is the security architecture to provide the authentication for the mobile application with various security mechanisms such as mobile banking and multimedia services, which is specified by 3GPP.

3GPP provides both the symmetric key based architecture in [2], and the asymmetric key based architecture in [3]. The symmetric key based architecture us the Authentication and Key Agreement (AKA) algorithm to share the key between the mobile device and the BSF (Bootstrapping Function), which is used for the request of the NAF (Network Application Function). And the asymmetric key based architecture use the certificate for the authentication, which is stored in the universal subscriber identity module (USIM) or the mobile device. Figure 1 shows the overall process of the generic bootstrapping architecture. (The figure is available from the Wikipedia.)

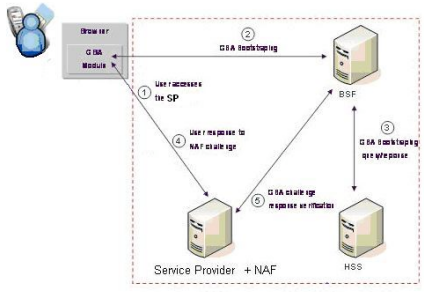

Figure 1 The process of generic bootstrapping architecture

2.1.1. Generic Bootstrapping Architecture (GBA)

GBA is based on the symmetric cryptosystems that is specified in [2]. The architecture consists of four important entities: Bootstrapping Function (BSF), Network Application Function (NAF), User Equipment (UE), and Home Subscriber Server (HSS). HSS has the initial key share with UE, who gives the authentication vectors to BSF. BSFs are located in each domain, which gives the authentication information to NAF. NAF provides the 3rd party services to UE.

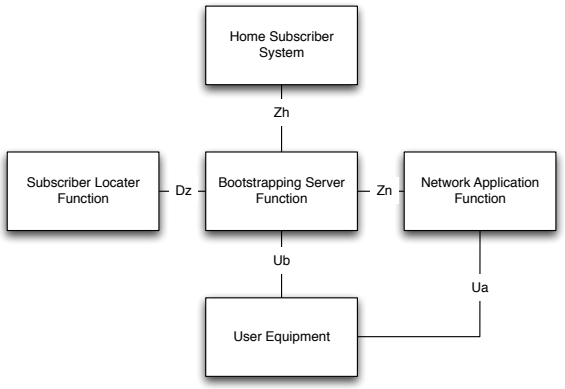

Figure 2 Generic bootstrapping architecture (GBA)

2.1.2. Support for Subscriber Certificate (SSC)

SSC is based on the asymmetric cryptosystems that is specified in [3]. In SSC, NAF's role is the PKC portal, which issues certificates for UE. The PKI portal issues the certificate of the UE, and sends the certificate of the operator CA. However, for the secure communication between NAF and UE, BSF should have the shared secret with NAF and UE.

The PKI portal can be the registration authority (RA) that manage the authentication request, and the certification authority (CA). However the role of CA is available from the PKI infrastructure, thus mostly the PKI portal only acts the role of CA.

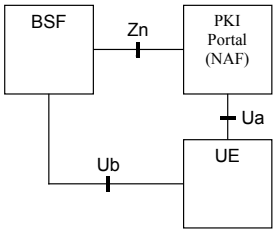

Figure 3 Support for Subscriber Certificate

2.2. Public Key Management Issues

There are several issues on public key management in SSC [3]. Storing the public key pair in the USIM or the terminal.

Storing the public key pair in the USIM is more secure, while it has limited computational power.

The PKI portal is necessary for issuing the certificate of public keys in SSC. That means the 'another' secure channel is required to transfer the certificate to users, which requires the role of BSF that has the pre-shared symmetric key with users.

2.3. Security Issues in the Next Generation Mobile Network

Applying the current security architecture directly to the next generation mobile network is known to be insufficient with several security problems; Lack of security consideration of hetero-network environments, limits from symmetric key cryptosystem, threats on the permanent identities of users, etc. [8]

3. Our Novel Design of GAA with IDBC

Our motivation is to overcome such a key management problem mentioned above. We applied ID-based cryptosystem (IDBC) that has the benefit due to the efficiency of public key invocation in our design.

3.1. ID-based Cryptosystem

ID-based cryptosystem is based on properties of pairing.

Assume an additive group G_1 over q. P is the generator of G_1.We can define following cryptographic problem.

- **Elliptic Curve Discrete Logarithm Problem (ECDLP)**: With given $P, P' \in G_1$, find an integer n, which satisfies $P = nP'$.

Let us consider an additive group G_1 and a multiplicative group G_2 of the same order q. Assume that the discrete logarithm problem is hard in both groups. Let P be a generator of G_1, and $\hat{e}: G_1 \times G_1 \rightarrow G_2$ a bilinear map satisfying the following properties:

1. Bilinearity: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in Z$.
2. Non-degeneracy: if $\hat{e}(P, Q) = 1$ for all $Q \in G_1$, then $P = \mathrm{O}$.
3. Computability: there exists an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

With such groups G_1 and G_2, we can define hard cryptographic problems like computational Diffie-Hellman (CDH) problem, Decision Diffie-Hellman (DDH) problem, and Gap Diffie-Hellman (GDH) problem.

To construct the bilinear pairing, we can use the Weil pairing and Tate pairing. G_1 is a cyclic subgroup of the additive group of points of a supersingular elliptic curve $E(F_P)$ over a finite field while G_2 is a cyclic subgroup of the multiplicative group associated to a finite extension of F_P.

For the details of ID based cryptography, refer [7].

3.2. GAA with IDBC

3.2.1. Key Generation

Key Generation Center (KGC) generates a random integer $s \in Z_P^*$, which will be the master secret of KGC. Each subscriber owns the unique identity ID. KGC generate $sH(ID)$ for each subscriber, where the public knows the hash function $H: Z_P^* \; ! \; G_1$. The multiplication of s and $H(ID)$ is the point multiplication over the elliptic curve.

$sH(ID)$ is the secret key of the subscriber (stored in USIM), denoted as **SK_USIM**.

3.2.2. Key Request

Figure 1 shows the terminal 's key request to USIM. At first, the terminal requests **TERM_REQ,** the terminal identity **TERM_ID,** the random integer generated by the terminal **RAND**, and the time stamp by the terminal **TS**, where **TERM_REQ** is the request of the terminal, **Term_ID** is the

identity of the terminal, **RAND** is the random integer generated by the terminal, and **TS** is the timestamp.

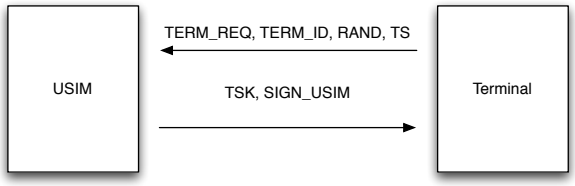

Figure 4 USIM send TSK to Terminal

The USIM returns **TSK**, and the signature of USIM **SIGN_USIM**, which is computed as follows;

$$\mathbf{TSK} = \mathbf{RAND} \cdot \mathbf{SK\_USIM} \quad (1)$$

$$\mathbf{SIGN\_USIM} = \mathbf{SIGN}_{\mathbf{SK\_USIM}}(\mathbf{Term\_ID} \,\|\, \mathbf{USIM\_ID} \,\|\, \mathbf{RAND} \,\|\, \mathbf{TS}) \quad (2)$$

The symbol . denotes the point multiplication over Elliptic curve. The symbol $\mathbf{SIGN}_{\mathbf{SK\_USIM}}\mathbf{(M)}$ denotes that the signature of message **M** signed by the secret key of USIM, **SK_USIM**.

After this step, the terminal is keeping **TSK**, **RAND**, **TS** and **SIGN_USIM**.

3.2.3. Terminal – BSF

If there is no shared information with NAF, the terminal has to contact BSF.

The terminal sends **TERM_ID**, **KEY_REQ**, **SIGN_TSK**, **RAND**, **USIM_ID**, **TS,** and **SIGN_USIM** to BSF.

SIGN_TSK is computed as follows:

$$\mathbf{SIGN\_TSK} = \mathbf{SIGN}_{\mathbf{TSK}}(\mathbf{KEY\_REQ}) \quad (3)$$

The symbol $\mathbf{SIGN}_{\mathbf{TSK}}\mathbf{(M)}$ denotes that the signature of message **M** signed by the temporal private key **TSK**.

BSF verifies **SIGN_USIM** and **SIGN_TSK**. The validity of **TSK** is available from verifying **RAND** with **SIGN_USIM**.

When the verification is succeeded, BSF stores **RAND** and **TS** with **TERM_ID**, and sends the response **KEY_RES** back.

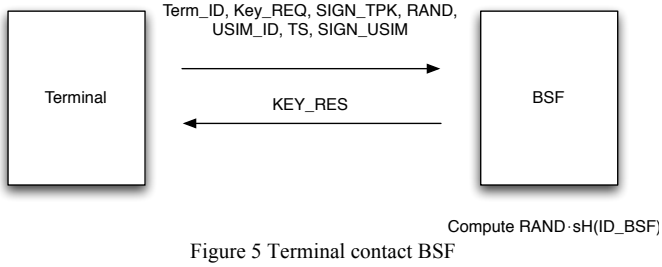

Figure 5 Terminal contact BSF

Figure 5 shows that the terminal contacts BSF to send the parameters for authentication.

3.2.4. Terminal – NAF – BSF

When the terminal contacts NAF, NAF has to be able to authenticate the terminal.

The terminal sends **TERM_ID**, **APPL_ID, and SIGN_TSK** to NAF, where **APPL_ID** is the identity of the application, and **SIGN_TSK** is the signature as follows;

$$\mathrm{SIGN\_TSK} = \mathrm{SIGN}_{\mathrm{TSK}}(\mathrm{TERM\_ID} \| \mathrm{APPL\_ID}) \quad (4)$$

IF NAF already authorized **TSK**, NAF verifies **SIGN_TSK**. In other case, NAF sends **TERM_ID** to BSF and requests the related information. BSF returns **RAND** and **TS** those are used for NAF to verify **SIGN_TSK**.

If the signature is valid, NAF provides its service to the terminal. Figure 6 shows that the terminal requests services to NAF and NAF authenticates the terminal from BSF.

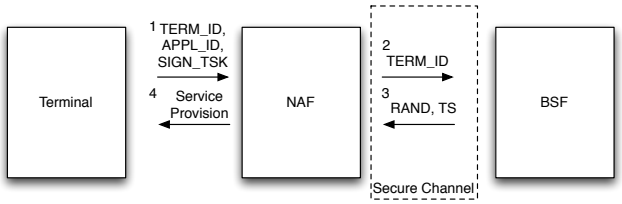

Figure 6 Terminal request services to NAF

3.2.5. Terminal – NAF, no BSF

Our model can remove the rold of the BSF in the architecture. In this case, the terminal sends **Term_ID, KEY_REQ, APPL_ID, SIGN_TSK, RAND, USIM_ID, TS, SIGN** can request the service to NAF, as shown in Figure 7.

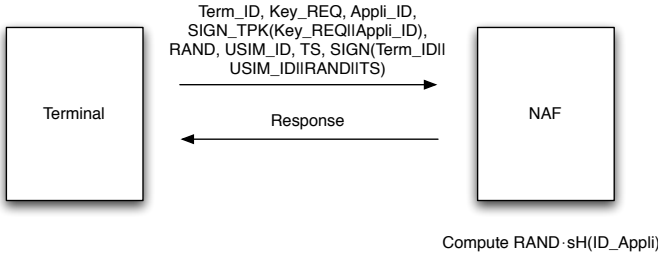

Figure 7 Terminal requests service to NAF only

Figure 8 briefly shows the overall process of our design.

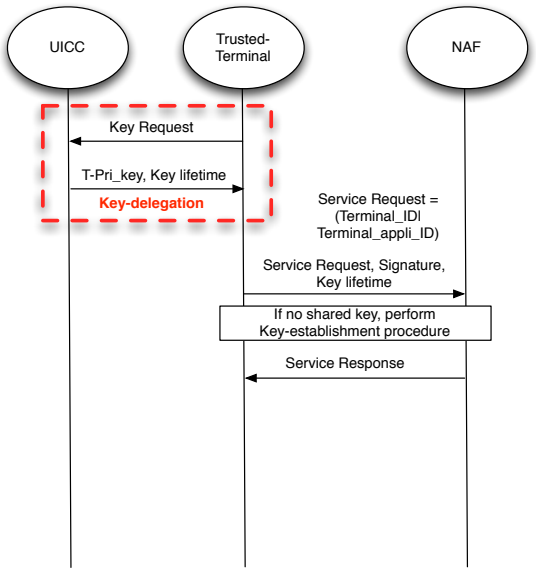

Figure 8 Overview of the proposed architecture

4. Security Analysis

The security of the architecture is based on the intractability of discrete logarithm problem.

We assume that the private key in the USIM is stored in secure. The security of USIM is considered as the security of the security storage of USIM, and the out of focus in this paper. When the terminal requests the temporary secret key **TSK** to the USIM, the USIM computes the Eq (1). The secret key is $sH(USIM\_ID)$, and **TSK** is $rsH(USIM\_ID)$. When **TSK**, r and $H(USIM\_ID)$ is known to terminal, the probability that the terminal knows the original secret key $sH(USIM\_ID)$ is same as the probability of solving ECDLP.

Even the terminal is compromised and TSK is sent to other adversary, the adversary should be able to generate **SIGN_USIM** for the freshness of **TS**.

Finally, we show that the **TSK** can be substituted with the original SK as follows:

1. Key exchange with **SK**

$$e(SK_{USIM}, Pub\_Key_{NAF}) = e(sH(ID_{USIM}), H(ID_{NAF}))$$
$$= e(H(ID_{USIM}), sH(ID_{NAF})) = e(Pub\_Key_{USIM}, SK_{NAF}))$$

2. Key exchange with **TSK**

$$e(TSK_{USIM}, Pub\_Key_{NAF}) = e(RAND \cdot sH(ID_{USIM}), H(ID_{NAF}))$$
$$= e(H(ID_{USIM}), RAND \cdot sH(ID_{NAF})) = e(Pub\_Key_{USIM}, TSK_{NAF})$$

Thus, **TSK** can be used as **SK** in secure.

5. Comparison

In this section, we compare our proposed design with current 3GPP generic authentication architecture as in the table 1.

	GBA[2]	**SSC[3]**	**Proposed**
Key type	Symmetric	Asymmetric	ID-based
HSS	Required	Required	Free
BSF	Required	Required	Free
Certificate management	N/A	Required	Free
Availability	Low	High	High
Standard	TS 33.220	TS 33.221	N/A
# of comm.	18 (7)	13 (7)	8/6 (4)

Applying the ID-based cryptosystem, we could reduce the number of communication from 18 ~ 13 times to 8 ~ 6 times.

6. Conclusion

In this paper, we argued the problem in the current generic authentication architecture of 3GPP and proposed the new design of GAA based on ID-based cryptosystem that has several benefits on public key management. Our design enables easy public key management that also prevents the leakage of private key in the USIM. Even though the pairing computation in IDBC has relatively large computational overhead, we propose the novel solution that we delegate the computation to the terminal.

Acknowledgment

This paper was the result of 'Next Generation Mobile Network Platform Security,' sponsored by Samsung-ICU Center Project.

References

[1] 3GPP Technical Report 33.919 3G Security; Generic Authentication Architecture (GAA); System description
[2] 3GPP Technical Specification 33.220 Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture
[3] 3GPP Technical Specification 33.221 Generic Authentication Architecture (GAA); Support for Subscriber Certificate
[4] 3GPP Technical Specification 33.102 3G Security; Security Architecture
[5] 3GPP Technical Specification 33.401 3GPP System Architecture Evolution (SAE); Security Architecture
[6] 3GPP TR 33.821 Rational and track of security decisions in Long Term Evolution (LTE) RAN/ 3GPP System Architecture Evolution (SAE)
[7] G. Kambourakis, and A. Rouskas, "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems," EURASIP Journal on Wireless Comm. And Networking. Vol.1, pp. 184-197, 2004
[8] L. Martin, "Introduction to Identity-Based Encryption", ISBN-13: 978-1-59693-238-8, published by Artech House, Inc., 685 Canton Street, Norwood, MA 02062, 2008