# Concealing IMSI in 5G Network Using Identity Based Cryptography

Mohsin Khan and Valtteri Niemi

University of Helsinki, Department of Computer Science,
P.O. Box 68 (Gustaf Hällsträmin katu 2b)
FI-00014 University of Helsinki
Finland
{mohsin.khan,valtteri.niemi}@helsinki.fi

**Abstract.** The aspirations for the next generation mobile network (5G) are high. It has a vision of improved security and privacy over the existing LTE network. Subscription privacy of a user has been a historical concern with all the previous generation mobile networks, namely GSM, UMTS, and LTE. While a little improvement have been achieved in securing the privacy of long-term identity of a subscriber, the so called IMSI catchers are still in existence even in the LTE and advanced LTE networks. This report looks into this problem of concealing long-term identity of a subscriber and presents different techniques of using public-key cryptography to tackle it. One special case of public-key crytography is identity based crypto. A rigorous comparison among the pros and cons of the different techniques show that identity based cryptograpy is a potential solution for securing the long-term identity privacy of a user in the 5G network.

## 1 Introduction

NGMN Alliance has pointed out the privacy of a user as a requirement of the 5G network under the requirement category of enhanced services [1]. In 3GPP TR 33.899 [2], subscribers' privacy is captured as one of the high level security requirements of the 5G network. However, in the context of diversified devices and the complex business and service model of 5G, it is important to define who is a subscriber and what subscriber-privacy means. According to 3GPP TR 21.905 [3] a subscriber is an entity (associated with one or more users) that is engaged in a subscription with a service provider. A subscription describes the commercial relationship between the subscriber and the service provider, cf. 3GPP TR 21.905 [3]. A subscription identifier is the identifier that uniquely identifies a subscription in the 3GPP system. The identifier is used to access networks based on 3GPP specifications. Subscription Privacy refers to the right to the protection to any information that (a) can be used to identify a subscription to whom such information relates, or (b) is or might be directly or indirectly linked to a subscription. This definition of privacy suggests to protect any personally identifiable information (PII) from an active or passive attacker. While it is important to classify the identifiers into PII and non-PII, the long-term identifier is surely a PII. In this report we will keep our discussion limited only to the case of long-term identifier of a subscriber. In the case of 2G (GSM), 3G (UMTS) and 4G (LTE) networks, this long-term identifier is known as international mobile subscriber identity (IMSI). Nevertheless, the same principles used in the solutions proposed in this report can be extended to conceal any PII.

One approach of protecting IMSI privacy is to use a temporary IMSI instead of the original IMSI and keep changing the temporary IMSI at a feasible frequency. Note that the temporary IMSI has to be assigned over a confidentiality protected channel and different entities of the network may assign different temporary IMSIs to the user equipment (UE). In the LTE network, the temporary IMSI assigned by serving network (SN) is called globally unique temporary identity (GUTI) and the home network (HN) does not assign any temporary IMSI to the UE. However, during the initial attachment of a UE to the SN, the UE has neither a GUTI nor a security context with the SN that can assign it with a GUTI. Besides, GUTI can be lost by either one or both of the UE and the SN. This forces the UE to reveal its IMSI to the SN to keep itself from permanently locked out of the network. This problem gives an opportunity to an active IMSI catcher (AICa) who impersonates a legitimate SN and forces the UE to run the initial attachment protocol. This also gives an opportunity to a passive IMSI catcher (PICa) to eavesdrop the IMSI sent in clear text. Solutions [5, 4] have been proposed by using temporary IMSI known as pseudonym assigned by the HN. While these solutions solve the cases of lost and unsynchronised GUTI, they still have the problem of lost or unsynchronised pseudonyms and also initial attachment. In this report we present how a security context can be set up in between the network (either with SN or HN) and the UE even before the identification of the UE so that the UE can use the security context to send its IMSI with confidentiality protection. Such a security context will mitigate the attack mounted by a PICa. Nevertheless, we show that an AICa would not be able to agree on a legitimate security context with the UE and consequently will not be able to reveal the IMSI.

In order to present a formal discussion we need to know what are the entities involved in this identification process, what are the communication interfaces among those entities and how much the entities can be trusted with the IMSI. As the architecture of 5G security is yet to be finalized, we present an abstraction of the involved entities and assume that whatever the security architecture of 5G eventually be, it will contain these entities and interfaces. This abstraction is directly extracted from LTE security architecture and we use some LTE acronyms to present the entities for better understanding. Figure 1 shows the entities. It involves the UE, serving radio network (eNB), serving core network (MME), HN. We have two more entities: PICa and AICa. The interface UE-NB in between UE and eNB is initially unprotected. Nevertheless, eNB-MME and MME-HSS are always protected and the security of these interfaces is out of the scope of this report. The PICas eavesdrop on the UE-eNB interface when it is unprotected to extract an IMSI. The AICas impersonate a legitimate SN and

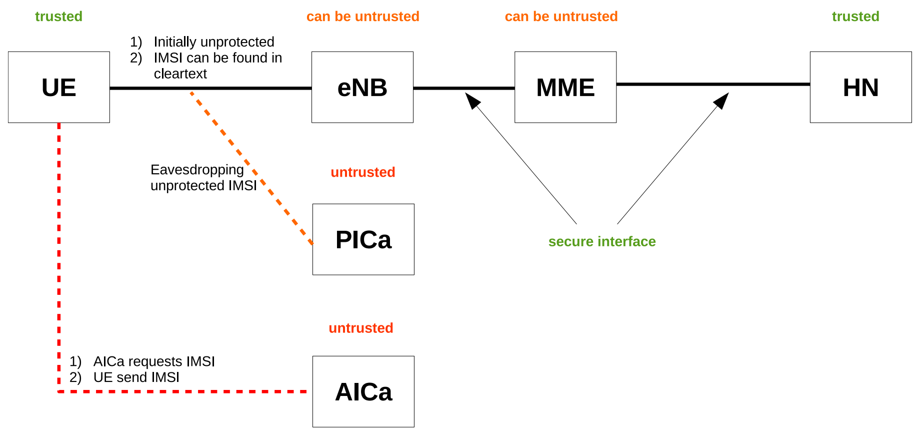


**Fig. 1.** High-level security architecture

run a legitimate protocol with the UE in order to reveal the IMSI. HN and UE both own the IMSI and they are trusted with it. Both of PICa and AICa are untrusted while it is technically possible to not trust eNB and MME. However, by some other specification in 3GPP TS xx.xxx it is required to reveal IMSI to the MME to enable lawful interception (LI) without involving HN.

We propose different solutions based on public-key cryptography which make the UE-eNB interface protected even during the initial attachment to fight against the PICa. Our solutions also stop the AICa from running a legitimate protocol successfully that could reveal the IMSI. However, there are other 5G requirements which our solutions should also meet. Such requirements are: reduced signalling overhead, improved control plane latency, concealing all the parts of IMSI (MCC, MNC and MSIN). To avoid the downgrade attack, the solutions need to be backward compatible with the legacy networks. Also, in the case of public-key, the complexity involved in setting a PKI and revocation of a publick-key need to be considered with high importance. Considering all these requirements, we evaluate our solutions based on the following criteria:

1. Concealed from PICa, AICa, eNB, MME
2. Parts of the IMSI concealed
3. Signalling overhead
4. Latency
5. Backward compatibility
6. PKI complexity
7. Public-key revocation and re-provisioning

While the choice of the solution is dependent on how much want to achieve, hybrid solution using identity based public-key cryptography and pseudonyms appear to be a promising solution.

In Section 2 we present a quick intro to identity based cryptography (IBC). In Section 3 we present the solutions. In Section 4, we present a rigorous solution based on the aforementioned evaluation criteria. Finally we conclude the paper in Section 6

## 2 IBC in the Jargon of Cryptography

Modern-day cryptography can be broadly categorized into two categories depending on how the keys are used to encrypt and decrypt the message. In symmetric key cryptography the sender and receiver share a secret key which is used for encryption and decryption both. In public-key cryptography the receiver has a pair of keys. One of the keys is public and the other is private. The public key is used by the sender to encrypt the message and the private key is used by the receiver to decrypt the message. While the challenge in symmetric key cryptography is to create a key known only by the sender and receiver but no one else, one major challenge in public-key cryptography is to authenticate the public key.

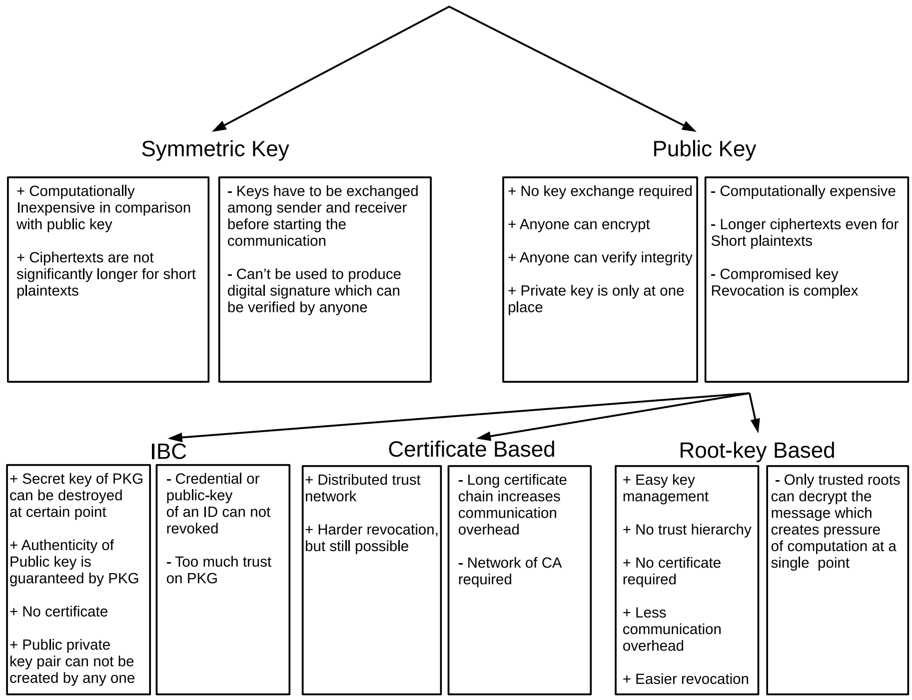


**Fig. 2.** IBC in the Jargon of Cryptography

Based on the authentication mechanism, public-key cryptography can be categorized into three more categories:

1. Certificate based
2. Root-key based
3. Identity based, which is known as IBC

Figure 2 shows this categorization with advantages and disadvantages of the respective categories. In the certificate based case, the public key is signed by a trusted third party. In the root-key based case, no runtime authentication of the public key is required because a very limited number of public key is used in the system and all the senders are pre-provisioned with all the existing public keys. In the IBC case, the public key of a receiver is computed from the identity of the receiver and the public key of a trusted third party. However, the private key of the receiver is computed from the identity of the receiver and the private key of the trusted third party. This private key has to be securely provisioned to the receiver by the trusted third party. In this case, even though an extra one-time burden of private key provisioning is required, the sender does not need to authenticate the public key of a receiver, because if the public key is not authentic, the receiver will not have the private key and any message encrypted by the public key will never be decrypted. In other words, the authenticity of the public key in IBC is guranteed by the trusted third party. Usually in IBC, the trusted third party is known as the private key generator (PKG). While in the certificate based and root-key based case it is possible to revoke the public key of a receiver, it is impossible to revoke the public key in IBC unless the identity itself is revoked. In Figure 3 we show how IBC works pictorially.

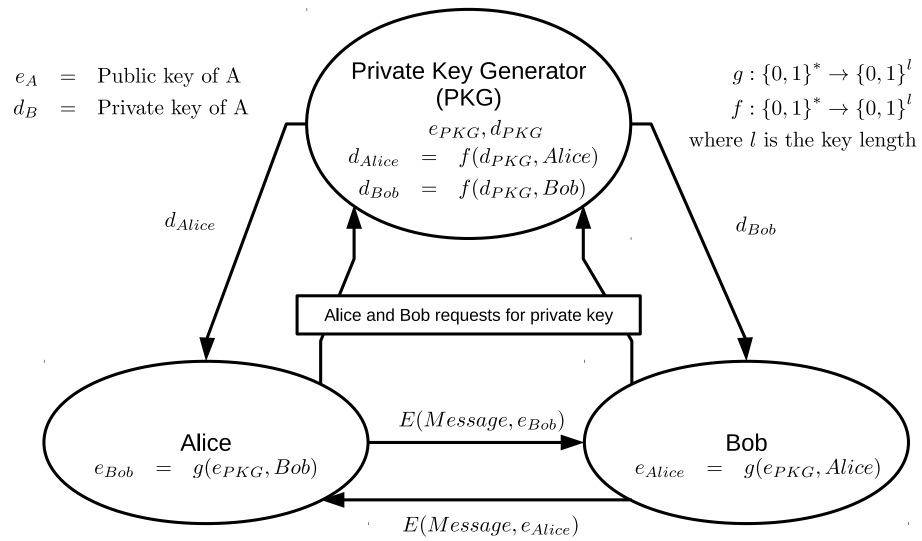


**Fig. 3.** IBC mechanism

# 3 Solutions

# 4 Evaluation

Here we use public key cryptography which may or may not be based on identity based crypto to secure the privacy of the long term identity of a mobile phone user called IMSI (International mobile subscriber identity). We discuss different techniques of using the public key cryptography:

1. Identity based crypto based on the identity of SN where the HN is the key generator
2. HN assigned public private key pair for each SN
3. HN owned public private key pair

In the consequent sections we describe the aforementioned techniques in further detail.

# 5 Based on Identity of Serving Network

In this technique the HN has a public and private key pair. Every phone knows the public key of the HN. Whenever a SN asks the phone to provide its IMSI, the phone computes the public key of the SN using the public key of the HN. Then the phone encrypts the IMSI with the computed public key of the SN and sends it to the SN along with the HN identity. The SN obtains (possibly already have obtained) its private key from the mentioned HN. Using this private key, the SN can decrypt IMSI. Figure **??** represents the high level protocol.

## 5.1 Concerns and Solutions

1. How to provision, revoke and re-provision the public key of HN in the phone?
2. How to black list a SN?

## 5.2 Based on HN generated public private key pair for every SN

# 6 Conclusion

# 7 Acknowledgement

# References

[1] NGMN 5G White Paper V1.0 [cited Jan, 2017]. Available at: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf
[2] 3GPP TR 33.899 V0.6.0 [cited Jan, 2017]. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

[3] 3GPP TR 21.905 [cited Jan, 2017]. Available at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558

[4] Karl Norrman, Mats Nslund, Elena Dubrova: Protecting IMSI and User Privacy in 5G Networks. 2nd International Workshop on 5G Security

[5] Philip Ginzboorg, Valtteri Niemi: Privacy of the long-term identities in cellular networks. Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications Pages 167-175