

Privacy Protected Subscriber Identification in 5G Network

Mohsin Khan and Valtteri Niemi

University of Helsinki, Department of Computer Science,
P.O. Box 68 (Gustaf H  llstr  min 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 encryption to tackle it. One special case of public-key encryption is identity based encryption. A rigorous comparison with the pros and cons among the different techniques show that identity based encryption is a potential solution for securing the long-term identity privacy of a user in the 5G network.

1 Introduction

The 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 [4] 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 [4]. 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 protect 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 attacker. While

it may be difficult to draw a clear boundary between PII and non-PII, the long-term identifier is surely a PII. In this report we will restrict our discussion only to the case of identification of an UE using long-term identifier of the relevant 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. An IMSI is usually presented as a 15 digit number but can be shorter. The first 3 digits are the mobile country code (MCC), which are followed by the mobile network code (MNC), either 2 digits or 3 digits. The length of the MNC depends on the value of the MCC. The remaining digits are the mobile subscription identification number (MSIN) within the network's customer base [3]

One approach of protecting IMSI privacy is to use a temporary identifier instead of the actual IMSI and keep changing the temporary identifier at a feasible frequency. Note that the temporary identifier has to be assigned over a confidentiality protected channel and different entities of the network may assign different temporary identifiers to the user equipment (UE). In the LTE network, the temporary identifier assigned by serving network (SN) is called globally unique temporary identity (GUTI) and the home network (HN) does not assign any temporary identifier 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 would force 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 (AIC) 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 (PIC) to eavesdrop the IMSI sent in clear text. Solutions [6, 5] 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 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 PIC. Nevertheless, we show that an AIC would not be able to agree on a legitimate security context with the UE and consequently will not be able to find out the IMSI.

In order to present a formal discussion we need to know what are the entities involved in this identification process and what are the communication interfaces between those entities. We also need to know which entities can be entrusted with the IMSI of a subscriber. As the architecture of 5G is yet to be finalized, we present an abstraction of the involved entities and assume that whatever the architecture of 5G eventually be, it will contain something for each of these entities and something for each of these interfaces. This abstraction is directly extracted from LTE architecture. Figure 1 shows the entities. It involves the

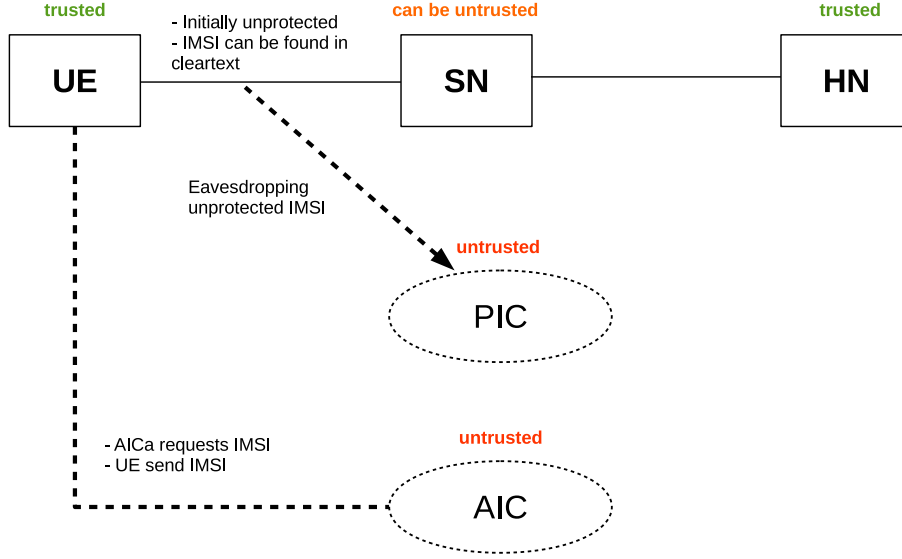


Fig. 1. High-level security architecture

UE, serving network (SN) and HN. Both of the SN and HN consist of radio access network (RAN) and core network (CN). The RAN of SN provides the connectivity in between UE and CN of SN. On the other hand, the CN of SN connects itself with the CN of HN. However, we do not present such granularity of SN and HN, because in our discussion it is sufficient to treat the SN and HN as single abstract entities. Note that in a non-roaming situation, the SN and HN are the same network. There are two more entities which are not part of the network but relevant in our discussion, because they attack the network. They are PIC and AIC. The interface UE-SN is a logical interface in between UE and SN. This interface is initially unprotected. The logical interface SN-HN in between SN and HN is protected and the security of these interfaces is out of the scope of this report. The PICs eavesdrop on the UE-RAN interface when it is unprotected to extract an IMSI. The AICs impersonate a legitimate SN and run a legitimate looking protocol with the UE in order to find out the IMSI. HN and UE both know the IMSI and they are trusted. Both of PIC and AIC are untrusted. It is in principle possible not to trust SN. However, by another specification in 3GPP TS **xx.xxx** it is required to reveal IMSI to the SN to enable lawful interception (LI) without involving HN.

We propose different solutions based on public-key encryption that make the UE-SN interface protected even during the initial attachment in order to fight against the PIC. Our solutions also stop the AIC from running a legitimate protocol successfully that could force the UE to reveal the IMSI. However, there are other 5G requirements which our solutions should also meet. Reduced signalling overhead, improved control plane latency are two such requirements. Concealing

all the parts of IMSI, namely, MCC, MNC and MSIN has been identified as another requirement. Also, in the case of public-key, the complexity involved in setting a PKI and revocation of a public-key need to be considered with high importance. In some cases the public key of an entity is pre-provisioned to all the potential senders in the system. If this public key is revoked and a new public-private key pair is generated by this entity, then the new public key needs to be re-provisioned to all those entities that were pre-provisioned with the old public key. Considering all these requirements, we evaluate our solutions based on the following criteria:

1. Concealed from PIC, AIC, SN
2. Parts of the IMSI concealed
3. Signalling overhead
4. Latency
5. PKI complexity
6. Public-key revocation and re-provisioning

We also want to see if any of these solutions would work in a heterogeneous situation where one or more of the entities involved would come from the legacy networks. Apparently, none of the legacy networks use public-key encryption. On the other hand, all of the solutions presented in this report use public-key encryption. Therefore, it can be said that none of the solutions presented in this report will work in such a heterogeneous situation. While the choice of the solution is dependent on how much we want to achieve, hybrid solution using identity based public-key encryption and pseudonyms appear to be a promising approach.

In Section 2 we present a quick introduction to the different kind of public-key encryption we have used in this report. In Section 3 we present the solutions. In Section 4, we present a rigorous evaluation of the presented solutions based on the aforementioned evaluation criteria. Finally we conclude the paper in Section 5

2 Identity Based Encryption (IBE) in the Jargon of Encryption

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

Public-key encryption can be further categorized into three more subcategories based on the authentication mechanism used to verify the public keys:

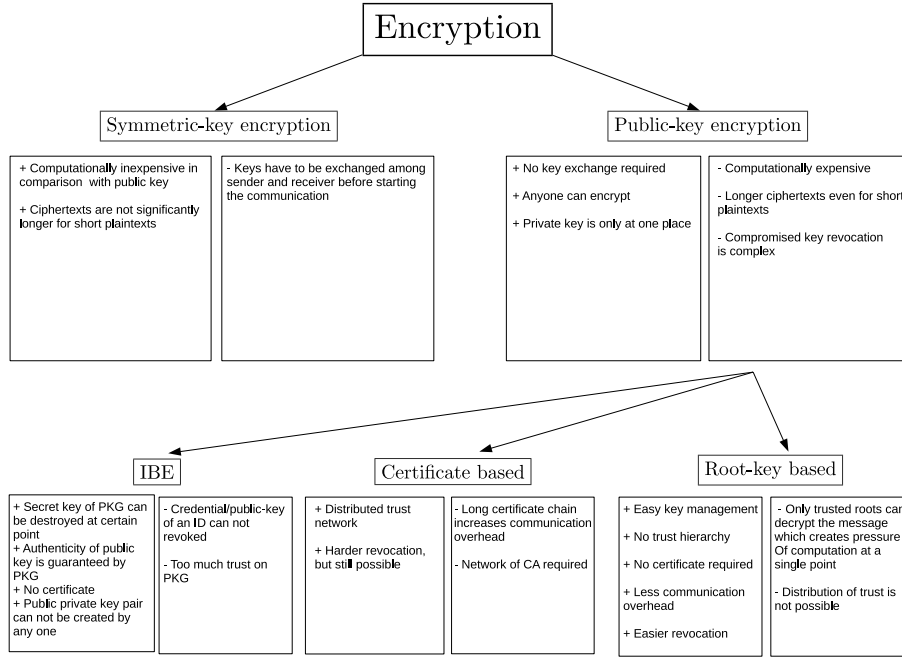


Fig. 2. IBE in the Jargon of Encryption

1. Certificate based encryption
2. Root-key based encryption
3. IBE

Figure 2 shows this categorization with advantages and disadvantages of the respective categories. Please note that this classification is drawn considering only the encryption operation. Different classifications could be drawn based on other cryptographic operations for example digital signature, hashing or MAC. Nonetheless, we use this classification, because in this report we present solutions based on the public-key encryption and we want to come up with at least one solution using each of the possible subcategories of public-key encryption. We believe this is a systematic approach which makes the comparative evaluation easier and meaningful.

In the certificate based encryption, the public key is signed by a trusted third party. The sender of the message has to be pre-provisioned with the root certificate so that the sender can authenticate the public key of the receiver. In the root-key based encryption, no runtime authentication of the public key is required, because a very limited number of public keys are used in the system and all the senders are pre-provisioned with all the existing public keys. In IBE, the public key of a receiver is computed from the identity of the receiver and the public key of a trusted third party. The public key of the trusted third party has to be provisioned to sender. The private key of the receiver is computed from

the identity of the receiver and the private key of the trusted third party. The private key of the receiver has to be securely provisioned to the receiver by the trusted third party.

In the next section we present solutions based on different public-key encryption schemes. While presenting the solutions we will discuss more about how these different kind of public-key encryption works.

3 Solutions

It is beneficial to introduce some notation here before delving into the solutions.

1. $hnid = MCC||MNC$ identifies the HN
2. $snid = MCC||MNC$ identifies the SN
3. e_A is the public key of entity A
4. d_A is the private key of entity A
5. $\mathcal{X}_{A,B}(e_A, e_B)$ is the certificate of the public key e_A of A issued and signed by B which can be verified using the public key e_B . The certificate is a guarantee from B that the public key e_A is owned by A .
6. E, D are the encryption and decryption functions respectively

3.1 Certificate Based Public-key Encryption

In certificate based public-key cryptography, certificates digitally signed by trusted third parties are used to authenticate the ownership of a public key. The trusted third party who can sign the certificate is called a certificate authority (CA). It is possible to build a chain of trust in certificate based public-key cryptography by allowing an entity to become a CA who is certified by another CA. A certificate contains a digital signature which allows anyone to verify the validity of the certificate by verifying the digital signature using the public key of the CA who provided the certificate. There has to exist at least one CA in a chain of trust whom the verifier already trusts. There might exist entities who certifies themselves and some verifiers trust these entities. The entities having a self signed certificate who are trusted by verifiers are considered as the root CA for those verifiers and the corresponding certificates are called root certificates. To use certificate based public-key cryptography to secure IMSI privacy, we need to figure out few things first: who are the root CAs and who else can be a CA, who are the entities that own a public key, how a certificate can be revoked and how the UE can be re-provisioned with a new root certificate if required.

We choose the HN of a subscriber as the root CA for the subscriber. This is a reasonable choice, because in any case the HN knows the IMSI of a subscriber. In the later phase of the attachment when an authentication protocol will take place, the UE will most probably have to reveal the IMSI of the subscriber to the HN. So, the HN has to be entrusted with the IMSI itself. As a result the choice of entrusting the HN with the key which protects the IMSI is reasonable. HN owns a self signed certificate which is the root certificate. Every UE having

a subscription of the HN is provisioned with the root certificate. An SN owns a public key certified by HNs.

The solution has three different phases as presented in in Figure 3. In the provisioning phase the network generate public-private key pair and provision the public key to all its subscribers. As shown in step 1 of this phase, the HN generates a public-private key pair and generates a certificate of the public key signed by the HN itself. In step 2, a UE is provisioned with the self signed certificate which was generated in step 1. Please note that step 1 is performed when HN is installed. Step 2 is performed when a UE is provisioned with the subscription of the HN. However, in case of compromised private key of HN, the provisioning phase (both step 1 and 2) is required to be performed again. We will discuss this issue later in this subsection.

During the roaming agreement in between two networks, the SN obtains a certificate from the HN. In step 1 of this phase, the SN sends its public key e_{snid} and $snid$ to the HN. The HN generates a certificate $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$. This certificate is a guarantee from the HN that the public key e_{snid} is owned by the network identified by $snid$ and is verifiable by the public key e_{hnid} .

In the identification phase, the SN broadcasts the its identity in step 1. The UE decide to attach with the SN in step 2 and sends $hnid, e_{hnid}$ to the SN in step 3. In step 4, the SN looks up for the certificate $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$. In case it exists at the disposal of the SN, in step 5 the SN sends $\mathcal{X}_{snid,hnid}(e_{snid}, e_{hnid})$ to the UE. The UE verifies the certificate in step 6 and extracts the public key e_{snid} from the certificate. If the certificate is verified as valid, then in step 7 the UE sends the IMSI to the SN encrypted by the public key of the SN. To avoid the ciphertext to be the same every time, the UE concatenates a *salt* at the end of the IMSI of agreed length before encryption. SN decrypts the ciphertext, discard the salt from the tail and extracts the IMSI. This completes the identification of a UE to SN. Figure 3 shows the protocol in detail. Note that in the roaming agreement phase the SN does not need to get the certificate exactly from the HN, but the SN can get it from any CA who is trusted in by the HN in the chain of trust.

This approach can not conceal MCC and MNC. It coneals MSIN from AIC, PIC. The IMSI is revealed entirely at SN. It requires a full round trip signalling in between UE and SN before sending the encrypted MSIN. It carries $hnid$ from UE to SN and in return carries the public-key certificate back from SN to UE. Public keys are quite large, length of a minimum ciphertext is also very long comparatively, and the certificate chain can be quite long. Consequently it adds significant signalling overhead. Also, public-key cryptography is computationally heavier than that of symmetric-key cryptography. As a result, latency will increase significantly to verify the certificate and encrypt the IMSI. Nevertheless, once an UE is identified by the network, the network assigns a GUTI to the UE. It is a question for further research to evaluate the effect of this extra signalling overhead and increased latency. This solution is not backward compatible with LTE, UMTS and GSM. It doesn't require to establish any new trusted authority,

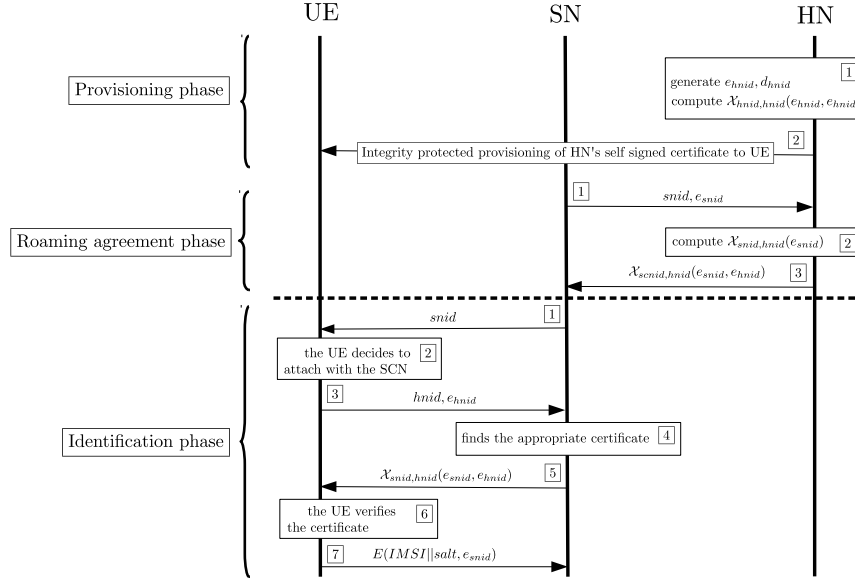


Fig. 3. Privacy protected UE identification using certificate based public-key encryption

so PKI complexity is very little. However, revocation of the public-key of an SN and HN is not trivial and need to be investigated closely.

Every CA in the system maintains a list of revoked public keys which were certified (at the first place) by it or by any other CA trusted by it. If there is a revocation, the CA who provided the certificate at the first place updates its revoked list and the CA updates its CA with the information. The UE periodically runs a protocol with HN to download the latest revoked public keys. If a dishonest SN presents an UE with the certificate which is already revoked but the UE has not yet been able to download it, then the MSIN will be revealed to the SN. However, such a dishonest SN will fail to run a successful authentication protocol. As soon as the UE come in touch with a legitimate SN, it identifies itself successfully, runs a successful authentication protocol, and download the latest revocation list from the HN. Thereafter the dishonest HN will not be able to reveal the MSIN any more. This implies that an AIC can mount an attack if it was once trusted by the HN as a legitimate SN but is no more trusted by the HN and the UE is not yet updated with the withdrawal of the trust. The existence of such an AIC is apparently extremely rare. The time window this attack allows to track a subscriber is also very small. Altogether this makes the attack very expensive. However, if the private key of an SN is stolen, both PIC and AIC can mount attacks until the public key is revoked.

When the private key of an HN is compromised, the HN updates itself with a new public-private key pair and generates a new root certificate. All the relevant certificates in the system get updated with the required changes according to the standard PKI procedure. However, every UE that has a subscription with the HN needs to be re-provisioned with the new root certificate. The re-provisioned is required because an AIC with the knowledge of the compromised private key will be able to mount a successful attack and find the IMSI. However, there is a synchronization problem need to be considered in this case. If an SN is updated with the new root certificate and the UE does not have the new root certificate, then the UE will never be able to verify the certificate presented by a legitimate SN. To circumvent this problem the SN stores certificates chained with all the root certificates used by an HN. The SN first checks the e_{hnid} sent by the UE. The SN then finds the certificate provided by the HN in which the root certificate is of e_{hnid} . Once the UE is identified by the SN and authentication becomes successful, the HN knows the location of the UE. At this point the HN can send the new root certificate to the UE integrity protected by the master symmetric key shared by the HN and the USIM. Another way is to publish the new root certificate in the public media with integrity protection so that anyone can download the root certificate using some other internet connection. The need for re-provisioning the UE with a new root certificate is an extremely rare event. In case the root private key is stolen by an attacker, it allows the attacker to act as both AIC or PIC. Once the need for existing root certificate revocation and provisioning of a new one is identified, it does not allow the attacker a long time window to track the UEs. However, protecting the confidentiality of a private key and detecting the compromise of a private key is a whole different security question and we do not delve into that in this report.

3.2 Certificate Based Public-key Cryptography with a very short trust chain

The use of a very short trust chain is exactly the same mechanism as described in section 3.2 except that only a HN can be a CA. As a result the chain of trust is very short and consequently the certificate chains are not very long. Also as only an HN is a CA, the revocation of a public-key is found completely in HN at any point of time. Whenever the UE is attached to a legitimate network, it can download the revocation list from the HN. Figure 4 shows the protocol in detail. If the HN's public key need to be changed and provisioned again to the UE, it can be done in the same way as discussed in 3.2.

This protocol has the downside of heavy computational requirements and signalling overhead due to large size of public key and ciphertext. However, due to short certificate chain, it reduces the signalling overhead and computational latency comparatively.

Nevertheless, the burden of exchanging the certificates and verifying them can be avoided to some extent by periodically provisioning the UE from the HN by the public key of the probable SNs the UE might visit in near future. If the SN asks for the IMSI from the UE, the UE looks for a public key of the SN in the

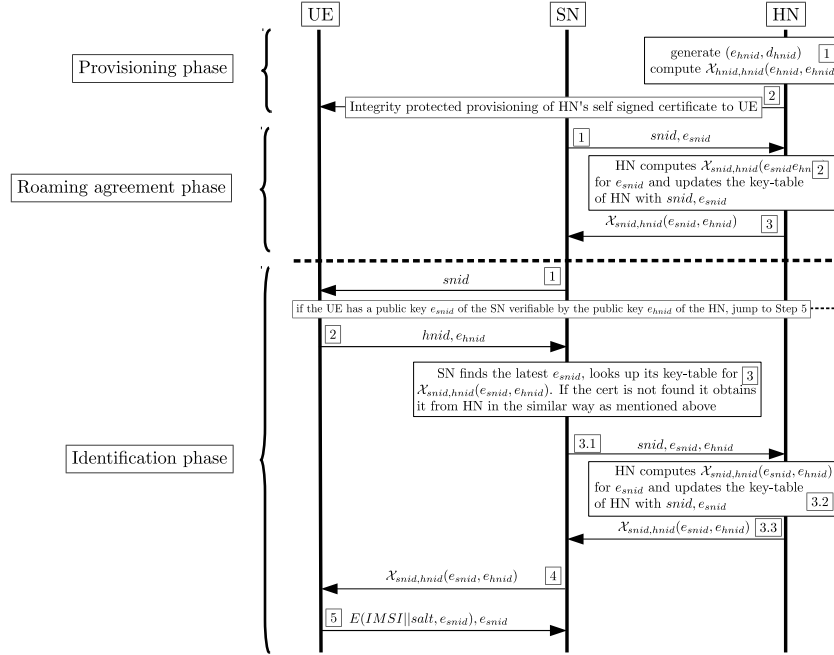


Fig. 4. Privacy protected UE identification using certificate based public-key cryptography with a short trust chain

key-table of the UE provisioned by HN. If it finds a public key e_{snid} , it encrypts the IMSI with the public key and sends the ciphertext to the SN via RAN along with e_{snid} without asking a certificate for the public key from the SN. If an SN is likely to be visited by an UE, the HN will most likely provision the UE with the public key of the SN. Hence, the exchanges of certificates are most likely the cases when AICs are asking for the IMSI. In such a case, the cost of heavy computation and signalling overhead can be considered as the price of detecting AICs. With these modifications the protocol evolves to the one presented in Figure 5.

3.3 Solution based on a Single Root-key

This is called root-key based solution because there is only one public key that an UE needs to know about. It is the public key of the HN and we call it to be the root-key. This public key is provisioned to all the UE which have subscriptions with the HN. Whenever an UE is in need of identifying itself to a SN with the IMSI, the UE encrypts the IMSI with the public root key and sends the result to the SN along with the $hnid$. Note that the UE concatenates a random salt at the end of the IMSI before encryption to avoid having the same encryption result every time. The SN sends the encrypted IMSI to the appropriate HN. The HN

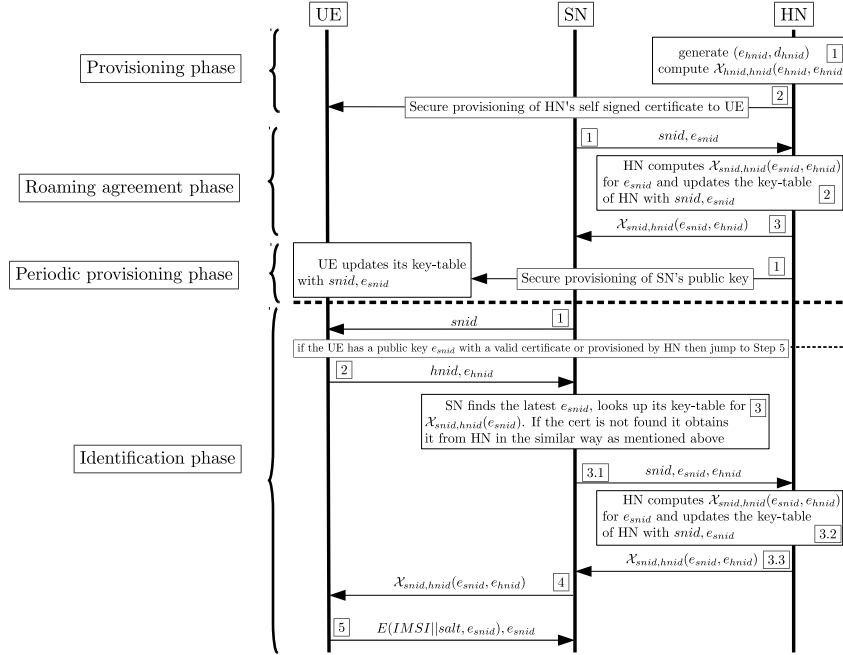


Fig. 5. Privacy protected UE identification using certificate based public-key cryptography with a short trust chain and pre-provisioned public key of the SNs

decrypts and extracts the IMSI. To facilitate LI, the HN sends back IMSI to SN with both integrity and confidentiality protection. Figure 6 shows the protocol in detail.

This approach can not conceal $hnid$. It conceals MSIN from AIC, PIC, RAN and SN. It doesn't need to transfer and verify the certificate each time the protocol is run. This approach reduces the signalling and computational overhead compared to certificate-based approach. However, the problem of heavier computation for public-key encryption and large ciphertext expansion remains as downsides of this solution. Nevertheless, once an UE is identified by the network, the network assigns a GUTI to the UE. It is a question for further research to evaluate the effect of these downsides in signalling overhead and increased latency. This solution is not backward compatible with LTE, UMTS and GSM. It doesn't require to establish any new trusted authority, so there is no PKI complexity involved.

When the private key of the HN is compromised, the HN generates a new pair of keys. All the UEs of the HN has to be re-provisioned with the new public key. If not, then someone who has access to the private key will be able to eavesdrop the encrypted IMSI and decrypt it. Also someone who gets access to the private key will be able to mount an active attack. However, if the public

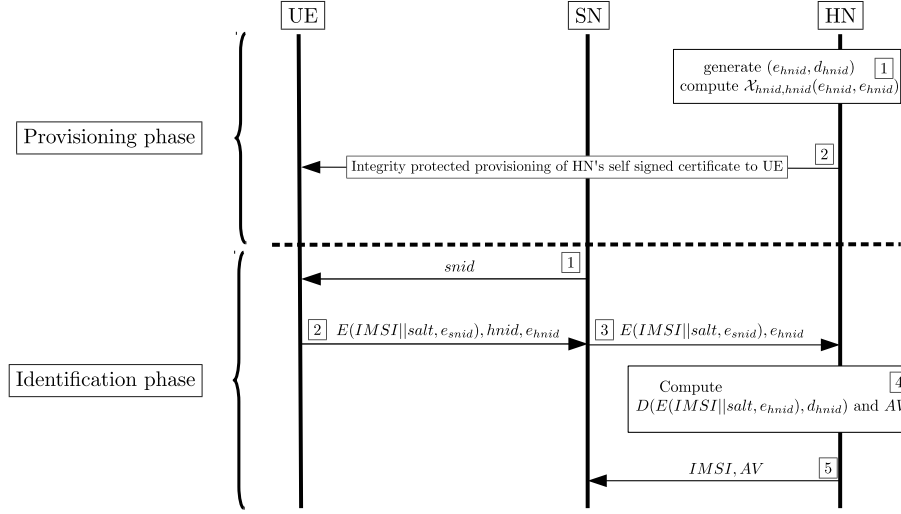
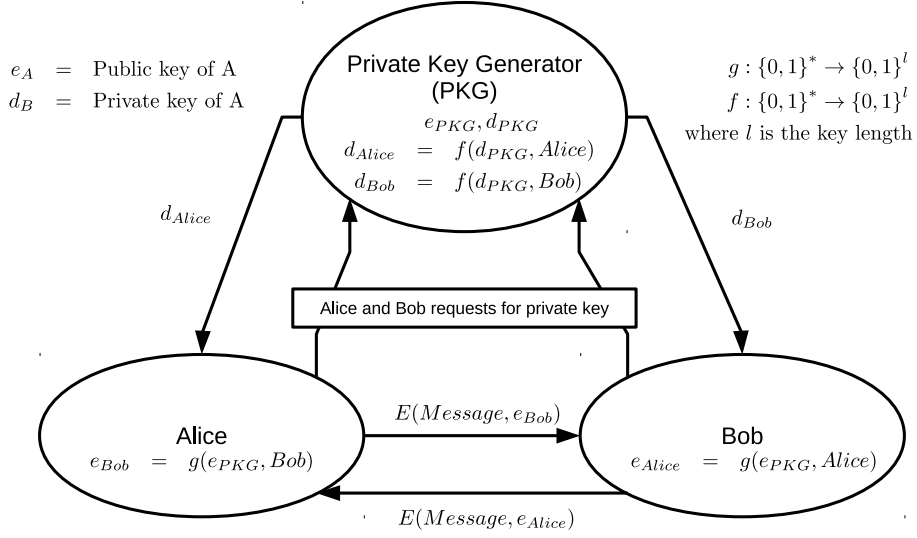
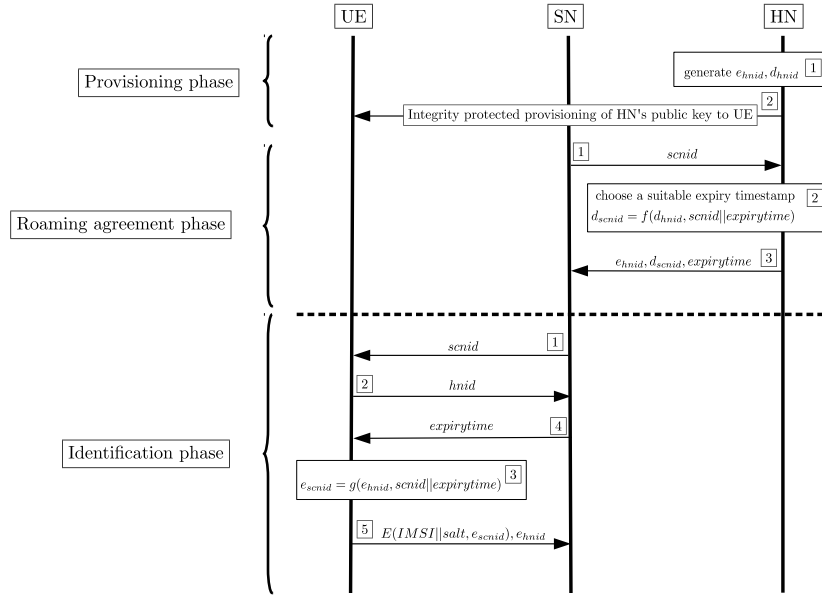


Fig. 6. Privacy protected UE identification using a single root-key

key in the HN is changed and an UE not provisioned with the new public key sends the encrypted IMSI to the HN via a legitimate SN, the HN will not be able to decrypt it with the new private key. To circumvent this problem, the HN provides a key identifier while provisioning an UE with a public key. And the UE sends the key identifier (kid) along with the encrypted IMSI to inform the HN which private key should be used to decrypt the IMSI.

3.4 Solution based on IBC

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. The sender does not need to authenticate the public-key, 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 guaranteed 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 7 we show how IBC works pictorially.

**Fig. 7.** IBC mechanism**Fig. 8.** Privacy protected UE identification using IBC

4 Evaluation

5 Conclusion

6 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 TS 23.003 V14.2.0 [cited Jan, 2017]. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=729>
- [4] 3GPP TR 21.905 [cited Jan, 2017]. Available at: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558>
- [5] Karl Norrman, Mats Näslund, Elena Dubrova: Protecting IMSI and User Privacy in 5G Networks. 2nd International Workshop on 5G Security
- [6] 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