3GPP TSG SA WG3 Security — S3#29 **S3-030397**
15 - 18 July 2003
San Francisco, USA

Agenda Item: **7.9 Support for Subscriber Certificates**

Source: **Nortel Networks**

Title: **User authentication by Service Platforms**

Document for: **Discussion and Decision**

1. Introduction

This contribution considers the relationship between the more general problem of "User authentication by a service platform" and the Support for Subscriber Certificates work currently on-going in SA3. We conclude that there is a need for 3GPP to make some decisions on the principles that will be followed in the overall Security architecture selections for various 3GPP work items when addressing the problem of user authentication by various service platforms.

The general problem of "User authentication by a service platform" appears within 3GPP PS domain work more and more often. Whenever a new service is designed, there is a requirement to ensure that only authorised users access the service. To do this, we need to securely identify the user in some way ("authentication").

For example, in IMS, the S-CSCF needs to securely identify the user as part of the registration procedure and the P-CSCF needs to securely identify the user for each non-REGISTER message. There will be similar requirements for MBMS and other services in future. For example, in WLAN there is a requirement to securely identify the users when they attempt a tunnel establishment.

There are several approaches to this problem. In order to avoid proliferation of different approaches within the 3GPP system (and consequent duplication of functionality), we believe that there is a need to consider whether a common approach should be recommended for future applications.

2. Discussion

There are in principle four ways to securely identify the sender of a request/message in a 3GPP system:

1) By completing a SIM or AKA authentication exchange between the user and the server requiring authentication

2) By the user signing the message with some key (e.g., Integrity Key) which was agreed during some previous SIM or AKA authentication exchange

3) By the user signing the message with a Digital Certificate

4) If the network is secure against IP address spoofing, by checking the source IP address of the message against the address allocated to the user

We consider each of these in turn.

2.1 SIM/AKA exchange

This is the approach taken by the S-CSCF for the IMS Registration phase and also by the 3GPP AAA server for WLAN Authentication. This approach requires:

- A challenge/response message exchange
- Access by the server to Authentication Vectors from the AuC
- Processing in the UICC card (potentially slow)

2.2 Signature based on previously derived Keys

This approach requires a previous authentication exchange to have securely generated some kind of Integrity Key. For example SIM and AKA exchanges do this.

Subsequently, messages signed with this key could only have originated from the same user as that participating in the original authentication exchange. So the source of the message can be securely identified.

Usually, this method is used to verify the source of subsequent messages in some association, after an initial authentication exchange. For example, the P-CSCF uses this to verify the source of subsequent messages after IMS Registration.

However, the same approach could be used to authenticate the user in some subsequent association, as long as secure means are available to provide the IK to the server. For example, this is one option which could be used for authenticating a tunnel establishment request from a WLAN user.

2.3 Digital certificates

Digital Certificates (including 3GPP Subscriber Certificates) allow a user to securely identify themselves without an additional message exchange. The user signs the message using their private key and includes their certificate. The certificate includes their public key which can be used to verify the signature.

The signature proves that the user knows the private key. The certificate provides the correct identity of the owner of the private key, and is signed by the Certification Authority to prove this.

This approach can be used in standard IETF security protocols such as TLS.

2.4 Source IP address

Some networks can be made secure against address spoofing (for example with ingress filtering and appropriate filters at the GGSN).

In this case, the Source IP address of packets reliably identifies the user. A server wishing to authenticate a user by this means needs to obtain the identity (e.g. IMSI) of the user to which this address is allocated from the GGSN or RADIUS server.

3. Comparison

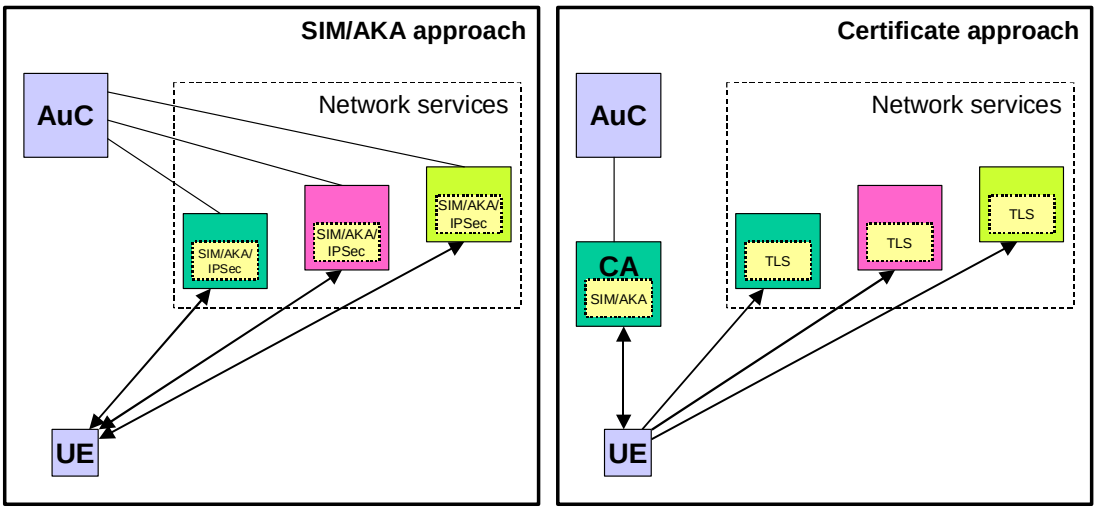
Firstly, we do not consider Option 4 (Source IP Address) further as it is not generally applicable for authentication various service platforms. Also, even in networks which are secure against spoofing, this security may not be ‘strong enough’ to base charging on.

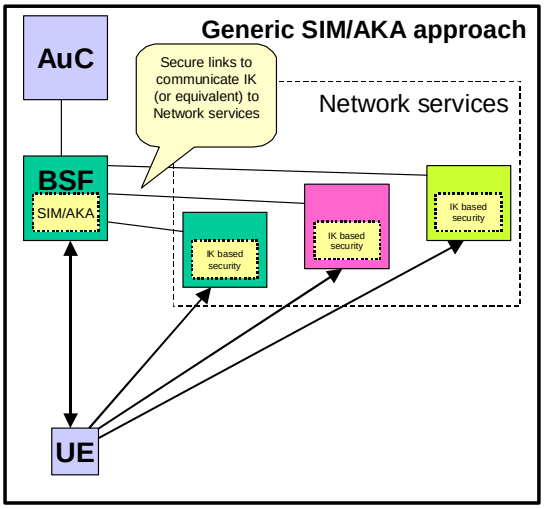
Secondly, for Option 2, we consider the idea of performing a SIM/AKA exchange with a general-purpose server function (e.g., Bootstrapping Server Function) and passing the resulting key to the server that needs to authenticate the user.

Specifically, we compare SIM/AKA exchanges – either directly with the service platform, or with a general-purpose server with Digital Certificates, more specifically, 3GPP Subscriber Certificates work that is on-going in SA3.

A 3GPP user obtains a Subscriber Certificate from a Certificate Authority server in the network. This process involves a SIM/AKA exchange, for the user to prove their identity. Subsequently, the 3GPP subscribers can use the certificate to prove their identity to other users or service platforms, by standard (including non-3GPP specific) means, such as TLS.

A comparison of the architectural impact is shown in the following figures:





From the above figures, we can see the approaches have the following consequences:

SIM/AKA approach:

- Each new service requiring authentication must be extended to support the 3GPP-specific SIM/AKA protocols and to obtain Authentication Vectors from the AuC
- Each new service consumes more Authentication Vectors, placing additional load on the AuC and increasing the possibility of mis-synchronization of Sequence numbers
- Each authentication requires a request/response exchange and (slow) processing on the UICC

Generic SIM/AKA approach (BSF):

- A general-purpose Bootstrapping Server Function must be deployed and managed
- Each new service requiring authentication must be extended to support the 3GPP-specific protocol with the BSF, to obtain the Integrity Key (or equivalent). The usage of this key between UE and service may or may not be 3GPP-specific
- As above, each new service consumes Authentication Vectors and authentication requires a SIM/AKA exchange/processing etc. (This is because the Integrity Key needs to be regenerated for each separate service).

Certificate approach:

- A general purpose Certification Authority server must be deployed and managed
- A SIM/AKA request response is required to obtain a certificate before services can be accessed (but a single certificate may be long-lived – days or months)
- Once the long-lived certificates are issued
- Only standard IETF security capabilities (e.g. TLS) are required on the individual servers
- The issuance of short-term certificates could also be achieved by authenticating the users using the long-term certificates previously issued by the home network (by using the initial run of the SIM/AKA exchange).

A primary comparison point is the location of the 3GPP-specific SIM/AKA functionality and the associated link to the AuC. In the both BSF and Certificate approach, this functionality is centralised in a general-purpose server, compared to duplicating it in every new service platform.

A secondary comparison point is the usage of Authentication vectors and the time taken to perform the authentication. With the Certificate approach, Authentication vectors are consumed only at certificate generation (which may be done rarely).

Our concern is that operators and manufactures should not be required to develop and deploy all three approaches.

4. Recommendations

As a result of the above analysis, we propose the following recommendations:

1) For each new 3GPP service, a single one of the above approaches should be chosen

2) 3GPP should develop some design criteria for this choice, so that it is not made independently for each service. This is because:

A large number of services using the SIM/AKA approach has system implications extending beyond the service itself – specifically the AuC load, consumption of Authentication Vectors and duplication of functionality.

The more services using SIM/AKA, the less strong is the case for a general-purpose solution.

3) 3GPP should pursue only one of the general-purpose approaches – once the decision has been made to follow a general-purpose approach, there does not seem to be a strong argument for two of them!

Current discussions on this topic seem to stall with the assertion that 'not all operators will deploy subscriber certificates' and so security for new services should not be tied to Subscriber Certificates. If continued, this approach leads to Subscriber Certificates never being used: there will always be a requirement for a non-certificate based solution and supporting both solutions is undesirable, so only the non-certificate based solution will be specified.

Subscriber Certificates should be seen as a general-purpose security tool, and as with any general-purpose tool, a decision is needed on when it makes sense to switch over to using it, instead of re-inventing the same capabilities separately for each new service.

Proposal 1:

If the above recommendations are agreed, at some point in the future, we propose that 3GPP should switch to using this general-purpose tool. Our proposal would be to do this sooner, rather than later.

If it is not agreed to make such a switch, then we believe this questions the whole point of the "Support for Subscriber Certificates" Work Item.

Proposal 2:

Further, we propose that the current work on Support for Subscriber certificates (including the current architectures under development by SA3) be suitably updated to take the "certificate approach" and combine the both BSF and NAF functionalities into one entity.
