3GPP TSG SA WG3 Security — S3#29 ad hoc **S3z030008**
3 – 4 September 2003
Antwerp, Belgium

Agenda Item: 5.2

Source: Nokia

Title: Proposal for Generic Authentication Architecture

Document for: Discussion/Decision/Approval

1. INTRODUCTION

In S3 # 29 meeting it was decided that to reduce potential security and technical problems and also save costs, a generic authentication architecture (GAA) should be established and used with R6+ new services as much as applicable. Other fora - OMA, Liberty Alliance etc. - do and will define their own service authentication and authorization protocols and specifications. (See Tdoc S2-032645 for presentation on Liberty Alliance given to SA1 and SA2 in July 2003.) 3GPP should not try to provide an alternative for each of them separately, but rather a general tool that can be used with all of these.

Currently there are four candidate GAA models:

1. Bootstrapping Function (BSF): UE and the network bootstrap shared secret from AKA.

2. Based on BSF and subscriber certificates: a PKI portal network application function (NAF) certifies the UE's public key, and that operation is secured with shared secret established between UE and BSF. In that approach some services can use shared key technology, while others can use asymmetric key technology for authentication.

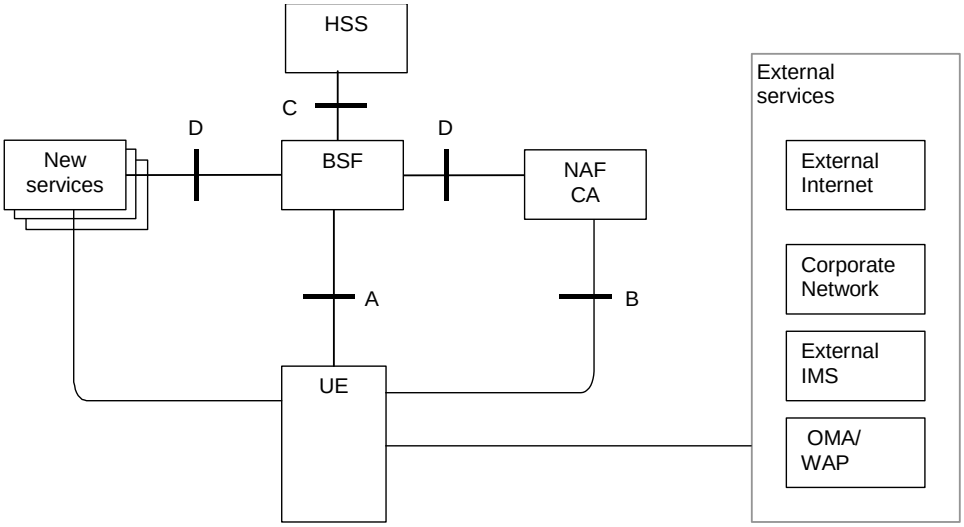

Figure 1. Architecture of model 2

3. Subscriber certificates only, as proposed in [S3-030397]. However, the enrollment operation, in which PKI portal certifies UE's public key, logically requires bootstrapping a shared key from AKA. Thus from the network architecture view, models 2 and 3 are close.

4. A shared secret is established between UE and HTTP authentication proxy (AP) based on AKAv2. The services data traffic flows through that proxy (see Figure 2) In addition it has been agreed in SA#29 meeting that AP will be a TLS tunnel (see [RFC2246]) endpoint.

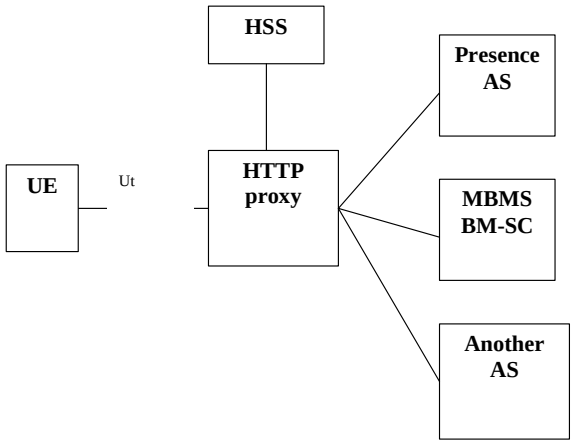

Figure 2 Architecture of model 4 (based on Figure 1 in [S3-030371]).

2. ANALYSIS

2.1 The drawbacks of model 4

This model is essentially a replication of Ut interface solution for all R6+ services, such as MBMS, and also other new services. Such replication to all services has several drawbacks.

This solution is limited to HTTP-based services, because the service traffic must flow through HTTP proxy. In other words, the applicability of the model to new services is not clear.

- As discussed in the last SA3 meeting, all services (i.e, user) data as well as security signaling would flow through a TLS tunnel endpoint, which makes HTTP proxy a bottleneck and a single point of failure. Both traffic load or security signalling may cause system failure. For example, overload caused by data traffic of a single service disrupts both the security signalling and the data traffic of all services.

- It would create dependency on IETF standardization due to AKAv2 draft progress. It would be better to have RFC of AKAv2, before endorsing it in 3GPP.

- It seems that supporting services in visited network is harder with this model as compared to the other models. Since service data traffic must flow through the HTTP proxy, the proxy has to be replicated in the visited network to support services in the visited network. In contrast, a server (NAF) could be in the visited network in models 1 and 2, but it is not necessary to replicate BSF in the visited network.

2.2 The coexistence of authentication based on shared and asymmetric key technologies

On the one hand, authentication using asymmetric key technology is flexible in that it does not require - but does not prevent - real-time interaction with GAA server for signature verification. Also, for historical reasons, there exist applications today, both in cellular and non-cellular terminals, which are ready to use that technology.

On the other hand, verifying a signature made with shared key (i.e. message authentication code, MAC) requires less computation; and the real-time interaction with GAA for each

signature verification that is mandated by the technology may be just what a service needs, e.g. when a service provider wants to be sure that the signing key is fresh.

Thus, the fact that GAA must support a variety of services whose nature is not known beforehand, seems to justify the co-existence of authentications based on shared and asymmetric key technologies (model 2) in GAA. This is further discussed below.

1. Different services have different requirements, e.g. due to their different owners, and thus either shared key technology may fit better with one service, while asymmetric key technology may fit better with another service. As an example, it may not be feasible for HTTP servers maintained by external content providers to communicate with GAA in real-time. In such cases, certificate-based client authentication would bring great deal of extensibility to service deployment.

2. Basic authentication based on shared key is technically simpler than basic authentication based on asymmetric keys. However, provisioning addional user information, such as phone number, to end-applications is easier to do in certificates, than directly from BSF, which would require an interface supporting that additional information.

Therefore we believe that model 2 is preferable because it gives network operators and service providers more freedom and flexibility.

It might be possible to migrate a service from shared key to asymmetric key technology. Moreover, as Alcatel pointed out in email discussion, Ut interface authentication may utilize both technologies: Without support for subscriber certificates, TLS can be used for server authentication only. A key shared with GAA server will then be used in authenticating the UE towards the server, (e.g., with http-digest). When there is support for subscriber certificates, the authenication can be simplified so that certificates are used in both client and server authentication with TLS. In general, however, a service should not be required to use both technologies for authentication.

3. Conclusion

Bootstrapping a shared key based on AKA is needed in all four models. The main drawbacks of model 4 were discussed in section 2.1. The main advantage of model 2 over 1 or 3 is that network operators and service providers can choose the authentication technology that better fits a particular service (see section 2.2). It's main disadvantage, as compared to model 3, is the need to develop UE applications that can utilize bootstrapped keys. However, this is not a serious drawback, because such applications can be added incrementally, according to the need.

In summary, we feel that model 2, which offers both technological choices, is preferable as it gives most flexibility to operators and service providers. We propose to adapt model 2 for GAA.

4. References

[S3-030397] "User authentication by Service platforms", S3#29, Nortel Networks.

[S2-032645] "Liberty Alliance Overview" presentation, S2#33, Nokia.

[S3-030367] "Access to Application Servers using HTTP in MBMS", S3#29, Ericsson.

[S3-030371] "Access to Application Servers using HTTP in Presence/Ut interface", S3#29, Ericsson.

[RFC2246] The TLS Protocol, Version 1.0, T. Dierks et al. IETF. January 1999.