3GPP TSG SA WG3 Security — adhoc **S3z030003**
3 - 4 Sept 2003
Antwerp, Belgium

Agenda Item: **GAA**

Source: **Siemens**

Title: **Generic Authentication Architecture requirements.**

Document for: **Discussion and Decision**

1. Introduction

At SA3#29 it was agreed to start work towards an appropriate Generic Authentication Architecture (GAA) common to all Rel-6 and future releases. The features currently being worked on for Release 6 are MBMS, presence (Ut reference point), support for subscriber certificates and 3G-WLAN interworking (network access and UE initiated tunnelling). More features may be added in future 3GPP releases. It may also be useful to apply the GAA to features defined outside 3GPP (e.g. by OMA).

An email discussion on the requirements on a GAA was held after SA3#29, which terminated on 28 August. This document summarises the requirements resulting from this discussion. SA3 is asked to endorse these requirements and use them as the basis for their future work on a GAA.

An accompanying document explains how the comments received during the email discussion were dealt with.

2. List of requirements on GAA

General requirements:

1. A Generic Authentication Architecture (GAA) shall provide shared keys to entities for use with 3G security features for Release 6 and future releases. Features already specified for Release 5 and earlier releases shall not be affected by the GAA.
2. This provision of shared keys shall be based on the 3G AKA infrastructure (bootstrapping from AKA).
3. The GAA should be applicable as widely as possible to 3G security features for Release 6 and future releases, whether they are http-based or not.
4. The co-existence of several bootstrapping procedures in the 3G architecture should be avoided. In particular, the co-existence of a procedure for bootstrapping of HTTP-based services (as in S3-030367 and S3-030371) and a procedure for generic bootstrapping, as described in the context of support for subscriber certificates (S3-030317), should be avoided.
5. Dependencies on external bodies should be avoided. This would still allow to re-use completed external specifications if seen beneficial.
6. The GAA should respect the HSS/HLR-related security architecture guidelines, as documented in S3-030460. If further guidelines and other criteria regarding service provision or the impact on other entities are agreed by SA3 in the future these should be taken into account in the design as well.
7. Traffic bottlenecks should be avoided. (In particular, it should be investigated whether an HTTP authentication proxy could be such a bottleneck.)
8. The GAA should be able to support applications requiring end-to-end security.

9. The usefulness of the cryptographic separation of keys among applications should be further investigated under the aspect of future-proofing the GAA. If found that such a separation may be useful the GAA should be able to support it.
10. The GAA should support scenarios which require mutual authentication between UE and application server, based on the bootstrapped shared secret. This should not preclude the use of the GAA in scenarios where mutual authentication is provided also using other means (e.g. network certificates).
11. The Generic Architecture should be able to allow the application servers and the terminal to acquire (re-)fresh keys for use.
12. It would be desirable for the GAA to be applicable to non-3GPP security features.
13. For Release 6, the GAA should concentrate on home-provided services, i.e.the authentication is always performed by a server in the home network. But the GAA should not prevent future extension to a scenario where the authentication is performed by a server in a visited networks.

Further remarks:

1. It needs to be clarified whether the use of subscriber certificates for authentication should be within the scope of the GAA, or whether the GAA should be limited to the provision of shared secrets (which may, of course, be used to obtain subscriber certificates, as specified in the draft TS on Support for Subscriber Certificates).
2. A suitable trade-off between the generality of the GAA and potential efficiency gains of customised solutions has to be found (potential inefficiencies: additional protocol runs, use of "heavy" protocols such as TLS when not needed).
3. Potential attacks should be carefully studied (Mitm attacks in tunneled authentication, missing link between identities at different layers, secure separation of authentication and key management functionality (BSF) from application traffic, etc.).
4. SA3 must decide to which features the GAA shall apply.
5. Discovery of BSF and / or AP by UE is to be clarified.

Proposal

SA3 is asked to endorse these requirements and use them as the basis for their future work on a GAA. The document should be updated for future meetings as needed.

3GPP TSG SA WG3 Security — adhoc **attachment to S3z030Si1**
3 - 4 Sept 2003
Antwerp, Belgium

Agenda Item: **GAA**

Source: **Siemens**

Title: **Summary of email discussion on GAA requirements and disposition of comments**

Document for: **Information**

1. Introduction

This document explains how the comments received during the email discussion on GAA requirements were taken into account in the updated version of the requirements.

2. Summary of email discussion

The email discussion was started by Günther Horn on 1 August proposing the following list of requirements:

General requirements:

1. A Generic Authentication Architecture (GAA) shall provide shared keys to entities which will use them in 3G Rel6+ security features.
2. This provision of shared keys shall be based on the 3G AKA infrastructure (bootstrapping from AKA).
3. The GAA should be applicable as widely as possible to 3G Rel6+ security features.
4. The co-existence of several bootstrapping procedures in the 3G architecture should be avoided. In particular, the co-existence of a procedure for bootstrapping of HTTP-based services (as in S3-030367 and S3-030371) and a procedure for generic bootstrapping, as described in the context of support for subscriber certificates (S3-030317), should be avoided.
5. Dependencies on external bodies should be avoided.
6. The GAA should respect the HSS/HLR-related security architecture guidelines, as documented in S3-030460.
7. Traffic bottlenecks should be avoided. (In particular, it should be investigated whether an HTTP authentication proxy could be such a bottleneck.)
8. The GAA should be able to support applications requiring end-to-end security (avoid criticism WAP has suffered for its gateway solution).
9. The usefulness for the cryptographic separation of keys among applications should be further investigated under the aspect of future-proofing the GAA. If found that such a separation may be useful the GAA should be able to support it.
10. The GAA should support scenarios which require mutual authentication between UE and application server, based on the bootstrapped shared secret.

Further remarks:

1. The role of the use of subscriber certificates needs to be clarified.
2. A suitable trade-off between the generality of the GAA and potential efficiency gains of customised solutions has to be found (potential inefficiencies: additional protocol runs, use of “heavy” protocols such as TLS if not needed).
3. Potential attacks should be carefully studied (Mitm in tunneled authentication, missing link between identities at different layers, etc.).

The following comments were received on the SA3 list:

Tao Haukka wrote on 20 August:

“A new name instead of GAA should be found.” But no new name was suggested. I left the name for the moment. This is supported by Peter’s email.

Bullet 5: sentence added, as suggested.

Bullet 6: “Guidelines regarding entities other than the HSS should be also respected.” Fine, but the only such guidelines SA3 has agreed at the moment are the ones relating to the HSS. A slightly weakened sentence was included.

Bullet 10: “It mandates that mutual authentication must be based on the bootstrapped shared secret.” This is a misunderstanding. Bullet 10 only says that scenarios should be supported where the mutual authentication is based on the shared secret. This does not rule out other scenarios. A clarifying sentence was added.

Bullet 11: requirement added, as suggested.

Annelies van Moffaert wrote on 21 August:

“ Does the role of the use of subscriber certificates form part of the GAA discussion?” The scope of the GAA needs indeed to be discussed. I reformulated the remark for clarification.

“ Could you explain a bit or is there a reference to the criticism on WAP gateway solution you refer to as an argument for requiring support of end-to-end security?” This was mentioned by Colin at SA3#29. WAP was criticised because e.g. banks wanted to use WAP security for communication with their customers, but did not like the idea that MNOs could read the communication, because the security was hop-by-hop. I am not sure how relevant the WAP discussion is to a GAA, so I removed the reference to WAP, but the GAA should be general enough to satisfy requirements for E2E security. To be sure, when a shared secret is bootstrapped from AKA then the MNO has always a possibility to compromise any security based on that shared secret.

Sharat Chander wrote on 21 August:

“ a. Does a user always have to initiate the request for a cert from the operator?
b. Is there a way by which users can be granted certs, but w/o a need for them to oin any way intervene”
My understanding is that, as far as the work on support for Subscriber Certificates is concerned, intervention by a human user is not necessarily required, rather this could be handled automatically by the UE.

Peter Howard wrote on 22 August:

the following new requirement is proposed:

"It would be desirable for the GAA to be applicable to non-3GPP security

features." This was added as requirement 12.

Bengt Sahlin wrote on 27 August:

“ It is unclear "Rel6+" means”. A clarification was added.

”We also think that the requirements are currently not covering issues related to roaming scenarios.“ A new requirement 13 was added.

Mauro Castagno wrote on 28 August:

“ assuming that a GAA will be "decided" for Rel6 onwards, could you kindly explain to me which kind of "things" would be expected to be authenticated using the GAA and which others would continue to be authenticated "as usual", that is as for Rel5 downwards?”

It should be discussed at the ad hoc meeting to which features the GAA should be applied. Features already specified for Release 5 should not be touched. I added some clarification to requirement 1, and added remark 4.