3GPP TSG SA WG3 Security **S3-010494**

October 16-19, 2001

Sydney, Australia

Agenda Item: 7.3

Source: Ericsson

Title: On access independence and authentication

Document for: Discussion and decision

1. Scope and objectives

In [TS33.203] the requirement is that IMS AKA shall be used however this does not seem to be in line with the access independence requirement. The scope of this document is to suggest that IMS AKA shall be optional to use and not mandated. However whenever a UE uses the ISIM and the IMPI then the HN shall trigger IMS AKA. It is proposed that TS33.203 shall not rule out any other IETF authentication scheme like e.g. HTTP Digest or similar but then the user should use a different identity e.g. a user name for those authentication mechanisms. It is assumed that this is enough for fulfilling the requirements in [TS22.228] for access independence and not to mandate 3GPP specific solutions.

It is also proposed that the IMPI is defined in a standardised format making it easy for the HSS to recognise and trigger IMS AKA. The format for the IMPI is not specified here only the requirement as such.

2 Background

In [TS22.228] the following requirements can be identified:

1. The possibility for IP multimedia applications to be provided without a reduction in privacy, security, or authentication compared to corresponding GPRS and circuit switched services
2. Access independence shall be supported. It is desirable that an operator should be able to offer services to their subscribers regardless of how they obtain an IP connection (e.g. GPRS, fixed lines, LAN).
3. It is important that commercially available IP multimedia applications are supported. In general compatibility shall be with these IP multimedia applications instead of building 3GPP-specific solutions.

Regarding the first bullet point the [TS33.203] will fulfil this requirement when the work in IETF has been finished e.g. security mode setup and get IMS AKA into place. It has also been the goal from SA3 to fulfil also bullet point 2 by using IETF RFCs. Another example is the definition of the ISIM. However in the current version of [TS33.203] the following requirement is specified:

- The HN shall choose the EAP AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the AKA scheme are transported by SIP and embedded in EAP.

The author of this contribution is of the opinion that this is not compliant with bullet point number 2 and should be modified accordingly.

It has also been the goal for SA3 to fulfil also the last requirement, i.e. bullet point number three. This is solved by using IETF RFCs and develop drafts in IETF that fulfil the requirements draft developed by 3GPP, cf. [draft-garcia].

3 Proposal

It is proposed in this contribution that IMS AKA shall be one option for the operators to authenticate the IM subscribers. The TS33.203 shall not exclude other IETF mechanisms e.g. already existent in SIP like HTTP Digest. If the operators policy states that IMS AKA should be used TS33.203 shall provide with the appropriate requirements for that.

Since there are several schemes available developed in IETF like HTTP Basic, HTTP digest and GSS-API to name a few some standardisation work in SA3 is needed if the solution for R5 shall be generic and support several authentication schemes. Security issues are e.g. bidding down attacks. It is therefore proposed in this contribution that the IMPI that is stored in the ISIM shall trigger IMS AKA. Hence if an operator wants to use e.g. HTTP Digest the IMPI shall not be used for that. Instead a subscriber shall be given an user name different from the IMPI which is used for any other authentication mechanism. The IMPI and a user name can both take the form of a NAI but the IMPI can be, according to [TS23.228], based on the IMSI. Any other username should not be based on the IMSI.

A mechanism like HTTP digest will not as IMS AKA offer the same level of protection of signalling but it could be a choice of an operator to use HTTP digest in certain situations but the user gets e.g. then only access to lightweight services. Another alternative could be that WTLS or IPSec based on certificates sets-up a secure channel between the UE and the P-CSCF before authenticating the user but the concept of digital certificates is currently not within the scope of aSIP and [TS33.203] but should not be ruled out by [TS33.203].

In order to avoid adding complexity to the HSS it is proposed that the IMPI that is downloaded into the ISIM uses some standardised format making it possible to optimise the choice of authentication algorithm in the HSS i.e. IMS AKA.

4 Changes Needed to TS33.203

4.1 5.1.1 Authentication of the subscriber and the network

5.1.1 Authentication of the subscriber and the network

[Editor's note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network]

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The exact details of the subscriber profile are FFS but it will contain information on the subscriber that may not be revealed to an external partner, cf. [3]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests an IM-service the S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorization of IM-services).

An IM subscriber may use the concept of the ISIM or if the operator policy allows it any other standard IETF mechanism not specified in this technical specification. If the ISIM is used the user will have an IMPI which is shared by the HSS and the ISIM. This IMPI shall not be used for manually entered user names like e.g. in HTTP digest.

All SIP-signaling will take place over the PS-domain in the user plane i.e. IM-services are essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides with a transport service and QoS.

For IM-services a new security association is required between the mobile and the IM CN SS before access is granted to IM-services. The Home Network or a 3rd party even (which does not have to be an UMTS operator) provides the user with the IM-services.

The mechanism for mutual authentication in UMTS is called UMTS AKA. It is a challenge response protocol and the AuC in the Home Stratum derives the challenge. A Quintet containing the challenge is sent from the Home Stratum to the Serving Network. The Quintet contains the expected response XRES and also a message authentication code MAC. The Serving Network compares the response from the UE with the XRES and if they match the UE has been authenticated. The UE calculates an expected MAC, XMAC, and compares this with the received MAC and if they match the UE has authenticated the Serving Network.

The AKA-protocol is a secure protocol developed for UMTS and it will be reused for IM-services and then called IMS AKA. The user identity that is used and authenticated by the IMS AKA mechanism is the IMPI.

The Home Network authenticates the subscriber at registrations or re-registrations only. In order to re-authenticate a subscriber the Home Network can force a re-registration by using e.g. a re-registration timer.

4.2 6.1 Authentication and key agreement

6.1 Authentication and key agreement

[Editor's note: This section shall describe in detail how the authentication is performed and how the keys, IK and CK, are derived and delivered to the different nodes.]

The scheme for authentication and key agreement in the IM CN SS, which is specified in detail in this specification, is called IMS AKA, which is based on a special user identity i.e. the IMPI. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 3. Furthermore a security association is established between the UE and the P-CSCF. The ISIM and the HSS keeps track of the counters SQN_{ISIM} and SQN_{HSS} for the IM-domain. The handling of the SQN can be as in [1]. IMS AKA is based on EAP, cf. [7], and the AKA extension to EAP and HTTP, cf. [8] and [9] respectively.

When the ISIM and the IMPI is used ~~The~~ the HN shall choose the EAP AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the AKA scheme are transported by SIP and embedded in EAP. The user may have other identities than the IMPI e.g. a user name, which is used for any other IETF authentication scheme. It should be noted that other IETF authentication schemes may not provide with key management procedures and hence not SIP-signalling protection as specified in this specification.

~~*[Editors Note: Shall the HN choose EAP AKA for 3GPP-access or is it to be an option for the HN to choose either EAP AKA or perhaps any other mechanism e.g. HTTP digest depending on policy?]*~~

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. For each user it is the HSS that keeps track of the counter SQN_{HSS}. The requirements on the SQN handling both in the Home Network i.e. the HSS and the ISIM are specified in [1]. The AMF field can be used in the same way as in [1].

The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI. . The IMPI shall be in a standardised format such that the HSS can choose IMS AKA in an optimal way based on the IMPI. The HSS may choose other authentication schemes for other user identities or user names than the IMPI.

References

[TS22.228] 3GPP TSG SA WG1, TS 22.228, Release 5, Service requirements for IP Multimedia, Core Network Subsystem Stage 1 ; v5.2.0, June 2001

[TS23.228] 3GPP TSG SA WG2, TS 23.228, Release 5, IP Multimedia (IM) Subsystem, Core Network Subsystem Stage 2 ; v5.1.0, June 2001

[TS33.203] 3GPP TSG SA WG3, TS 33.203, Release 5, Access security for IP-based services, Core Network Subsystem Stage 2 ; v0.6.0, September 2001

[draft-garcia] IETF, SIPPING Working Group I-D, draft-garcia-sipping-3gpp-reqs-00, Networking group, October 2001