3GPP TSG WG3 S3#17bis
Madrid, Spain
25rd April – 26th April, 2001

Tdoc S3z-010036

Agenda Item: TBD

Source: Ericsson

Title: ~~Different o~~Open issues for aSIP

Document for: Discussion and decision

1 Scope and objectives

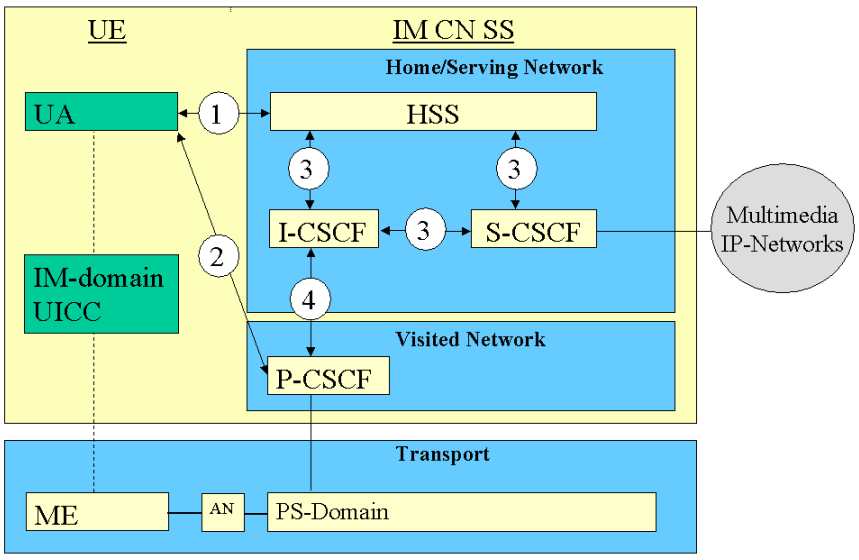
The scope for this document is to discuss several open issues and that S3 adopts the concepts as working assumption for the future work on aSIP.

In this document the following issues and solutions are discussed and proposed

1 The use of SASL AKA in SIP
2 That SIP is extended with a CMS protection mechanism
3 A security mode set-up mechanism

2 Background

At the SA3#17 meeting in Göteborg it was decided that the Home Network should perform the authentication of the IM Subscriber. At the same meeting it was also decided that the protection i.e. integrity and confidentiality protection should be provided in a hop-by-hop fashion i.e. a security association between the UE and the P-CSCF. The security architecture below is taken from the TS 33.203 v020 that should be viewed as an example since it is left FFS in which node authentication should take place, cf. [S3-010100~~.~~].



With this as the framework and working assumption there are still several aspects that are open and needs to be solved. The scope for this contribution is to highlight these issues and also propose solutions, which could be adopted as working assumptions within S3.

The open issues discussed in the contribution is

- what protocol to use for authenticating the subscriber
- what mechanism to use for protecting the SIP-signaling
- security mode set-up is also discussed.

The protocols used between the UE and the P-CSCF is SIP, Session Initiation Protocol. A working assumption in SA3 has been that AKA defined in R'99 shall be reused. However currently within IETF SIP AKA has not been defined. Nokia in SA3 #14 in [S3-000456] presented a proposal how AKA could fit into the SIP protocol by extending the protocol that is also the current working assumption. However in this contribution it is proposed to define the SIP AKA mechanism by using SASL cf. [RFC2222], ~~Simple Authentication and Security protocol~~ which is a protocol defined for several authentication mechanisms for e.g. Kerberos and SMTP etc. It is straightforward to introduce new authentication mechanisms within the framework of SASL. However SASL is not at the moment defined for SIP so this is the extension which is needed with this proposal rather than a specific SIP extension for AKA.

It is also for further study, which protocol to use for protecting the SIP signaling. The discussions so far have indicated that either IPSec or a solution at SIP level could be used. In this paper several existing IETF solutions are described, compared and analyzed. Ericsson believes that one should avoid defining a totally new mechanism for SIP.

Another important aspect, which has not been analyzed in S3 thus far, is security mode set-up. In this paper this is also introduced and discussed.

3 Authentication issues

3.1 Introduction

The current working assumption in 3GPP SA3 for is to reuse the AKA mechanism specified in R'99 by introducing a new mechanism within SIP the SIP AKA, cf. TR 33.8xx 030 or [S3-000456]. ~~xxxxx. This was based on a contribution from Nokia, S3-00xxxx.~~ Even though it is a good solution it is not clear that it fulfils the requirement for access independence. One aspect of access independence as we define it is that many authentication mechanisms shall be possible. It is obvious that one can add more authentication modes to the already existing basic, digest and PGP mode of http authentication. The problem is that it is rather cumbersome from a specification perspective. This is why we suggest that a more generic approach is adopted.

The scope of this discussion is to introduce the SASL protocol, which could be used to achieve access independent authentication. ~~instead of the SIP AKA~~. The paper also introduces a possible way to use SASL to carry AKA within SIP.

The objective with the discussion is that S3 adopts SASL as the working assumption for authenticating IM-subscribers. This makes it easier to handle several different authentication schemes especially from a terminal point of view.

Currently SIP has adopted two HTTP based authentication mechanisms; HTTP basic and digest. These two mechanisms are also already used in WAP terminals. Both protocols carry passwords and are simple challenge response protocols. The basic protocols transmits the password in clear whereas the digest protocol is somewhat stronger and transmits a MD5 checksum of the username, the password, a given nonce value, the HTTP method, and the requested URI.

SASL is a protocol that can be used for authenticating a user to a server and for optionally negotiating a security layer for subsequent protocol interactions. This document focuses on the authentication part and not the option. SASL is designed for protocols like PAP and CHAP but currently there is no extension for HTTP but there is a draft and the work is ongoing in IETF.~~.~~

3.2 How to use SASL within SIP

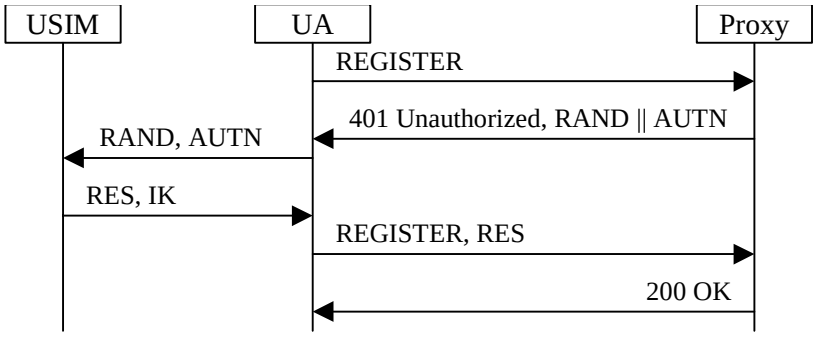
When a user sends a Register request to a SIP proxy it will receive a 401 unauthorized response which will include the WWW Authenticate field which should include a sasl-challenge containing the AKA parameters i.e.:

WWW-Authenticate=” WWW-Authenticate” “SASL” “mechanism=” “3GPP-AKA” “id=” SESSION ID “value=” RAND||AUTN

The user checks the MAC and then sends a response back or the RES in a new Register message (or AUTS/Failure etc) e.g.s

Authorization=” Authorization” ” “SASL” “mechanism=” “3GPP-AKA” “id=” SESSION ID “value=” RES

For the AUTN, the RAND, the RES value etc the ~~B~~base 64 format shall be used. If the RES is authentic the user will receive a 200 OK back.



4 Protection Mechanisms

The scope of the discussion is the integrity protection of SIP signaling traffic from the UE to the P-CSCF. It is recognized that existing security mechanisms could be reused for this purpose, though the SA3 must analyze which, if any, of these mechanisms should be selected. Ericsson proposes that SA3 should NOT develop any new mechanisms in view of the many existing ones that could be applied.

The main objectives of this section are the following: (1) to list the existing mechanisms that could potentially be used to protect the SIP packets and (2) to list the various factors that affect the decision about the selection of the mechanism.

First we list those existing mechanisms that could be employed to provide integrity and optionally confidentiality protection. Only those mechanisms have been listed that can be run using solely symmetric cryptography.

- The IPsec AH protocol [RFC 2402]. We will assume that the transport mode is used.
- The IPsec ESP protocol [RFC 2406]. Again, transport mode is assumed for ESP.
- Cryptographic Message Syntax (CMS) [RFC 2630].
- S/MIME [RFC 2633] which is related to CMS.
- PGP and PGP/MIME ~~[RFC XXX].~~
- A yet-to-be developed application level optimized for SIP. This option is not studied further in this document.

Next we list those factors that affect the decision on which mechanism to select:

- The amount of extra bandwidth needed for the signaling through the use of the mechanisms. We can differentiate between the fixed costs of the mechanism and the variable costs related to the size of the protected packet. Encoding formats such as binary vs. base64 will have an effect here.

- Whether the mechanism is compatible with a compression scheme or not. Work is starting in IETF to define signaling compression mechanisms. As far as only integrity protection is provided, the compression does not matter. If encryption is also provided, then compression should be done before encryption, which in practice

means doing both all the way between the terminal and the P-CSCF. It is expected that the signaling bursts are short enough to not get full benefit from the underlying ROHC compression that is used for RTP traffic.

- The computational requirements of the mechanisms. There doesn't seem to be significant difference between the mechanisms, given that all use roughly similar algorithms.

- The implementation complexity of the mechanisms. This is harder to estimate, but one should note that regardless of the chosen mechanism, it is likely to restricted to a small subset of the more general standard. For instance, IPsec does not need IKE since UMTS AKA will be used to derive keys, and only the symmetric ciphering parts of CMS would be employed, not the public key and certificate mechanisms.

- Reuse of the mechanism for other purposes in the terminal. For instance, a mechanism might be used for IM domain and other purposes, or another mechanism could be used both for hop-by-hop and end-to-end security within the IM domain. Also, mechanisms that are typically already found on existing terminals should be preferred.

- Stability and completeness of the specifications for the mechanism. For some mechanisms it might be necessary to supplement them with new functionality before they can be used in this context.

- Suitability of the mechanisms for use outside the 3GPP domain in the IETF. This may be a useful feature, given that the 3GPP may need to do some of the standardization for the multimedia domain security through IETF, and because many terminals will support multiple accesses, not juts 3G.

- The last but not lest important factor is the possibility to use the solution end-to-end. Although not in the current set of requirements for IPMM security this is foreseen as a very likely requirement for future releases.

Ericsson proposes to define the security mechanisms at SIP level, using a S/MIME, CMS (PKCS#7) based format, mainly because of the ease which ~~WAP~~ terminal manufacturers could implement this on their phones, and because the same scheme could perhaps be used also for later end-to-end security in SIP. As an alternative to SIP level security IPSec-ESP with fixed policies could be studied. This would be a somewhat more bandwidth-efficient mechanism due to the longer headers and base64 encoding in CMS.

5 Security Mode Setup for SIP

Traditionally, security mechanisms have included a so-called security mode setup procedure. The purpose of this procedure is to agree on the used encryption / integrity protection algorithm, and to signal the start of the cryptographic protection for the traffic.

In the case of IP multimedia signaling, a crucial aspect is the delays introduced by the security mechanisms. For this purpose we propose that the SA3 consider whether an additional setup signaling pair for this purpose could be eliminated. Instead, it may be possible to provide the setup in an integrated manner in the existing SIP message flow. In the following way, for instance:

- The first registration message can contain the offered algorithms from the terminal's perspective. The P-CSCF can respond with the selected algorithm in the next message(s).

- The cryptographic protection starts at a predefined place in the SIP flow. The first message from the terminal after it has received AUTN and RAND will be always protected.

Conclusions

The SASL protocol was introduced and concluded as being more generic than the SIP AKA and would support access independent authentication.

A list of different mechanisms that can protect was presented together with different important factors that should be taken into account when making the decision which mechanism to choose. Ericsson proposes that the protection shall take place at SIP-level using a S/MIME, CMS based format.

In this paper it is proposed that the security protection setup should be integrated with SIP e.g. the integrity protection could from the terminal side start when the response to the challenge is sent.

References

[S3-000456] 3GPP TSG SA WG3 Security: Source Nokia; *UMTS AKA in SIP;* July 2000.

[RFC 2222] IETF RFC 2222: *Simple Authentication and Security Layer (SASL);* Oct. 1997.

[S3-010100] 3GPP TSG SA WG3 Security, S3-010100: *Proposal on IM domain access security;* SA WG3 #17, Göteborg, 27 Feb – 2 March 2001

ERICSSON

Open Issues for aSIP

Krister Boman, Jari Arkko, Stefan Andersson

Ericsson

April 24th, 2001

Issues to Discuss

1. Protocol details for the authentication
2. Protection mechanism for next messages
3. Security mode set-up

ERICSSON

Role of This Contribution

This purpose of this contribution is to:

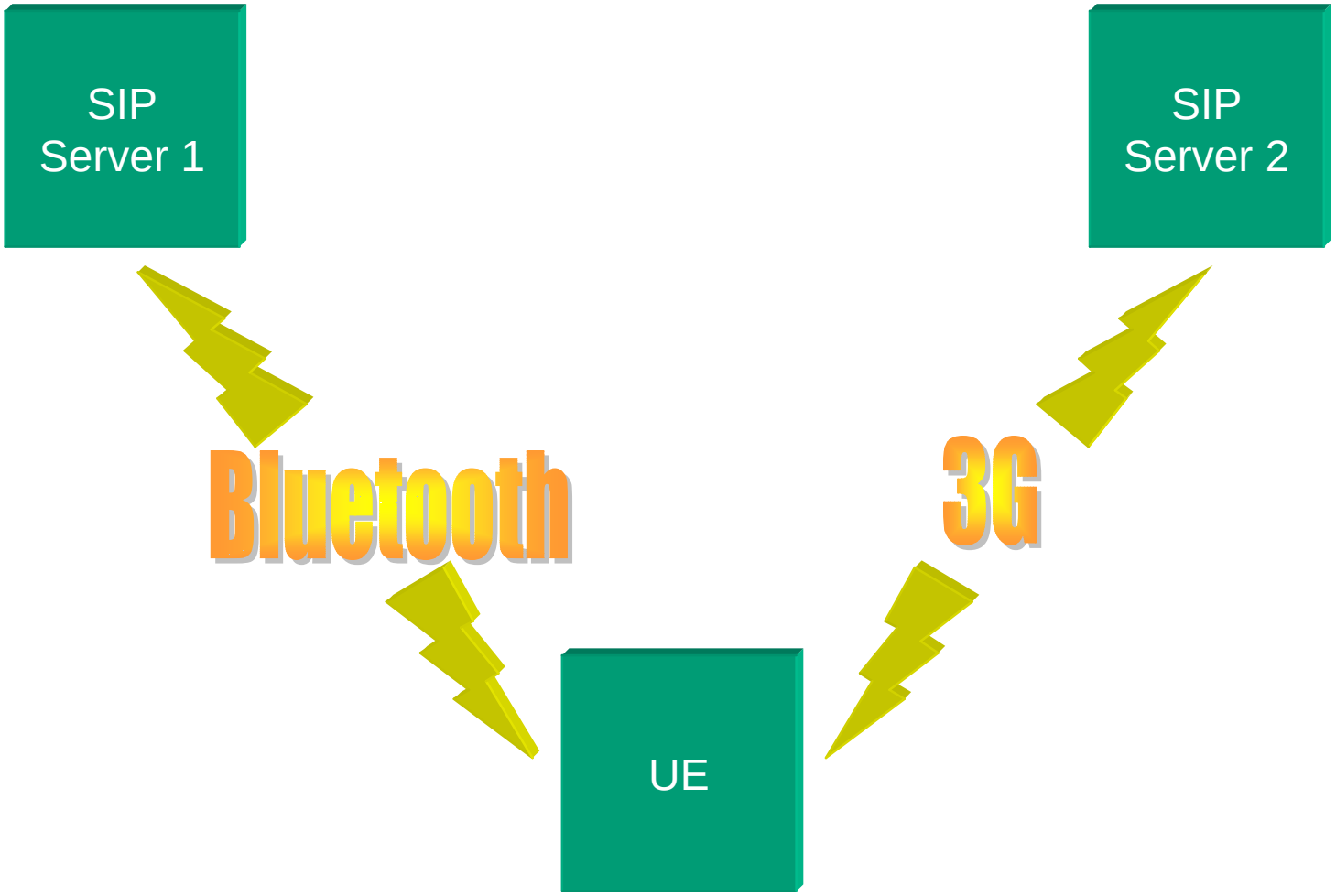
- Present factors affecting the choices in the above issues
- Propose preliminary working assumptions for the above issues

Main factors to keep in mind:

- Access independence
- Reusing existing security schemes
- Growth of the end-to-end model
- Minimization of additional round-trip delays

Authentication Protocol Details

Factor: Access Independence

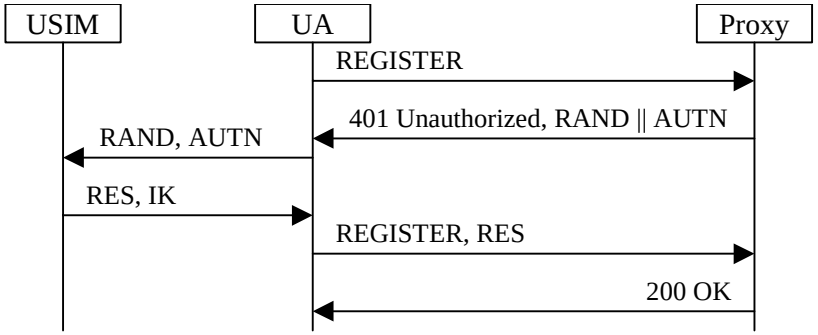


Consequences

- Can not not always assume AKA
- Other possible schemes:
  - PKIs
  - EAP
  - Kerberos
  - …
- We may want to add some generality to our SIP extensions for authentication
- Not to support the above schemes, but to allow others to add other schemes easily
- With less changes to end-devices, and perhaps no changes to proxies

Generality Example

- Instead of defining how to use AKA in SIP…
- Define how to use SASL in SIP and
- Define how to use AKA in SASL



(SASL for HTTP is being defined, but one issue in it is that the specifications aren't stable yet and there are competing proposals.)

ERICSSON

Protection Mechanism for Next Messages

Factor: Reuse

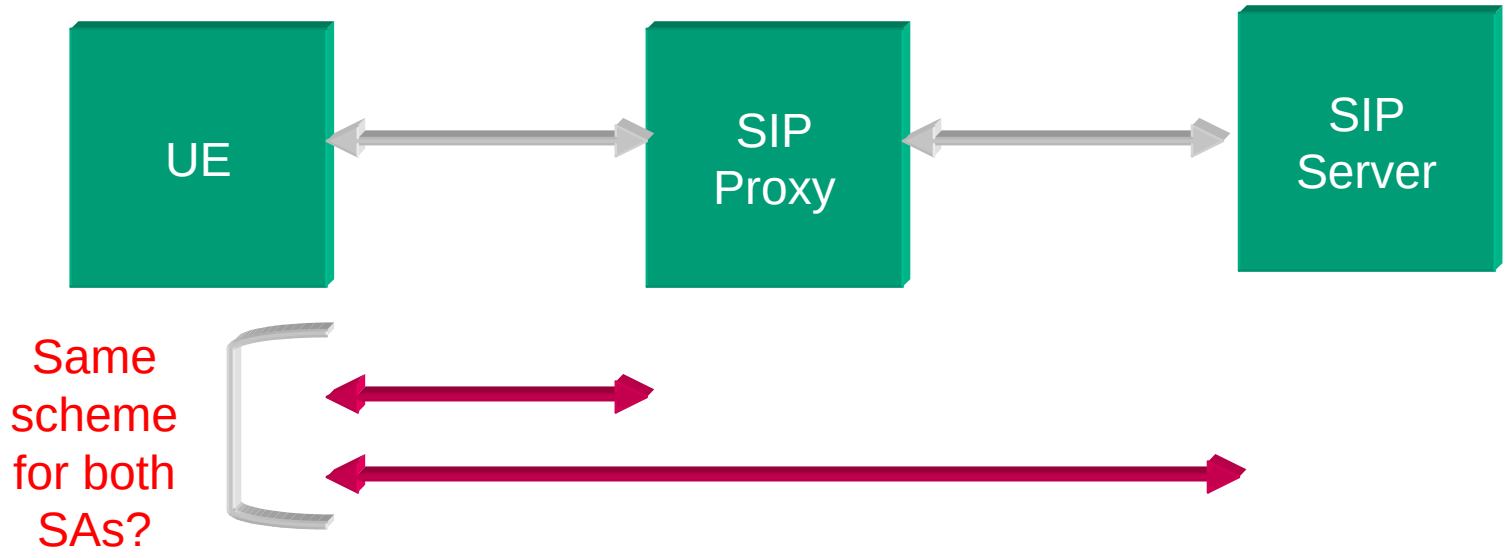
- Let's not develop a new scheme
- Pick one from
  - IPsec
  - S/MIME or CMS
  - PGP
  - …

ERICSSON

Criteria to Evaluation Mechanism Candidates

- Extra bandwidth – slight advantage for IPsec
- Compatibility with compression – similar issue
- Computational requirements – about the same
- Implementation complexity – about the same?
- Reuse – in products and for other purposes; an advantage for S/MIME
- Status and completeness of specifications – S/MIME needs some work
- Suitability for also Internet applications – same

Factor: Growth of the End-to-End Model



Security Mode Set-up

Factor: Avoid Delay

- The delay budget is full already

- => Use a fixed position security mode set-up scheme
- => Use piggypacking

- E.g.:
  - Algorithm proposals piggypacked to the first message to server
  - Server responds with selected algorithm
  - Next message from client is always protected

Conclusions

Main factors to keep in mind:

- Access independence
- Reusing existing security schemes
- Growth of the end-to-end model
- Minimization of additional round-trip delays