3GPP TSG SA WG3 Security — S3#29 **S3-030357**
15 –18 July 2003
San Francisco, USA

Source:	**Nokia**
Title:	**Generic secure message exchange using HTTP Digest Authentication**
Document for:	**Discussion and Decision**
Agenda Item:	**7.9 (Support for subscriber certificates)**

1. Introduction

Currently, one of the alternatives for Protocol B in [TS-SSC] is based on HTTP Digest Authentication [RFC2617]. In subscriber certificate case, HTTP Digest Authentication is used to authenticate and integrity protect HTTP requests and responses that contain certificate enrollment messages (e.g., PKCS#10 request and issued certificate). The other alternative for protocol B is to use a subset of CMPv2 [S3-030347]. CMPv2 can use the bootstrapped security association directly for authentication and integrity protection. Though the decision has not yet been made, there are reasons to choose this subset of CMPv2 for subscriber certificate delivery because the full CMPv2 supports certificate lifecycle management.

Nevertheless, the HTTP Digest Authentication model can also be used as a generic authentication and integrity protection method towards any new NAF. If a new NAF uses BSF-based security association, it could use this generic method to authenticate the UE (and UE authenticate the NAF) and integrity protect any payload being transferred between NAF and UE. As a generic method, it will speed up the specification of new NAFs since the authentication and message integrity protection part of protocol B are taken care of by HTTP Digest Authentication. It will also ease the implementation of BSF-based authentication in NAFs because there would be one well-defined way to do it.

This contribution describes this “generic secure message exchange using HTTP Digest Authentication” and proposes to add this description to [TS-SSC] as an informative annex.

2. Discussion

The sequence diagram in Figure 1 describes the generic secure message exchange with HTTP Digest Authentication. The conversation may take place inside a server-authenticated TLS [RFC2246] tunnel in which case TLS handshake has taken place before step 1.

In step 1, UE sends an empty HTTP request to a NAF. In step 2, NAF responds with HTTP response code 401 “Unauthorized” which contains a WWW-Authenticate header. The header instructs the UE to use HTTP Digest Authentication with a bootstrapped security association. Quality of protection (qop) attribute is set to “auth-int” meaning that the payload of the following HTTP requests and responses should integrity protected. The realm attribute contains two parts. The first part is a constant string “3GPP-bootstrapping” instructing the UE to use a bootstrapped security association. The second part is the DNS name of the NAF.

In step 3, the UE shall verify that the second part of the realm attribute does in fact correspond to the server it is talking to. In particular, if the conversation is taking place inside a server-authenticated TLS tunnel, the UE shall verify that the server name in the server’s TLS certificate matches the server name in the realm attribute of the WWW-Authenticate header. The UE generates client-payload containing the message it wants to send to the server. Then it will generate the HTTP request by calculating the Authorization

header values using the transaction identifier (base64 encoded) it received from the BSF as username and the session key K (base64 encoded) as the password, and send the request to NAF in step 4.

When NAF receives the request in step 5, it will verify the Authorization header by fetching the session key K from the bootstrapping server using protocol D and the transaction identifier. After successful retrieval, NAF calculates the corresponding digest values using K, and compares the calculated values with the received values in the Authorization header. The NAF shall also verify that the DNS name in the realm attribute matches its own. If the conversation is taking place inside a server-authenticated TLS tunnel, the NAF shall also verify that this DNS name is the same as that of the TLS server. If the verification succeeds, the incoming client-payload request is taken in for further processing. Thereafter, the NAF will generate a HTTP response containing the server-payload it wants to send back to the client in step 6. The NAF may use session key K to integrity protect and authenticate the response.

In step 7, UE receives the response and verifies the Authentication-Info header. If the verification succeeds, the UE can accept the server-payload for further processing.

Additional messages can be exchanged using steps 3 through 7 as many times as is necessary. The following HTTP request and responses must be constructed according to RFC 2617 (e.g., nc parameter must be incremented by one with each new HTTP request made by UE).

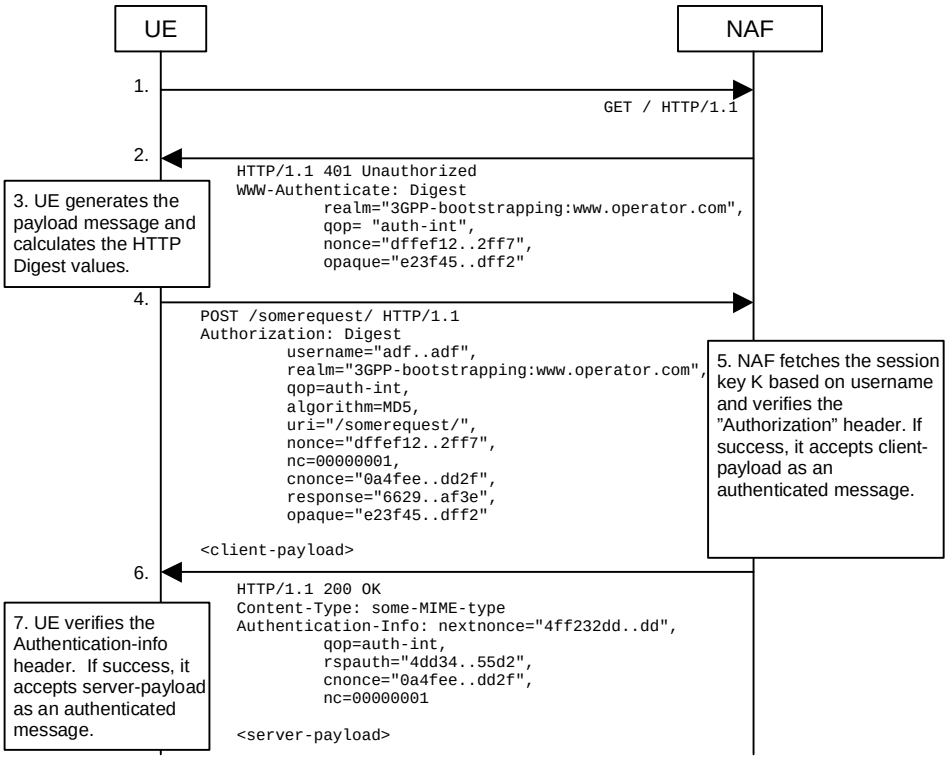

Figure 1. Generic secure message exchange using HTTP Digest Authentication and bootstrapped security association.

3. Proposal

We propose to add the description of this generic secure message exchange using HTTP Digest Authentication to [TS-SSC] as an informative annex.

4. References

[RFC2617] Franks J., et al, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[TS-SSC] Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6), V0.2.0.

[S3-030347] CMPv2 profile for 3GPP subscriber certificate enrollment, SSH Communications.

[RFC2246] Dierks T., et al, “The TLS Protocol, Version 1.0”, RFC 2246, January 1999.