**3GPP TSG SA WG3 Security** **S3-030371**

**15th – 18th July, 2003**

**San Francisco, CA, USA**

**Agenda Item:** Presence (7.18)

**Source:** Ericsson

**Title:** Access to Application Servers using HTTP in Presence/Ut interface

**Document for:** Discussion/Decision

# 1. Introduction

This document discusses on HTTP security solutions for the Presence/Ut interface. In chapter 2 and 3, the problems and solutions for potential SQN synchronization failure related to the re-use of AKA with several HTTP based applications. In addition, this document will further clarify the open issues and "objections" raised by SA3 in the previous meeting.

The document promotes architectural means to solve the problem. It is suggested that SA3 should take a working assumption that access to all such applications can be implemented using HTTP proxy as a centralized access point.

# 2. Problem statement

It seems that SA3 has a clear interest of re-using AKA with several applications. For this reason, all new applications that re-use AKA authentication, such as Presence Ut interface or MBMS, should consider carefully about the potential problems related to synchronization failures.

AKA authentication challenges need to arrive to USIM at specific order [TS 33.102]. Otherwise, USIM will generate a synchronization failure message.

For the freshness checking purposes, the AKA challenge includes a sequence number (SQN). The SQN space is divided into subspaces by using an index (IND). IND is part of SQN, and it refers to an array in the USIM where the highest used SQNs are stored. If every new SQN(IND) is greater than the previously used SQN with the same index value, then the freshness of the challenge is guaranteed. Implementations may also use a parameter L to set a limit to the highest acceptable difference between the new SQN and the highest previously accepted SQN anywhere in the array. Small values in parameter L may cause more SQN synchronization failure problems if the same USIM is used with several applications.

Possibility that the USIM will reject a valid authentication challenge depends a lot on the USIM/ISIM implementation and how they are deployed. Since these issues are Operator dependent, they cannot be solved by SA3 without changing [TS 33.102]. Using the current specifications, there are still some ways to cope with the problem depending on the USIM/ISIM implementation. For example, one or more IND values from the SQN array in the USIM/ISIM can be dedicated for specific application. In theory, the maximum number of applications using the same USIM/ISIM is the size of SQN array. In practice, several IND values may need to be reserved for one application in order to find a balance between risks for synchronization failures, load of HSS, and frequency of authentication. Also, the number of AVs returned at a time to the entity requesting them is an important deployment decision.

Ericsson believes that the remaining means to solve the problem without changing USIM/ISIM standards boils down to following two:

1. Minimizing the number of network entities that are able to request Authentication Vectors (AVs) for the same USIM.

2. The frequency of authentication.

The next section describes how this can be achieved in HTTP context.

# 3. Solution

The number of network entities requesting AVs for the same USIM should be kept in minimum also in HTTP context. This can be achieved already now by centralizing the interface to HSS for fewer nodes in the implementations. It would also be possible to standardize such architecture in 3GPP.

Ericsson has studied solution based on the use of Reverse HTTP proxy. Term reverse proxy is often used to referee to certain alternate uses of a proxy server. For example, reverse proxy can be used outside the firewall to represent a secure content server to a client outside. It typically prevents unauthorized access to data inside secured network. In 3GPP context, the reverse HTTP proxy could be used both as an authenticator on behalf of Application Servers, and as a centralized access point to HSS in order to minimize the risk for potential synchronization failures with AKA SQNs.

The use of reverse HTTP proxy could lead to a centralization approach, in which all new interfaces using the same protocol could be implemented in a centralized node. For example, Presence/Ut interface and access to MBMS BM-SC will most probably all use HTTP as the transport protocol. In this case, the implementation strategy could be to provide access to all these functions via a HTTP proxy, see Figure 1. Because the interfaces towards HSS are now minimized, the danger of causing synchronization failures in the USIM is much less than if all different applications used separate interface. The interface between UE and HTTP proxy is protected using TLS. Only one TLS connection should be used between the UE and the HTTP Proxy even when communicating with several Application Servers. The solution does not require new AVs for the proxy each time a new TLS connection is established if the HTTP Digest AKAv2 passwords are re-used.

HTTP proxy should be seen as a functional node rather than as a fixed network entity. If the Mobile Operator had only one Application Server, then the functionality of the proxy is not necessarily needed. This helps in creating different implementation strategies, e.g. having a migration path from one Application Server to several ones.

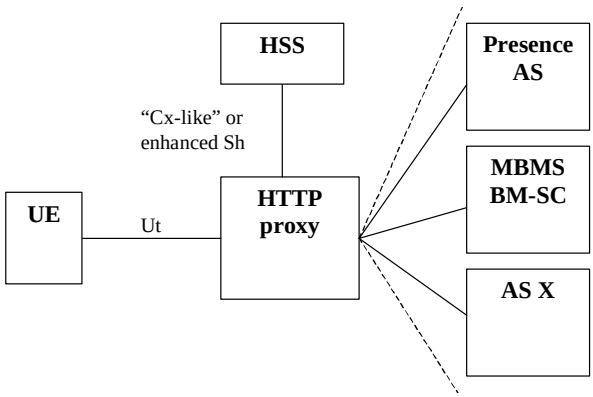



Figure 1: Optimized implementation of HTTP access to Presence AS and MBMS BM-SC

Even though Presence/Ut does not currently have any use scenario that would require access to Application Servers in the Visited Network, the same kind of implementation could be possible. In this case, the HTTP proxy in the home network would require also AAA server functionality, but it could still take responsibility of distributing AKA AVs in specific order in order to avoid synchronization failures, see figure 2. This requires enhancements for Diameter Multimedia application to work with AAA proxies; however, this work is already progressing in IETF [draft-belinchon-aaa-diameter-mm-app-01.txt].

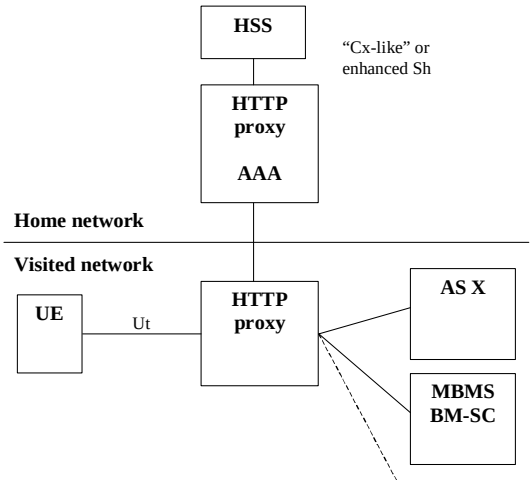



Figure 2: Optimized implementation of HTTP access to Application Servers in the Visited Network (note currently in the scope of Presence)

The interface between HTTP proxy and the Application Servers could use TLS in order to have more security. However, this should be a policy decision by the Operator. This interface should also be enhanced using similar approach that is currently used in IMS, i.e. allowing the proxy to communicate the asserted identity to the AS. This kind of extension should not be a problem because HTTP in general is considered as a "common good" and it already has been extended locally as well as globally. Several alternative solutions exist. For example, this could be achieved by including authentication specific information to HTTP cookies. More specifically, the cookies could include information about the authenticated identity, authentication method, time of authentication, session related information, access type (PS, CS, fixed) and even end-user IP-address information. Alternatively, some existing header could be re-used (e.g. some potential extension header from OMA) or a 3GPP extension header could be developed following the HTTP extension framework [RFC2774]. Also, the re-use of Authorization header to carry identity information could be considered.

The frequency of authentication may also affects to the deployment model that is used when USIM/ISIM is used for several applications. In the HTTP context, HTTP Digest AKAv2 passwords can be re-used if needed (see more details in Ericsson contribution related to AKAv2). However, the benefits of using this mechanism are implementation dependent, and for this reason, the mechanisms should be seen as an additional tool for building Operator dependent security architecture rather than as a general mechanism.

# 3.1 Presence/Ut

This part discusses the feedback from SA3#28.

## 3.1.1 AKAv2 RFC status in IETF

Ericsson solution is partly based on standardization work done in IETF. This can be seen as a risk from SA3 point of view.

Ericsson would like to present the following issues as reasons why this argument should not be used to reject AKAv2:

- SA Plenary has concluded that September 2003 is too early for Release 6 deadline. Currently, it seems that the release will not be closed until March 2004 or even June 2004. There is no reason to limit Release 6 work to RFC's only at this phase. Also, Release 6 has already other work items that have such dependencies, such as WLAN.

- Standardization of HTTP Digest AKA (RFC 3310) was pioneering work in IETF. This work did not only open HTTP Digest authentication framework for AKA, but also set up the organizational processes and namespaces for future AKA algorithm versions. The standardization work related to AKAv2 is expected to be much easier because most of the work has already been done in RFC 3310.

- IETF, and especially SIP WG should have a clear interest of allowing the standardization of AKAv2. The reason for this is that most application layer protocols, such as SIP, seem to develop toward the use of TLS as a

common security mechanism. The use of AKAv1 with TLS cannot be recommended because of the interleaving attack.

### 3.1.2 New Cx-like interface needed

Creating of new Cx-like interface should not be a problem because in practice this would mean copying most of the details from existing work. Alternatively, the Sh interface, that already exists between Application Servers and HSS, could be enhanced to include authentication, authorization and accounting related aspects. In any case, this is for CN4 to decide.

### 3.1.3 Number of elements having an interface towards HSS

The HTTP proxy based solution can minimize the number of new elements having an interface towards HSS to one.

### 3.1.4 Heavy consumption of AVs

The use of HTTP proxy as a gateway for several Application Servers lowers the use of AVs significantly.

Also, it has been demonstrated that the passwords generated using HTTP Digest AKAv2 can be re-used.

### 3.1.5 Effects on SQN handling

It is true that re-using AKA with several applications would affect SQN handling. Unfortunately, there is very little that SA3 can do for solving these issues because USIM implementations are very much Operator dependent. This document has promoted architectural means to solve potential problems related to this issue.

### 3.1.6 Server authentication is done twice

This issue is not necessarily specific to Ericsson's preferred solution but can be seen as a potential issue related to all proposed solutions. TLS includes server authentication, and so does HTTP Digest and HTTP Digest AKA. Ericsson is not aware of any mechanisms that could be used to avoid double authentication of the network if TLS is used.

### 3.1.7 Details of proxy functionality are missing

More details on proxy functionality are given in this documents, section 3 and Appendix 1.

## 4. Recommendations

Ericsson proposes that SA3 takes a working assumption that access to all applications that use HTTP as a transport protocol, and that re-use AKA for authentication, can be implemented using a reverse HTTP proxy in order to solve potential synchronization problems as described in chapter 3.

SA3 should inform SA2 and CN4 that architectural means would play an important role when solving the problems related to potential SQN synchronization failures.

SA3 should also involve SA1 and SA2 to the evaluation of the solutions based on HTTP authentication proxy because Nokia's version includes a dependency to subscriber certificate work. The consequence of building a migration path towards subscriber certificates is not a security issue. It is not clear to Ericsson what is appropriate time plan for building PKI for subscribers in 3GPP system, and if such (duplicate) authentication infrastructure is needed at all for a Mobile Operator that as thus far solely built the relationship with its customers upon the SIM card/UICC.

## 5. References

[draft-belinchon-aaa-diameter-mm-app-01.txt] Diameter Multimedia Application, IETF, Work in progress, June 16 2003.

[S3-030223] Key management for the use of http at the Mt reference point in the IMS, source: Siemens, SA3#28.

[S3-030224] Security protocols for the use of HTTP at the Mt reference point in the IMS, source: Siemens, SA3#28.

[S3-030245] HTTP Security in Mt interface, source: Ericsson, SA3#28.

[S3-030256] Analysis of HTTP authentication, source: Nokia, SA3#28.

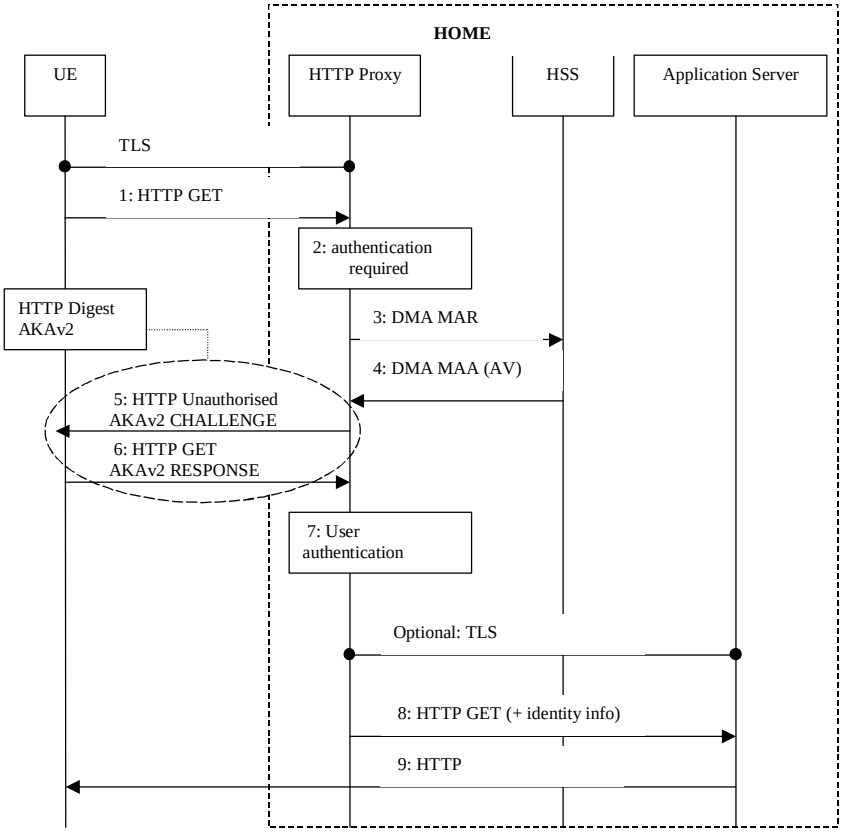
[S3-030325] LS on security solutions for the Ut reference point, source: CN1, N1-030933.

[S3-030337] LS on adapting Cx interface protocols for security purposes, source: CN4, N4-030722.

[TS 33.102] 3GPP, 3G Security; Security Architecture.

# Annex A

## A.1 Authentication proxy in home network:




DMA MAR & MAA: Commands of Diameter Multimedia Application currently developed in IETF, see more in (draft-belinchon-aaa-diameter-mm-app-01.txt).