3GPP TSG SA WG3 Security **S3-030721**

18th – 21th November, 2003

Munich, Germany

Agenda Item:	Presence, GAA
Source:	Ericsson
Title:	Challenges in using shared-secret TLS with NAFs
Document for:	Discussion/Decision

1. Introduction

SA3 has been discussing on an interesting new approach for using TLS in application servers and proxies. The approach is based on a internet-draft currently developed in IETF [Shared-secret-TLS]. This document intends to identify the challenges and standardization gaps in order to make shared-secret TLS useful and secure with 3GPP specific services.

2. Challenges and standardization gaps

2.1 TLS implementations

Shared-secret TLS should be seen as an optimization for full standard TLS. This optimization may benefit some use situation, however, it does not help implementation in general. For example, Web-browsers that are used to access services in the open Internet must anyhow have full TLS implementation or otherwise the end-user is not able to use some common services, such as banking services, in the Internet securely.

SA3 should adopt a working assumption that shared-secret TLS can only be defined as an optimization for TLS. Both the client and the NAF must always have full TLS implementation.

2.2 Shared-secret TLS capabilities

In order to use shared-secret TLS, both the client and the NAF needs to know that the other end is able to use the mechanism. Procedure where the UE just decided to use the shared-secret TLS without somehow knowing that one particular NAF really supports it is not appropriate. Firstly, it will cause some additional load in the UE side if the shared-secret TLS is not support in the NAF. Secondly, it will lower the flexibility of future development of the network because some UEs will always assume that shared-secret TLS will be used.

There may be several ways to overcome this problem. For example, it may require the use of Handshake Protocol at the beginning of shared-secret TLS session. However, note that this kind of procedure is not part of [Shared-secret-TLS] draft.

On the other hand, if the use of shared-secret TLS is limited to Authentication Proxy, and if SA3 decides to use “forwarding proxy” approach, the information about TLS capabilities of the proxy could be uploaded to the UE using OMA Device Management mechanisms. Alternatively, suitability of DNS could also be further studied.

SA3 should adopt a working assumption that capability negotiation is required if shared-secret TLS is adopted as a solution to access some NAF securely.

2.3 Negotiation of security parameters

Shared-secret TLS is based on the idea of re-using session caching mechanism (i.e. resumed sessions) directly with symmetric keys in order to avoid public-key operations. However, the caching mechanism does not include any negotiation mechanism for TLS security parameters, such as encryption, MAC algorithms or pseudo-random functions (PRF). In order to negotiate these parameters, SA3 must specify how to extend the shared-secret-TLS for 3GPP use, e.g.

by re-useing some parts of TLS Handshake Protocol. This requires breaking some general TLS related rule for not using the Handshake Protocols with resumed sessions. The use of Handshake Protocol may not be a problem, however, this kind of protocol misuse increases the possibility that some security and/or implementation problems may appear in the future.

If the Handshake Protocol is not used, it is also possible that shared-secret TLS is restricted for certain security parameters, and consequently the use of this mechanism is limited to time when these security parameters are known to be secure.

SA3 should be aware that shared-secret-TLS draft does not provide complete solution for 3GPP. SA3 can not avoid defining extensions to the draft in order to solve the negotiation problem.

2.4 Key agreement between UE and NAF

In order to use shared-key TLS, both the UE and NAF need to agree on session ID and key. [Shared-secret-TLS] does not specify how the agreement is done. Instead, the key agreement is seen as an application specific problem. Generally speaking, it is assumed that the client will know the session ID and the key before contacting NAF with TLS.

There are at least two ways of implementing this in GBA. Assuming that UE knows that a NAF supports shared-secret TLS, it could in theory start using TLS directly without using application layer protocols first. However, this solution may need changes to the TLS in the NAF side since the NAF needs to have access to key identifier before contacting BSF. Alternatively, the key agreement could be done at application layer, as already proposed in [S3-030576].

It is proposed that SA3 adopts a working assumption that key agreement for shared-secret TLS is always done at application layer in order to avoid additional changes to TLS in NAF.

2.5 Shared-secret TLS with authentication proxy

SA3 is currently discussing two different models for authentication proxy (AP), i.e. the so-called “forwarding” and “reverse” proxy. The “forwarding” proxy requires some additional configuration mechanism for UE to know the IP-address and services behind the proxy. On the other hand, the “reverse” proxy is transparent to the UE, and no configuration is needed. Instead, standard DNS procedures are used.

Depending on the decisions related to the other issues presented in this document, e.g. whether the configuration mechanism is also needed to negotiate on shared-secret TLS capabilities, SA3 should consider the suitability of shared-secret TLS with alternative proxy models. It may mean that shared-secret TLS fits better with the “forwarding” proxy than with “reverse” proxy.

3. Conclusions

This document has identified some potential issues related to the use of [Shared-secret-TLS] with NAFs. Even though shared-secret TLS is seen as an interesting approach for 3GPP, there are still many open issues related to the approach.

It is proposed that SA3 adopts the following working assumptions related to the potential use of shared-secret TLS with NAFs:

- Shared-secret TLS is seen as an optimization for TLS. Both the client and the NAF must also have full TLS implementation in addition to shared-secret TLS.
- The minimum implementation should include the normal TLS. Shared-secret TLS can only be optional for implementations.
- The solution should include a capability for negotiating between different TLS models. In particular, the NAF should be able to inform UE that it is able to use shared-secret TLS.
- Negotiation of TLS related security parameters needs to be further specified.

It must be stressed that the solution based [Shared-secret-TLS] must also include 3GPP specific extensions. It is very important that SA3 actively analyses the security and implementation properties of the solution before considering it as a working assumption. Note also that security analysis performed by IETF may not complete because IETF is focusing only to the scope of [Shared-secret-TLS] draft.

It should also be noted that GBA itself has some open issues that may affect the usefulness of shared-secret-TLS with NAFs. For example, it is not clear yet what is the lifetime of the bootstrapped keys.

4. References

[S3-030576] Comparison of different solutions for GBA and AP based AS: standard TLS versus shared secret based TLS, contribution from Alcatel to SA3#30, Povoa do Varzim, Portugal, 6-10 October, 2003.

[Shared-secret-TLS] Use of Shared Keys in the TLS Protocol, draft-ietf-tls-sharedkeys-02, work in progress, IETF, October 2003.