3GPP TSG SA WG3 Security — S3#24 **S3-~~020xxx~~020372**

9 - 12 July 2002

Helsinki, Finland

Source: **Hutchison 3G UK**

Title: **SA and registration lifetimes**

Document for: **Discussion/Decision**

Agenda Item: **7.1~~x.x~~**

Introduction

This contribution looks at the relationship between the ~~l~~expiry ~~if~~etimes of registrations and the lifetimes of SAs at the P-CSCF and UE.

T~~SA3 has been using the working assumption that t~~he expiry time~~r~~ of a registration will be used to set the lifetime of an SA. Without some further clarification, this can cause the problems described in the next section. ~~, although there is no explicit text to describe exactly how this relation happens (careful here there may be some text, probably stronger than a working assumption).~~

Timing Issues

Whatever mechanism is selected to handle registration lifetimes and the expiry time of SA~~s lifetimes~~, it is important to ensure ~~never end up in the position~~ that an IMPU is never registered for longer than ~~the lifetime of~~ the SA that will be used to protect the traffic to/from that IMPU will live, as a registered UE will become unreachable.~~.~~

~~This document does not consider possible inconsistent states between the UE, P-CSCF and S-CSCF caused by losing (even after re-transmissions) messages.~~

There are two process~~es~~ that affect at least one of the expiry time of registrations and the lifetime~~s~~ of ~~registrations and~~ SAs, that is, registrations without authentications and registrations with authentications.

Firstly we consider a registration without an authentication. Suppose a subscriber has already registered IMPU1 until time X and the P-CSCF and UE contain a corresponding SA that will also expiry at time X. The subscriber then tries to register IMPU2. The S-CSCF accepts this registration attempt without an authentication and sets the registration of IMPU2 to expire at time Y (see below diagram).

UE	P-CSCF	S-CSCF
IMPU1 registered until time X		IMPU1 registered until time X
SA that lives until time X	SA that lives until time X	
---------- Registration of IMPU2 without an authentication ----------		
IMPU1 registered until time X		IMPU1 registered until time X
IMPU2 registered until time Y		IMPU2 registered until time Y
SA that lives until time X	SA that lives until time X	

If Y is later than X, then the SA will expire before the registration and a registered IMPU could become unreachable.

This problem can be avoided by applying one (and only one is necessary) of the following rules in the network

1. For registrations without authentication, the expiry timer of the registration shall be set to no longer than the longest remaining time of all the currently registered IMPUs for that IMPI.
2. The P-CSCF monitors the expiry timer of all registrations without authentication for an IMPI and increases the lifetime of the latest SA for that IMPI to ensure the SA lives longer than any registration.

From a security perspective, the first rule seems to be the most sensible. Put another way, the rule says if that the latest a user has IMPU registered until is time X and it wants to register an IMPU until time Y later than X, it requires an authentication. This also avoids the need for P-CSCF to monitor the lifetimes of all registrations without authentications and adjust the lifetimes of SAs accordingly.

Secondly we consider a registration with an authentication. Suppose a subscriber has already registered an IMPU with expiry time X and the P-CSCF and UE contain a corresponding SA that has will also expiry after time X. The subscriber then tries to register a further IMPU. The S-CSCF accepts this registration attempt only after an authentication and set the expiry timer of this registration to Y (see the below diagram)

UE	**P-CSCF**	**S-CSCF**
IMPU1 registered until time X		IMPU1 registered until time X
SA that lives until time X	SA that lives until time X	
---------- Registration of IMPU2 with an authentication ----------		
IMPU1 registered until time X		IMPU1 registered until time X
IMPU2 registered until time Y		IMPU2 registered until time Y
SA that lives until time Y	SA that lives until time Y	

Note: the previous SA may be kept for a short time to enable smooth handover

If Y is less than X, then the SA will expire before the registration and a registered IMPU could become unreachable.

The sensible way to avoid this problem is to set the lifetime of the SA to expire at least as late as the registration and of the previous SA.

~~The problem can be avoided by either stopping the problem from happening by putting restrictions on the registration lifetimes (rule a) or taking corrective action on the SA lifetimes at the P-CSCF and UE (rule b).~~

~~A registration without authentication increases the lifetime of a registration, this suggests that one of two rules should be applied;~~

~~1a) the expiry time of the registration is not allowed to more than the lifetime of the current SA.~~

~~1b) the lifetime of the SA needs to be increased (if necessary) to at least that of the expiry time of the registration~~

~~An authentication requires one of the following rules to be applied;~~

~~2a) the registration timer of the new registration must be longer than any current registration timer.~~

~~2b) the expiry time of the new SA must be at least as long as the previous SA.~~

~~Comparison of Rules 1a and 1b~~

~~Rule 1a puts a restriction on the lifetimes of registrations. It also requires the S-CSCF to keep a timer for each IMPI. It means that to register an IMPU for a long time may require an authentication. This would probably only an issue, if getting towards the end of all registration lifetimes in the S-CSCF. Without a detailed analysis it seems that this method would force more registrations without authentication and authentications. It is hard to say exactly to what extent there will be additional registrations and authentications.~~

~~Perhaps the strongest arguments in favour of rule 1a are negative implications on the selection of rule 1b.~~

~~Rule 1b means that an SA lifetime will be extended (possibly only at the application layer). This means the P-CSCF will need to look at the expiry time of every registration in order to update the lifetime of the SA. This could seem odd in the sense that an SA is negotiated for a certain lifetime (at the application layer) and then the lifetime gets extended (at the application layer). An alternative view is that an SA is negotiated for an effectively limitless lifetime (at the network layer) but with a (changeable) expiry time at the application layer.~~

~~One issue that was raised in the IMS drafting session of the last SA3 meeting was that with the IP layer SAs held effectively at two layers, it is possible to have an SA left at the network layer after it is deleted from the application layer (e.g. failure at application layer or bad implementation). Using rule 1b means that the lifetime of the SA needs to be continually extended, whereas with Rule 1a it is set after the authentication is successful and left until the SA is deleted (due to either the expiry time being exceeded or the SA becoming obsolete). This means that if Rule 1a is selected, it is less likely to have an SA left at the network layer given that it is possible to update the expiry time of the SA at the network layer once the authentication is successful. This could be done by either updating the expiry time only of the SA or deleting the odd version of the SA and adding a new version of the SA with updated expiry time.~~

~~The best rule here is …….~~

~~Comparison of Rules 2a and 2b~~

~~Rule 2a puts a limitation on setting registration timers and the storage variable in the S-CSCF to know the expiry time of the previous SA.~~

~~Rule 2b requires some small amount of processing once the authentication is successful.~~

~~Clearly Rule 2b seems the most sensible.~~

Proposed T<u>ext to Cover Suggested Functionality</u>~~ext for TS 33.102~~

<u>This section proposes some text to cover the above decisions. The exact text, where to put the text into the document and potentially even which document the text should be in needs to be decided once there is agreed text for the SA handling.</u>

For <u>registrations without an authentication, the proposed text is as follows:</u>~~rule 1x we need text along the following lines:~~

~~"……"~~ <u>"For registrations without authentication, the S-CSCF shall set the expiry timer of the registration to be not larger than the largest current expiry timer of all registered IMPU related (via their IMPI) to the IMPU being registered"</u>

For <u>registrations with an authentication, the proposed text is as follows:</u> ~~rule 2b we need text along the following lines:~~

"Once the P-CSCF/UE considers the authentication to be successful, it sets the SA lifetime to be <u>using the larg</u>est of the registration expiry and the time left before the ~~qual to the maximum of the~~ previous ~~SA's lifetime and the registration~~ expir<u>es</u>~~y lifetime~~."

~~Generic text (maybe not needed)~~

~~"If the UE has an SA with only short lifetime and a registration with a longer lifetime, then the UE should send an unprotected register."~~