3GPP TSG-SA3 Meeting #21bis (aSIP ad-hoc) ***Tdoc S3z020014***
Antwerp, Belgium, 31 January-1 February 2002

Source: Ericsson

Title: On the use of KSI-IMS

Document for: Discussion

Agenda item: 8

1 Scope and Objectives

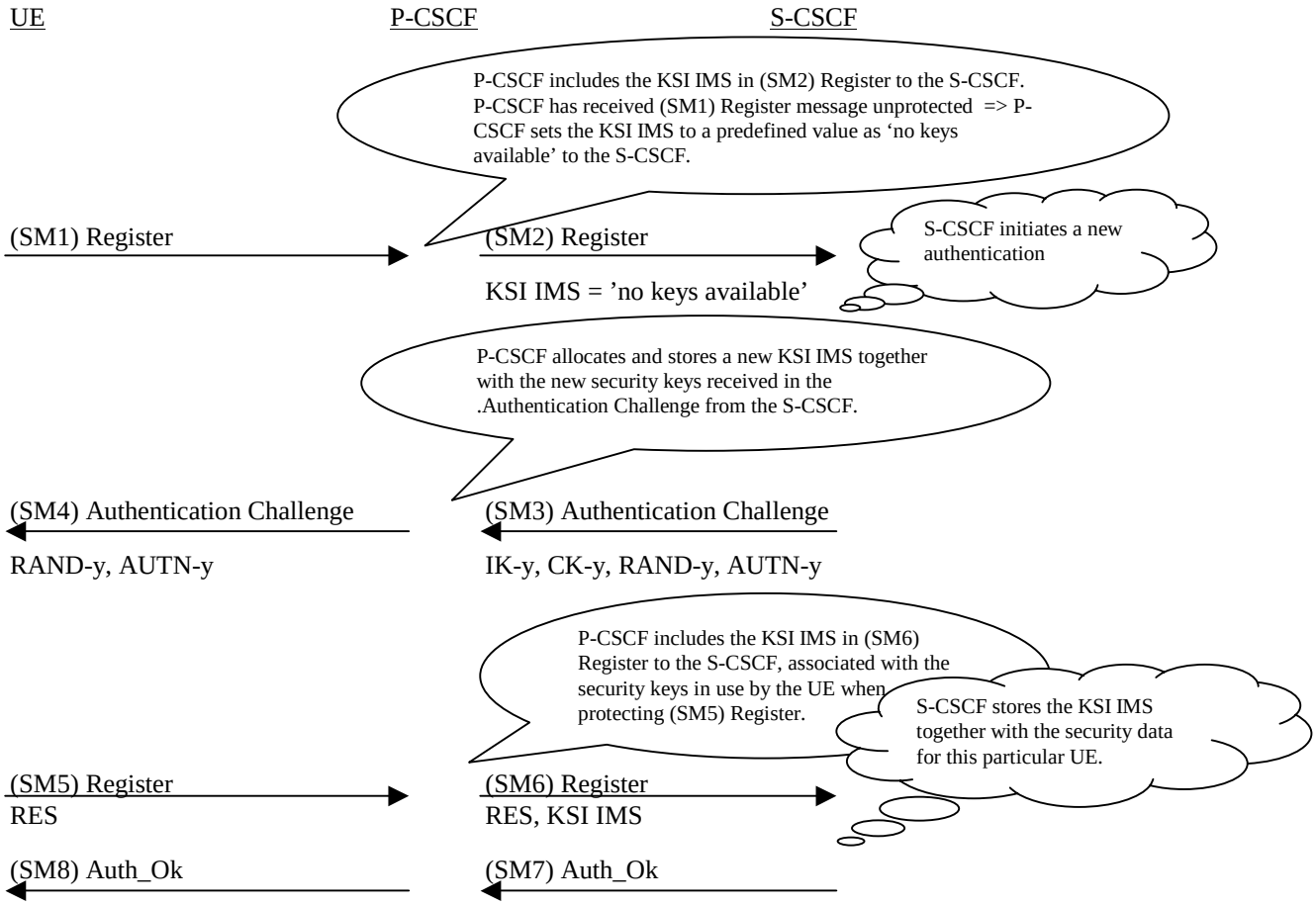
This contribution introduces the use of a new identifier, Key Set Identifier for IMS (KSI IMS), and discuss how it could be used in order to address some open items of our security architecture defined in TS 33.203.

2 Key Set Identifier for IMS

It seems that there is a need for the visited environment (P-CSCF) to inform the home environment (S-CSCF) on some details with regards to the level of protection offered to the first hop between UE and P-CSCF, so HN can then be able to apply ceirtain security policies.

This contribution proposes that the P-CSCF allocates and stores a new identifier each time the S-CSCF triggers an IMS-AKA procedure during a Register procedure. This identifier will be associated and stored in the P-CSCF together with the new security key set received from the S-CSCF, in the (SM3) Authentication Challenge message. We hereafter name this identifier as Key Set Identifier for IMS or KSI-IMS.

Find below an overview of the process …



The allocation and storage of KSI-IMS at P-CSCF and further transmission and storage at S-CSCF as proposed above could be used to address different open items in the security architecture defined in 33.203 as described in the following sub-chapters.

2.1 Indication from the P-CSCF to the S-CSCF – Initial Registration

It is S3 working assumption that intial registrations shall be always authenticated while it will be up to the policy of the operator whether re-registrations shall be re-authenticated or not. Note that we are considering that re-registrations will be issued making use of a valid SA between UE and P-CSCF, while REGISTER messages sent in clear will be considered as initial registrations.

This is also N1´s working assumption and to this respect N1 mentions in LS S3-020029 the following statement …

> *"CN1 additionally notes that :-*
>
> > *The P-CSCF has an association between IMPI and IK after the first registration. The P-CSCF will also have a list of all registered IMPU that are associated with this IMPI and IK. This data can be used to verify the integrity of subsequent messages. It is therefore not necessary to include IMPI in every INVITE request from the UE as the INVITE will be integrity checked.*
> >
> > *The very first REGISTER request must be authenticated. Later REGISTER messages can be integrity protected using IK. If the S-CSCF is aware of this protection, it could decide to REGISTER an IMPU without further authentication, depending on operator policy etc. However, authentication is mandated for REGISTER messages that are not integrity protected.*
>
> *The second of these implies that **the P-CSCF needs to indicate to the S-CSCF if a received REGISTER request was integrity protected or not**. CN1 is studying how this may be done, and requests guidance on the information that the S-CSCF may require e.g. the IK used, how long it has been in use etc."*

When the P-CSCF receives a (SM1) Register message from the UE, which is not protected, then the P-CSCF shall encode the new parameter KSI IMS to a predefined value as 'no keys available'. The KSI IMS shall be used as an indicator to the S-CSCF in order to notify the S-CSCF that the (SM1) Register message from the UE was not protected. This shall trigger the S-CSCF to perform a authentication of the UE. In the same fashion, during re-registration procedures the P-CSCF shall include in SM2 the value of KSI IMS used for protection of the re-REGISTER message from the UE. The S-CSCF will detect that a valid SA is already in place and it will be up to the operator´s policy whether to trigger a re-authentication and session key update procedure.

2.2. Indication from the P-CSCF to the S-CSCF - integrity protection check of (SM5) Register has failed

Our current understanding of chapter 7.3.1.1 in TS 33.203, is that the P-CSCF shall forward a (SM5) Register message from the UE to the S-CSCF, even if the (SM5) Register message failed the integrity protection check in the P-CSCF. In this case the KSI IMS *could* be used as an indication from the P-CSCF to the S-CSCF to inform the S-CSCF about the failed integrity check, by setting the KSI IMS in the (SM6) Register message to a predefine value as 'integrity check failure'. If this assumption is incorrect then chapter 7.3.1.1 needs to be clarified.

2.3. Prevention of Identity Spoofing (the fraudulent user attack)

During our last S3 meeting, Tdoc S3-010633 highligthed the potential attack using fraudulent IMPUs over valid integrity protected paths. S3 proposed a preliminary number of potential solutions to N1 in LS S3-010673 amongst which N1 prefers to download the list of explicitly and implicitly registered IMPUs in separate SUBSCRIBE/NOTIFY methods from S-CSCF to P-CSCF (LS S3-020029).

In this contribution Ericsson would like to present and discuss another alternative solution to this problem, which has not been considered neither by S3 nor N1. This proposal is based on the assumption that P-CSCF makes available to S-CSCF the KSI IMS value allocated during each IMS AKA procedure in SM6 (KSI IMS). The S-CSCF stores this value together with the rest of user´s service profile information and when an INVITE message reaches S-CSCF (including IMPU and KSI IMS), S-CSCF will be able to check whether the IMPU included in the INVITE message is allowed to use the SA indicated by KSI IMS.

Ericsson believes that this is a simple and robust solution to the problem, which does not require the use of additional SIP methods (i.e. solution in current working assumption in N1 requires the use of SUBSCRIBE/NOTIFY methods in order to download list of IMPUs from S-CSCF to P-CSCF).

3 Conclusion

The introduction of KSI IMS as described above could solve issues like:

- the P-CSCF can indicate to the S-CSCF when the P-CSCF has received a (SM1) Register message from the UE which was not integrity protected;
- the P-CSCF can indicate to the S-CSCF when the P-CSCF has received a (SM5) Register message from the UE which has failed the integrity protection check in the P-CSCF.
- If the KSI IMS is included in the INVITE messages from the P-CSCF to the S-CSCF, then the S-CSCF could detect the fraudulent user attack described in the Tdoc S3-010633 discussed at the SA3 meeting #21 by checking whether the correct user has initiated the INVITE with one of it's one IMPU.

4 Proposal

It is proposed that SA3 agrees to introduce the KSI IMS (as a working assumption) described in this paper. I t is also proposed that SA3 sends an LS to N1, asking N1 whether this is a suitable solution to provide the required indication to S-CSCF of whether REGISTER messages are protected or not at the first hop. N1 shall be also consulted on whether the introduction and use of KSI IMS would be a much more optimized solution to the fraudulent user attacks as described in this paper.