3GPP TSG SA WG3 Security — S3#26 **S3-020628**
19- 22 November 2002
Oxford, UK

Agenda Item: IMS~~7.2TBD~~

Source: Ericsson

Title: Re-use and re-transmission of RAND and AUTN ~~Security needs: Evaluation of UTRAN IP transport interfaces~~On registering several public identities in IM CN ~~SS~~

Document for: Information~~Discussion/Decision~~

1 General~~Scope and objectives~~

At the SA3 meeting in Munich, Ericsson presented a CR in Tdoc S3-020548 on the "Re-use and retransmission of RAND and AUTN". We proposed to delete an editor note based on the findings in the reason for change. There were comments during the meeting that some of the conclusion in the Reason for change could be lifted into the CR to 33.203 as requirements. Ericsson presented a new version of the CR in Tdoc S3-020560, in the same meeting.

As no conclusion could be reached on S3-020560, as some companies felt that they needed more time to sort out what requirements actually already is included in the standard SIP specifications, Ericsson started an e-mail discussion in order to be able to agree a new version of the CR at the SA3#26 meeting.

The following PPT slides with comments from Ericsson and also a new version of the CR in Tdoc S3-020590 was sent out:


Re-use and re-transmission of ...


S3-020590_CR-Ericsson-Retransm...

During the e-mail discussion we received comments from Adrian Escott at Hutchinson on the S3 reflector:

"From your analysis, it seems as though an AV should only re-transmitted by the S-CSCF as part of the normal SIP re-transmissions in the transaction layer. Hence there are very clear and definite circumstances for a re-transmission. This does not seem well reflected in the last sentence added by the CR, which states that in general AVs are not re-tranmitted.

It seems to me better to replace the last sentence of the CR "In general therefore the S-CSCF shall use a quintet only once. " with something along the lines of the following: "Therefore there shall be no re-transmission of AVs, except as part of the normal SIP transaction layer re-tranmission procedures".

I also think there was some dicussion about not using quintet at the Munich meeting. Finally, it might be alright to include the paragraph as a direct replacement for the editor's note rather than at the end, as it only short and does not in my opinion affect the flow of the section."

The new version of the CR presented in this meeting, has been updated with Adrians comments - slightly modified.

~~This paper discusses the enhancement of NDS/IP specification to cover the control plane of IP UTRAN as~~

proposed in [9].

Ericsson proposes:

SA3 should consider updating the WID for Release 6, cf. [10], to include a link to the work in SA1 on Network Sharing

SA3 should investigate if a new Security Domain should be defined in TS33.210 to capture the Network Sharing Scenarios which potentially can affect the security requirements for the Iu interface

SA3 should investigate if UTRAN can be defined as a Security Domain in particular it is not clear if the protection of e.g. Iub and Iur should be regarded as Zb interfaces

The scope for this contribution is to discuss different requirements needed and different alternatives on how to register several public identities in IM CN SS.

Ericsson proposes that the UE and the P-CSCF shall have one SA for each registered IMPU (IM Public Identity) due to the requirement with additional S-CSCFs for future releases. This means that each REGISTER message with the aim of registering an IMPU should be authenticated.

2 Background

The proposal in [9], to encrypt and integrity protect the control plane over the IP based Iu interface, seems to be a sensible recommendation considering the sensitivity of the conveyed information (e.g. the session keys for the air link, the control to set on/off the encryption on the air link). NDS extension as Zb interface could be the right choice. However SA1 is currently working on Requirements for Network Sharing cf. [7] that was not included in the discussion in [9] but should be considered in the work on enhancing NDS for Release 6. In [8] a number of scenarios have been identified e.g. a scenario called 'Common Spectrum Network Sharing'. In this scenario a multiple number of Iu interfaces belonging to different Operators are connected to one UTRAN. Ericsson believes that the enhancement of TS33.210 should include an investigation if a new Security Domain is required for defining a new Za interface i.e. a SEG concept between UTRAN and CN. However the protection of the other interfaces in UTRAN should require further investigation. Threats and trust models validating the need of security on such interfaces should be investigated and weighed towards the implications that adding security would bring.

Currently Ericsson believes that a compelling investigation including threats and risks are missing and it is believed that the cost issue can be overwhelming. In particular on the Iub interface where a low-cost solution for the Node B:s may be wanted by the operator. Extending the NDS security to Node B:s means requiring both IPsec and IKE etc. Key management appears to be a troublesome issue due to the immense number of involved nodes (the UTRAN network is complex and comprises tens of thousands of nodes). There is a need for a simple key management solution and it should be further investigated what solution is the right choice.In [23.228] it is a requirement that a user shall have one IM private identity (IMPI) and several IM public identities (IMPU(s)). The IMPI and at least one IMPU is stored in the ISIM, IM SIM. It is the private identity, i.e the IMPI, which is used for authenticating the subscriber. The user sends a SIP REGISTER towards the registrar, which is the S-CSCF, and the registrar performs the authentication. The registrar sends a challenge to the user, which in turns sends, a response back that is checked by the S-CSCF.

The REGISTER sent by the user towards the registrar:

REGISTER sip: ---

Via: ----

From: IMPI

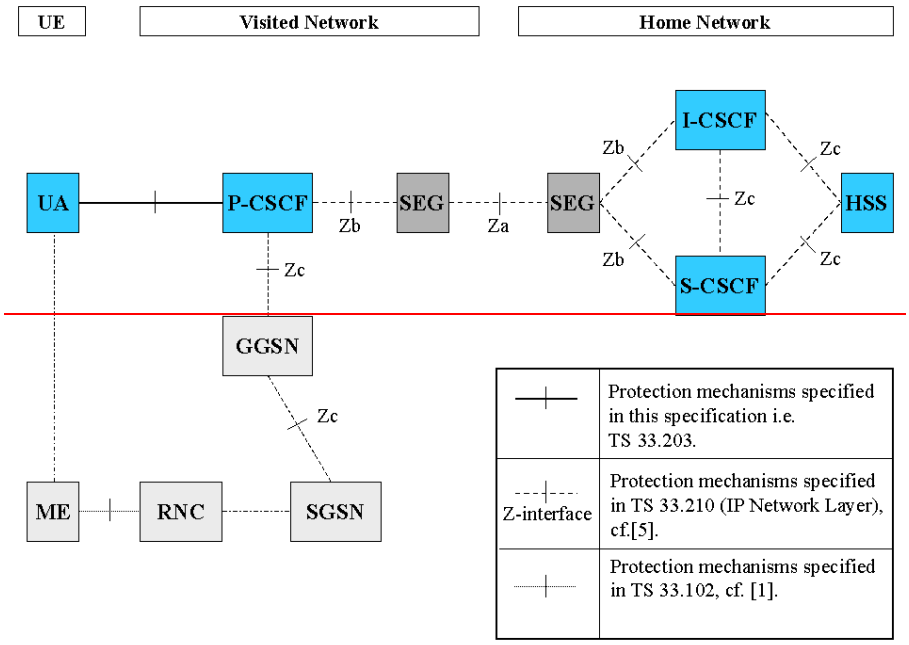
To: IMPU

Call-ID: ----

Cseq: 1 REGISTER

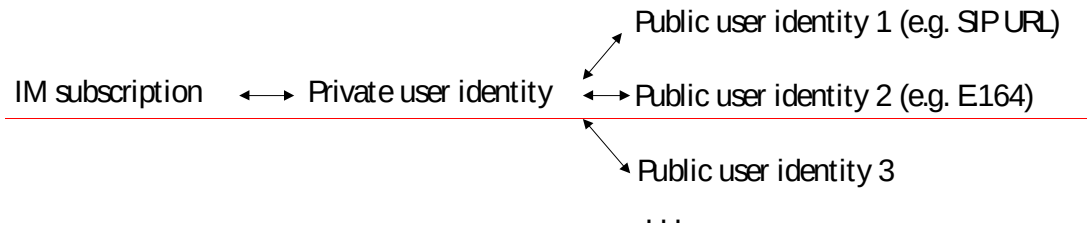
Content-Length: 0

The S-CSCF gets the Authentication vector from the HSS, which includes the challenge, and the key(s), IK and optionally the CK.



~~Figure: An overview of the security architecture for the IM CN SS and its relationship to NDS i.e. TS 33.210.~~

~~The relationship between the IMPI and the IMPUs are specified in [23.228] as:~~



~~In [23.228] it is specified that the HN operator is responsible for the assignment of the IMPI and IMPUs. Furthermore it is also said in [23.228] that identities that are not defined by the operator may exist, cf. chapter 4.3.3.4. Regarding the assignment of an S-CSCF for a user it is specified that an S-CSCF is assigned at registrations however for future releases it should not be precluded that additional S-CSCFs might be assigned, see chapter 5.2.2.1.~~

~~A registration will last for some specified time which can be included in the "expire" and the registrar can increase or decrease this time depending on the policy, cf. [SIP] chapter 7.4. If the user does not include the "expire" then he will by default be registered for one hour, cf. SIP chapter 7.4. It is possible for a user to de-register all identities by sending a REGISTER with a wildcard "*" in the Contact with an expire header with value 0, cf. [SIP] in chapter 7.6.~~

~~In [33.203] it is mentioned in an editor's note that it is optional to implement confidentiality protection and it should be applied at the same level as the integrity protection. This means that neither the IMPI nor the IMPU should be used as an SPI since both of these could be encrypted. Hence the P-CSCF needs some other SPI to do that. Here we assume that such an SPI is in place but so far this SPI is not specified in [33.203]. It could however be based on what is included in the From: field but then this field may not be encrypted.~~

~~3 Issues~~

~~In this section different alternatives for registering an IM subscriber and its IMPUs in the S-CSCF. Also the different security implications are discussed and its compliance with [23.228].~~

3.1 One SA Alternative 1

In this alternative the subscriber registers several IMPUs at the same time in one S-CSCF.

REGISTER sip: ---

Via: ----

From: IMPI

To: IMPU1, IMPU2, IMPU3

Call-ID: ---

Cseq: 1 REGISTER

Content-Length: 0

The major drawback with this alternative is that it is not compliant with SIP since it needs an extension making it possible to include several identities in the To: field.

There will only be one SA between the UE and the P-CSCF. All subsequent SIP messages can be protected by the defined SA and negotiated algorithms except when a new REGISTER is sent from a user. Then it is assumed that if the authentication is successful that all current IMPUs are released in the S-CSCF. Note that the identities are all registered in one and the same S-CSCF.

An advantage with this alternative is that all IMPUs that the user wants to register are registered with performing only one authentication. The handling of the validity of the SA is also simple since a new SA is only derived at expiration or when the user wants to register new IMPUs. It is assumed that the user can only register a limited number of IMPUs such that the limited bandwidth over the radio channel is taken into account.

3.2 One SA Alternative 2

In this alternative the subscriber registers one IMPU at the time i.e. first the UE sends

REGISTER sip: ---

Via: ----

From: IMPI

To: IMPU1

Call-ID: ----

Cseq: 1 REGISTER

Content-Length: 0

And then the UE after some time sends e.g.

REGISTER sip: ---

Via: ----

From: IMPI

To: IMPU3

Call-ID: ---

Cseq: 1 REGISTER

Content-Length: 0

Assuming that when the user registers IMPU1 the user has not yet been registered and that the REGISTER message is unprotected and hence there exist no SA between the UE and the P-CSCF. The S-CSCF will send a challenge to the user and when the user has been authenticated and received the 200 OK message the SA will be in place and it could be based on an SPI.

After some unknown time the user might want to REGISTER IMPU3 and then the UE could apply the keys derived with the first REGISTER message. This means that there must be a mechanism in place such that the UE treats the REGISTER messages differently. The solution to this is that the UE checks that it has a valid SA and uses that. The S-CSCF not only has to keep the IMPUs that are registered but also the corresponding IMPI.

When receiving the REGISTER(IMPU3) message the S-CSCF might not have to perform an authentication. The S-CSCF checks that the IMPI is registered and that the registration has not expired. Let us assume that the subscriber wanted to register IMPU3 1800s after IMPU1 was registered. This means that the S-CSCF has to decide weather to decrease the wanted expire time of 3600 s to 1800 s for IMPU3 or accept the 3600 s and perform an authentication in order to define a new SA. This new SA should then be used for all IMPUs registered thus far. Furthermore IMPU1 should be de-registered or re-registered after about another 1800 s. Whether authentication was performed or not the S-CSCF sends a 200 OK back to the UE.

With this scenario it is only possible to register a user in one S-CSCF since only one S-CSCF should keep track of the validity of the SA, i.e. the expiration time related with the registration, between the UE and the P-CSCF. This does not seem to be compliant with the requirement of additional S-CSCFs in future releases.

When the UE de-registers one or all IMPUs the S-CSCF could rely on the existing SA and implicitly rely on that it received an authentic de-register otherwise it could send a challenge towards the user.

3.3 Several SAs- Alternative 3

When sending the first REGISTER the IMPU1 is registered in the S-CSCF as in alternative 2.

In the second message the user wants to register IMPU3. With this alternative the REGISTER message is treated in the same way as for the case when the user REGISTERed IMPU1 i.e. the REGISTER message is not assumed to implicitly be protected i.e. a valid SA exist between the UE and the P-CSCF.

This means that the S-CSCF will perform a new authentication and a new SA is derived for IMPU3. This would mean that the UE has to keep track on several SAs as well as the P-CSCF, one SA for each registered IMPU. This solution does not exclude the scenario that different S-CSCFs, based on e.g. the profile related to the IMPU, are used when registering different IMPUs.

This gives more freedom in treating e.g. the expiration time since it would be set individually for each IMPU. Probably the SQN would anyway be related to the IMPI such that the ISIM does not have to keep track on several SQNs for each public identity. This model is more complicated from the number of SAs point of view. However from a security point of view this model means that different S-CSCFs can take care of different SAs and IMPUs and expiration times related to the SA. Furthermore this alternative is compliant with the requirement for additional S-CSCFs. This requirement seems to make it difficult to use the optimization with sending several AVs to the S-CSCFs. It is an issue that should be further analyzed.

For each mobile originated de-registration the S-CSCF could implicitly rely on the existing SA also in this alternative. It could also be possible to authenticate de-registrations as well in order to reduce the threat for DoS attacks. The S-CSCFs has to keep track on the expiration times individually for each IMPU.

3 4 Conclusions

As a conclusion, encryption and integrity protection of the control plane over the Iu interface seems reasonable i.e. as suggested in [9]. An extension to TS 33.210 NDS/IP is recommended, potentially by implementing Zb interface. However the work on Network Sharing in SA1 needs to be considered. In particular it is not clear whether a new security domain needs to be defined when considering securing the communication between the CN and UTRAN.

The contribution from Nokia, cf. [9], recommends integrity protection (with low priority) of the control plane over other IP-based interfaces (i.e. Iur, Iub, Iupc, Iur-g and Iu-BC). Ericsson recommends SA3 to request further study of threats and trust models for such interfaces considering not only the risks but also the cost aspects should security on those interfaces be included in TS33.210. Ericsson proposes that security for those interfaces is introduced at a later stage only if proven necessary.This contribution has presented three different alternatives for registering a subscriber and his/hers IMPUs. Two alternatives that defined only one SA between the UE and the P-CSCF. And one alternative with several SAs, one for each registered IMPU, was also described.

It seems that Alternative 3 is the only one that is compliant with the requirements in [23.228]. Also each new REGISTER message has to be authenticated. It is the understanding of Ericsson that Alternative 3, reflecting the requirements above, is the alternative that should be adopted by SA3. This means that the proposal with sending several AVs to the S-CSCFs should be analysed further for this scenario.

Furthermore it is not clear what "…. identities that are not defined by the operator may exist" imply, cf. [23.228] section 4.3.3.4. Does this mean that the subscriber could actually define his own IMPUs?

It has also been defined that IMPI and IMPU cannot be used as identifier, i.e. if they are encrypted, and a more general SPI should in that case be used. One other possibility would be to let the From field to be un-protected, i.e. not the whole SIP message is encrypted. Anyway from a general SIP perspective To: and Via: fields can not

be encrypted end to end. This issue has not yet been discussed in SA3.

One further requirement that has to be defined by SA3 is whether de-registrations should be authenticated in the S-CSCF or if the HN in should rely on the hop-by-hop security.

References

[23.228] 3G TS 23.228 (v500): "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; IP Multimedia (IM) Subsystem".

[33.203] 3G TS 33.203 (v040): "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA3; Access Security for IP-based services".

[SIP] IETF RFC 2543bis-03 (2001) "SIP: Session Initiation Protocol" [1] 3GPP TS 25.412 UTRAN Iu interface signalling transport

[2] 3GPP TS 25.422 UTRAN Iur interface signalling transport

[3] 3GPP TS 25.432 UTRAN Iub interface: signalling transport

[4] 3GPP TS 25.452 UTRAN Iupc interface signalling transport

[5] 3GPP TS 43.930 Iur-g interface, Stage 2

[6] 3GPP TS 25.419 UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)

[7] TSG SA, TSGS#14(01)739, Proposed WID: Service Requirements for Network Sharing.

[8] 3GPP TR 22.951v1.0.0 Service Aspects and Requirements for Network Sharing

[9] SA3-020536, Security need evaluation of UTRAN and GERAN IP transport interfaces, Nokia

[10] TSGS#17(02)0513, Work Item Description, Network Domain Security; IP network layer security (NDS/IP) for Release 6