Source: Ericsson L.M.
Subject: Security
Title: Distribution and Use of Current Security Context Data

Meeting: S3#11, Mainz, 22nd–24th February
Tdoc #: S3-000139
For: Discussion

1. Introduction

Tdoc S3-99545 on "Distribution of authentication data within one serving network domain" was presented at S3#9 meeting and approved at last SA#6 plenary meeting (CR34). That CR introduced the enhancement of the distribution of 'current security context data' between R'99 VLRs/SGSNs.

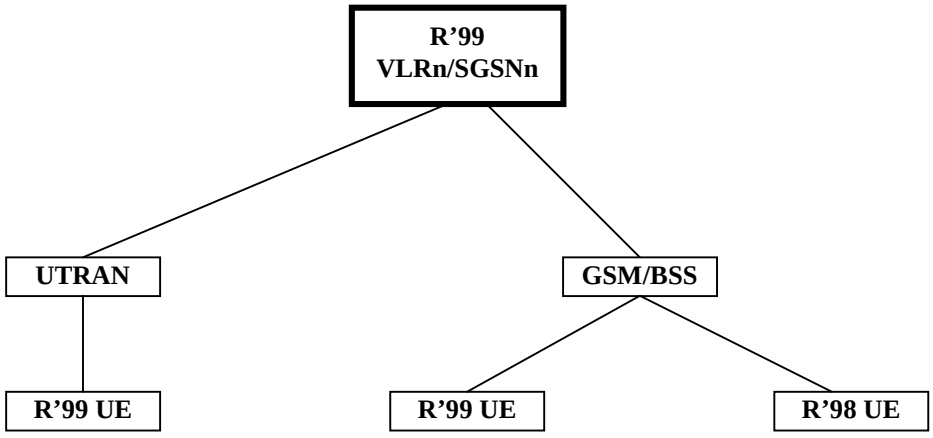
Tdoc S3-000049 on "Enhanced Distribution of Authentication Data within own Service Network Domain" was presented at last S3 meeting and postponed until further clarifications were included.

This contribution tries to present the different scenarios for the reception and use of 'current security context data' at R'99 VLRn/SGSNn. For each scenario, it will be studied whether the keys currently in use at VLRo/SGSNo can be used at VLRn/SGSNn in order to authenticate the subscriber using local authentication.

A text for inclusion in TS 33.102 is proposed based on the outcome of this study. Provided that the situations described here present changes in the security context, this text shall be placed under Chapter 6.8 on 'Interoperation and Handover between UMTS and GSM'.

2. Scenarios for reception/use of 'current security context data'

The following figure presents the different combinations of RAN and UE under R'99 VLRn/SGSNn, and the different combination of 'current security context data' under each access type:



Scenario 1

VLRn/SGSNn received ***Kc+CKSN*** as current security context data and the subscriber roams to the VLRn/SGSNn with a ***R'98 UE under GSM BSS***.

This scenario also requires a GSM security context, so received current security context data can be used.

Scenario 2

VLRn/SGSNn received ***CK+IK+KSI*** as current security context data and the subscriber roams to the VLRn/SGSNn with a ***R'98 UE under GSM BSS***.

This scenario means that we have a subscriber with a USIM that has changed mobile release while roaming (R'99 UE → R'98 UE). Security context also changes (UMTS → GSM) and a set of keys different of the ones currently in used at VLRo/SGSNo is required.

Received current security context data can not be used. This information shall be discarded and a new AKA procedure performed.

Scenario 3

VLRn/SGSNn received ***Kc+CKSN*** as current security context data and the subscriber roams to the VLRn/SGSNn with a ***R'99 UE under GSM BSS***.

This scenario means that we have either a GSM subscriber or a UMTS subscriber that changed mobile release while roaming (R'98 UE → R'99 UE).

For a GSM subscriber, the security context does not change and received current security context data can be used.

For a UMTS subscriber, the security context changes from GSM to UMTS and a set of keys different of the ones currently in used at VLRo/SGSNo is required. This information shall be discarded and a new AKA procedure performed.

Mind that VLRn will not have any indication of whether the subscriber is GSM or UMTS unless unused AVs are also received from VLRo (Triplets → GSM Subscriber, Quintuplets → UMTS subscriber). If this is the case, received current security context data shall be discarded and a new AKA procedure performed.

> **Note:** The last situation described (Kc received with no unused AVs) will not present any problem for a R'99 SGSNn. According to an already approved CR at N2B (Tdoc N2B-000352 CR to 29.060 on 'Distribution of Security Data'), R'99 SGSNo indicates in 'Security Mode' parameter the type of security keys (GSM/UMTS) and the type of AVs (quintuplets vs triplets, if any) passed to the R'99 SGSNn.

Scenario 4

VLRn/SGSNn received ***CK+IK+KSI*** as current security context data and the subscriber roams to the VLRn/SGSNn with a ***R'99 UE under GSM BSS***.

This scenario means that we have a subscriber with a USIM that was under UMTS security context at VLRo/SGSNo.

Security context does not change at VLRn/SGSNn, so received current security context data can be used.

Scenario 5

VLRn/SGSNn received ***Kc+CKSN*** as current security context data and the subscriber roams to the VLRn/SGSNn with a ***R'99 UE under UTRAN***.

This scenario means that we have either a GSM subscriber or a UMTS subscriber that changed mobile release while roaming (R'98 UE → R'99 UE).

For a GSM subscriber, the security context does not change and received current security context data can be used (VLRn/SGSNn and R'99 UE need to derive CK, IK from original Kc).

For a UMTS subscriber, the security context changes from GSM to UMTS and a set of keys different of the ones currently in used at VLRo/SGSNo is required. This information shall be discarded and a new AKA procedure performed.

Mind that VLRn will not have any indication of whether the subscriber is GSM or UMTS unless unused AVs are also received from VLRo (Triplets → GSM Subscriber, Quintuplets → UMTS subscriber). If this is the case, received current security context data shall be discarded and a new AKA procedure performed.

> **Note:** The last situation described (Kc received with no unused AVs) will not present any problem for a R'99 SGSNn. According to an already approved CR at N2B (Tdoc N2B-000352 CR to 29.060 on 'Distribution of Security Data'), R'99 SGSNo indicates in 'Security Mode' parameter the type of security keys (GSM/UMTS) and the type of AVs (quintuplets vs triplets, if any) passed to the R'99 SGSNn.

Scenario 6

VLRn/SGSNn received ***CK+IK+KSI*** as current security context data and the subscriber roams to the VLRn/SGSNn with a ***R'99 UE under UTRAN***.

This scenario means that we have a subscriber with a USIM that was under UMTS security context at VLRo/SGSNo.

Security context does not change at VLRn/SGSNn, so received current security context data can be used.

3. Conclusion

Summing up, received current security context data can not be used when:

a. There is a change of security context from VLRo/SGSNo to VLRn/SGSNn. This change of security context is caused by a change of UE release while roaming (R'99 UE ←→ R'98 UE).

b. Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 UE under GSM BSS or UTRAN.

The following conditions for the use of current security context data at VLRn/SGSNn are then proposed to be stated in TS 33.102 under Chapter 6.8 on 'Interoperation and Handover between UMTS and GSM':

" ……

VLRn/SGSNn shall not use current security context data received from VLRo/SGSNo to authenticate the subscriber using local authentication in the following cases:

i) Security context to be established at VLRn/SGSNn requires a different set of keys than the one currently in use at VLRo/SGSNo. This change of security context is caused by a change of UE release (R'99 UE ←→ R'98 UE) when the user registered at VLRn/SGSNn.

ii) Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 UE (under GSM BSS or UTRAN). In this situation, VLRn have no indication of whether the subscriber is GSM or UMTS and it is not able to decide whether Kc received can be used (in case the subscriber were a GSM subscriber).

In these two cases, received current security context data shall be discarded and a new AKA procedure shall be performed.

……"

4. References

Tdoc S3-99545: CR 34 to 33.102 on "Distribution of authentication data within one serving network domain"

Tdoc S3-000049: CR to 33.102 on "Enhanced Distribution of authentication data within one serving network domain"

Tdoc N2B-000352: CR to 29.060 on "Distribution of security data"

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	**CR**	**034**	Current Version:	3.2.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submision to TSG SA #6 *list TSG meeting no. here ↑* for approval **X** for information *(only one box should be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM [ ] ME [ ] UTRAN [ ] Core Network [X]

Source: TSG SA WG 3 **Date:** 1999-Dec-9

Subject: Distribution of authentication data within one serving network domain

3G Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	[ ]
A	Corresponds to a correction in a 2G specification	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Reason for change: The modification allows that the user is authenticated using local authentication after a location/routing area update in a new MSC/VLR or SGSN. The use of that options lowers the number of quintets that are used by avoiding authentication and key establishment when there is no reason for from a security viewpoint. The secure reduction of the number of authentication and key agreement protocol runs results in a reduced amount of required signalling and Authentication Centre activity.

Clauses affected: 6.3.4

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other 2G core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments: The changes bring TS 33.102 in line with TS 23.060, especially section 6.8.1.2, that describes the information elements sent from one SGSN to another SGSN on an intersystem change for PS services.

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain

The purpose of this procedure is to provide a newly visited MSC/VLR or SGSN with temporary authentication data from a previously visited MSC/VLR or SGSN within the same serving network domain.

The procedure is shown in Figure 10.

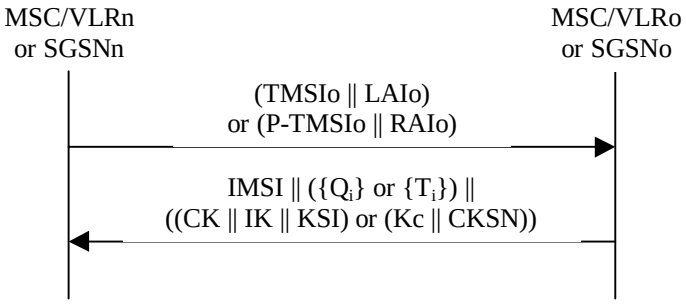


Figure 10: Distribution of IMSI and temporary authentication data within one serving network domain

The procedure shall be invoked by the newly visited MSC/VLRn (resp. SGSNn) after the receipt of a location update request (resp. routing area update request) from the user wherein the user is identified by means of a temporary user identity TMSIo (resp. P-TMSIo) and the location area identity LAIo (resp. routing area identity RAIo) under the jurisdiction of a previously visited MSC/VLRo or SGSNo that belongs to the same serving network domain as the newly visited MSC/VLRn or SGSNn.

The protocol steps are as follows:

a) The MSC/VLRn (resp. SGSNn) sends a *user identity request* to the MSC/VLRo (or SGSNo), this message contains TMSIo and LAIo (resp. P-TMSIo and RAIo).

b) The MSC/VLRo (resp. SGSNo) searches the user data in the database.

   If the user is found, the MSC/VLRo (resp. SGSNo) shall send a *user identity response* back that

   i) shall include the IMSI,

   ii) may include a number of unused authentication vectors (quintets or triplets) and

   iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

   The MSC/VLRo or SGSNo subsequently deletes the authentication vectors which have been sent and the data elements on the current security context.

   If the user cannot be identified the MSC/VLRo or SGSNo shall send a *user identity response* indicating that the user identity cannot be retrieved.

c) If the MSC/VLRn or SGSNn receives a *user identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context that may be included.

   If the MSC/VLRn or SGSNn receives a *user identity response* indicating that the user could not be identified, it shall initiate the user identification procedure described in 6.2.

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 **CR** **046** Current Version: 3.3.1

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submision to TSG SA #7 *list TSG meeting no. here ↑* for approval **X** for information *(only one box should be marked with an X)*

Form: 3G CR cover sheet, version 1.0 *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf*

Proposed change affects: *(at least one should be marked with an X)* USIM [ ] ME [ ] UTRAN [ ] Core Network [X]

Source: Ericsson **Date:** 2000-01-17

Subject: Clarification on enhanced Distribution of authentication data within one serving network domain

3G Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Reason for change: This CR specifies the behaviour of new VLR/SGSN when the keys of the current security context have been received from old VLR/SGSN.

Clauses affected: 6.3.4

Other specs affected:

Other 3G core specifications	X	→ List of CRs:	29.002
Other 2G core specifications		→ List of CRs:	
MS test specifications		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain

The purpose of this procedure is to provide a newly visited MSC/VLR or SGSN with temporary authentication data from a previously visited MSC/VLR or SGSN within the same serving network domain.

The procedure is shown in Figure 11.

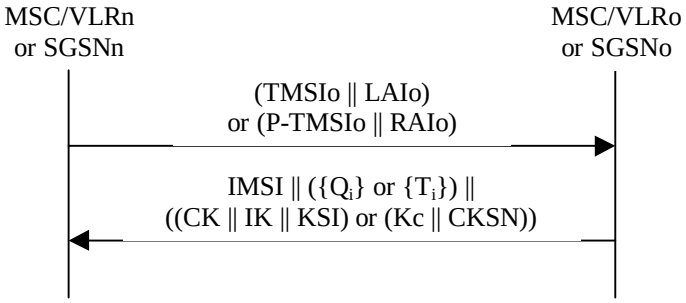


Figure 11: Distribution of IMSI and temporary authentication data within one serving network domain

The procedure shall be invoked by the newly visited MSC/VLRn (resp. SGSNn) after the receipt of a location update request (resp. routing area update request) from the user wherein the user is identified by means of a temporary user identity TMSIo (resp. P-TMSIo) and the location area identity LAIo (resp. routing area identity RAIo) under the jurisdiction of a previously visited MSC/VLRo or SGSNo that belongs to the same serving network domain as the newly visited MSC/VLRn or SGSNn.

The protocol steps are as follows:

a) The MSC/VLRn (resp. SGSNn) sends a *user identity request* to the MSC/VLRo (or SGSNo), this message contains TMSIo and LAIo (resp. P-TMSIo and RAIo).

b) The MSC/VLRo (resp. SGSNo) searches the user data in the database.

   If the user is found, the MSC/VLRo (resp. SGSNo) shall send a *user identity response* back that

   i) shall include the IMSI,

   ii) may include a number of unused authentication vectors (quintets or triplets) and

   iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

   The MSC/VLRo or SGSNo subsequently deletes the authentication vectors which have been sent and the data elements on the current security context.

   If the user cannot be identified the MSC/VLRo or SGSNo shall send a *user identity response* indicating that the user identity cannot be retrieved.

c) If the MSC/VLRn or SGSNn receives a *user identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context that may be included. Note that if a different security context is required at MSC/VLRn (resp. SGSNn), the information regarding current security context data received from MSC/VLRo (resp. SGSNo) can not be used to authenticate the subscriber using local authentication. A new authentication and key agreement procedure shall be performed in this case.

If the MSC/VLRn or SGSNn receives a *user identity response* indicating that the user could not be identified, it shall initiate the user identification procedure described in 6.2.