TSG-T WG3 (USIM) meeting #8
Bonn, 23 - 25 August, 1999

Tdoc T3-99215

TSG-SA WG3 (Security) meeting #4
London, 16-18 June 1999

TSGS-WG3#4(99)190

To: 3GPP TSGs S2, T3

Copy: 3GPP TSG N2

Source: 3GPP TSG S3

Title: Interoperation between UMTS and GSM

SA3 have started to consider solutions for secure interoperation between GSM and UMTS. The following scenarios are being considered:

1. Registration of a UMTS user in a GSM BSS, including authentication and key agreement
2. Intersystem handover of a UMTS user from UTRAN to GSM BSS
3. Intersystem handover of a UMTS user from GSM BSS to UTRAN
4. Registration of a GSM user in a UTRAN, including authentication and key agreement
5. Intersystem handover of a GSM user from GSM BSS to UTRAN
6. Intersystem handover of a GSM user from UTRAN to GSM BSS

We currently assume that UMTS users with dual mode terminals only have an association with one (UMTS) HLR/AuC. This HLR/AuC can send appropriate authentication vectors to both UMTS and GSM networks. Solutions being considered involve the distribution and use of combined GSM/UMTS authentication vectors or the use of conversion functions to derive GSM security parameters from UMTS security parameters and vice versa.

For example using conversion functions, authentication and key agreement involving UMTS users registering on a GSM BSS could be achieved using a GSM challenge, response and cipher key derived from the corresponding parameters in a UMTS authentication vector produced by the user's UMTS HLR/AuC. In this case the user's USIM or UE would have to implement the same conversion functions to derive the appropriate GSM parameters. Similarly, authentication and key agreement involving GSM users registering on a UTRAN could be achieved using a UMTS challenge, response, cipher key and integrity key derived from the corresponding parameters in a GSM authentication vector produced by the user's GSM HLR/AuC. In this case the user's dual mode mobile would have to implement the same conversion functions to derive the appropriate UMTS parameters (the functions are implemented on the dual mode mobile to avoid modifications to GSM SIMs).

S2 are asked to comment on the feasibility of reauthentication at intersystem handover. We currently assume that it is *not* feasible to perform a reauthentication at intersystem handover. Instead, it is assumed that the appropriate keys must be available in the access network at handover so that GSM ciphering, or UMTS ciphering and integrity protection can be enabled. Various options are being considered for passing these keys between and within GSM BSS and UTRAN, some of which involve the use of conversion functions. However, many of the details cannot be worked out until UMTS inter-system handover procedures have been defined. These procedures should of course be developed taking security issues into consideration.

Preliminary evaluation of the current proposals has focused on security issues. This has involved considering the level of security provided for various schemes in different interoperation scenarios. The efficiency of the schemes and their impact on the system architecture has also been studied. An important goal has been to take maximum advantage of the compatibility between the GSM and UMTS authentication and key agreement schemes to minimise the amount of extra functionality required to support interoperation. It should be noted that the conversion functions under study are unkeyed and are computationally quite simple.

To complete this work, extensive liaison with S2 and T3 is envisaged. It is hoped that this work item can be progressed at the proposed joint meeting between S2, S3 and T3 on 24th August in Bonn. In the meantime comments on the attached temporary documents s3-99158 and s3-99166 would be appreciated.

Attachments: s3-99158 and s3-99166

TSG-SA WG3 (Security) meeting #4
London, 16-18 June 1999

TSGS-WG3#4(99)158

Agenda Item:

Source: Siemens Atea[1]

Title: Interoperation between UMTS and GSM

Document for: Decision

---

1. Different scenarios and requirements

In this document we study interoperation between UMTS users and networks and GSM users and networks. This comprises the following:

1) **Registration** of a user of one type in a network of the other type, typically including authentication and key agreement. This includes:

   a) **Registration of a UMTS user in a GSM serving network.** [Highest priority] In countries with existing GSM networks, UMTS networks are expected to be introduced in islands; for nation-wide coverage for GSM-like services the UMTS user will have to rely on the existing GSM network coverage. ***This is called USIM roaming.***

   b) **Registration of a GSM user in a UMTS serving network.** [Low priority] Whether there is an important need for GSM users to access the UMTS network is under dispute. This scenario might be interesting for GSM operators who want to offer their customers roaming opportunities in those countries that are covered by a UMTS network but not with a GSM network. ***This is called GSIM roaming.***

2) **Inter-system handover** of a user from a network of one type to a network of the other type. This includes:

   a) **Inter-system handover from a UTRAN to a GSM BSS**

      i) **Of a UMTS user.** [High priority] Inter-system handover will provide service continuation when the UMTS user leaves an area with UMTS coverage. ***This is part of USIM inter-system handover.***

      ii) **Of a GSM user.** [Lowest priority] Inter-system handover will provide service continuation when the GSM user leaves an area of UMTS coverage. ***This is part of GSIM inter-system handover.***

   b) **Inter-system handover from a GSM BSS to a UTRAN**

      i) **Of a UMTS user.** [Medium priority] This type of handover would allow a UMTS user who initiated a service through a GSM BSS in an area without UMTS coverage, to be handed over to a UTRAN. As soon as he is handed over, he may also initiate extra (UMTS) service capabilities. This type of handover also allows users who initiated service through a UTRAN and then were subsequently handed over to a GSM BSS, to be handed back into the UTRAN as soon as possible. ***This is part of USIM inter-system handover.***

      ii) **Of a GSM user.** [Lowest priority] Inter-system handover will provide service continuation when the GSM user leaves an area of GSM coverage. ***This is part of GSIM inter-system handover.***

A solution is required for inter-system handover between a GSM BSS and a UTRAN controlled by the same UMTS MSC/VLR, and also for inter-system handover to and from a GSM MSC/VLR controlled GSM BSS.

*In the following * denotes a derived key or authentication response, i.e. a GSM key or authentication response which has been derived from a UMTS key or authentication response, or a UMTS key which has been derived from a GSM key.*

2. Mechanism 1

Ericsson [S3-99113] outlined a mechanism for USIM roaming and inter-system handover.

The mechanism can be summarised as follows:

[1] This work acknowledges the ACTS USECA project.

1) **Generation of an authentication vector.** The UMTS HLR/AuC generates a RAND and derives from that the UMTS authentication parameters XRES, AUTN, CK and IK and in addition, it derives (from the same RAND) a GSM cipher key Kc (and optionally a GSM expected response XSRES[2]). In this way an extended UMTS/GSM authentication vector is generated.

2) **Distribution of an authentication vector.** The UMTS/GSM authentication vector is distributed to UMTS or GSM VLRs that support inter-system handover for UMTS users.

3) **UMTS user authentication in UTRAN.** When a user is registered through a UTRAN, the controlling VLR initiates UMTS authentication, i.e., the authentication request contains RAND and AUTN. Upon receipt, the USIM computes the UMTS response RES, the UMTS access link keys CK and IK and the GSM cipher key Kc. It sends back RES. After successful authentication, the network and user select the UMTS access link keys CK and IK.

4) **UMTS user authentication in GSM BSS.** When a user is registered through a GSM BSS, the controlling VLR initiates GSM authentication, i.e., the authentication request contains only RAND. Upon receipt, the USIM computes the UMTS response XRES (or optionally a GSM response SRES), the UMTS access link keys CK and IK, the GSM cipher key Kc. After successful authentication network and user select the GSM cipher key Kc*.

5) **Inter-system handover of UMTS user from GSM BSS to UTRAN.** At the network side the old GSM BSC sends CK, IK and Kc to the UMTS VLR which controls the new RNC. The VLR then passes CK, IK and Kc to the new RNC which selects CK and IK. At the user end, the dual-mode user equipment selects CK and IK.

6) **Inter-system handover of UMTS user from UTRAN to GSM BSS.** At the network side the old UMTS RNC sends CK, IK and Kc to the new GSM or UMTS VLR which controls the new GSM BSC. The VLR then passes CK, IK and Kc to the new BSC which selects Kc. At the user end, the dual-mode user equipment selects Kc.

This scheme cannot be used to authenticate a GSM user in a UMTS network since the GSIM has no way of computing CK, IK.

3. Alternative mechanisms

A major disadvantage of the above scheme is that it does not support GSIM roaming without additional functionality. We now present an alternative scheme which does support GSIM roaming.

First we consider USIM roaming:

1) **Generation of an authentication vector.** The UMTS HLR/AuC generates a RAND and derives from that the UMTS authentication parameters XRES, AUTN, CK and IK. No GSM cipher key Kc* is generated.

2) **Distribution of an authentication vector.** The distribution depends on the type of VLR that requests authentication vectors:

   a) UMTS VLR (controlling UTRAN or both UTRAN and GSM BSS) receive UMTS authentication vectors.

   b) GSM VLR (controlling only GSM BSS) receive GSM authentication vectors (RAND*, SRES*, Kc*). The HLR/AuC constructs them from the UMTS authentication vectors in the following way: RAND* = RAND, SRES* = c1(XRES) and Kc* = c2(CK).

3) **UMTS user authentication in UTRAN.** When a UMTS user is registered through a UTRAN, the controlling VLR initiates UMTS authentication and key agreement. No GSM cipher key Kc* is derived.

4) **UMTS user authentication in GSM BSS.** When a UMTS user is registered through a GSM BSS, the controlling VLR initiates GSM authentication and key agreement. This is done using a UMTS authentication vector or a GSM authentication vector, depending on the type of VLR controlling the GSM BSS:

   a) A user registered to a GSM BSS controlled by a UMTS VLR (controlling GSM BSS or both UTRAN and GSM BSS). The UMTS VLR converts the UMTS authentication vector into a GSM authentication vector in the same way as the HLR/AuC did before it distributed authentication data to a GSM VLR, see 2) b). The UMTS VLR sends RAND* to the user. The USIM derives RES and CK and converts these parameters to their GSM counterparts in the same way as the VLR did: RES* = c1(RES) and Kc* = c2(CK).

   b) A user registered to a GSM BSS controlled by a GSM VLR (controlling only GSM BSS). The GSM VLR sends the UMTS user RAND*. The USIM derives RES* and Kc* is the same way as in a GSM BSS controlled by a UMTS VLR (see 4)a)).

5) **Inter-system handover of UMTS user from GSM BSS to UTRAN.** At the network side the old GSM BSC sends Kc* to the new RNC which derives CK* and IK* from Kc*: CK* = c3(Kc*) and IK* = c4(Kc*). At the user end, the dual-mode user equipment derives CK* and IK* in the same way.

[2] It is for further study whether XSRES should be different from XRES.

6) **Inter-system handover of UMTS user from UTRAN to GSM BSS.** At the network side the old UMTS RNC derives CK: Kc*=c2(CK) which it passes to the new GSM BSC. At the user end, the dual-mode user equipment derives Kc* in the same way.

A potential problem with the above approach is that if a user hands back into a UTRAN from a GBSS after having been authenticated in the UTRAN, it will use derived UMTS access link keys rather than the original UMTS access link keys of full strength and effective key length. To avoid this problem an alternative way of handling the access keys at handover is proposed below:

5') **Inter-system handover of UMTS user from GSM BSS to UTRAN.** At the network side the old GSM BSC derives CK* and IK* from Kc*: CK* = c3(Kc*) and IK* = c4(Kc*) and passes CK*, IK* and Kc* to the new RNC. At the user end, the dual-mode user equipment derives CK* and IK* in the same way.

6') **Inter-system handover of UMTS user from UTRAN to GSM BSS.** At the network side the old UMTS RNC derives Kc* from CK: Kc* = c2(CK) and passes CK, IK and Kc* to the new BSC. At the user end, the dual-mode user equipment derives Kc* in the same way.

All functionality is now in place for GSIM roaming:

1) **Generation of an authentication vector.** The GSM HLR/AuC generates a GSM authentication vector that consists of (RAND*, SRES*, Kc*).

2) **Distribution of an authentication vector.** The GSM HLR/AuC distributes GSM authentication vectors to all VLRs, regardless of type.

3) **GSM user authentication in UTRAN.** When a GSM user is registered through a UTRAN, the controlling VLR initiates GSM authentication and key agreement. It sends RAND* to the user. The user derives RES* and Kc*. The dual-mode user equipment sends RES* back to the network. The VLR compares RES* with SRES*. After successful authentication and agreement of a GSM cipher key Kc*, the VLR as well as the user equipment derive UMTS access link keys as already explained under inter-system handover of UMTS users from GSM BSS to UTRAN: CK = c3(Kc*) and IK = c4(Kc*).

4) **GSM user authentication in GSM BSS.** When a UMTS user is registered through a GSM BSS, the controlling VLR initiates GSM authentication and key agreement.

5) **Inter-system handover of GSM user from GSM BSS to UTRAN.** The procedure is identical to the one explained under inter-system handover of a UMTS user from GSM BSS to UTRAN At the network side the old GSM BSC sends Kc* to the new RNC which derives CK* and IK* from Kc*: CK* = c3(Kc*) and IK* = c4(Kc*). At the user end, the dual-mode user equipment derives CK* and IK* in the same way.

6) **Inter-system handover of GSM user from UTRAN to GSM BSS.** The procedure is identical to the one explained under inter-system handover of a GSM user from UTRAN to GSM BSS. At the network side the old UMTS RNC derives CK: Kc*=c2(CK) which it passes to the new GSM BSC. At the user end, the dual-mode user equipment derives Kc* in the same way.

The alternative way of handling the access keys at handover has the following affect on inter-system handover for GSM users.

5') **Inter-system handover of GSM user from GSM BSS to UTRAN.** The procedure is identical to the one for the USIM roaming case. At the network side the old GSM BSC derives CK* and IK* from Kc*: CK* = c3(Kc*) and IK* = c4(Kc*) and passes CK*, IK* and Kc* to the new RNC. At the user end, the dual-mode user equipment derives CK* and IK* in the same way.

6') **Inter-system handover of GSM user from UTRAN to GSM BSS.** The procedure is identical to the one explained under inter-system handover of a GSM user from UTRAN to GSM BSS. At the network side the old UMTS RNC derives Kc* from CK: Kc* = c2(CK) and passes CK, IK and Kc* to the new BSC. At the user end, the dual-mode user equipment derives Kc* in the same way.

4. Evaluation

In this section we evaluate the three mechanisms proposed above:

– Mechanism 1 – Ericsson mechanism

– Mechanism 2 – Alternative mechanism – first variant

– Mechanism 3 – Alternative mechanism – second variant

4.1 Security

UMTS authentication and key agreement offer the following additional features compared with GSM authentication and key agreement:

- key freshness assurance of the access link keys
- longer effective key lengths of the access link keys

The following tables describes which features are provided for different interoperation scenarios.

	UMTS user		GSM users	
	strong keys	freshness	strong keys	freshness
Registered in UTRAN	y	y	n	n
Handover from UTRAN to GSM BSS after initial registration in UTRAN (1st, 3rd, 5th, … inter-system handover)	n	y	n	n
Handover from GSM BSS to UTRAN after initial registration in UTRAN (2nd, 4th, 6th , … inter-system handover)	y n y	y	n	n
Registered in GSM BSS	n	n	n	n
Handover from GSM BSS to UTRAN after initial registration in GSM BSS (1st, 3rd, 5th, … inter-system handover)	y n n	n	n	n
Handover from UTRAN to GSM BSS after initial registration in GSM BSS (2nd, 4th, 6th , … inter-system handover)	n	n	n	n

None of the new UMTS security features are offered to GSM subscribers.

None of the new UMTS security features are offered to UMTS users that register in a GSM BSS.

Key freshness is offered to UMTS users that start there service in a UTRAN, not to users starting their service in the GSM BSS.

All mechanisms also provide strong keys to UMTS users that start there service in the UTRAN as long as they are not handed from the UTRAN to the GSM BSS (where they have weaker keys).

The mechanisms are different in the key strength that is provided to them when they are handed over from a GSM BSS to a UTRAN. Mechanism 1 always provides full UMTS strength keys. Mechanism 3 provide full UMTS strength keys when the user has initially started his service in the UTRAN, otherwise it provides access link keys derived from and with the effective key length of the GSM cipher key. Mechanism 3 always provide access link keys with the effective key length of the GSM cipher key after a handover from a GSM BSS.

The level of security provided by mechanism 2 and 3 is acceptable, as the user has accepted the key strength of the GSM cipher key when he registered and started service in the GSM BSS or when he was handed over from to the GSM BSS. UMTS users that do not want to communicate with the GSM cipher key strength should not allow registration in or handover to GSM BSS.

4.2 Impact on system architecture

Mechanism 1 requires support for the storage of UMTS/GSM authentication vectors in all VLR controlling GSM BSS and UTRAN and the distribution of UMTS/GSM authentication vectors from UMTS HLR/AuC to all VLR (resulting in a higher signalling load between HLR and VLR and between VLRs). It requires the GSM BSC and the UMTS RNC to store UMTS ad GSM access link keys. It requires the UMTS AuC and the USIM to implement GSM A3/A8, possibly the algorithms the operators are already using.

Mechanism 2 requires the implementation of conversion functions c1—c4 in the UMTS VLR, UMTS HLR/AuC and mobile equipment. It does not require modifications to GSM network equipment

Mechanism 3 requires the conversion function c1—c4 of mechanism 2 in the UMTS VLR, UMTS HLR/AuC and mobile equipment. In addition it requires storage of UMTS access link keys in the GSM BSC and of GSM cipher keys in the UMTS RNC.

Both mechanism 1 and 3 need to pass both GSM and UMTS access link keys between GSM BSCs and UMTS RNCs, whereas mechanism 2 only passes GSM cipher keys (between UMTS RNCs and GSM BSCs or between two GSM BSCs) or UMTS access link keys (between two UMTS RNCs) around.

4.3 Computational efficiency

Mechanism 1 computes the GSM cipher key more efficiently than mechanisms 2 and 3 do. However, mechanism 1 computes and distributes this cipher key regardless of whether the UMTS user is likely to roam into a GSM network or not. Therefore, the scheme is most efficient when the probability of roaming and handover to GSM is high.

Mechanism 2 derives new access link keys each time an inter-system handover occurs. Mechanism 3 derives new access link keys only at the first inter-system handover during a connection. Further inter-system handovers, no additional derivations are required.

Mechanism 2 and 3 only derive GSM access link keys when they are needed. Therefore, these schemes are computationally efficient when the probability of handover into GSM is low.

5. Conclusion

Mechanisms 2 and 3 offer an acceptable level of security to UMTS users when roaming in GSM networks or when handed over between UTRAN and GSM BSS. Nevertheless, mechanism 1 provides a slightly better level op security, after hand-over from the GSM BSS.

Mechanism 2 provides GSIM and USIM roaming and handover without additional functionality being required, whereas a straightforward extension to mechanism 1 would require GSM systems to be upgraded with UMTS security functionality (this applies to HLR/AuC, VLR, UE and SIM). As the coverage area of the UMTS networks is likely to increase over time, and the need for inter-system roaming and handover is likely to decrease, the network load for mechanisms 2 and 3 should decrease too, while for mechanism 1 it remains unchanged. All of this points to mechanisms 2 and 3 being preferred over mechanism 1.

Mechanism 2 and 3 re-use the functions implemented in the USIM and in the HLR/AuC as much as possible and hence exploits the compatibility of the UMTS and the GSM authentication mechanism. They have the further distinct advantage that no modifications to existing GSM VLRs are required.

The differences between mechanism 2 and 3 are:

- mechanism 3 requires the UMTS RNC to store GSM cipher keys after handover from GSM BSS, and requires the GSM BSC to store UTRAN access link keys after handover from UTRAN, whereas with mechanism 2 each system only stores its own access link keys;
- mechanism 2 derives new access link keys at each handover, whereas mechanism 3 derives new access link keys only at the first inter-system handover.

Mechanisms 2 and 3 offer an acceptable level of security to UMTS users when roaming in GSM networks or when handed over between UTRAN and GSM BSS.

SOURCE ERICSSON

TITLE: DESIGN FOR SECURE AND SIMPLE INTEROPERATION BETWEEN UMTS AND GSM

DOCUMENT FOR: DISCUSSION

AGENDA ITEM: ……

1 SCOPE

This contribution describes a secure, simple and efficient solution for GSM/UMTS interoperability and handover.

The technical problem is not to handle a GSM SIM in a UMTS environment but to handle UMTS subscribers in a mixed UMTS GSM world.

2 SYSTEM ASSUMPTIONS

A terminal classmark will exist which makes it possible for the network to determine if the terminal contains a GSM SIM or a USIM. This to enable the network to adapt to the UE/(U)SIM capabilities.

3 SECURITY PRINCIPLES

A terminal with a USIM as identification module using a UTRAN access network should only accept the full use of authentic UMTS security parameters and mechanisms. **This means that it should not be possible for the network to downgrade security for USIM users.** If it were, then a false base station attack would be possible.

In UTRAN, UMTS security mechanisms are applied, i.e. both the confidentiality mechanism and the integrity mechanism are operational. This is independent of the use of a SIM or a USIM.

In GSM access networks, GSM security mechanisms are applied independent of USIM or SIM use.

3.1 Implications

Networks capable of handover between GSM and UMTS have to update their AuC/HLR's and MSC/VLR's to handle UMTS security.

4 OPTIMISATION PRINCIPLES

The GSM parameters of a UMTS subscriber are derived from the UMTS parameters. GSM RES equals the first 32 bits of UMTS RES. GSM Kc is calculated from UMTS CK and IK.

With IK = (i1, i2) and CK = (c1, c2) a simple and secure way to define Kc would be to let Kc = i1 $\oplus$ i2 $\oplus$ c1 $\oplus$ c2 ($\oplus$ = xor)).

4.1 Terminal side

4.1.1 SIM as identity module in UMTS environment

The terminal operates the SIM exactly as in GSM. At authentication RES and Kc are calculated and RES is sent back to the network where it is compared to the first 32 bits of XRES.

Then the terminal derives CK and IK from Kc by applying standardised algorithms.

4.1.2 USIM as identity module in GSM environment

The terminal operates the USIM as usual. It inputs RAND and receives RES, CK and IK as the result. Auth is not checked. RES is returned to the network and Kc is derived from CK and IK.

4.2 Network side

On the network side the MSC/VLRS handle UMTS quintuplets for UMTS subscribers and GSM triplets for GSM subscribers.

4.2.1 GSM authentication of UMTS user

When parameters for a GSM authentication is requested the MSC/VLR does the necessary computations to derive SRES and Kc and then transfers the data.

4.2.2 UMTS authentication of GSM user

The MSC/VLR performs the same calculations as the terminal to calculate XRES, CK and IK. A bogus Auth may also be produced. The parameters are then transferred to the RNC.

4.3 Implications

The design principles above imply that an AuC only has to generate UMTS quintuplets for a UMTS subscriber as his GSM triplets can be derived from the UMTS parameters. Consequently the MSC/HLR's and MSC/VLR's only have to handle UMTS quintuplets which make them simpler and saves storage and transmission capacity

Pure GSM networks may request triplets from UMTS HLR's and a UMTS VLR can calculate simulated UMTS quintuples from GSM triplets.

5 CONCLUSIONS

The design above fulfils all security requirements and is based on straightforward security principles which makes it efficient and simple to implement.