GSM Switching, Services and Protocols: Second Edition. Jörg Eberspächer,
Hans-Jörg Vögel and Christian Bettstetter

Print ISBN 0-471-49903-X Online ISBN 0-470-84174-5

GSM

Switching, Services and Protocols
Second Edition

GSM

Switching, Services and Protocols
Second Edition

Jörg Eberspächer
Technische Universität München, Germany

Hans-Jörg Vögel
The Fantastic Corporation, Switzerland

and

Christian Bettstetter
Technische Universität München, Germany

JOHN WILEY & SONS, LTD
Chichester · New York · Weinheim · Brisbane · Singapore · Toronto

6.3.1 Protection of Subscriber Identity

The intent of this function is to prevent disclosing which subscriber is using which resources in the network, by listening to the signaling traffic on the radio channel. On one hand this should ensure the confidentiality of user data and signaling traffic, on the other hand it should also prevent localizing and tracking of a mobile station. This means above all that the *International Mobile Subscriber Identity* (IMSI) should not be transmitted as clear text, i.e. unencrypted.

Instead of the IMSI, one uses a *Temporary Mobile Subscriber Identity* (TMSI) on the radio channel for identification of subscribers. The TMSI is temporary and has only local validity, which means that a subscriber can only be uniquely identified by TMSI and the *Location Area ID* (LAI). The association between IMSI and TMSI is stored in the VLR.

The TMSI is issued by the VLR, at the latest, when the mobile station changes from one *Location Area* (LA) into another (location updating). When a new location area is entered, this is noticed by the mobile station (Section 3.2.5) which reports to the new VLR with the old LAI and TMSI (LAI*old* and TMSI*old*, Figure 6.19). The VLR then issues a new TMSI for the MS. This TMSI is transmitted in encrypted form.

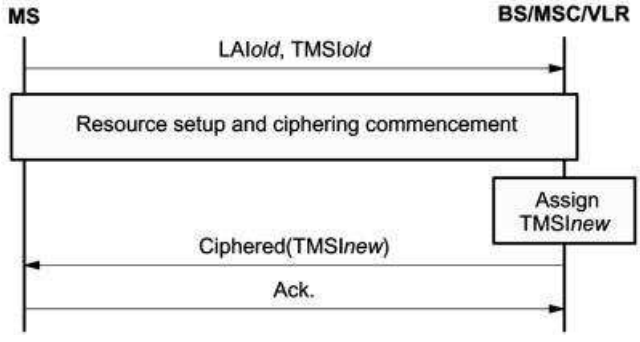

Figure 6.19: Encrypted transmission of the temporary subscriber identity

The subscriber identity is thus protected against eavesdropping in two ways: first, the temporary TMSI is used on the radio channel instead of the IMSI; second, each new TMSI is transmitted in encrypted form.

In the case of database failures, if the VLR database is partially lost or no correct subscriber data is available (loss of TMSI, TMSI unknown at VLR, etc.), the GSM standard provides for a positive acknowledgement of the subscriber identity. For this subscriber identification, the IMSI must be transmitted as clear text (Figure 6.20) before encryption is turned on. Once the IMSI is known, encryption can be restarted and a new TMSI can be assigned.

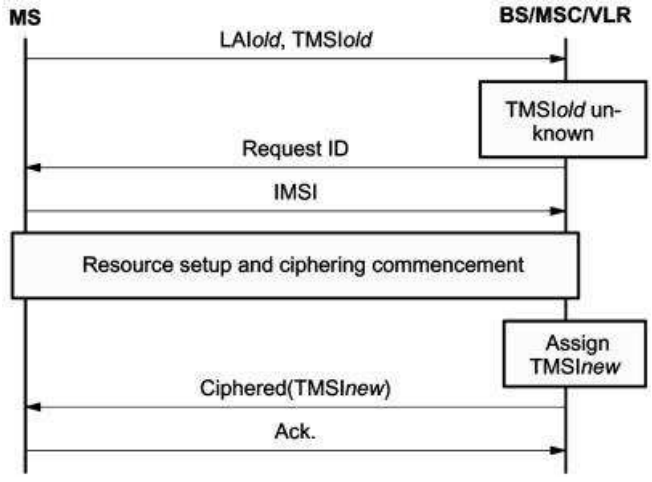

Figure 6.20: Clear text transmission of the IMSI when the TMSI is unknown

6.3.2 Verification of Subscriber Identity

When a subscriber is added to a home network for the first time, a *Subscriber Authentication Key* (Ki) is assigned in addition to the IMSI to enable the verification of the subscriber identity (also known as authentication). All security functions are based on the secrecy of this key. At the network side, the key Ki is stored in the *Authentication Center* (AUC) of the home PLMN. At the subscriber side, it is stored on the SIM card of the subscriber.

The process of authenticating a subscriber is essentially based on the A3 algorithm, which is performed at the network side as well as at the subscriber side (Figure 6.21). This algorithm calculates independently on both sides (MS and network) the *Signature Response* (SRES) from the authentication key Ki and a *Random Number* (RAND) offered by the network. The MS transmits its SRES value to the network which compares it with its calculated value. If both values agree, the authentication was successful. Each execution of the algorithm A3 is performed with a new value of the random number RAND which

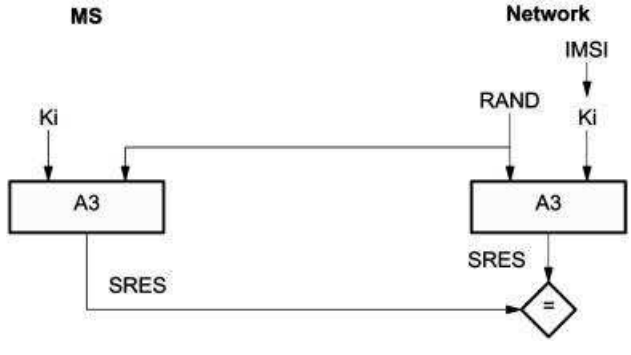

Figure 6.21: Principle of subscriber authentication

cannot be predetermined; in this way recording the channel transmission and playing it back cannot be used to fake an identity.

6.3.3 Generating Security Data

At the network side, the 2-tuple (RAND, SRES) need not be calculated each time when authentication has to be done. Rather the AUC can calculate a set of (RAND, SRES) 2-tuples in advance, store them in the HLR, and send them on demand to the requesting VLR. The VLR stores this set (RAND[n], SRES[n]) and uses a new 2-tuple from this set for each authentication procedure. Each 2-tuple is used only once; so new 2-tuples continue to be requested from the HLR/AUC.

This procedure, to let security data (Kc, RAND, SRES) be calculated in advance by the AUC has the advantage that the secret authentication key Ki of a subscriber can be kept exclusively within the AUC, which ensures a higher level of confidentiality. A somewhat less secure variant is to supply the currently needed key Ki to the local VLR which then generates the security data locally.

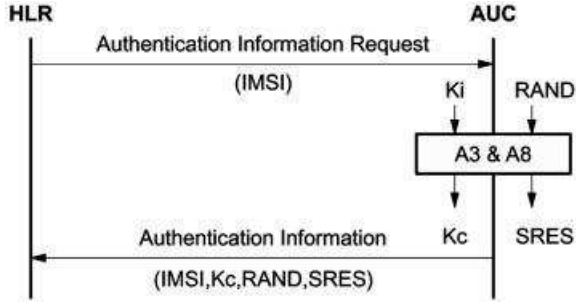

Figure 6.22: Generation of a set of security data for the HLR

If the key Ki is kept exclusively in the AUC, the AUC has to generate a set of security data for a specific IMSI on demand from the HLR (Figure 6.22): the random number RAND is generated and the pertinent signature SRES is calculated with the A3 algorithm, whereas the A8 algorithm generates the encryption key Kc.

The set of security data, a 3-tuple consisting of Kc, RAND, and SRES, is sent to the HLR and stored there. In most cases, the HLR keeps a supply of security data (e.g. 5), which can then be transmitted to the local VLR, so that one does not have to wait for the AUC to generate and transmit a new key. When there is a change of LA into one belonging to a new VLR, the sets of security data can be passed on to the new VLR. This ensures that the subscriber identity IMSI is transmitted only once through the air, namely when no TMSI has yet been assigned (see registration) or when this data has been lost. Afterwards the (encrypted) TMSI can be used for communicating with the MS.

If the IMSI is stored on the network side only in the AUC, all authentication procedures can be performed with the 2-tuples (RAND, SRES) which were precalculated by the AUC. Besides relieving the load on the VLR (no execution of the A3 algorithm), this kind of

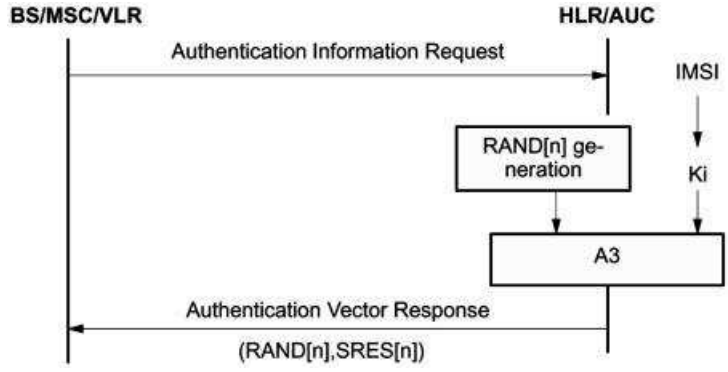

Figure 6.23: Highly secure authentication (no transmission of Ki)

subscriber identification (Figure 6.23) has the other advantage of being particularly secure, because confidential data, especially Ki, need not be transmitted over the air. It should be used especially when the subscriber is roaming in a network of a foreign operator, since it avoids passing of security-critical data over the network boundary.

The less secure variant (Figure 6.24) should only be used within a PLMN. In this case, the secret (security-critical) key Ki is transmitted each time from the HLR/AUC to the current VLR, which executes the algorithm A3 for each authentication.

Figure 6.24: Weakly secure authentication (transmission of Ki to VLR)

6.3.4 Encryption of Signaling and Payload Data

The encryption of transmitted data is a special characteristic of GSM networks that distinguishes the offered service from analog cellular and fixed ISDN networks. This encryption is performed at the transmitting side after channel coding and interleaving and immediately preceding modulation (Figure 6.25). On the receiving side, decryption directly follows the demodulation of the data stream.

A *Cipher Key* (Kc) for the encryption of user data is generated at each side using the generator algorithm A8 and the random number RAND of the authentication process

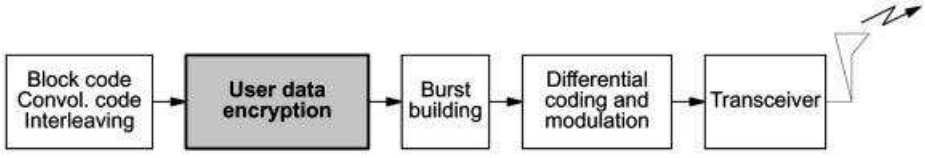

Figure 6.25: Encryption of payload data in the GSM transport chain

(Figure 6.26). This key Kc is then used in the encryption algorithm A5 for the symmetric encryption of user data. At the network side, the values of Kc are calculated in the AUC/HLR simultaneously with the values for SRES. The keys Kc are combined with the 2-tuples (RAND, SRES) to produce 3-tuples, which are stored at the HLR/AUC and supplied on demand, in case the subscriber identification key Ki is only known to the HLR (Section 6.3.2). In the case of the VLR having access to the key Ki, the VLR can calculate Kc directly.

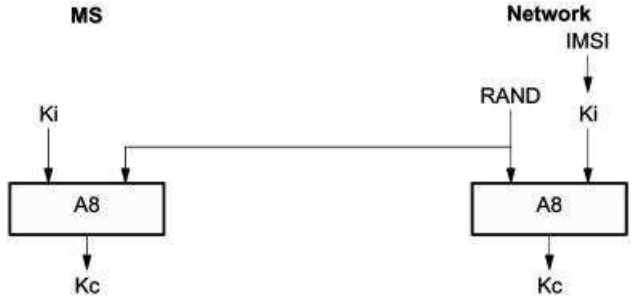

Figure 6.26: Generation of the cipher key Kc

The encryption of signaling and user data is performed at the mobile station as well as at the base station (Figure 6.27). This is a case of symmetric encryption, i.e. ciphering and deciphering are performed with the same key Kc and the A5 algorithm.

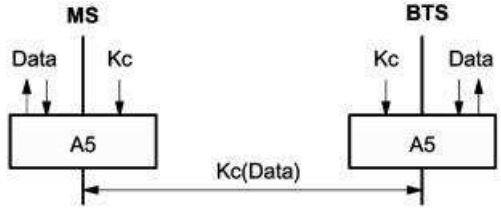

Figure 6.27: Principle of symmetric encryption of user data

Based on the secret key Ki stored in the network, the cipher key Kc for a connection or signaling transaction can be generated at both sides, and the BTS and MS can decipher each other's data. Signaling and user data are encrypted together (TCH/SACCH/FACCH);

for dedicated signaling channels (SDCCH) the same method is used as for traffic channels. This process is also called a *stream cipher*, i.e. ciphering uses a bit stream which is added bitwise to the data to be enciphered (Figure 6.28).

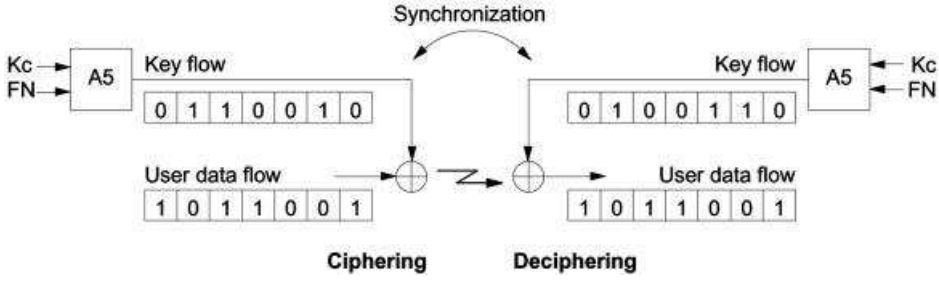

Figure 6.28: Combining payload data stream and ciphering stream

Deciphering consists of performing an additional EXCLUSIVE OR operation of the enciphered data stream with the ciphering stream. The *Frame Number* (FN) of the current TDMA frame within a hyperframe (see Section 5.3.1) is another input for the A5 algorithm besides the key Kc, which is generated anew for each connection or transaction. The current frame number is broadcast on the *Synchronization Channel* (SCH) and is thus available any time to all mobile stations currently in the cell. Synchronization between ciphering and deciphering processes is thus performed through FN.

However, the problem of synchronizing the activation of the ciphering mode has to be solved first: the deciphering mechanism on one side has to be started at precisely the correct moment. This process is started under network control, immediately after the authentication procedure is complete or when the key Kc has been supplied to the base station (BS); see Figure 6.29.

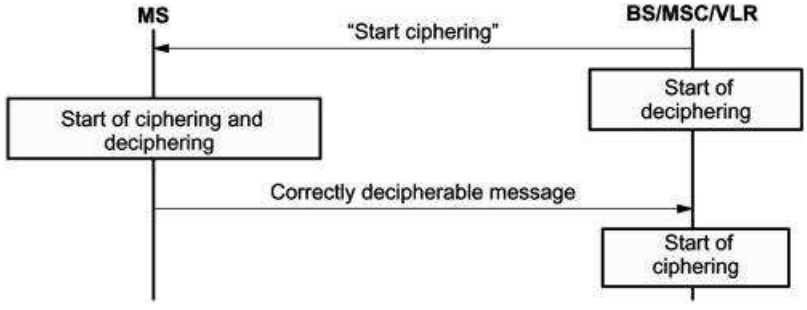

Figure 6.29: Synchronized start of the ciphering process

The network, i.e. the BTS, transmits to the mobile station the request to start its (de)ciphering process, and it starts its own deciphering process. The mobile station then starts its ciphering and deciphering. The first ciphered message from the MS which reaches the network and is correctly deciphered leads to the start of the ciphering process on the network side.