226

CEPT CCH/GSM

The Hague, 23-25 March 1983

GSM doc. 29/83

(s. Doc 5/NL)

To the chairmen of CD, CS and SF.

THE NEED FOR ENCRYPTION IN MOBILE SYSTEMS.

1. The GSM group has for the time being identified the possible requirement for encryption in the following cases:

   - protection of the call handling information (e.g. subscriber identity);
   - protection of the communication on the radio path (both voice and non-voice);
   - protection of operation and maintenance information exchanged between mobile networks (e.g. charging information).

   WG SF is invited to consider other possible requirements.

2. Operational requirements

2.1 Protection of the call handling information.

It should not be possible for any unauthorized person, including another land mobile subscriber, to illegaly set up a call. One possible method could be the use of a keyword together with a public encryption mechanism as illustrated in Annex 1.

When devising such a scheme the following should be taken into account:

- it should not be necessary to change the information related to the protection mechanism during the life time of the mobile station (e.g. 10-15 years). Must is that the key which is carried by the mobile is secure
- It should not be possible to derive the protection information from the knowledge of the mobile station identity* and/or the directory number of the mobile subscriber.

2.2 Protection of the communication on the radio path

The following should be taken into consideration:

- It should be possible to limit the protection to the radio path (e.g. in the case of certain speech processing techniques on the radio path it will not be possible to use end-to-end encryption).
- If a "master-key" is allocated to each mobile station, this key should not be made known to any other network than the home network of the mobile station.

* The mobile station identity is used on the radio path for identifying the calling or called mobile station.

- the method chosen should be as similar as possible to the methods to be used in the fixed networks.

2.3 Protection of operation and maintenance information

The methods to be chosen should be in accordance with the methods to be used for exchange of similar information in the fixed networks.

Annex 1 The following procedure could serve as an example (see fig. 1).

The mobile station starts a call by sending its radio identity (i) to the mobile exchange.

The mobile exchange selects the key K_i, corresponding with i.

Subsequently the mobile exchange generates a random number N which is encryped with K_i. The resulting signal f (N, K_i) is sent to the mobile station. After decryption by the mobile station with the same key K_i, the number N results. Then N is processed e.g. an inversion. The resulting $\overline{N}$ is encrypted again with K_i.

The signal f ($\overline{N}$, K_i) is sent back to the mobile exchange.

Unambiquous identification follows in this case from checking the result of the modulo-2 sum ($\overline{N} \oplus N$).

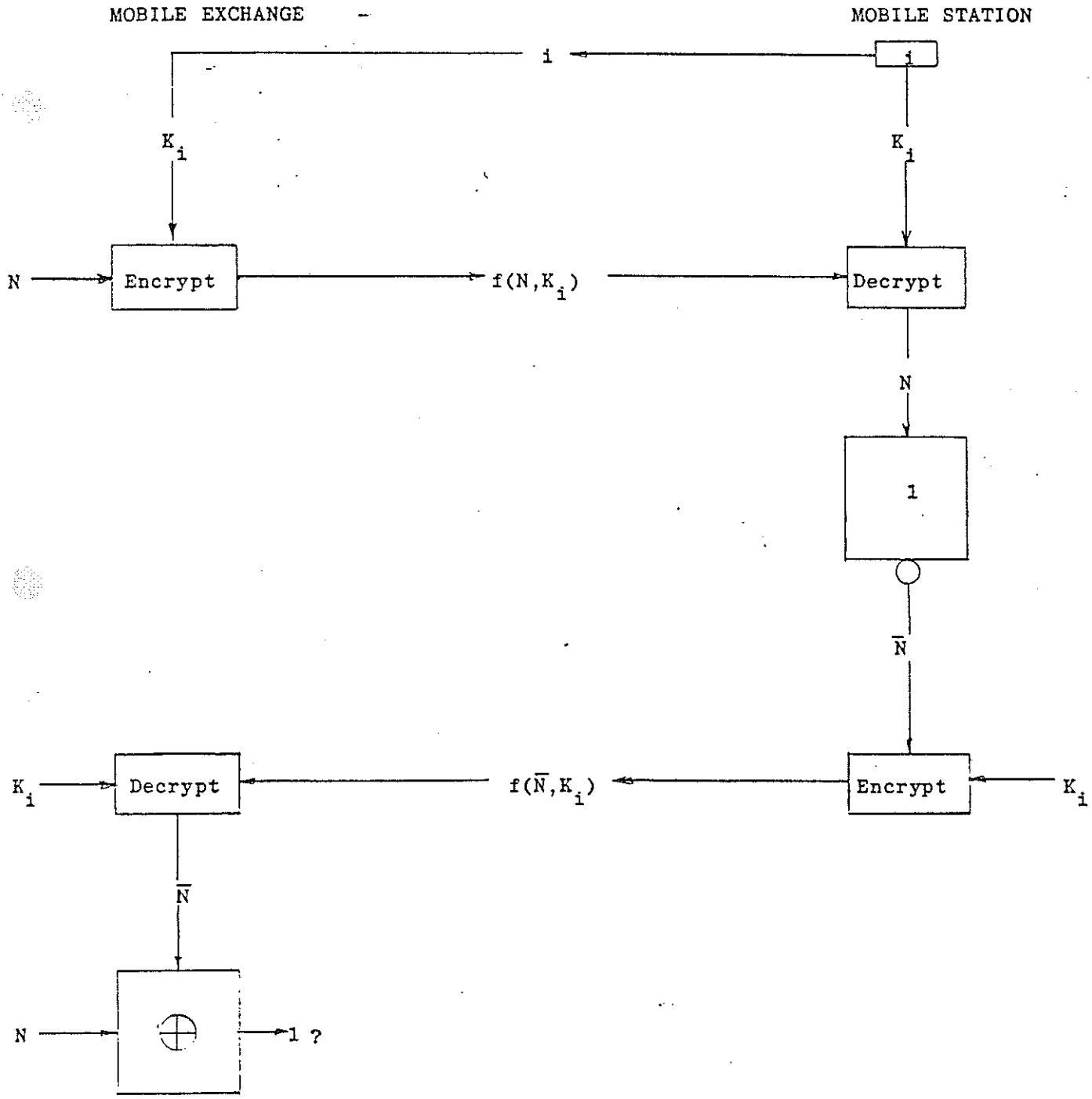

fig 1

A possible procedure for protection of mobile station identification