Zeitschrift: Technische Mitteilungen / Schweizerische Post-, Telefon- und Telegrafenbetriebe = Bulletin technique / Entreprise des postes, téléphones et télégraphes suisses = Bollettino tecnico / Azienda delle poste, dei telefoni e dei telegrafi svizzeri

Herausgeber: Schweizerische Post-, Telefon- und Telegrafenbetriebe

Band: 70 (1992)

Heft: 4

Artikel: Die Sicherheit von Natel D GSM

Autor: Rueppel, Rainer A. / Massey, James L.

DOI: https://doi.org/10.5169/seals-873982

Die Sicherheit von Natel D GSM[1]

Rainer A. RUEPPEL und James L. MASSEY, Zürich

1 Einführung

Die «Groupe spécial mobile» (GSM) wurde 1982 ins Leben gerufen, um die Spezifikationen für ein paneuropäisches, zellulares Mobilkommunikationssystem zu erarbeiten. Die GSM-Empfehlungen wurden durch das Europäische Institut für Fernmeldenormen (ETSI) veröffentlicht. In der Schweiz werden die GSM-Dienste *Natel D GSM* genannt, und ein Pilotsystem wurde für die Weltausstellung der Telekommunikation, Telecom 91, im Oktober 1991 in Genf installiert. Offiziell werden die Natel-D-GSM-Dienste im Frühjahr 1993 eingeführt.

Ein Mobilkommunikationsdienst bietet besondere Sicherheitsprobleme. Beispielsweise ist es hier nicht mehr möglich, den Benützer mit der physischen Leitung, die zwischen seinen Räumlichkeiten und den lokalen Zentralen installiert ist, zu identifizieren. Einen Benützer zu authentifizieren, der sich an einer beliebigen Stelle ins Netz einschalten kann, ist nur mit Verschlüsselungstechniken möglich.

2 Sicherheitsprobleme

Folgende Gefährdungen liegen jeder Mobilkommunikationsumgebung zugrunde:

1. Verlust der Vertraulichkeit
   Weil GSM den Funkweg benützt, um zwischen den mobilen Teilnehmern und der Basisstation zu verkehren, kann im Prinzip jedermann einen Empfänger auf die Verbindung abstimmen und jede ausgetauschte Information abhören. Dass diese Gefahr tatsächlich besteht, zeigt die Tatsache, dass in den Vereinigten Staaten Anwälte und Ärzte von Gesetzes wegen nicht über Klienten und deren Angelegenheiten am Autotelefon diskutieren dürfen.
2. Illegale Benützung des Dienstes
   Ein Grundproblem jedes Dienstes ist dessen gerechte Verrechnung. Nicht autorisierten Benützern muss jede Verwendung oder Blockierung des Netzes verunmöglicht werden. Zudem muss verhindert werden, dass sich autorisierte Benützer für einen anderen Benützer ausgeben und Anrufe auf dessen Rechnung tätigen. Folglich ist auch die korrekte Identifikation jedes autorisierten Benützers erforderlich.
3. Ortung
   Auch wenn die Kommunikation zwischen Mobil- und Basisstation verschlüsselt wird, ist es möglich, durch das Abhören der Signalisierung auf der Funkstrecke die Routen und Bewegungen einer verfolgten Person festzustellen. Sicherzustellen, dass ein Teilnehmer nicht geortet werden kann, widerspricht teilweise der Aufgabe der Benützerauthentifikation. Eine Lösung dieses Problems besteht darin, den Benützern zeitlich begrenzte, zufällige Pseudonyme zuzuordnen.

3 Sicherheitsdienste

Um den besonderen Gefährdungen zu begegnen, denen mobile Funkverbindungen unterliegen, wurden bei GSM die folgenden Sicherheitsdienste spezifiziert:

- Benützerauthentifikation
- Vertraulichkeit der Daten
- Benützerpseudonyme.

31 Benützerauthentifikation

Um die missbräuchliche Verwendung zu verunmöglichen und die gerechte Verrechnung sicherzustellen, werden die Benützer jedesmal neu authentifiziert, wenn sie sich ans Netz anschalten. Der verwendete Ablauf beruht auf einem Abfrage- und Antwortprotokoll. Der Benützer sendet zuerst seine internationale Mobilteilneh-

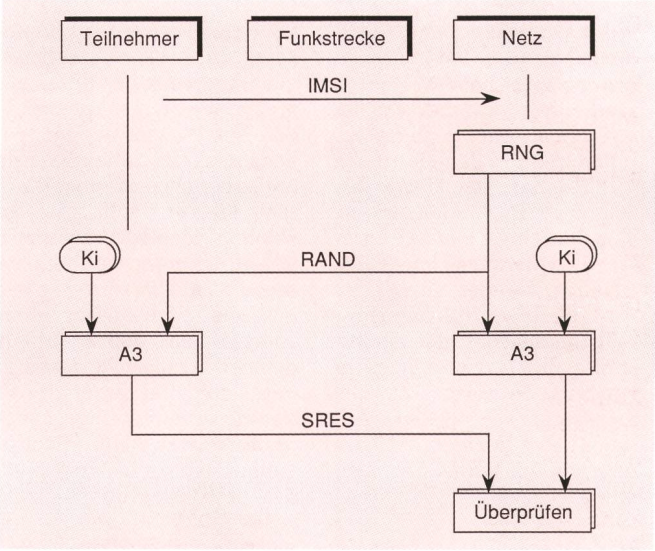

Fig. 1 Prinzip des Authentifikationsprotokolls

[1] Vortrag, gehalten in englischer Sprache am Berner Technologie-Forum 1991. Übersetzt durch die Redaktion.

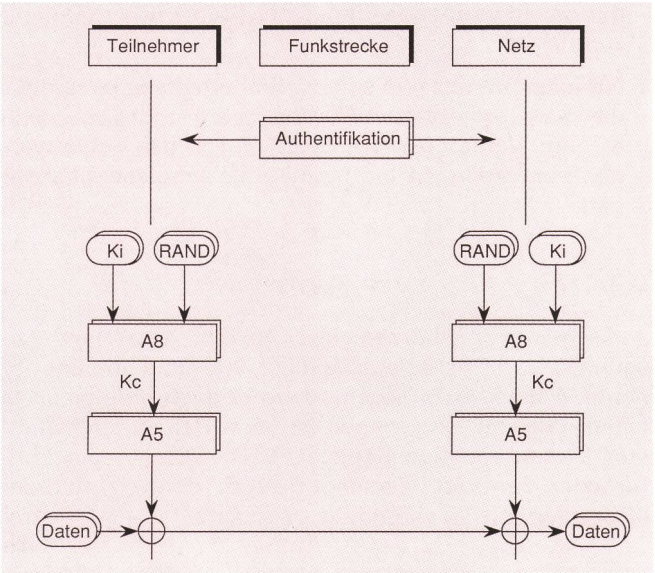

Fig. 2 Verschlüsselung der Funkstrecke

meridentität (International Mobile Subscriber Identity, IMSI), dann fordert das Netz vom Teilnehmer mit einer Zufallszahl (RAND), die aus einem Zufallszahlengenerator (RNG) stammt, eine Antwort an. Der Teilnehmer muss dieser Anforderung genügen, indem er eine «Signed Response» (SRES, bedeutet soviel wie «unterzeichnete Antwort») zurücksendet. Diese erzeugt er durch Anwendung des Authentifikationsalgorithmus A3 auf die Zufallszahl RAND unter Verwendung seines persönlichen Authentifikationsschlüssels K_i als Parameter. *Figur 1* zeigt das Prinzip dieses Authentifikationsprotokolls.

Um die Netzknoten von der Aufgabe zu entlasten, die Zufallszahlen zu erzeugen und die «Signed Responses» zu berechnen, und um zu vermeiden, dass die Netzknoten den persönlichen Teilnehmerauthentifikationsschlüssel K_i kennen müssen, sind diese sicherheitsrelevanten Informationen durch das Authentifikationszentrum vorberechnet und im Heimbereichsregister (Home Location Register, HLR) und möglicherweise auch in einem Besucherregister (Visited Location Register, VLR) gespeichert.

Das fremde, vom Teilnehmer besuchte Netz braucht vom Authentifikationsschlüssel K_i oder vom Authentifikationsalgorithmus A3, der im Heimnetz verwendet wird, überhaupt nichts zu wissen. Stattdessen erfragt das besuchte Netz die Authentifikations- und Verschlüsselungsinformation vom Heimnetz des Benützers.

32 Datenvertraulichkeit

Um das passive Abhören zu vermeiden, wird die Verbindung auf der Funkstrecke mit dem Algorithmus A5 verschlüsselt. Der dazu benötigte Schlüssel K_c ist von der Zufallszahl RAND und vom Teilnehmerauthentifikationsschlüssel K_i abgeleitet, und zwar unter Verwendung eines Algorithmus A8. Er wird im Teilnehmeridentitätsmodul (Subscriber Identity Module, SIM) erzeugt; damit kann vermieden werden, dass der Schlüssel K_c auf der Funkstrecke übertragen werden muss. Bevor diese Vertraulichkeitsfunktion wirksam werden kann, muss die Teilnehmerauthentifikation ordnungsgemäss stattgefunden haben *(Fig. 2)*.

Um die Vertraulichkeitsfunktion zu aktivieren, sendet das Netz eine Meldung, die «Ciphering Command Mode Message», zur Mobilstation. Nach Empfang dieser Meldung beginnt die Mobilstation mit dem Verschlüsseln. Um Kompatibilitätsprobleme zu vermeiden, ist der Verschlüsselungsalgorithmus A5 für das ganze GSM-Netz festgelegt. Er befindet sich im nichtpersönlichen Teil der Mobilstation, genannt Mobilausrüstung.

33 Benützerpseudonyme

Damit der Weg eines Teilnehmers nicht durch Abhören der beim Verbindungsaufbau ausgetauschten Identifikationsinformation verfolgt werden kann, wird ein Benützerpseudonym eingeführt. Diese zeitlich begrenzte Identifikation wird dem Benützer nach der ordnungsgemässen Authentifikation zugeteilt *(Fig. 3)*. Der Wert dieser «Temporary Mobile Subscriber Identity» (TMSI) wird durch das Netz gewählt und in verschlüsselter Form zum Teilnehmer übermittelt. Sie ist eine lokale Identität und nur in einem bestimmten Gebiet gültig. Der Benützer kann eine neue TMSI anfordern.

Wenn ein Benützer in ein neues Gebiet einfährt, kann er sich mit seiner wahren Identität (IMSI) oder mit seinem Pseudonym (TMSI) identifizieren. Letzteres muss dabei mit der entsprechenden örtlichen Identität «Location Area Identity» (LAI) versehen sein, um dem Netz zu ermöglichen, die für die Authentifikation nötige Information anzufordern. Sobald die Identität festgestellt ist, kann ein neues Pseudonym zugeordnet werden.

4 Sicherheitsverwaltung

Die Sicherheitsverwaltung ist jener Teil der Netzverwaltung, der sich mit Operationen ausserhalb der normalen Kommunikationsabläufe befasst, die aber zur Unterstützung und Steuerung der Sicherheitsaspekte dieser Kommunikation benötigt werden. Aufgabe der Sicherheitsverwaltung ist die Steuerung und Verteilung der sicherheitsbezogenen Information, um

- den Teilnehmern Sicherheitsdienste zur Verfügung zu stellen
- den Zugang zu den Netzknoten zu steuern
- sicherheitsrelevante Ereignisse anzuzeigen.

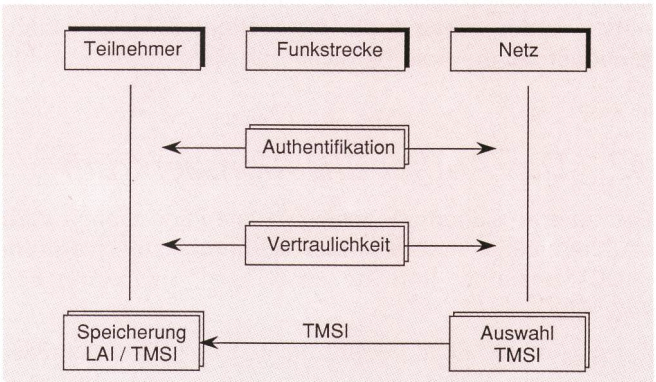

Fig. 3 Zuordnung eines Benützerpseudonyms

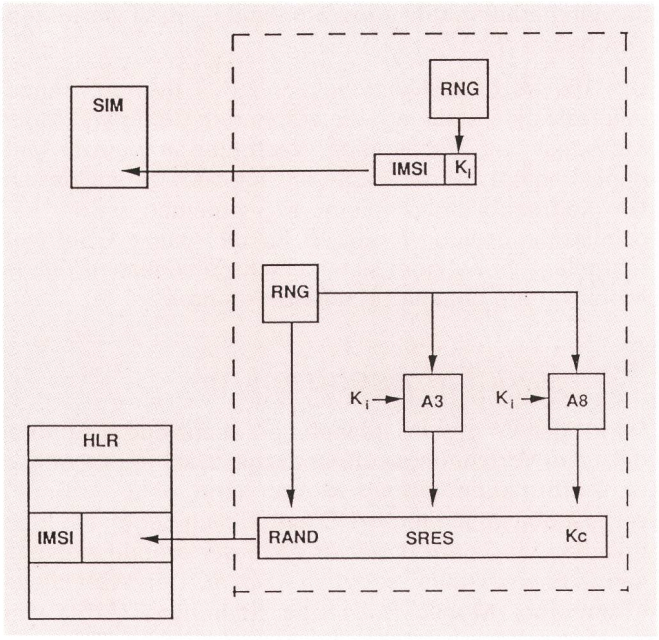

Fig. 4 Aufgaben des Authentifikationszentrums

Die Sicherheitsverwaltung hat nichts zu tun mit dem Übertragen von sicherheitsbezogener Information innerhalb der Protokolle beim Verbindungsaufbau.

41 Benützereintrag

Jeder neue Teilnehmer erhält bei der Anmeldung von der Administration eine persönliche Nummer, die «International Mobile Subscriber Identity» (IMSI), und ein persönliches Sicherheitsmodul, das «Subscriber Identity Module» (SIM). Das SIM enthält unter anderem:

- die internationale Mobilteilnehmeridentität (IMSI) des Teilnehmers
- den Teilnehmerauthentifikationsschlüssel K_i
- den Authentifikationsalgorithmus A3
- die persönliche Identifikationsnummer (PIN) des Teilnehmers.

Das Sicherheitsmodul kann entweder eine Chipkarte oder ein Einsteckmodul sein. Es dient dazu, alle persönlichen und geheimen Benützerdaten sicher zu speichern und Authentifikationsantworten und Codierschlüssel zu berechnen. Das Modul muss in die Mobilausrüstung eingesteckt werden, die den Funksenderempfänger und den Verschlüsselungsalgorithmus enthält. Es personalisiert die Mobilausrüstung und bildet mit ihr zusammen die Mobilstation (MS). Die GSM-Dienste können genutzt werden, sobald die internationale Mobilteilnehmeridentität im Heimbereichsregister aktiviert worden ist.

42 Das Authentifikationszentrum

Die für alle Sicherheitsbelange zuständige Einheit wird «Authentication Center» oder Authentifikationszentrum (AUC) genannt. Ihm obliegen zwei Hauptaufgaben *(Fig. 4)*:

1. Das Authentifikationszentrum hat für jeden Benützer in seinem Sicherheitsbereich den persönlichen Authentifikationsschlüssel (K_i) zu erzeugen und diesen mit der Identität des Benützers (IMSI) in Verbindung zu bringen.
2. Für jeden Benützer in seinem Sicherheitsbereich muss der Satz von Authentifikationsdaten und Schlüsseln erzeugt werden (RAND, SRES, K_c). Diese Sätze werden auf Verlangen ins Heimbereichsregister übertragen.

43 Der Heimbereich

Jeder Benützer gehört zu einem Heimbereich (Home Location Area). Das ist das Teilnetz, in dem seine permanente Wohnadresse liegt und wo er auch permanent in einem Register eingetragen ist, dem Heimbereichsregister (Home Location Register, HLR). Dieses speichert, für jeden Benützer in seinem Bereich, den vom Authentifikationszentrum erzeugten Datensatz.

44 Der besuchte Bereich

Wenn sich ein Benützer in ein anderes Teilnetz begibt, muss auch die ihn betreffende sicherheitsbezogene Information in dieses übertragen werden. Ein weiteres Register, das Besucherregister (Visited Location Register, VLR) dient dazu, vorübergehend alle diese Information zu speichern. *Figur 5* zeigt den Authentifikationsvorgang für eine besuchende Mobilstation.

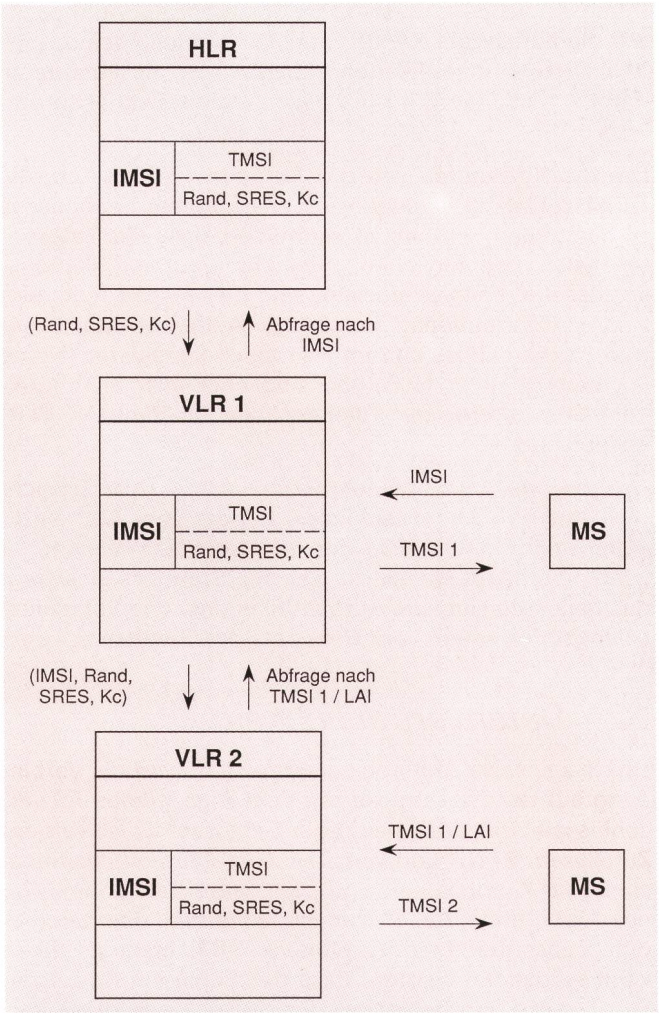

Fig. 5 Authentifikation einer besuchenden Mobilstation

Das Besucherregister kann die Information auf zwei verschiedene Arten erhalten:

1. Die besuchende Mobilstation deklariert ihre Identität (IMSI). Das Besucherregister verlangt die nötigen sicherheitsrelevanten Informationen vom Heimregister dieses Besuchers. Nach Erhalt des entsprechenden Datensatzes kann das besuchte Teilnetz den Benützer authentifizieren und sicher mit ihm verkehren.
2. Die besuchende Mobilstation deklariert ihr Pseudonym TMSI zusammen mit der Kennung des Aufenthaltsbereichs (Location Area Identity, LAI) des vorher besuchten Teilnetzes. Anschliessend fordert das Besucherregister die nötige sicherheitsbezogene Information vom früheren Besucherregister in dem von LAI bezeichneten Teilnetz an. Im Falle, dass das frühere Besucherregister nicht mehr im Besitz der nötigen Information ist, wird das Heimregister den Datensatz direkt liefern.

Zum Authentifizieren des Benützers sendet das Besucherregister nun die Zufallszahl RAND über die Zentrale und die Basisstation zum Benützer und erhält die Antwort SRES. Nach erfolgreicher Authentifikation erzeugt das Besucherregister ein Pseudonym TMSI und sendet dieses und den zugehörigen Schlüssel zur Mobilzentrale für die weitere Verwendung.

5 Diskussion

Die Sicherheitsarchitektur des GSM-Systems bietet einen Vertraulichkeitsdienst. Dieser ist gewissen Beschränkungen unterworfen. Erstens ist er nur auf der Funkstrecke wirksam, also gibt es keine End-zu-End-Sicherheit. Sobald die Meldungen die Funkstrecke verlassen und ins Telefonnetz gelangen, werden sie unverschlüsselt weitergeleitet. Eine passive Anzapfung kann hier bereits zum Erfolg führen. Auch gibt es hier keine Geheimhaltung gegenüber dem Netzbetreiber. Dieses Problem wiegt bei Anrufen von einer Mobilstation im Ausland noch schwerer, wenn die Meldungen die Netze mehrerer Netzbetreiber durchlaufen.

Die Sicherheitsarchitektur des GSM-Systems verwendet Benützerpseudonyme, damit der Weg des Benützers nicht verfolgt werden kann. Auch dies ist nur auf der Funkstrecke wirksam. Die Netzbetreiber kennen die wahre Identität der Benützer; tatsächlich ist es ja das Netz, das die Pseudonyme zuordnet. Somit ist es einem Netzbetreiber möglich, den Weg eines Benützers aufzuzeichnen, wenn er dies will.

Alle im GSM-System verwendeten Algorithmen sind vertraulich. Während der Authentifikationsalgorithmus A3 und der Schlüsselerzeugungsalgorithmus A8 als nationale Angelegenheit betrachtet werden, kann der Verschlüsselungsalgorithmus A5 nur mit der Zustimmung aller Netzbetreiber geändert werden. A3 und A8 könnten im Prinzip von jeder Administration oder Gesellschaft, die ein Mobilnetz betreibt, unabhängig festgelegt werden. Normalerweise werden sich die Netzbetreiber aber auf die Vorschläge für A3 und A8 beziehen, die in der Betriebsvereinbarung (Memorandum of Understanding) festgelegt sind. Obschon alle diese Algorithmen vertraulich sind, wird eine grosse Zahl von Leuten Zugang zu ihnen haben. Deshalb wird jeder Netzbetreiber klarlegen müssen, welchen Sicherheitsgrad er seinen Kunden tatsächlich anbietet und welche Verantwortung und Verbindlichkeit er übernimmt.

6 Schlussfolgerung

GSM ist ein Schritt in die richtige Richtung. Die Notwendigkeit besonderer Sicherheitsdienste in der öffentlichen Fernmeldeumgebung ist noch nicht lange anerkannt. Für die nächste Generation von Mobilfunksystemen scheint es aber wünschenswert, in dem Sinne wirklich asymmetrische Sicherheitsdienste anzubieten, so dass es für den Benützer nicht erforderlich ist, dem Netz zu vertrauen, um seine Geheimhaltung sicherzustellen. Vielmehr sollte der Benützer seine eigenen Geheimschlüssel und Pseudonyme wählen können und diese selber gegenüber dem Netz authentifizieren, ohne dass er sie irgend jemandem preisgeben muss. Dies ergäbe die Möglichkeit für echte End-zu-End-Vertraulichkeit.

Adresse der Autoren:

Rainer A. Rueppel
Security Engineering
Bahnhofstrasse 242
8623 Wetzikon

Prof. James L. Massey
Institut für Signal- und Informationsverarbeitung
ETH-Zentrum
8092 Zürich

Bibliographie

[1] *Stadelmann H. T.* Natel D GSM, das digitale paneuropäische Mobilkommunikationssystem. Bern, Techn. Mitt. PTT, 69 (1991) 9, S. 383.
[2] ETSI/TC GSM. Recommendations 2.09, 3.20, 12.xx.

Glossar

A3 Authentication algorithm — Authentifikationsalgorithmus
A5 Signalling data and user data encryption algorithm — Algorithmus für Verschlüsselung der Signalisierungs- und Teilnehmerdaten
A8 Ciphering key generating algorithm — Algorithmus zum Erzeugen des Codierungsschlüssels
AUC Authentication Centre — Authentifikationszentrum
GSM Global System for Mobile Communications — Weltweites Mobilkommunikationssystem (die Abkürzung GSM stand ursprünglich für «Groupe spécial mobile»)
HLR Home Location Register — Heimbereichsregister
IMSI International Mobile Subscriber Identity — Internationale Mobilteilnehmeridentität
K_c Cipher key — (Codierungs-)Schlüssel
K_i Individual subscriber authentication key — Persönlicher Teilnehmerauthentifikationsschlüssel
LAI Location Area Identity — Kennung des Aufenthaltsbereichs
MS Mobile Station — Mobilstation
MSC Mobile-services Switching Centre — Mobilkommunikations-Vermittlungsstelle
PIN Personal Identification Number — Persönliche Identifikationsnummer
PLMN Public Land Mobile Network — Öffentliches Landmobilfunknetz
RAND Random Number (authentication) — Zufallszahl für Authentifikation
RNG Random Number Generator — Zufallszahlengenerator
SIM Subscriber Identity Module — Teilnehmeridentitätsmodul
SRES Signed Response (authentication) — «Unterzeichnete Antwort»
TMSI Temporary Mobile Subscriber Identity — Temporäre Mobilteilnehmeridentität
VLR Visitor Location Register — Besucherregister

Zusammenfassung

Die Sicherheit von Natel D GSM

Wie jede Mobilkommunikationsumgebung bietet Natel D GSM auch einige besondere Sicherheitsprobleme. Die Autoren befassen sich mit diesen Gefährdungen und erläutern die Sicherheitsdienste, die zu ihrer Lösung spezifiziert wurden. Sie zeigen, wie diese Dienste im «Sicherheitsverwaltungs»-Teil der GSM-Netzverwaltung ablaufen, und behandeln schliesslich Sicherheitsaspekte des Gesamtsystems, das sowohl die Funkstrecke als auch einen Teil des Telefonnetzes umfasst.

Résumé

La sécurité du système Natel D GSM

Comme tout système de communication mobile, le Natel D GSM soulève aussi certains problèmes relatifs à la sécurité. Les auteurs passent en revue les dangers à envisager et expliquent les services de sécurité susceptibles d'y remédier. Ils montrent comment ces services s'intègrent dans la gestion des réseaux GSM, dans l'entité dite «gestion de la sécurité», et traitent le système en général sous l'aspect de la sécurité qui comprend aussi bien le circuit radioélectrique qu'une partie du réseau téléphonique.

Riassunto

Natel D GSM: il problema della sicurezza

Come per ogni sistema di comunicazione mobile anche per il Natel D GSM quello della sicurezza è un problema particolare. Gli autori se ne occupano e illustrano i «servizi di sicurezza» specificati per risolverlo; mostrano quindi come tali servizi vengono svolti nella parte della gestione della rete GSM riservata alla sicurezza; trattano infine gli aspetti concernenti la sicurezza del sistema globale, vale a dire della tratta radioelettrica e di una parte della rete telefonica.

Summary

The Security of Natel D GSM

The Natel D GSM System, as any mobile communications environment, presents some special security problems. The authors illustrate these threats and comment on the security services specified to solve them. They show how the services are treated in the «Security Management» part of the GSM network management, and finally assess the overall security of the system, including radio path and telephone network.