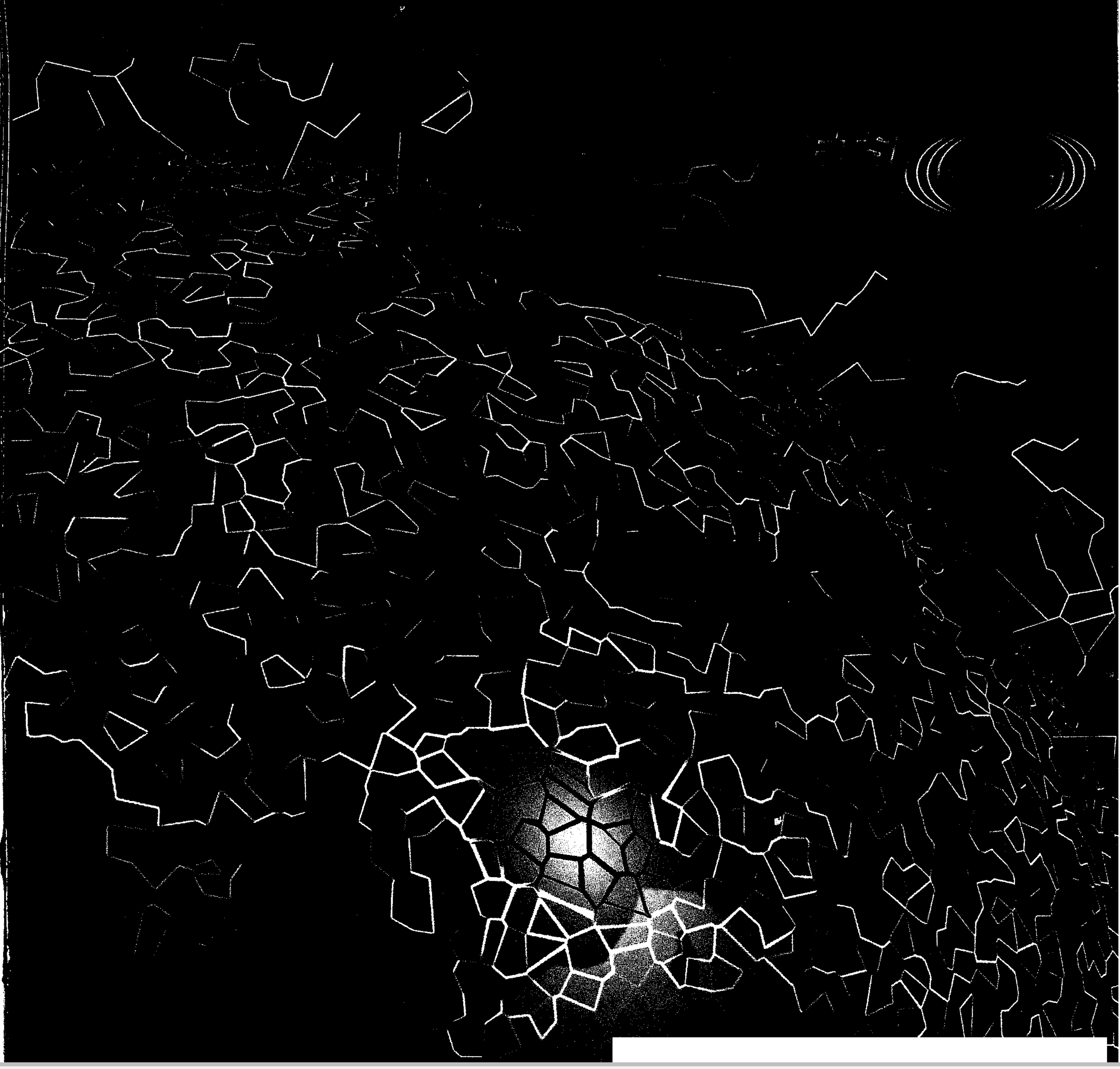
The State of the Art 1995

European Telecommunications Standardization and the



European Telecommunications Standardization and the Information Society – The State of the Art 1995 –

Published by
Atalink Ltd
40 Bowling Green Lane
London EC1R 0NE
United Kingdom
Telephone: +44 (0) 171 278 0333
Facsimile: +44 (0) 171 837 6135
Internet address
talk@atalink.demon.co.uk

On behalf of the
European Telecommunications Standards Institute
650 Route des Lucioles
F-06921 Sophia Antipolis Cedex
France
Telephone: +33 92 94 42 00
Facsimile: +33 93 65 47 16

Publisher
Charles Gregoriou

Editor
Mark Harrington

Editorial Committee
Malcolm Butler, Christopher J Corbett
Mark Harrington, Kirit Lathia
Miguel Pellon, Karl Heinz Rosenbrock

Coordinator-in-Chief
Christopher J Corbett

Sub-Editors (United Kingdom)
Beverly Wing
Auriol de Stacpoole

Editorial Coordination (France)
Frédérique Chauvel, Nathalie Kounakoff
Ulli Merz

Production Manager
Nancy Clarke

Production
Sally Hooker
Chris Hutchings
Meg Lawrence

Marketing
Philip Charles, Geoff Farmer
Mike Walsh, Stuart Ferguson
Mark Hall

Computersetting
Lynx Graphics Ltd, London, England

Origination
Stones Digital Imaging, Potters Bar, England

Printing
Cradley Print, West Midlands, England

Paper
Printed on G Print Matt 115gsm

Front Cover Design and Origination
GS Communication – Sophia Antipolis, France

Acknowledgements

The publishers would like to thank all those individuals who have contributed to this publication. Special thanks are extended to the authors for the time and effort spent in writing their substantial articles. Our utmost gratitude is extended to the Editorial Committee for their many hours spent travelling to meetings in order to spend many more hours planning the editorial structure of the publication and directing its content. We would like to thank Motorola for the kind use of their videoconferencing facilities. We would also like to thank Karl Heinz Rosenbrock and Christopher J Corbett for their invaluable assistance and guidance throughout the many months spent preparing this publication.

Copyright

This publication has been prepared wholly upon information supplied by the contributors and whilst the publishers trust that its content will be of interest to readers, its accuracy cannot be guaranteed. The publishers are unable to accept, and hereby expressly disclaim, any liability for the consequences of any inaccuracies, errors or omissions in such information whether occurring during the processing of such information for publication or otherwise. No representations, whether within the meaning of the Misrepresentation Act 1967 or otherwise, warranties or endorsements of any information contained herein are given or intended and full verification of all informa-

The Subscriber Identity Module

Dr. Klaus Vedder, Giesecke & Devrient GmbH and, Chairman ETSI Sub Technical Committee SMG 9.

The Global System for Mobile communications (GSM) is the first international system employing a smart card as a secure device for the authentication of the subscription and the subscriber. The smart card, which is called the Subscriber Identity Module (SIM), contains subscription and security related data as well as user data. This article discusses the role of the SIM as an important part of the security built into GSM and as a token for services rendered to subscribers and operators.

Cashless payment transactions at the point of sale: the

The idea of using a microprocessor or "smart" card for the authentication of a subscriber in a mobile network goes back to the early 1980s when discussions in Germany led to the use of microprocessor cards in the analogue mobile network "Netz-C". These ideas coincided with the early discussions about the design of a multi-national mobile network which would allow the user to roam on a previously unknown scale, the Global System for Mobile communications (GSM).

The Sub Technical Committee SMG 9 "SIM aspects" was established in April 1994 as the successor of the Subscriber Identity Module Expert Group (SIMEG) which had been founded in 1988 as a Working Party of what is now Sub Technical Committee SMG 1 "Services and facilities". The scope of SIMEG was to look into the functional characteristics of a subscriber identity module and its development. It was the common understanding that an Integrated Circuit card having the format of a credit card (the so-called ID-1 card) would be one of them. Two additional implementations were considered for quite some time: a Plug-in module which could be used for mobiles too small to accept an ID-1 card, and a module which would be an integral part of the mobile. Though the "integral" module had the obvious advantage that it required no extra interface in the mobile, it was considered not to be suitable for the requirements of GSM. The problems concerned mainly the handling of security related data. It would be difficult, if not impossible, for the operators to use their own specific security algorithms and to keep very close control of the secret keys and other operator specific data without a dedicated security module. It was also believed that "non-personal" mobiles would open up the market for all manufacturers and reduce trade barriers as every mobile could be used in every network. The discussions on the Plug-in module concentrated mainly on the use of Surface Mounted Device (SMD) packages for housing the chip and a cutting away "excessive" plastic from an ID-1 card. The latter, which had been proposed by the author, was eventually accepted as the realization of the "semi-permanent" Plug-in SIM[1,2].

The split of a Mobile Station (MS) into a radio part, the Mobile Equipment (ME), which does not contain any subscription related information, and a subscription part, the SIM, gives the network operator, on whose behalf the SIM is issued, complete control over all subscription and security related data. The concept of a removable SIM adds a new dimension of mobility to the subscription. The SIM is thus an integral part of the overall security system of each, and therefore all networks, and a token for the mobility of the subscriber.

The main specifications dealing with the SIM are the description of its functionality, Technical Specification GSM 02.17[1] and the specification of its interface to the ME Technical Specification GSM 11.11[2]. Tests of the SIM/ME interface are contained in Technical Specification GSM 11.10 which specifies the type approval of the Mobile Station. For the interested reader more detailed information on all aspects of GSM can be found in Hillebrand[3] and, Mouly and Pautet[4].

The following sections discuss the security services provided by GSM and the role played by the SIM as a secure device for storing keys and algorithms, briefly introduce the microcomputer contained in the SIM and discuss access to the SIM. This is followed by a description of the main services supported by the SIM. The handling of SIMs and an outlook of services and features to come, conclude this overview.

Security services and the SIM

One of the novel security services of GSM is the possibility to encipher the link between the Mobile Station (MS) and the Base Station for the protection of user and signalling data against eavesdropping. Special ciphers have been developed for this purpose. They are integrated into the Mobile Equipment as a dedicated piece of silicon. The key for enciphering the data is derived by the SIM as part of the authentication process. The network can only authenticate the SIM if it knows its identity. As this has to be sent by the Mobile Station over the air interface, temporary identities are used to counteract the tracing of the whereabouts of a user.

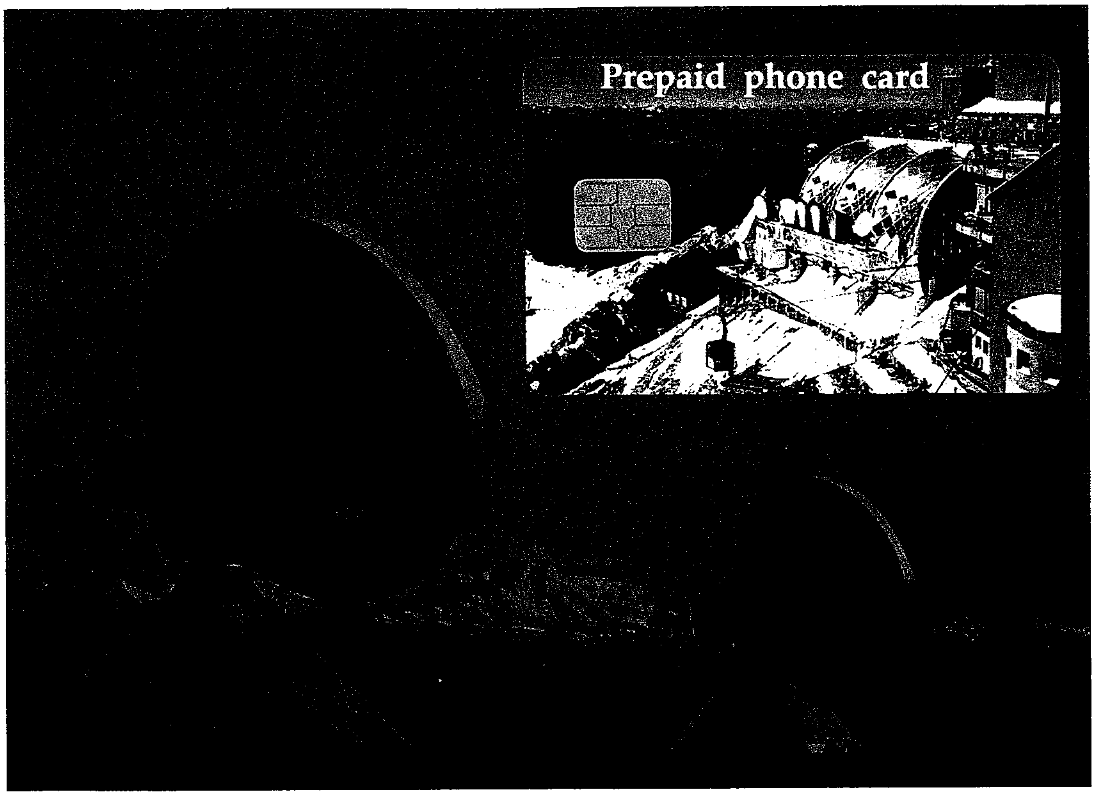
More precisely, the **temporary identities** prevent the tracing of the location of a user by intercepting the user's identity on the air interface. Clearly, the International Mobile Subscriber Identity (IMSI), which uniquely identifies the subscriber worldwide [illegible] of a session if there are no other means to identify a subscriber. This is, for instance, the case when the subscriber uses the SIM for the very first time. After a successful authentication the network assigns a Temporary Mobile Subscriber Identifier (TMSI) to the SIM and transmits this identifier after the activation of the cipher process in an enciphered form to the MS where it is deciphered. The MS stores the temporary identity in the SIM. This TMSI will be used instead of the IMSI whenever possible until a new TMSI is assigned to the SIM. Reassignment takes place at defined times by each operator.

Authentication is the "corroboration that an entity is the one claimed" or, in terms of GSM, the verification of the identity of the SIM or the subscriber. The illegitimate use of a service is certainly of concern with respect to proper billing. The not so obvious illegitimate use is masquerading. Impersonating a subscriber and claiming afterwards that this subscriber (or to be more precise the subscriber's SIM) must have been in a particular location at a particular time is certainly not a very widespread threat but one which could prove very serious indeed in certain circumstances. Cloning of security relevant subscription data needs to be ruled out.

The main players in the authentication process of the subscriber are the SIM and the Authentication Centre (AuC) of the home network. Both contain the (operator specific) authentication algorithm, denoted by A3, and the secret authentication key Ki which is unique to each

Glossary

ADM	ADMinistrative
AuC	Authentication Centre
CBMI	Cell Broadcast Message Identifier
EEPROM	Electrically Erasable Programmable Read Only Memory
GSM	Global System for Mobile communications
HLR	Home Location Register
ID	IDentity
IMSI	International Mobile Subscriber Identity
ME	Mobile Equipment
MS	Mobile Station
MSISDN	Mobile Station ISDN number
PIN	Personal Identification Number
PUK	PIN Unblocking Key
RAM	Random Access Memory
ROM	Read Only Memory
SIM	Subscriber Identity Module
SMG	Special Mobile Group
TMSI	Temporary Mobile Subscriber Identity
VLR	Visitor Location Register



G&D supplied more than 100 million prepaid phone cards and subscriber cards in EEPROM-technology to international telephone network operators.

Copyright: Bavaria/Giesecke & Devrient GmbH

SIM. The AuC is usually part of a Home Location Register (HLR) which contains the data about the subscription and the user. The method employed between the HLR/AuC and the SIM is a Challenge-Response mechanism using "non-predictable numbers".

Once the (home) network has received an authentication request and established the (claimed) identity of the SIM it transmits a non-predictable number RAND as a *challenge* to the ME which sends it to the SIM. The SIM computes the *response* to the *challenge* by using the algorithm A3 with RAND and the key Ki stored in the SIM as input data. The response is transmitted to the (visited) network where it is compared with the value computed by the home network which has used the same algorithm with the same RAND and the key associated with the identity claimed by the subscriber. The MS is granted access to the network only if the *response* received from the MS and the value computed by the home network are equal. For only in this case can it be assumed that the SIM is in possession of the right subscriber key Ki and that, therefore, its identity is the one claimed.

Accompanying the Challenge-Response pairs calculated in the HLR/AuC is a new cipher key Kc. This is computed using Ki and the same non-predictable number RAND with an (operator specific) algorithm called A8. The purpose of enciphering is to ensure the privacy of the user information carried in both traffic and signalling channels and of user-related signalling elements on the radio path. The activation of this service is controlled by the network. It is started by the base station by sending a "start cipher" command to the MS. One or two standard cipher algorithms, denoted by A5/1 and A5/2, are contained as a dedicated piece of silicon in Mobile Equipment and Base Stations.

The 64 bit key Kc, which controls the generation of the key stream by the cipher algorithm A5, is calculated in the SIM during the authentication process using the same A8 as the home network and the same input as for the authentication process. No additional input data is thus required and there is no need to send secret data or even Kc over the air interface. Furthermore, "bypassing" the authentication procedure by, say, manipulating the comparison of challenge and response, is of no use to the fraudster as the Mobile Station and Base Station will use different cipher keys resulting in an indecipherable garbled message.

A functional description of these security services is contained in Technical Specification GSM 02.09[5]. Such a description is, by its very nature, not sufficient to ensure interoperability between net-

DOCKET
ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.