Josep Domingo-Ferrer
Joachim Posegga
Daniel Schreckling (Eds.)

LNCS 3928

Smart Card Research and Advanced Applications

7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006
Tarragona, Spain, April 2006
Proceedings

ifip

Springer

Josep Domingo-Ferrer Joachim Posegga
Daniel Schreckling (Eds.)

Smart Card Research and Advanced Applications

7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006
Tarragona, Spain, April 19-21, 2006
Proceedings

Springer

Volume Editors

Josep Domingo-Ferrer
Universitat Rovira i Virgili, Departament d'Enginyeria Informatica i Matematiques,
Av. Paisos Catalans 26, 43007 Tarragona, Catalonia, Spain
E-mail: josep.domingo@urv.net

Joachim Posegga
Daniel Schreckling
Universität Hamburg
Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)
Fachbereich Informatik
Vogt-Kölln-Str. 30, 22527 Hamburg, Germany
E-mail: {posegga,schreckling}@informatik.uni-hamburg.de

Library of Congress Control Number: 2006922624

CR Subject Classification (1998): E.3, K.6.5, C.3, D.4.6, K.4.1, E.4, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-33311-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-33311-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11733447 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 3928

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Preface

Smart cards are an established security research area with a very unique property: it integrates numerous subfields of IT Security, which often appear scattered and only loosely connected. Smart card research unites them by providing a common goal: advancing the state of the art of designing and deploying small tokens to increase the security in Information Technology.

CARDIS has a tradition of more than one decade, and has established itself as the premier conference for research results in smart card technology. As smart card research is unique, so is CARDIS; the conference successfully attracts academic and industrial researchers without compromising in either way. CARDIS accommodates applied research results as well as theoretical contributions that might or might not become practically relevant. The key to making such a mixture attractive to both academia and industry is simple: quality of contributions and relevance to the overall subject.

This year's CARDIS made it easy to continue this tradition: we received 76 papers, nearly all of them relevant to the focus of CARDIS and presenting high-quality research results. The Program Committee worked hard on selecting the best 25 papers to be presented at the conference.

We are very grateful to the members of the Program Committee and the additional referees for generously spending their time on the difficult task of assessing the value of submitted papers. Daniel Schreckling provided invaluable assistance in handling submissions, managing review reports and editing the proceedings. The assistance of Jordi Castellà in handling practical aspects of the conference preparation is also greatly appreciated.

Financial support by the following organizations is gratefully acknowledged: IEEE Spain Section, Rovira i Virgili University (ETSE, DEIM) and Spain's Ministry of Science and Education.

Finally, we would also like to thank all those who have submitted papers to IFIP CARDIS 2006, and encourage them to stay with CARDIS in subsequent years. The authors of the accepted papers certainly deserve the highest respect, since it is they who wrote this book.

January 2006

Josep Domingo-Ferrer
Joachim Posegga

Organization

CARDIS 2006 was organized by the Universitat Rovira i Virgili, Catalonia, Spain.

Conference Organization

Conference General Chair	Josep Domingo-Ferrer (Universitat Rovira i Virgili, Catalonia, Spain)
Program Committee Chair	Joachim Posegga (University of Hamburg, Germany)
Advisory Committee	José A. Delgado-Penín (IEEE Spain Section Chair, Spain)

Program Committee

Boris Balacheff (Hewlett-Packard Labs, UK)
Bertrand du Castel (Axalto, USA)
Josep Domingo-Ferrer (Universitat Rovira i Virgili, Catalonia, Spain)
Dieter Gollmann (TU Hamburg-Harburg, Germany)
Louis Guillou (France Télécom, France)
Pieter Hartel (University of Twente, Netherlands)
Peter Honeyman (University of Michigan, USA)
Dirk Husemann (IBM Research, Switzerland)
Eduardo de Jong (Sun Microsystems, USA)
Jean-Louis Lanet (Gemplus Labs, France)
Javier Lopez (University of Malaga, Spain)
Bernd Meyer (Siemens AG, Germany)
Mike Montgomery (Axalto, USA)
Pierre Paradinas (CNAM, France)
Jean-Jacques Quisquater (Université Catholique de Louvain, Belgium)
Francesc Sebé (Universitat Rovira i Virgili, Catalonia, Spain)
François-Xavier Standaert (Université Catholique de Louvain, Belgium)
Jean-Jacques Vandewalle (Gemplus Labs, France)

Additional Referees

A. Ali
V. Benjumea
D. Bolzoni
E. Brier
R. Brinkman
I. Buhan
M. Casassa-Mont
J. Castellà-Roca
J. Cederquist
L. Chen
M. Ciet
R. Corin
M. Czenko
M. Dekker
G.M. de Dormale
J.B. Fischer
C. Fontaine
P. Girard
B. Gonzalvo
D. Gross-Amblard
H. Handschuh
K. Harrisson
Z. HuanGuo
M. Johns
M. Joye
A. Kargl
K. Lu
F. Macé
A. Maña
W. Mao
A. Martínez-Ballesté
A. Muñoz E. Peeters
H.C. Pöhls
E. Prouff
R. Roman
A. Saptawijaya
D. Schreckling
J. Seedorf
D. Simplot-Ryl
A. Solanas
A. Viejo-Galicia
L.Y. Wei
A. Zych

Lecture Notes in Computer Science

For information about Vols. 1–3823

please contact your bookseller or Springer

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3927: J. Hespanha, A. Tiwari (Eds.), Hybrid Systems: Computation and Control. XII, 584 pages. 2006.

Vol. 3925: A. Valmari (Ed.), Model Checking Software. X, 307 pages. 2006.

Vol. 3924: P. Sestoft (Ed.), Programming Languages and Systems. XII, 343 pages. 2006.

Vol. 3923: A. Mycroft, A. Zeller (Eds.), Compiler Construction. XIII, 277 pages. 2006.

Vol. 3922: L. Baresi, R. Heckel (Eds.), Fundamental Approaches to Software Engineering. XIII, 427 pages. 2006.

Vol. 3921: L. Aceto, A. Ingólfsdóttir (Eds.), Foundations of Software Science and Computation Structures. XV, 447 pages. 2006.

Vol. 3920: H. Hermanns, J. Palsberg (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. XIV, 506 pages. 2006.

Vol. 3916: J. Li, Q. Yang, A.-H. Tan (Eds.), Data Mining for Biomedical Applications. VIII, 155 pages. 2006. (Sublibrary LNBI).

Vol. 3915: R. Nayak, M.J. Zaki (Eds.), Knowledge Discovery from XML Documents. VIII, 105 pages. 2006.

Vol. 3907: F. Rothlauf, J. Branke, S. Cagnoni, E. Costa, C. Cotta, R. Drechsler, E. Lutton, P. Machado, J.H. Moore, J. Romero, G.D. Smith, G. Squillero, H. Takagi (Eds.), Applications of Evolutionary Computing. XXIV, 813 pages. 2006.

Vol. 3906: J. Gottlieb, G.R. Raidl (Eds.), Evolutionary Computation in Combinatorial Optimization. XI, 293 pages. 2006.

Vol. 3905: P. Collet, M. Tomassini, M. Ebner, S. Gustafson, A. Ekárt (Eds.), Genetic Programming. XI, 361 pages. 2006.

Vol. 3904: M. Baldoni, U. Endriss, A. Omicini, P. Torroni (Eds.), Declarative Agent Languages and Technologies III. XII, 245 pages. 2006. (Sublibrary LNAI).

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3901: P.M. Hill (Ed.), Logic Based Program Synthesis and Transformation. X, 179 pages. 2006.

Vol. 3899: S. Frintrop, VOCUS: A Visual Attention System for Object Detection and Goal-Directed Search. XIV, 216 pages. 2006. (Sublibrary LNAI).

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3896: Y. Ioannidis, M.H. Scholl, J.W. Schmidt, F. Matthes, M. Hatzopoulos, K. Boehm, A. Kemper, T. Grust, C. Boehm (Eds.), Advances in Database Technology - EDBT 2006. XIV, 1208 pages. 2006.

Vol. 3895: O. Goldreich, A.L. Rosenberg, A.L. Selman (Eds.), Theoretical Computer Science. XII, 399 pages. 2006.

Vol. 3894: W. Grass, B. Sick, K. Waldschmidt (Eds.), Architecture of Computing Systems - ARCS 2006. XII, 496 pages. 2006.

Vol. 3890: S.G. Thompson, R. Ghanea-Hercock (Eds.), Defence Applications of Multi-Agent Systems. XII, 141 pages. 2006. (Sublibrary LNAI).

Vol. 3889: J. Rosca, D. Erdogmus, J.C. Príncipe, S. Haykin (Eds.), Independent Component Analysis and Blind Signal Separation. XXI, 980 pages. 2006.

Vol. 3888: D. Draheim, G. Weber (Eds.), Trends in Enterprise Application Architecture. IX, 145 pages. 2006.

Vol. 3887: J.R. Correa, A. Hevia, M. Kiwi (Eds.), LATIN 2006: Theoretical Informatics. XVI, 814 pages. 2006.

Vol. 3886: E.G. Bremer, J. Hakenberg, E.-H.(S.) Han, D. Berrar, W. Dubitzky (Eds.), Knowledge Discovery in Life Science Literature. XIV, 147 pages. 2006. (Sublibrary LNBI).

Vol. 3885: V. Torra, Y. Narukawa, A. Valls, J. Domingo-Ferrer (Eds.), Modeling Decisions for Artificial Intelligence. XII, 374 pages. 2006. (Sublibrary LNAI).

Vol. 3884: B. Durand, W. Thomas (Eds.), STACS 2006. XIV, 714 pages. 2006.

Vol. 3881: S. Gibet, N. Courty, J.-F. Kamp (Eds.), Gesture in Human-Computer Interaction and Simulation. XIII, 344 pages. 2006. (Sublibrary LNAI).

Vol. 3880: A. Rashid, M. Aksit (Eds.), Transactions on Aspect-Oriented Software Development I. IX, 335 pages. 2006.

Vol. 3879: T. Erlebach, G. Persinao (Eds.), Approximation and Online Algorithms. X, 349 pages. 2006.

Vol. 3878: A. Gelbukh (Ed.), Computational Linguistics and Intelligent Text Processing. XVII, 589 pages. 2006.

Vol. 3877: M. Detyniecki, J.M. Jose, A. Nürnberger, C. J. '. van Rijsbergen (Eds.), Adaptive Multimedia Retrieval: User, Context, and Feedback. XI, 279 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3875: S. Ur, E. Bin, Y. Wolfsthal (Eds.), Hardware and Software, Verification and Testing. X, 265 pages. 2006.

Vol. 3874: R. Missaoui, J. Schmidt (Eds.), Formal Concept Analysis. X, 309 pages. 2006. (Sublibrary LNAI).

Vol. 3873: L. Maicher, J. Park (Eds.), Charting the Topic Maps Research and Applications Landscape. VIII, 281 pages. 2006. (Sublibrary LNAI).

Vol. 3872: H. Bunke, A. L. Spitz (Eds.), Document Analysis Systems VII. XIII, 630 pages. 2006.

Vol. 3870: S. Spaccapietra, P. Atzeni, W.W. Chu, T. Catarci, K.P. Sycara (Eds.), Journal on Data Semantics V. XIII, 237 pages. 2006.

Vol. 3869: S. Renals, S. Bengio (Eds.), Machine Learning for Multimodal Interaction. XIII, 490 pages. 2006.

Vol. 3868: K. Römer, H. Karl, F. Mattern (Eds.), Wireless Sensor Networks. XI, 342 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3865: W. Shen, K.-M. Chao, Z. Lin, J.-P.A. Barthès, A. James (Eds.), Computer Supported Cooperative Work in Design II. XII, 659 pages. 2006.

Vol. 3863: M. Kohlhase (Ed.), Mathematical Knowledge Management. XI, 405 pages. 2006. (Sublibrary LNAI).

Vol. 3862: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 267 pages. 2006. (Sublibrary LNAI).

Vol. 3861: J. Dix, S.J. Hegner (Eds.), Foundations of Information and Knowledge Systems. X, 331 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3857: M.P.C. Fossorier, H. Imai, S. Lin, A. Poli (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. XI, 350 pages. 2006.

Vol. 3855: E. A. Emerson, K.S. Namjoshi (Eds.), Verification, Model Checking, and Abstract Interpretation. XI, 443 pages. 2005.

Vol. 3854: I. Stavrakakis, M. Smirnov (Eds.), Autonomic Communication. XIII, 303 pages. 2006.

Vol. 3853: A.J. Ijspeert, T. Masuzawa, S. Kusumoto (Eds.), Biologically Inspired Approaches to Advanced Information Technology. XIV, 388 pages. 2006.

Vol. 3852: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part II. XXXI, 977 pages. 2006.

Vol. 3851: P.J. Narayanan, S.K. Nayar, H.-Y. Shum (Eds.), Computer Vision – ACCV 2006, Part I. XXXI, 973 pages. 2006.

Vol. 3850: R. Freund, G. Păun, G. Rozenberg, A. Salomaa (Eds.), Membrane Computing. IX, 371 pages. 2006.

Vol. 3849: I. Bloch, A. Petrosino, A.G.B. Tettamanzi (Eds.), Fuzzy Logic and Applications. XIV, 438 pages. 2006. (Sublibrary LNAI).

Vol. 3848: J.-F. Boulicaut, L. De Raedt, H. Mannila (Eds.), Constraint-Based Mining and Inductive Databases. X, 401 pages. 2006. (Sublibrary LNAI).

Vol. 3847: K.P. Jantke, A. Lunzer, N. Spyratos, Y. Tanaka (Eds.), Federation over the Web. X, 215 pages. 2006. (Sublibrary LNAI).

Vol. 3846: H. J. van den Herik, Y. Björnsson, N.S. Netanyahu (Eds.), Computers and Games. XIV, 333 pages. 2006.

Vol. 3845: J. Farré, I. Litovsky, S. Schmitz (Eds.), Implementation and Application of Automata. XIII, 360 pages. 2006.

Vol. 3844: J.-M. Bruel (Ed.), Satellite Events at the MoDELS 2005 Conference. XIII, 360 pages. 2006.

Vol. 3843: P. Healy, N.S. Nikolov (Eds.), Graph Drawing. XVII, 536 pages. 2006.

Vol. 3842: H.T. Shen, J. Li, M. Li, J. Ni, W. Wang (Eds.), Advanced Web and Network Technologies, and Applications. XXVII, 1057 pages. 2006.

Vol. 3841: X. Zhou, J. Li, H.T. Shen, M. Kitsuregawa, Y. Zhang (Eds.), Frontiers of WWW Research and Development - APWeb 2006. XXIV, 1223 pages. 2006.

Vol. 3840: M. Li, B. Boehm, L.J. Osterweil (Eds.), Unifying the Software Process Spectrum. XVI, 522 pages. 2006.

Vol. 3839: J.-C. Filliâtre, C. Paulin-Mohring, B. Werner (Eds.), Types for Proofs and Programs. VIII, 275 pages. 2006.

Vol. 3838: A. Middeldorp, V. van Oostrom, F. van Raamsdonk, R. de Vrijer (Eds.), Processes, Terms and Cycles: Steps on the Road to Infinity. XVIII, 639 pages. 2005.

Vol. 3837: K. Cho, P. Jacquet (Eds.), Technologies for Advanced Heterogeneous Networks. IX, 307 pages. 2005.

Vol. 3836: J.-M. Pierson (Ed.), Data Management in Grids. X, 143 pages. 2006.

Vol. 3835: G. Sutcliffe, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIV, 744 pages. 2005. (Sublibrary LNAI).

Vol. 3834: D.G. Feitelson, E. Frachtenberg, L. Rudolph, U. Schwiegelshohn (Eds.), Job Scheduling Strategies for Parallel Processing. VIII, 283 pages. 2005.

Vol. 3833: K.-J. Li, C. Vangenot (Eds.), Web and Wireless Geographical Information Systems. XI, 309 pages. 2005.

Vol. 3832: D. Zhang, A.K. Jain (Eds.), Advances in Biometrics. XX, 796 pages. 2005.

Vol. 3831: J. Wiedermann, G. Tel, J. Pokorný, M. Bieliková, J. Štuller (Eds.), SOFSEM 2006: Theory and Practice of Computer Science. XV, 576 pages. 2006.

Vol. 3830: D. Weyns, H. V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems II. VIII, 291 pages. 2006. (Sublibrary LNAI).

Vol. 3829: P. Pettersson, W. Yi (Eds.), Formal Modeling and Analysis of Timed Systems. IX, 305 pages. 2005.

Vol. 3828: X. Deng, Y. Ye (Eds.), Internet and Network Economics. XVII, 1106 pages. 2005.

Vol. 3827: X. Deng, D.-Z. Du (Eds.), Algorithms and Computation. XX, 1190 pages. 2005.

Vol. 3826: B. Benatallah, F. Casati, P. Traverso (Eds.), Service-Oriented Computing - ICSOC 2005. XVIII, 597 pages. 2005.

Vol. 3824: L.T. Yang, M. Amamiya, Z. Liu, M. Guo, F.J. Rammig (Eds.), Embedded and Ubiquitous Computing – EUC 2005. XXIII, 1204 pages. 2005.

¥624.00元

Table of Contents

Smart Card Applications

Side Channel Attacks

Smart Card Networking

Cryptographic Protocols

RFID Security

Formal Methods

Design, Installation and Execution of a Security Agent for Mobile Stations

William G. Sirett*, John A. MacDonald**,
Keith Mayes, and Konstantinos Markantonakis

Smart Card Centre, Information Security Group,
Royal Holloway, University of London,
Egham, TW20 0EX, England
{w.g.sirett, k.markantonakis, keith.mayes}@rhul.ac.uk,
john@madgo.com

Abstract. In this paper we present a methodology and protocol for establishing a security context between a Mobile Operator's application server and a GSM/UMTS SIM card. The methodology assumes that the already issued Mobile Station is capable but unprepared. The proposed scheme creates a secure entity within the Mobile Station "Over The Air" (OTA). This secure entity can then be used for subsequent SIM authentications enabling m-Commerce, DRM or web service applications. To validate our proposal we have developed a proof of concept model to install and execute the security context using readily available J2ME, Java Card, J2SE and J2EE platforms, with the KToolBar MIDP2.0 emulator tool from Sun, and a Gemplus Java Card.

Keywords: Mobile Station, Security Agent, Application Deployment, Smart Card, GSM, Security Protocol, JSR177, MIDP2.0.

1 Introduction

The GSM network offers a wide scope of applications and benefits for mobile operators. The merits of a Mobile Station capable of implementing a *Security Agent* are well documented in the literature [17, 18]. In this paper we consider the deployment of a *Security Agent* that is comprised of two components: a device application executing resource-intensive tasks, and a secure entity application responsible for secure functionality. The secure entity is a tamper resistant [5] entity and in the case of this work is a GSM/UMTS SIM card. For some time the GSM network has allowed for "Over The Air" (OTA) SIM application installation with limited bandwidth capacity. To install these applications utilising a high bandwidth channel and a non-GSM specified protocol currently demands trust/keys being provided to the Mobile Device. This work considers the Mobile Device to be hostile. This raises a need for the same high bandwidth OTA functionality to be available whilst protecting against malicious equipment.

* This work was supported by sponsorship funding from the Smart Card Centre founded by Vodafone and G&D.

** This work was supported by sponsorship funding from Telefonica Móviles, España.

J. Domingo-Ferrer, J. Posegga, and D. Schreckling (Eds.): CARDIS 2006, LNCS 3928, pp. 1–15, 2006.

This work establishes a security context between a Mobile Operator Application and Mobile Station and proposes an authenticated key establishment protocol. By establishing session keys independent of the network security keys, we can provide integrity, authentication and confidentially at the application layer. In the GSM/3GPP mobile architecture [24], the user security context resides in two locations, the network HLR and the Operator issued tamper resistant SIM card. The Mobile Operator generally has much less control over the Mobile device than the SIM. Consequently they are more reluctant to load sensitive components or data into the device. This motivates the division of the *Security Agent* between the device and the SIM, where the SIM is responsible for particularly sensitive components. We propose a scenario where the Mobile Operator Application server communicates with the device resident component of the *Security Agent*. This subsequently uses the security services provided by the secure entity to establish authenticated keys.

In section 2 we review the design requirements for a *Security Agent* deployed on a GSM/3GPP Mobile Station. In section 3 we review our proposed authenticated key establishment scheme. A protocol for wireless installation of the *Security Agent* to a compatible but remote and unprepared Mobile Station (colloquially termed "OTA" and "backward compatible field installation") is detailed in section 4, whilst the protocol used to establish session integrity and confidentiality keys is presented in section 5. Finally, in section 6, we describe the Proof of Concept model constructed using readily available components and open source development tool kits and provide concluding remarks in section 7.

2 Design Requirements

A critical requirement is for a backward compatible field installable *Security Agent* designed to provide an authentication service using SIM based credentials. It is required to be executable on a significant proportion of globally standardised and deployed Mobile Stations. The design of our proposed *Security Agent* uses four widely adopted technologies and standards:

- ETSI TS03.48 Security Mechanism [1];
- SIM Application Toolkit (SAT) [12];
- MIDP2.0 J2ME Runtime Environment [15];
- UICC Java Card SIM cards [3].

2.1 ETSI TS03.48 Security Mechanism

ETSI TS03.48 [1] specifies a mechanism for providing end to end security for any Short Message Service (SMS) going to or from the SIM card. SMS messages contain a maximum of 140 bytes. SMS messages are sent in accordance with the SUBMIT_SMS format, and received with the SMS_DELIVER format. Translation from one format to the other is performed by the Short Message Service Centre (SMSC), an active component of the network. In an output SUBMIT_SMS packet, the 40 bytes of User Data are complemented by a 13 byte *Mandatory Header* and an optional variable length *User Data Header*.

- The *Mandatory Header* includes the Data Coding Scheme byte which specifies how the data is encoded, and the Protocol Identifier byte which specifies how the receiving mobile should process the message. One of these values, $0xF7$, specifies that the device should pass the whole packet to the SIM card.
- The *User Data Header* comprises a concatenation of tag, length and value (TLV) fields which describe the optional features that should be applied to the attached 140 bytes of user data. Of interest to our proposal are tag values $0x00$ and $0x70$, meaning Concatenated SMS and SAT Security respectively.
  - The concatenated SMS tag allows up to 255 SMSs to be concatenated. It is reported [13] that most operators limit this to approximately five, because of uncertain and indeterminate device operation when receiving larger numbers of SMS messages to be concatenated. Five messages represents a total payload of 5x140 = 700 bytes [18].
  - The presence of the SAT Security tag ($0x70$) indicates that the message contains an additional header, the *Command Header*, prior to the *User Data Header*. This comprises of 9 fields which define how the User Data is secured by:
    * specifying the cryptographic functions,
    * providing a replay protection counter,
    * quoting the sender's cryptographic integrity value for the secured *User Data Header*.

Through the use of this SAT Security mechanism it is possible to provide confidentiality and integrity services for up to 700 bytes of user data, when the data is sent between the Mobile Operator application server and the SIM card. Performance and payload are limited and applications are restricted.

2.2 SIM Application Toolkit

The SAT API allows an application on the SIM card to be informed of events by, and to issue commands to, the host mobile device. When an information flow is initiated to the SIM application, it is termed an event download, and when an information flow is initiated from the SIM application it is termed a proactive command. Using the proactive command SET_UP_EVENT_LIST, the SIM application can register to be informed of a number of events via the ISO/IEC 7816-4 ENVELOPE APDU command [8]. Of relevance to this paper is the SMS_PP or CELL_BROADCAST event, which downloads the contents of the received SMS to the SIM application as a compound TLV in the data field of an ENVELOPE APDU [13]. The SIM application's response to the ENVELOPE command is then returned to the sender in a response packet.

2.3 MIDP2.0 J2ME Runtime Environment

A Java application that runs on a Mobile Information Device Profile (MIDP) 2.0 device is known as a MIDlet and may be installed within a certain domain if

it complies with the domain-specific access control requirements [6]. There are 4 domains specified for GSM compliant devices:

- Untrusted,
- Trusted 3rd Party,
- Mobile Operator,
- Manufacturer.

A Domain Protection Root Certificate (DPRC) controls MIDlet access to a domain. The DPRC must be made available at a specified location in the SIM application [15]. The MExE [2] security framework, when making an access control decision relies on signature verification of the signed MIDlet using the public key contained within the DPRC. Successful verification of the digital signature allows the MIDlet to be installed into the appropriate domain of the device.

Any MIDlet within a domain enjoys a set of unique permissions provided by that domain. The permission model allows these installed MIDlets access to restricted and sensitive APIs. The Security and Trust Services API [16] specifies that access to three of the four defined packages is limited to MIDlets located within the operator domain. These packages are:

- SATSA–APDU
- SATSA–JCRMI
- SATSA–PKI

These provide the ability for MIDlets to access trusted elements (i.e. a SIM card) using APDU communication, invoke a method of a remote Java Card object and provide support for digital signatures and credential management. It is worth nothing the value of being able to process cryptographic functions upon the device, as well as the smart card, as the card is a constricted environment [19].

2.4 UICC Java Card SIM Cards

The Global Platform specification [10] is the industry standard interface for downloading applications and is the most important international specification for application management in multi-application smart cards [11, 21]. This standard allows card issuers to securely manage third party applications independently of the operating system provider. Mobile Operator are increasingly deploying UICC [3] Java Cards, where the SIM application [4] is just one of the possible java applications [9] that the card is capable of running. Java applications that run on smart cards are known as Applets. A Card Manager is responsible for ensuring that new Applets are integrity checked and their source authenticated prior to installation. This security service uses a secret key, K_{CI} that is embedded in the smart card prior to issue and termed the Card Issuer Key. Although a UICC SIM card can execute multiple Applets from different providers, the Card Manager application will be owned by the Mobile Operator who actually owns and issued the physical card.

3 The Proposed Scheme

Consider the scenario of having the requirement to remotely deploy our *Security Agent* to Mobile Stations in the field. The device is capable but unprepared; this section introduces the proposed scheme to install the *Security Agent*. This is again described as a protocol in section 4 and is represented in Fig. 1. The scheme is preparation for the execution protocol, detailed in section 5 that establishes session keys for future communication.

1. A small SAT application is securely installed OTA to the SIM using the TS03.48 mechanism.
2. The SAT application uses the proactive command SET_UP_EVENT_LIST to register to be informed, via the ISO/IEC 7816-4 `ENVELOPE` APDU command [8], when a SMS_PP or CELL_BROADCAST event occurs.
3. A corresponding SMS_PP or CELL_BROADCAST is sent to the device. The DPRC is contained within the payload of a of the concatenated SMS messages.
4. The device transfers the payload to the SAT application as a compound TLV in the data field of an `ENVELOPE` APDU command. The DPRC is stored in the appropriate location of the UICC SIM Card [15].
5. The SAT application retrieves the SIM's unique identifier, and returns it to the device as the response to the `ENVELOPE` command.
6. The unique identifier is then returned to the Mobile Operator application server. This acts as a proof of delivery of the DPRC and enables the Mobile Operator application server to reference the card's secret key K_{CI} and commence the MIDlet preparation and download process.
7. Using the SIM's unique identifier, the Mobile Operator constructs the appropriate *Security Agent* MIDlet containing the relevant install commands and

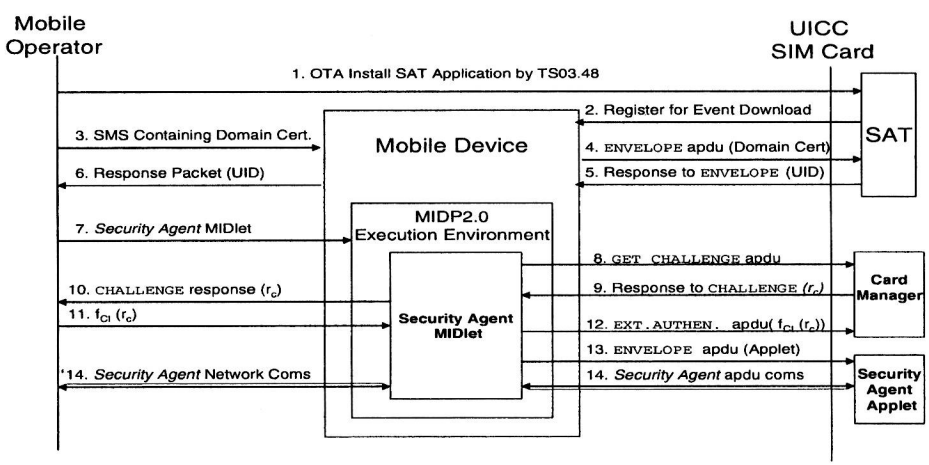

Fig. 1. Installation Scheme