Digital Forensic Analysis of SIM Cards

Mohamed T. Abdelazim, Nashwa AbdelBaki, Ahmed F. Shosha
Information Security Department, CIT School, Nile University, Cairo, Egypt

Abstract—Smart cards are fundamental technology in modern life. It is embedded in numerous devices such as GPS devices, ATM cards, Mobile SIM cards and many others. Mobile devices became the evolution of technology. It becomes smaller, faster and supports large storage capabilities. Digital forensics of mobile devices that maybe found in crime scene is becoming inevitable. The purpose of this research is to address the SIM cards digital forensics analysis. It presents sound forensic methodology and process of SIM cards forensic examination. In particular, the main aim of the research is to answer the following research questions: (1) what forensic evidence could be extracted from a SIM card and (2) what are limitations that may hinder a forensic analysis?

Keywords: SIM Cards; Smart Cards; Mobile Digital Forensics; SIM Card Forensics;

1. Introduction

Mobile forensics has become a rapidly important forensic domain, since mobile phones have become a common source of digital evidence. Nowadays, smart phones, tablets, and smart cards contain a large information storage with increasing capabilities [1] which provides an extensive source of information that could leverage forensic analysis and investigation.

Unfortunately, it’s a common knowledge that criminals don’t prefer using smart phones, because it can easily be tracked using different methods. As such, they may prefer to use prepaid phones known as “burner phones” or simple non-smart phones. Although, recent reports that Law Enforcement are confronted with criminals and terrorists that are increasingly using different smart phone models and Law Enforcement are facing difficulties decrypting digital evidence residual in those phone without the phone manufacturing support. This doesn’t mean that forensic analysis of non-smart phone is an obsolete domain. In fact, SIM cards forensic is a fundamental activity in any mobile phone forensics, and Law Enforcement are regularly in a situation where it is required to extract basic information from a phone SIM card.

The existing techniques, methods, software (including commercial or open source) in mobile phone forensics are focusing on the analysis of smart phones. For example, extracting artifacts of applications installed on the mobile operating system, i.e. Android or IOS; however very limited research addressing the forensic analysis of Mobile phone hardware or SIM card. In particular, SIM card forensics is disclosed forensic area, and currently limited to a set of commercial applications that could extract limited forensic artifacts. SIM cards are the gateway between the mobile phones and the network, they store information that could be used for reconstructing user’s activities, such as phone book, incoming and/or outgoing calls, sent and/or received messages, message’s timestamps, when the user power off or on his/her device, etc.

The main aim of the proposed research is to address the digital forensics aspects of SIM cards and providing open source library to support extracting sound forensic evidence from a SIM card. More importantly, the research attempt to answer the following questions: (1) what information could be stored in SIM cards, (2) what can be extracted and/or recovered to assist a forensic investigation, (3) and limitation of SIM cards forensic analysis.

The paper begins with a brief introduction about Smart phone forensics, Smart cards and SIM cards, in section Two. Section Three describes the forensic analysis methodology of SIM cards. Section Four addresses the methods and protocols that would enable communication with SIM cards and the SIM card’s file system structure. In section Five, the method to forensically acquire SIM cards is presented, and section Six presents the SMS forensic analysis methods. In section Seven, a Proof-of-Concept implementation for extraction of forensic evidence from SIM cards is introduced, and sample experiments on different SIM cards models are presented. Finally, the last section presents the research conclusion, limitations and draws the future work. In summary, the research contributions are the following:

- Review of SIM card structure and required development environment.
- Review of SIM card file system, identifiers types and structure.
- Listing of communication methods with a SIM card.
- Forensic method that allows extracting of digital evidence from a SIM card.
- A proof of concept implementation for the proposed forensic methodology.
- Forensic timeline analysis recovered messages from SIM card.

2. Overview and Backgrounds

SIM cards analysis is not a new research, however, it’s a disclosed research and very limited information about
it are publicly available. The earliest SIM cards forensic analysis research is presented in [2] where the SIM file system structure and data residual in a SIM card were briefly discussed. Other published research proposed set of forensics tools such as [3], [4] and SIMBruch presented in [5]. However, those tools only focused on extracting the basic information from a SIM card and didn’t provide clear description about the forensic techniques used to extract an evidence from the SIM card.

Moreover, the current available public forensic tools for SIM card analysis are not updated, and some of those tools are depending on the presence of specific currently unsupported hardware such as SIM readers compliant to PC/SC specification [6]. Because of those limitations, this research aims to provide an updated implementation that support extraction of digital evidence from modern SIM card models. Also, the proposed implementation is hardware agnostic and it communicates with a SIM card using the standard communication protocol. This will allows forensic researchers and/or Law Enforcement to use and extend the proposed research without having relied on a specific SIM hardware readers.

2.1 Smart Cards

Smart Cards are considered standalone embedded systems, where SIM cards are a subset of smart cards. Smart card’s architecture are consists of EEPROM, FLASH, and processor that could be used to store information or execute operating system [7]. In addition, the design of smart cards allows user applications to be developed and installed on the cards using Java card language [8].

In general, smart cards have three different types: Contact Cards, Contactless Cards, and Hybrid Cards [9].

- Contact Cards: This type requires direct contact with another hardware to exchange information and to read the information stored inside the card, such as credit cards, debit cards or loyalty cards [10].
- Contactless Cards: This type does not require any direct contact to any hardware. These cards communicate using RF protocol, wireless, or Bluetooth such as employee ID cards [11].
- Hybrid Cards: This type of cards is able to use both methods of communication either by direct contact or not, such as smart RFIDs, some credit cards models, and fingerprint cards [12], [13].

2.2 SIM Cards

SIM cards are contact cards. It is present in every mobile phone, and originally developed for secure communication and GPS devices. Unfortunately, SIM cards are becoming one of the main attack vectors that enable a remote access control over the device and to turn a mobile phone to a listening device and record the user’s conversations and/or to steal personal information [5], [2].

SIM cards could be accessed using the operating device or using external reader. It is considered very important in the mobile forensics process. It can be used to hide information or lock the mobile, which will make the mobile investigation harder, and can delete some information from the device at removal.

2.3 Development Environment

SIM cards development environment depends on Java technology known as Java card. Java card is structured to three main components [14]:

- Java card virtual machine: used for application installation and defining the features and services.
- Java card run-time: which handle context switching between applications.
- Java card API: which is a set of classes and interfaces to allow the application to use card services.

Java cards inherit the security from Java programing, this environment allows multi-application to be installed and run, which allow developing application or even malwares [15].

3. Methodology

In this section, the forensic analysis methodology applied in this research is presented in figure 1. It begins with data...
acquisition where the forensic data is extracted from the SIM using serial communication. In this stage a forensic write blocker is used to prevent any accidental attempt to tamper the SIM card file system or files’ content and to ensure a sound forensic analysis.

In the second stage, the acquired SIM card data is interpreted. This includes extracting the SIM file system and interpreting the file system structure for analysis.

In the third stage (aka. data analysis stage), forensic evidences were identified and highlighted. This includes for example, identifying files that contain the user phone book or incoming calls list, etc.

The final stage represent the forensic event reconstruction, where digital evidences are presented in timeline representation to assist forensic investigator to develop an understanding of the identified evidence context, reconstruct user behavior on the phone, and recover (or at least identify) evidence that may have deleted from the SIM card.

4. SIM Communication

Smart cards use two types of communication. (1) Application Protocol Data Unit command (APDU) that executes commands on binary level. (2) \texttt{AT} command, that is used to communicate with the SIM on the application level using well defined interfaces.

GSM communication protocol provides a set of well defined APIs to extract information from SIM cards. In particular, there are two possible methods for data extraction using (1) \texttt{AT} command or (2) accessing a memory address on a binary format. The back-draw with the later method is that not all memory addresses are available to be accessed, as SIM cards specification provides a set of restrictions and limitations on the executed command [16].

4.1 SIM File Identifier

SIM card file system consists of set of files in binary format. Figure 2 desrcies sample of SIM file system tree where there are three types of file identifiers [17]:

- Main Files (MF) that resides at memory address \texttt{0x3F00}. MF are considered the root directory for SIM file system.
- Dedicated Files (DF): it represents the application level for each service provided by SIM such as directories.
- Elementary File (EF): it holds the actual information which needs to be extracted for digital forensics.

Each type of file identifiers is consisted of header and body. All file identifiers have headers which hold the file size, permission access which could be summarized as five permissions [4], data storage type, and file ID. However only EF file has body which contains the actual data. Elementary files (EF) has mainly two types of data storage (1) Plain data where the date is stored under the EF file, which can be accessed by EF ID and file size; (2) List (records) where the data is stored as list (array), which can be accessed by record ID and record size.

5. Data Acquisition

SIM card forensic acquisition can be achieved by two methods (1) physical or (2) logical acquisition. In physical acquisition a bit-by-bit forensic image of SIM memory is acquired for analysis. In the logical acquisition, the SIM data structure, i.e. file system structure and content is extracted and parsed for analysis. In this research, logical forensic acquisition method is used. This will be enabled by extracting forensic data from a SIM card in native format and interprets it for forensic analysis. In the following we will present information that could be extracted from a SIM card:

- Integrated Circuit Card Identifier (ICCID): Each SIM is identified by a unique integrated circuit card identifier internationally. ICCID length is defined by GSM as 10 octets (20 digits). The address of EF file containing this information is \texttt{0x2FE2}.
- International Mobile Subscriber Identity (IMSI): Each SIM has a unique identifier on each individual network provider. IMSI size is 15 digits and its EF file located at address \texttt{0x6F07}.
- SIM operation mode: there are three operation modes which are, data, fax class 1, and fax class 2. Most SIM cards are operating in Data operation mode. Using \texttt{AT+FCLASS?} command we can retrieve the SIM operation mode.
- Service Provider Name (SPN): SP is the name of the service provider where the SIM is registered. The size is defined by GSM standard as 17 bytes. The EF \texttt{EF\_SPN} file holds this information located at address \texttt{0x6F46}.
- GSM Ciphering Key(Kc): Kc is one of two keys used to authenticate with GSM networks. This key is used...

Fig. 2: SIM File System Structure
along with Ki to perform the handshaking protocol. The key can be recovered from address 0x6F7E.

- SIM Service Table: This file EF_SST indicates which services are allocated or activated. Each service is constructed with two bits, the first bit indicates if the service allocated or not; “1” means allocated, “0” means not allocated. The second bit indicates if the service activated or not; “1” means activated, “0” means deactivated [16].

- Short Message Sent (SMS): To read SMS saved within the SIM we can use API AT+CMGL provided by GSM protocol. This command will return all the SMS within the SIM in hex format. SMS is considered point-to-point communication protocol. There are two types of SMS, first is data SMS which contains normal text, second data download SMS, which contains instructions or executable code to be executed on the SIM. After executing AT command to read the stored SMS on the SIM card, the result execution status code could be 90 00, 91 xx or 7F xx. In case of 90 00 or 91 xx then this means that the current record is data SMS and the user will get notification. In case of 7F xx then the current record is SIM data download and the user will not get a notification for this SMS. SIM data download messages are sent directly to be executed by SIM card.

Other Information like PIN key state, and phone operation mode also could be extracted with a specific API which we will demonstrate later.

6. SMS Forensics

Short Message Service (SMS) is essential artifacts in mobile phone forensics, by developing a solid knowledge about the SMS data structure and how SMS is stored in the SIM card, forensic analyst can use it to reconstruct a human activity in a mobile phone subject for forensic investigation. Each SIM card contains limited number of memory locations, commonly it uses 40 locations with length size of 176 bytes each to store incoming or outgoing SMS. Each location structured in two parts: (1) records the status that is defined by its first byte of the record, indicating if the record is used or free. (2) Message’s data; which holds the rest of the record with maximum size of 175 bytes.

Each SMS location initializes the first byte with “00” and the rest of the record with “FF” indicating unused location, at the point of incoming or outgoing new message, the message is stored in the first available free location. At the time of message deletion, the assigned record is reset to its initial value removing any trace of the original message.

By knowing that each message is marked by a timestamp and its stored location index, messages timeline construction can be achieved by providing time frame for received, sent, deleted, or overwritten messages which will be demonstrated later on[18].

7. SIM Card Forensics Proof-of-Concept

In this section, PoC to extract artifacts from a SIM card for forensic analysis purposes is developed. It allows extracting the basic information from the SIM subject for analysis, given into consideration to avoid any usage of write commands. This will ensure a sound forensic analysis and will avoid tampering with a SIM card as digital evidence. The PoC is developed based on the GSM communication protocol standard.

The developed software communicates with SIM card using serial communication. API interfaces is developed that can be used to extract certain pieces of information or for full data extraction using python programming language. It initiates a communication to the SIM card that allows executing a stream of AT commands on the SIM. By using AT commands we can avoid the need for having reader compatible with PC/SC specifications even using USB modem can achieve the same results.

The developed software extracts several valuable forensic artifacts, such as: saved contact lists, SMSs, the card identifier, service provider, part of the GSM location information, card service table, and many other information[19].

To ensure correctness of the PoC, a number of experiments are conducted using different SIM cards models that operates under different service providers, including one SIM card that is un-allocated to any service provider. The experiments are presented and results are explained, as follows:

7.1 Case 1.a:

In this experiment, we used operational SIM card working for several years in attempt to identify user activities and extract stored SMS. As such, we been able to extract raw date for valuable forensic information and interpret it as follows:

(1) Extracting the EF_LOCI that holds Temporary Mobile Subscriber Identity (TMSI), (2) Location Area Information (LAI), (3) TMSI TIME, and (4) Location update status. The EF_LOCI file size is “11” bytes. Using the AT commands to read the EF_LOCI address AT+CRSM=176, INT(0x6F7E), 0, 0, 11, it resulted the following:

CRSM:144,0,"5CD749D162F2201CDE000",OK

Another successful attempt to extract SIM service table using AT+CRSM=176, INT(0x6F38), 0, 0, 14 and SIM card response with the following:

CRSM:144,0,"9EEF19CFF3E000000FFFFFFFFFF",OK

In addition, we were able to extract the contact list saved on SIM card using AT+CPBR=<param1>, <param2>
command, which reads the phone book starting from `param1` to `param2`. SIM cards can hold about 255 record and using `AT+CPBR=?` we can get phone book properties, such as: how many records can be stored on the SIM, the maximum number of digits for each number, and the maximum number of character for each text. Below, a sample of the results:

1) Name: "Luck", Number: "01004677080"
2) Name: "Cris", Number: "01006059135"
3) Name: "Jaky", Number: "027180749"

Another extremely valuable forensic information to extract is "pin key status" for PIN1 and PIN2. This is enabled using `AT+CPIN?` that can be used to return the state of PIN1 key and `AT+CPIN2?` and get the state of PIN2. SIM operation mode can be extract using the same method. Below, a sample of the results:

Pin 1: READY
Pin 2: Not Found!
Operation Mode: Data

Another information that can be extracted is the SIM CCID and IMSI. This is enabled using `AT+CRSM=176, int(0x2FE2), 0, 0, 10` for CCID and `AT+CIMI` for IMSI, as follows:

CCID: 89**************385F
IMSI: 602**********385

For SMS forensic extraction, saved messages can be extracted using the following `AT+CMGL=4` command which will list all the messages including message header information and message content, as follows:

Message ID: 4
Message State: received read messages
Length: 30
Content: 0791021197002864640ED0457A7A1E6687E90008510101211471800A050037805050629029

SIM service provider name can also be extracted using the below code: `AT+CRSM=176, int(0x6F46), 0, 0, 17` for CCID and `AT+CIMI` for IMSI, as follows:

SIM CCID: 89**************052
SIM IMSI: Not Found!
Service provider name: ****
Operation Mode: Data

Based on the above experiments, one essential finding can be determined, in which is having non-registered SIM card does not refute the potential of having forensic artifacts, and necessity of investigating blank SIM card as it may contain valuable information.

7.2 Case 1.b:

In this experiment, a brand new SIM card is analyzed. The SIM does not contain any phone book records. Thus, we been able to extract limited raw data for some information and interpret it, as below: The SIM CCID, IMSI number, the stored SMS, operation mode, and PIN status were successfully extracted. However, SIM service table couldn’t be extracted. Below a sample of the resulted data:

Message ID: 9
Message State: stored unsent messages
Length: 22
Content: 07910221020020F0110000000000A81049503B30F83F2E6FA0B04028164

SIM CCID: 892**************213
SIM IMSI: 602**********941
Service provider name: ****
Operation Mode: Data

7.3 Case 2:

In this experiment, we used a blank card that was not activated with a service provider. Following, fabricated data, such as some phone book information, SMS information have been inserted and were forensically extracted. Since, the SIM was not registered to any service provider, the service provider name was set to the default value "FF", and fabricated data was correctly extracted. Below, a sample of the extracted data:

SIM CCID: 898**************0529
SIM IMSI: 460**********34
1) Name: "test name ", Number: "545465465"
2) Name: "SOS", Number: "112"
Message ID: 1
Message State: received read messages
Length: 25
Content: 00040681218564005090723151808A0AF37215407CDDF6F37
Operation Mode: Data
Service provider name: None

Based on the above experiments, one essential finding can be determined, in which is having non-registered SIM card does not refute the potential of having forensic artifacts, and necessity of investigating blank SIM card as it may contain valuable information.

7.4 Case 3.a:

In this experiment, a new SIM card that is locked with PIN key is analyzed. In this case, if the mobile phone restarted or powered off, user will not be access the SIM until a PIN key is entered. Below, a sample of the extracted information:

PIN Status: SIM PIN
SIM CCID: 89**************052
SIM IMSI: Not Found!
SIM Service Table(SST): Not Found!
Service provider name: ****
Operation Mode: Data

Based on the above output, we can conclude that essential information such as: IMSI, SST, phone book, and SMS are protected when PIN key is set. Thus, to allow extracting forensic artifacts from a SIM card, it’s essential to disable the set PIN key, otherwise forensic acquisition using this method will not be successful.
7.5 Case 3.b:
To ensure Case 3.a finding and conclusion, the same SIM card with PIN key disabled is forensically examined, and below is sample of the results:

SIM CCID: 894************052
SIM IMSI: 262*********205
1) Name: "M*****x", Number: "********"
2) Name: "Ta*******n", Number: "****"
3) Name: "Ko******er", Number: "****"
Message ID: 1
Message State: received read messages
Length: 159
Content: 0791947107160000040C91947107075200001251017060859080A0D7349BD7EB7DB6537485C4E83C4EC70DD452E87406276B...
Service provider name: ****
Operation Mode: Data
PIN Status: READY
SIM Service Table (SST): 9E3B140C27FE5DF85F888888

We can conclude that if SIM PIN key was disabled, a forensic analyst will be enabled to extract SIM content for analysis such as: IMSI, contact list and SIM service table.

7.6 Case 4:
In this experiment, we are using the SMS forensic information we have previously examined to construct SIM activities timeline. The experiment shows that each new SMS message is stored at the first empty location, where each SMS has its timestamp which was originated with the message. Using these two findings, we can reconstruct some of the SIM activities and provide timeline of the messages received. The experiment was conducted over operational SIM cards and different mobile phones (burner and smart phones) with few SMSs saved in an attempt to build timeframe of saved and/or deleted messages.

1) SMS in Smart Phones: Using operational SIM card placed in a smart phone, it was possible to extract messages received from entities such as: service providers and Banks, some advertisers, etc. However, user sent messages, were saved on the smart phone internal memory, not in the SIM card. Based on SMS timestamp, figure 3 displays received messages by its timestamp and the SIM storage index.

2) SMS in Burner/Non-Smart Phones: Using a burner or non-smart phone with operational SIM card, it is possible to extract, not only, the service provider messages, but also, the user messages received from other users. This emphasis the importance of SIM card forensic, in case of investigating non-smart phones; As in this case SIM cards may only be the viable digital evidence source.

Figure 3 explains PoC of the timeline representation for the received messages where the experiment was conducted using operational SIM card with “40” locations available and few messages saved. The graph shows the number of received messages on a particular day represented by overlayed bars i.e. at timestamp 2015-10-10 12:41:17 which shows that seven messages have been received and stored at locations “6” through “12”.

Also the graph represents the possibility of the message deletion at a certain timestamp which is represented by “red circle” i.e. at timestamp 2015-12-11 17:36:32 locations “2” through “5”. The rest of the empty locations “26” through “40” at timestamp 2015-10-10 12:41:17 have one of two possible meanings, (1) These locations have never been used; (2) These locations have been freed.

7.7 Case 5:
In this experiment, we are extracting the headers of the files by scanning the SIM address space starting from 0000 to FFFF using the GET RESPONSE command with instruction ID 192:

AT+CRSM=192,INT(File_ID),0,0

Below, a sample of extracted raw file header:

File ID: 6f38, File Header: 0000000A6F3804001BF
250 Int'l Conf. Securit

SMS timestamps and stored indexes, forensic analyst could

Limitation and constrains also were presented.

a SIM card, such as: SMS, phone book and card CCID.

a forensic analyst could extract vital forensic artifacts from

extraction were explained. The research demonstrated how

the communication methods that would enable forensic data

after the last stored SMS message, where there could be

currently possible to determine or confirm user activities

can't be recovered using the proposed approach in this

brute forcing the PIN key.

attempts to enter the PIN key, which hinder the method of

SIM card for forensics purposes will not be available using

in addition, most of SIM cards have only three

SIM card with the user’s messages, however deleted messages

is possible to identify if message(s) have been deleted or

overwritten. Also, the content of saved SMSs on the SIM

can be extracted.

The current ongoing research is to extend SMS forensics
to include messages sent from the mobile known as “USSD
codes” or the commands sent to the mobile known as “push
messages”, and investigating the file identifier header is also

essential which may allow bypassing PIN through changing

the file permissions in the header. Also, it may shed the light

on methods that might be used as an attack vector to install

malware on a smart phone.

8. Findings and Limitations

In this paper, the method and protocol to communicate

with SIM card for forensic analysis purposes is explained.

This includes, what information could be extracted, and how
to extract it. A proof-of-Concept implementation was also

introduced to automate the investigation and assist forensic

analysts. However, the developed software is confronted with

some limitations; Most notably, SIM cards that are protected

with PIN key. If it is active, extracting information form the

SIM card for forensics purposes will not be available using

this method. In addition, most of SIM cards have only three

tries to enter the PIN key, which hinder the method of

brute forcing the PIN key.

Although SMS messages can be extracted from the SIM
card with the user’s messages, however deleted messages
can’t be recovered using the proposed approach in this
research, which is an essential requirement in forensics
analysis. Another limitation to the current method, it is not
currently possible to determine or confirm user activities
after the last stored SMS message, where there could be
another messages received and deleted, the same scenario
also applied for the first recorded message.

9. Conclusion

In this research, SIM cards, SIM file system structure, and
the communication methods that would enable forensic data
extraction were explained. The research demonstrated how
a forensic analyst could extract vital forensic artifacts from
a SIM card, such as: SMS, phone book and card CCID.
Limitation and constrains also were presented.

SMS are core artifacts in forensics investigation. Using
SMS timestamps and stored indexes, forensic analyst could

construct a timeline for the SIM activities. In particular, it
is possible to identify if message(s) have been deleted or
overwritten. Also, the content of saved SMSs on the SIM
can be extracted.

The current ongoing research is to extend SMS forensics
to include messages sent from the mobile known as “USSD
codes” or the commands sent to the mobile known as “push
messages”, and investigating the file identifier header is also

essential which may allow bypassing PIN through changing
the file permissions in the header. Also, it may shed the light
on methods that might be used as an attack vector to install
malware on a smart phone.

Table 1 shows some of the byte representation for 15
bytes header. It differentiates between EF, DF and/or MF
files and identify the data structure for EF files which allows
extracting the raw data.

| Table 1: File Header byte mapping |
|-------------------|------------------|
| **Byte Number**   | **Description**  |
| 1-2               | Null bytes       |
| 3-4               | File Size        |
| 5-6               | File ID          |
| 14                | File data structure which differentiate DF and EF |
| 15                | Record Size (length) |

References

tool testing: A database driven approach,” International Journal of
subscriber identity modules,” in Proceedings of the Conference on
forensic sim tools,” in Security Technology, 2007 41st Annual IEEE
overview,” International Journal of Digital Evidence, vol. 5, no. 1,
[7] “Digital cellular telecommunications system (phase 2+); subscriber
identity module application programming interface (sim api) for java
card,” European Telecommunications Standards Institute, France,
2010.
Areas in Communications, IEEE Journal on, vol. 24, no. 2, pp. 381–
394, 2006.
[12] G. Koyanakis, “Contactless or hybrid contact-contactless smart card
designed to restrict the risks of fraud,” May 21 2002, uS Patent
6,390,375.
/getstarted-1970079.html
[15] “Digital cellular telecommunications system (phase 2+); specification
of the subscriber identity module - mobile equipment (sim-me)
interface, 3gpp ts 11.11,” European Telecommunications Standards
[16] “Universal mobile telecommunications system (umts); characteristics
of the usim application,” European Telecommunications Standards
[17] “Digital cellular telecommunications system (phase 2+); technical
realization of the short message service (sms) point-to-point (pp),”
European Telecommunications Standards Institute, France, Standard,