

Prism 3G uSIMetrix Overview

The Prism 3G UICC and USIM range

Prism Confidential

www.prism.co.za



Notice of Confidentiality

Please note this document has been prepared exclusively by Prism for the sole purpose of affording the intended recipient the opportunity to understand and evaluate the various competencies, technologies and solutions that Prism has to offer within the SIM space.

While we wish to present our credentials, products and services at the appropriate level of detail, please be advised that this document, as well all the information it contains, is strictly confidential to Prism Holdings Ltd. and to authorised staff of the intended recipient's company and its associated group companies.

Accordingly, access to this document in all its printed or electronic formats, use of the document, and any copying or dissemination of the document, is restricted exclusively to authorised personnel of the intended recipient's company and its associated group companies and relevant Prism employees.

In accessing this document, the intended recipient warrants that the information contained herein will be treated as confidential and that no content of any nature will be shared with any third party or unauthorised staff.

Thank you.

Table of Contents

1.	Introduction	5
2.	Key benefits and features of 3G USIM:	6
3.	UICC, USIM and SIM revisited	7
3.1.	Comparing SIM to USIM	8
3.1.1.	File Structure	8
3.1.2.	The USIM application.....	9
3.1.3.	An example: Prism 3G PhoneBook	10
3.1.4.	Access conditions.....	11
4.	The impact of UICC and USIM	12
4.1.	EEPROM Memory	12
4.2.	PIN Definitions	12
4.3.	The authentication algorithm.....	12
4.4.	WIB1.2 and WIB1.3	12
4.5.	3GPP USAT Interpreter	12
4.6.	Java and J2ME.....	13
5.	UICC - Benefits and Challenges	14
5.1.	Benefits of UICC	14
5.2.	Challenges of UICC	14
6.	Conclusion	15
	Appendix – Specifications Annotated	16
	Contact Us	18

Abbreviations

2G	Second Generation
3G	Third Generation
3GPP	Third Generation Partnership Project
ADF	Application Dedicated File
ADN	Abbreviated Dialing Numbers
BIP	Bearer Independent Protocol
CAT-TP	Card Application Toolkit – Transport Protocol
DF	Dedicated File
DRM	Digital Rights Management
EF	Elementary File
GSM	Global Standard for Mobile Communications
ICC	Integrated Circuit Chip
IMSI	International Mobile Subscriber Identity
ME	Mobile Equipment
OTA	Over The Air
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SMS	Short Message Service
STK	SIM Toolkit
UICC	Universal ICC
USAT	Universal SIM Application Toolkit
USIM	Universal Subscriber Identity Module
WAP	Wireless Application Protocol
WIB	Wireless Internet Browser
WIM	WAP Identification Module

1. Introduction

This document provides an introduction to Prism 3G uSIMetrix from the Mobile Network Operator's perspective. It supplies general information on UICC and USIM technology and it further presents perspectives from both the business and technology benefits viewpoints. Through the use of an example, the Prism 3G USIM Phonebook capabilities are discussed. In order to fully understand this document, a basic knowledge about 2G SIMs and GSM 2G profiles is necessary.



2. Key benefits and features of 3G USIM:

- A platform independent SIM and USIM allows for multiple applications to be built with ease
- A UICC configured with both SIM and USIM applications, supports seamless 2G, 3G network and handset compatibility (UICC is a smart card designed for multi-applications)
- UICC personalisation profiles are organised in such a fashion to enable simple configuration
- Strong anti-cloning protection using the advanced Milenage algorithm, and supports re-configuration of algorithm parameters
- Supports 2G authentication via 3G USIM
- Global or application specific phonebooks can be considered
- Phonebook entries can be hidden/unhidden
- Multiple IMSI's or phone accounts are simply supported
- Shared files between SIM/USIM can allow for efficient EEPROM memory use
- Optimised access condition structure promotes EEPROM memory efficiency
- Memory de-fragmentation becomes a USIM feature by default due to file sharing
- Global or Local PINs supported for UICC applications
- OTA, post issuance re-personalisation possible i.e. CREATE FILE, RESIZE 102.222
- UICC suited to JavaCard/Global platform (but not required by default)
- Multiple 03.48 security channels to suit multiple ways of programming and accessing the USIM
- CAT-TP/BIP protocols could be useful for direct PC to USIM communications when supported in handsets.

3. UICC, USIM and SIM revisited

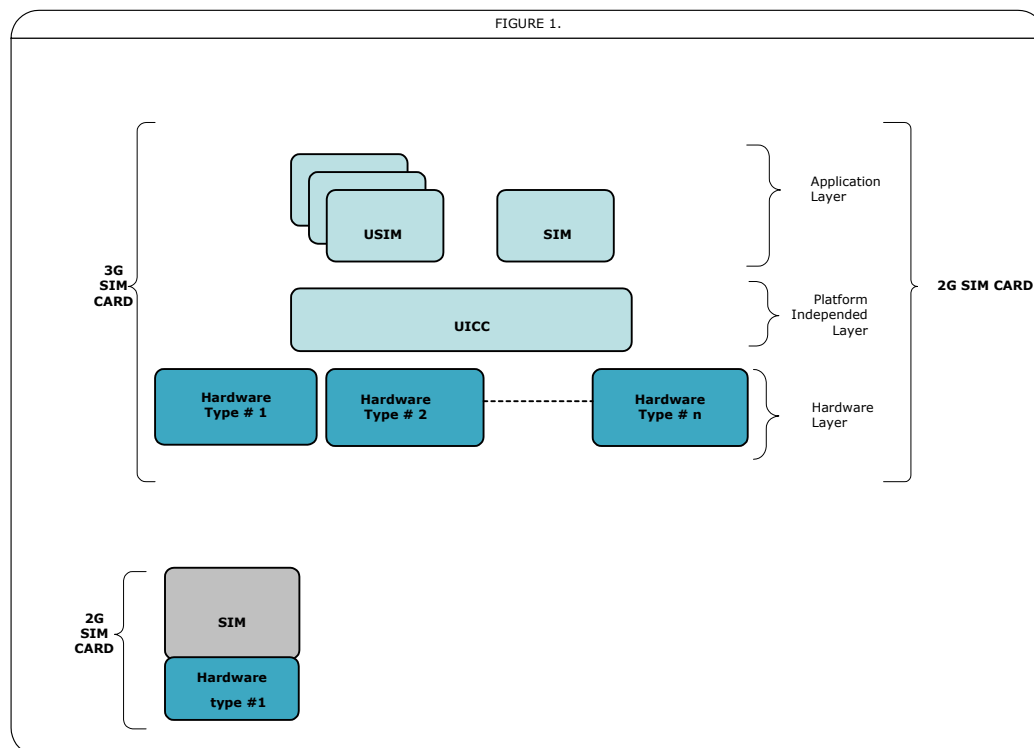
General definitions:

- **UICC:** the platform (O/S) on which applications may be built.
- **USIM:** the Universal Subscriber Identity Module application.
- **SIM:** the Subscriber Identity Module application (essentially the same as the GSM SIM). It runs on the UICC.

The most generic term for a smart card, i.e. a micro-controller based access module, is ICC. It is always a physical and logical entity and, in the context of this document, either a SIM or a UICC. The SIM is the ICC defined for 2G. The SIM was originally specified as one physical and logical entity, not distinguishing platform and application. In 3G, the SIM may also be an application on the 3G UICC, and then is only represented by its logical characteristics. If the SIM application is active, the UICC is functionally identical to a 2G SIM. The SIM application will only accept 2G commands. This is specified in GSM TS 11.11 / TS 51.011.

Unlike the SIM, the USIM is not a physical entity, but a purely logical application that resides on a UICC. It only accepts 3G commands and is therefore not compatible with a 2G ME. The USIM may provide mechanisms to support 2G authentication and key agreement to allow a 3G ME to access a 2G network (specified in 3G TS 31.102). The UICC is the physical and logical platform for the USIM. It does at least contain one USIM application and may additionally contain a SIM application. A Prism UICC contains both SIM and USIM applications. Furthermore, the UICC may contain additional USIMs and other applications, e.g. for mobile banking or mobile commerce purposes, if these fit with the basic physical and logical characteristics of the UICC (specified in 3G TS 31.101). Note that USIM and SIM do not interact, they can only share data.

The figure below represents the physical and logical abstraction of SIM and UISM on UICC.



In terms of 2G and 3G interoperability, the following can be concluded:

- 3G phone must accept a 2G SIM
- 3G SIM, in 3G phone, in 2G network must auth on 2G network
- 3G SIM, in 2G phone can use Milenage in 2G Authentication Center supporting Milenage
- 3G SIM will not work in a 2G phone, unless the SIM app is present

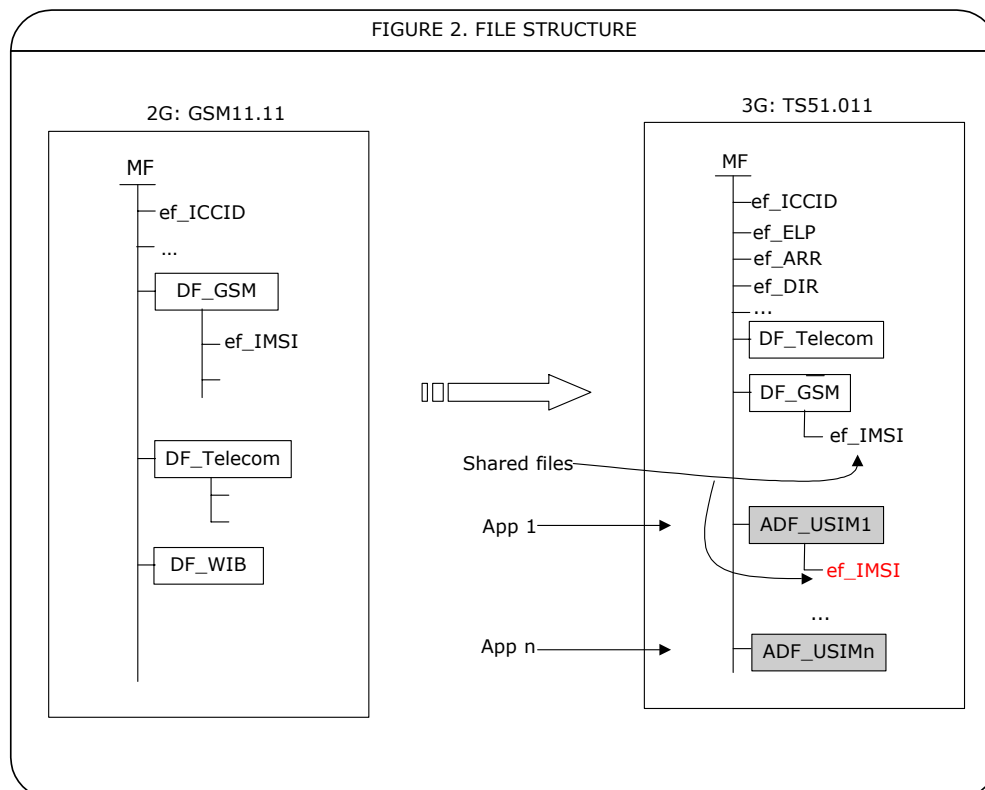
3.1. Comparing SIM to USIM

This section provides a technical description of the major differences between GSM11.11 and the TS51.011, namely the file structure, USIM application and the access conditions.

3.1.1. File Structure

For complete 2G-handset compatibility, the GSM11.11 file structure is replicated for SIM under USIM. In addition, the UICC/USIM file structure is added as indicated in the figure below. This permits multiple unique USIM applications to be configured with for example the same or different IMSI's. Each USIM application supports a Multi-record phonebook of 250 records x 250 bytes per ADN record. Hence, large phonebooks are easily supported since you can define as many ef_ADN files that are required.

The ef_DIR specifies all the applications present on the UICC i.e. a list of ADF's or USIM applications. The ef_ARR file specifies access conditions to all USIM files. SIM files still retain their access condition structure as per the 2G SIM specifications. Files between USIM and SIM applications can be shared by virtue of file pointers. This is a useful feature in memory - optimised profiles – which is common.

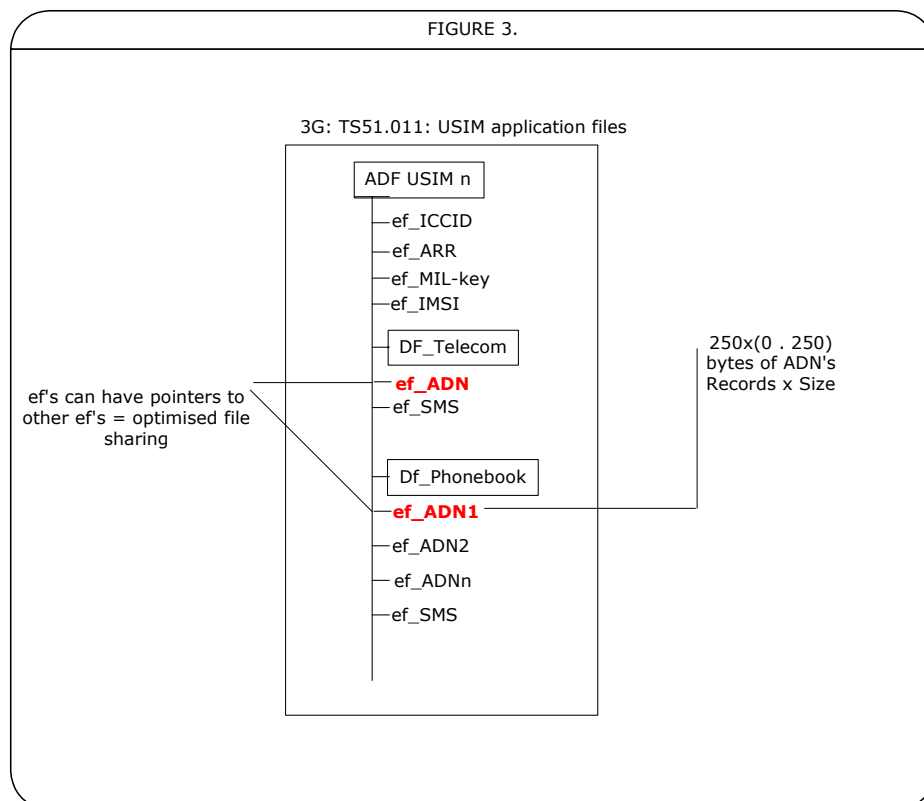


3.1.2. The USIM application

The UICC supports multiple application directories called ADF's in order to support multiple USIMs. For example a USIM can handle dual or N user accounts. Some useful points describing the capability of the USIM application are listed below:

- Subscriber authentication
- Phonebook:
 - Last active USIM app is selected on re-boot
 - Uniquely configured phonebooks of maximum 250x250bytes records each
 - Phonebook app supports multi-record entries:
 - a. x2 name fields per entry i.e. Chinese/English
 - b. xN numbers per entry, including email address
 - c. xN hidden entries
 - Can support 'group' creation – e.g. business numbers
 - Can support multiple groups
 - Note that some 3G handsets do not read all ef_ADN files, and only 250 records per ADN-file so for complete 2G backwards compatibility of ef_ADN's may require an additional STK/WIB/Java applet to manage.
 - Other phonebook features not in the USIM specifications may be useful:
 - a. Search for contact by character string i.e. "SUSAN"
 - b. Arrange frequently used numbers to appear at top of list
 - c. Auto reformat – name, surname, surname, name
 - d. Send multiple contacts to contact
 - e. Preferred number allocation

The figure below provides a good view of how USIM application files are structured:



3.1.3. An example: Prism 3G PhoneBook

The following presents an example of the Prism 3G USIM phonebook implementation or organisation and functionality. A USIM can support a Global or an application specific phonebook. All the phonebook files are personalised into the EF_PHONEBOOK directory of the USIM and configured.

For example:

- 1000 primary names and numbers
- 1000 secondary numbers
- 250 tertiary numbers
- 250 email addresses

To calculate 1000 names and phone numbers, you need 4 x 250 records.

Thus the phonebook will be stored as follows:

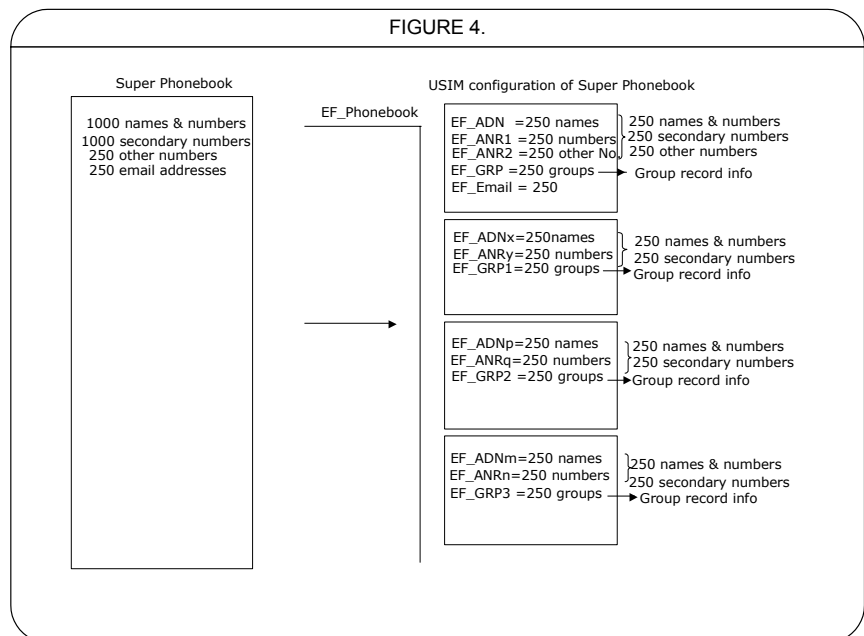
The first section will have:

- EF-ADN: 250 records. File record size restricted by GSM to 250. Note that this file will also be mapped to DF-TELECOM for 2G SIM compatibility.
- EF-ANR1: 250 records (2nd number record file i.e. matches primary ADN file)
- EF_ANR2: 250 other numbers
- EF-EMAIL: 250 records
- EF-GRP: 250 records (Grouping information file – contain same number of entries as ADNs)

The other three sections will have:

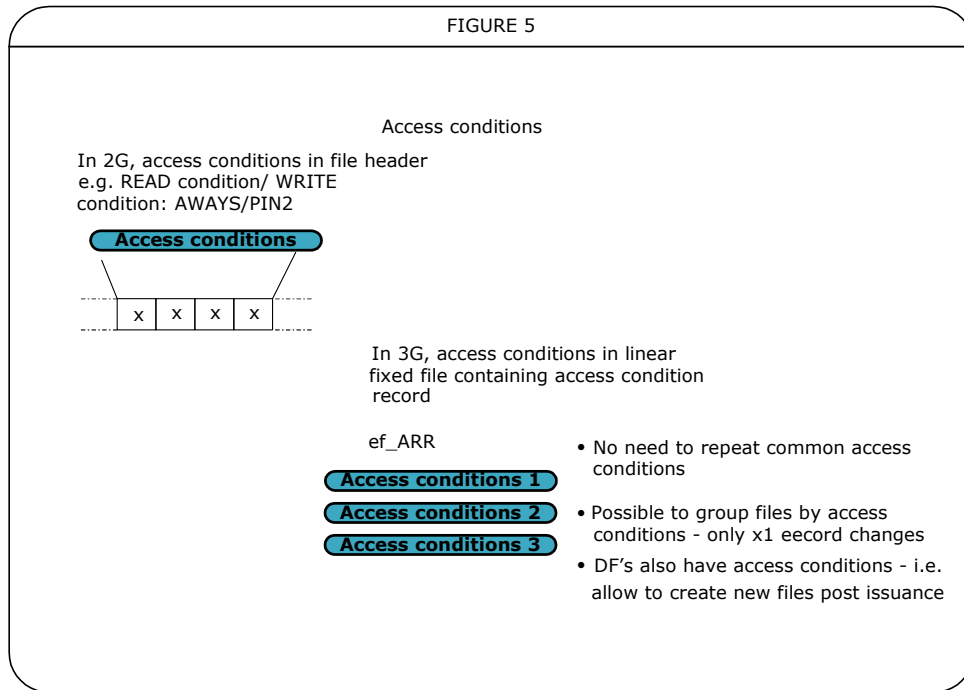
- EF-ADN2 250 records
- EF-ANR2: 250 records
- EF-GRP2: 250 records
-
- EF-ADN3: 250 records
- EF-ANR3: 250 records
- EF-GRP3: 250 records
-
- EF-ADN4: 250 records
- EF-ANR4: 250 records
- EF-GRP4: 250 records

Figure 41 3G Phonebook implementation:



3.1.4. Access conditions

Access conditions have changed; under 2G SIM, file access conditions were included in each SIM file header, whereas under USIM, access conditions are all grouped into one access condition file, called ef_ARR.



The memory optimisation benefits of ef_ARR are seen through sharing similar access conditions across multiple ef's. This means only one record needs to change to alter access conditions of all the associated group of files. DF's also have access conditions allowing one to alter or create new files post issuance.

4. The impact of UICC and USIM

4.1. EEPROM Memory

In UICC/USIM a DF or EF can easily be deleted, added or modified and the bulk of the EEPROM can easily be fragmented. The Prism mask therefore includes manual or auto de-fragmentation to cater for this issue:

- All DF's, EF's and java applets for example, stored as data objects with pointer references
- De-fragmentation achieved by moving data objects to be contiguous; following this internal pointers are updated as necessary
- When selecting a file, the object list is searched. Pointers to recently used files are cached, as are the internal identifiers main DFs, in order to improve performance. During defragmentation the file pointer caches are cleared
- Personalization turnaround time for static data improved
- This memory architecture make sit easy to begin to support encrypted profile images for the more security orientated profiles

4.2. PIN Definitions

On a UICC three types of PIN shall exist, namely the Universal PIN and the application PIN, as well as other types of PIN that shall exist on a UICC or application. This implies the following:

- 2G PINs are backwards compatible
- Multi-app card have separate sets of PINs for each applications
- PINs can be shared i.e. when a Global PIN is defined

4.3. The authentication algorithm

MILENAGE is the new algorithm set for authentication and key generation that is developed by ETSI's security algorithm group of experts (SAGE). Unlike GSM, security is no longer based on a single secret key, but multiple algorithms that are personalised by individual operators.

A typical 3G card is able to process Milenage algorithms much more rapidly than an average 8-bit SIM card. This is because the UICC is a multi-application platform and not a single application card like the SIM.

The recommended block cipher algorithm is Rijndael (AES). Milenage can be used to effect any comp128 algorithm authentication or challenge.

4.4. WIB1.2 and WIB1.3

SmartTrust WIB 1.2 or WIB1.3 files are defined outside the USIM application files. WIB operation is seamless within SIM or USIM ADF's.

4.5. 3GPP USAT Interpreter

3GPP defines an optional open browser specification STK environment called the USAT Interpreter. The USAT environment specifies its own client - the server protocol - and the client browser

environment. USAT files are defined outside of the USIM application files to ensure 2G backwards compatibility. USAT is provided as an optional feature with Prism SIM and USIM products.

4.6. Java and J2ME

Java is an open platform technology that allows independent and rapid development of value-add services. The interoperable and multi-application capabilities of Java, enables several applications to reside on the card at the same time. The UICC architecture being multi-application orientated itself, is particularly suited to an object orientated and protected machine environment such as Java, but it should be noted that UICC/USIM does not require Java by default. Prism provides USIM with Java as an optional feature environment. The JCP defines the operation and interaction of a handset based Java applet, called a Midlet, and the USIM or SIM, via a specification called JSR177. JSR177 applies to MIDP2.0 J2ME handsets and allows the Midlet and SIM/USIM to exchange information, such as authentication and permissions associated with DRM. Prism offers this support as an optional feature on SIM and USIMs.



5. UICC - Benefits and Challenges

5.1. Benefits of UICC

Subscriber benefits:

- Multi/Enhanced Phone Book supported by default in USIM configuration
- Global or application specific phonebooks
- PC phonebook synchronisation simpler
- Hidden phonebook entries supported for privacy - Private entries accessible by PIN
- Global/ local PIN, applications
- Multi-IMSI by default for business/user or multiple roaming accounts
- Generic SIM card possibility – user configuration at home possibilities in the future
- Access device for user auth – WLAN/WiFi

Mobile Network Operator benefits:

- Begin seamless 3G SIM migration in 2G network
- Begin seamless 3G handset migration in 2G network
- Support users roaming on 2G-3G combination networks
- Stronger anti-cloning – Milenage; ability to customise
- Backwards compatible to STK WIB/USAT/Proprietary backend
- True multi-app card OS i.e.: 3rd party multi-issuer support
- DRM/Dongle - content store/ forwarding protection
- OTA re-personalisation: SIM/USIM
- Object memory pool becomes a default – easier to manage applications and memory optimisation
- Use USIM as a generic Access device – not necessarily restricted to pure telecom
- Possible application enhancements using BIP and CAT-TP if provided in USIM

5.2. Challenges of UICC

Not to be underestimated are the 'real' factors affecting networks when rolling out USIMs:

- User education – “What does 3G USIM mean to the subscriber?”
- 3G handset compatibility/stability – are all USIM features supported?
- 3G network testing of USIM (OTA, Roaming)
- Configuration options for profiles – operator education – many more options
- SIM vendor implementation compatibility
- Security conditions different across USIM/SIM files
- Memory consumption: file sharing, defragmentation
- 3G phone book shared ADN/SMS space
- Shared IMSI, PIN
- OTA switchover SIM – USIM
- Smooth migration, interworking of STK/WIB applications under 2G
- 3rd party/content provider impact
- USAT interpreter (does it play a role?)
- Strategy WLAN/WiFi authentication and billing



6. Conclusion

The Third Generation is a reality and everyone wants to get their piece of the 3G pie.

It offers new and innovative services to a market of subscribers that are increasing daily - as are the number of mobile operators launching networks worldwide.

Historically, the SIM card was utilized as a secure and standard way of authenticating and billing the subscriber. Its role has developed with time and today it is a key component of the wireless network. The SIM card offers the operator the ability to provide a level of services beyond those supplied by the handset. The SIM card is the only network element in the wireless subscriber's hands which is controllable and thus represents the operator's exclusive link with the consumer.

With the high level of security in network access and user identification, the SIM card plays an even more important role by offering strengthened and personal security mechanisms.

We are however still in the early stages of 3G. For the operator it is essential then that the migration to 3G is as seamless as possible and thus recommended that 3G SIM cards, with both USIM and SIM applications are issued. In so doing, it is far simpler to promote the subscriber's migration through new profile activation.

From a subscriber perspective, the proposition would be bought on the basis of value added services available. The operator would undoubtedly be required to incorporate an educational/communication slant to collateral promoting the benefits of 3G.

Prism's uSIMetrix range places your services in the hands of your customers.

Appendix – Specifications Annotated

This section provides a consolidated view of most of the USIM and UICC specifications for reference.

UICC/USIM primary specifications

- 3GPP TS 31 101 V6.2.0 (2003-06): UICC-Terminal Interface; Physical and Logical Characteristics
This references 3GPP TS 31.102 and ETSI TS 102 221, with a handful of “refinements”.
- 3GPP TS 31.102 V6.5.0 (2004-03): Characteristics of the USIM application
- 3GPP TS 31.111 V6.1.0 (2004-03): USIM Application Toolkit (USAT)
- ETSI TS 102 221 V6.4.0 (2004-03): UICC-Terminal interface; Physical and logical characteristics
- ETSI TS 102 223 V5.2.0 (2003-06): Card Application Toolkit (CAT)

UICC/USIM authentication specifications

- 3GPP TS 35 205 V5.0.0 (2002-06): Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General
- 3GPP TS 35 206 V5.1.0 (2003-06): Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm specification
- 3GPP TS 35 207 V5.0.0 (2002-06): Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors’ test data
- 3GPP TS 35 208 V5.0.0 (2002-06): Specification of the MILENAGE algorithm set: An example algorithm Set for the 3GPP Authentication and Key Generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design conformance test data
- 3GPP TR 35 909 V5.0.0 (2002-05): Specification of the MILENAGE algorithm set: an example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation. This is a report, not a specification.

Test specifications

- 3GPP TS 31.120 V3.0.0 (2000-12): UICC-Terminal Interface; Physical, Electrical and Logical Test Specification
- 3GPP TS 31.121 V4.7.0 (2004-03): UICC-Terminal Interface; USIM Application Test specification
- 3GPP TS 31.122 V3.7.0 (2003-12): USIM conformance test specification
- 3GPP TS 31.048 (not released yet): Test specification for security mechanisms for the (U)SIM application toolkit

Useful specifications for understanding

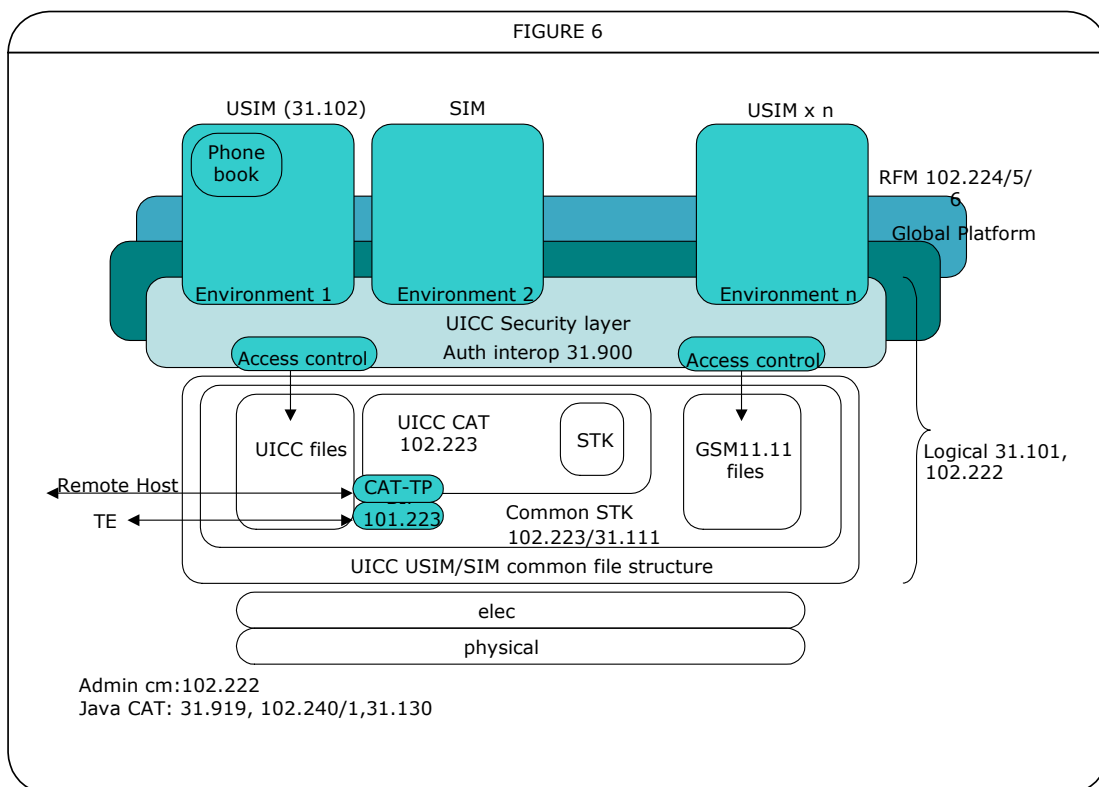
- 3GPP TS 21.111 V6.0.0 (2004-03): USIM and IC card requirements. This provides an overview of the USIM.

- 3GPP TS 51.011 V4.10.0 (2003-12): Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface. This specifies the SIM as a UICC application.
- 3GPP TS 51.014 V4.3.0 (2003-12): Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface. This is essentially the old GSM 11.14.
- 3GPP TR 31.900 V5.0.0 (2002-03): SIM/USIM Internal and External Interworking Aspects

Related specs for JavaCard & other

- 3GPP TS 31.103 V6.3.0 (2004-03): Characteristics of the IP Multimedia Services Identity Module (ISIM) application
- 3GPP TS 31.130 V6.0.0 (2004-03): (U)SIM Application Programming Interface; (U)SIM API for Java Card™
- 3GPP TR 31.919 V6.0.0 (2004-03): 2G/3G Java Card™ API based applet interworking
- ETSI TS 102 222 V6.2.0 (2003-09): Administrative commands for telecommunications applications
- ETSI TS 102 224 V6.0.0 (2002-04): Security mechanisms for UICC based Applications - Functional requirements
- ETSI TS 102 225 V6.2.0 (2003-06): Secured packet structure for UICC based applications
- ETSI TS 102 226 V6.5.0 (2003-09): Remote APDU structure for UICC based applications

The diagram below provides a useful reference to specifications' logical grouping relative to USIM and UICC architecture.



Contact Us

For more information on the Prism uSIMetrix range, please do not hesitate to contact us.

Prism Holdings Limited – Head Office, Johannesburg

e-mail	marketingteam@prism.co.za		
Phone	+27 (0)11 548 1000	Fax	+27 (0)11 467 3424
Physical	Buidling One Prism Business Park Ruby Close Fourways Sandton South Africa	Postal	PO BOX 901 Witkoppen 2068 Gauteng South Africa

The information contained in this document is owned by Prism Holdings Limited and you may not disclose, copy or in any way deal with or publish the content hereof (including attachments), all of which is subject to copyright. This document contains information intended to be informative only and shall in no manner bind Prism Holdings Limited or its subsidiaries (collectively referred to as "Prism"), nor does Prism accept any liability whatsoever as a result of any losses arising from persons placing reliance on any information contained in this document. Prism does not warrant the accuracy of the contents of this document, which is subject to change without prior notice.

www.prism.co.za

