1. Product Specifications

Chip Field	Description
Generic Description	64K JavaCard 2.1.1 WIB1.3 USIM
Platform	Atmel AT90SC25672RU
CPU Architecture	8-bit AVR
Technology	0.15uM CMOS
ROM	256Kb ROM Program Memory
Non-volatile memory	72 Kb EEPROM
RAM	6 Kb
Voltage range	Classes A, B, C (1.62V to 5.5V)
Internal operating frequency	Between 20 & 30 MHz
Operating temperature	-25^{o}C to +85^{o}C
Storage temperature	-40^{o}C to +125^{o}C
Endurance	Typically 500 000 write/erase cycles @ 25^{o}C per page
Data retention	Nominally 10 years at 25^{o}C
ESD Protection	Up to ±4000V
Pin Configurations	8-Pin

2. OS and Applications

2.1. General

Field	Description
GSM Application	3G USIM *or* 2G SIM (configurable during personalisation)
Total file space available *(EEPROM)*	**70252 Bytes** (including MF header)
Total code space used *(ROM)*	**253734 Bytes**

2.2. Network Authentication

Field	Description
Network Algorithms	• COMP128-1/2/3 (*configurable)* • Milenage
Additional security	• Attack detection • Randomised DPA table look-ups • Strong key generation (COMP128-1 only) • Authentication counter supported

2.3. Java

Parameter	Description
JavaCard Version	V2.1.1
Additional Features	• Support for 32-bit integers
RMI	• maximum exports = 16 • reserved heap data size = 256
ROM Heap	16 (*Internal/Proprietary)*
ROM-based Packages	• Nominal JavaCard 2.1.1 API • ETSI SIM applet API • Native method API • Extenable crypto API • Global Platform PIN handling API • AES Library API
Maximum crypto algorithm classes	10
Transient Buffer Size	3072 Bytes
Stack size	(240 x 2) Bytes

3. Specification Compliancy

3.1. ISO 7816 Specifications

Reference	Document Title	Version	Comments
ISO/IEC 7816-1	Identification Cards – Integrated Circuit(s) Cards With Contacts: Part 1: Physical Characteristics	2004 Release	SIM-applicable functionality added.
ISO/IEC 7816-2	Identification Cards – Integrated Circuit(s) Cards With Contacts: Part 2: Dimensions and Location of the Contacts	2004 Release	SIM-applicable functionality added.
ISO/IEC 7816-3	Identification Cards – Integrated Circuit(s) Cards With Contacts: Part 3: Electronic Signal and Transmission Protocols	2005 Release	SIM-applicable functionality added.
ISO/IEC 7816-4	Identification Cards – Integrated Circuit(s) Cards With Contacts: Part 4: Interindustry Commands for Interchange	2004 Release	SIM-applicable functionality added.

3.2. ETSI/3GPP Specifications

Reference	Document Title	Version	Comments
GSM 02.17 ETSI TS 100 922	Subscriber Identity Modules (SIM); Functional characteristics	8.0.0	SIM-applicable functionality added
3GPP TS 03.19 ETSI TS 101 476	GSM API for SIM toolkit stage 2	8.5.0	
GSM 03.38, ETSI TS 100 900	Alphabets and language-specific information	7.2.0	
3GPP TS 03.40 ETSI TS 100 901	Technical realization of the Short Message Service (SMS) Point-to-Point (PP)	7.5.0	
3GPP TS 03.48 ETSI TS 101 181	Security Mechanisms for SIM application toolkit; Stage 2	8.8.0	Excluded: * DS signature
GSM 04.08, Draft ETSI EN 300 940	Mobile radio interface layer 3 specification	7.4.0	
3GPP TS 04.11 ETSI TS 100 942	Point-to-Point (PP) Short Message Service (SMS) Support on Mobile Radio Interface	7.1.0	

Reference	Document Title	Version	Comments
3GPP TS 11.11 ETSI TS 100 977	Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface	8.9.1	
GSM 11.12	Specification of the 3V Subscriber Identity Module – Mobile Equipment (SIM-ME) interface	4.3.1	
3GPP TS 11.13 ETSI TS 101 955	Test Specification for SIM API for Java Card™	8.1.0	
3GPP TS 11.14	Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface.	8.15.0	
3GPP TS 11.17 ETSI TS 101 086	SIM test specification.	8.0.0	
GSM 11.18 ETSI TS 101 116	Specification of the 1.8 Volt Subscriber Identity Module – Mobile Equipment (SIM-ME) interface	7.0.1	
3GPP TS 21.111	USIM and IC card requirements	6.0.0	SIM-applicable functionality added
3G TS 23.038 ETSI TS 123 038	Alphabets and language-specific information	3.3.0	
3GPP TS 23.040 ETSI TS 123 040	Technical realization of Short Message Service (SMS)	6.5.0	
3GPP TS 23.048 ETSI TS 123 048	Security Mechanisms for the (U)SIM application toolkit; Stage 2	5.7.0	
3GPP TS 31.048	Security mechanisms for the (U)SIM application toolkit; Test specification	5.1.0	
3GPP TS 31.101 ETSI TS 131 101	UICC-terminal interface; Physical and logical characteristics	6.2.0	
3GPP TS 31.102	Characteristics of the USIM application	6.5.0	
3GPP TS 31.115 ETSI TS 131 115	Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	6.5.0	

Reference	Document Title	Version	Comments
3GPP TS 31.116 ETSI TS 131 116	Remote APDU structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications	6.8.0	
3GPP TS 31.122 ETSI TS 131 122	Universal Subscriber Identity Module (USIM) conformance test specification	6.1.0	
3GPP TR 31.900	SIM/USIM internal and external interworking aspects	5.5.0	
3GPP TR 31.919	2G/3G Java Card™ Application API based applet interworking	6.0.0	
3GPP TS 35.205 ETSI TS 135 205	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	5.0.0	
3GPP TS 35.206 ETSI TS 135 206	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: Algorithm specification	5.1.0	
3GPP TS 42.017	Subscriber Identity Modules (SIM); Functional characteristics	4.0.0	
3GPP TS 43.019 ETSI TS 143 019	Subscriber Identity Module Application Programming Interface (SIM API) for Java Card™	5.6.0	
3GPP TS 51.011	Specification of the Subscriber Identity Module – Mobile Equipment (SIM–ME) interface	4.11.0	
3GPP TS 51.013	Test specification for Subscriber Identity Module (SIM) Application Programming Interface (API) for Java Card™	5.6.1	
3GPP TS 51.014	Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface	4.4.0	

Reference	Document Title	Version	Comments
3GPP TS 51.017 ETSI TS 151 017	Subscriber Identity Module (SIM) test specification	4.1.0	Partly tested
ETSI TS 101 220	ETSI numbering system for telecommunication application providers	7.9.0	
ETSI TS 102 221	UICC-Terminal interface; Physical and logical characteristics	6.14.0	
ETSI TS 102 222	Administrative commands for telecommunications applications	6.10.0	Excluded: * Compound AC formats * File sizes > 64k
ETSI TS 102 225	Secured packet structure for UICC based applications	6.2.0	
ETSI TS 102 230	Physical, electrical and logical test specification	5.3.0	Partly tested

3.3. Java Card / Stepping Stones Specifications

Reference	Document Title	Version	Comments
JCVM 2.1.1	Java Card 2.1.1 Virtual Machine Specification	2.2.2	
JCRE 2.1.1	Java Card 2.1.1 Runtime Environment (JCRE) Specification	2.2.2	
JCAPI 2.1.1	Java Card 2.1.1 Application Programming Interface	2.2.2	All mandatory API's are included. See below for a list of optionally supported cryptographic algorithms
SS6	Interoperability Stepping Stones	Release 6, V1.00	

3.3.1. Supported Cryptographic Algorithms

Algorithm	Type	Description
DES	Ciphers	CBC with ISO 9797 M1 / ISO 9797 M2 / PKCS#5 / No padding
		ECB with ISO 9797 M1 / ISO 9797 M2 / PKCS#5 / No padding
	Signatures	MAC4 with ISO 9797 M1 / ISO 9797 M2 / PKCS#5 / No padding
		MAC8 with ISO 9797 M1 / ISO 9797 M2 / PKCS#5 / No padding
	Keys	8 / 16 / 24 byte lengths
	Signatures	MAC with no padding
RNG	Pseudo and Secure	

Algorithm	Type	Description
SHA	SHA-1	
CRC	ISO/IEC 3309 compliant CRC16	
	ISO/IEC 3309 compliant CRC32	

3.4. Global Platform Specifications

Reference	Document Title	Version	Comments
GP 2.1.1	Global Open Platform Card Specification; incl. Amendment A	V2.1.1	See below for details

Note[1]:
Global Platform functionality limitations / support:

- Security Domains:
  - Only DES keys supported.
  - Only the Issuer Security Domain is supported.
- Delegated management is not supported.
- Tokens and receipts are not supported.
- Secure channels / protocols are not supported
- Commands only partially supported:
  - INSTALL (for personalisation) – not supported.
  - SET STATUS – the status of a security domain cannot be set.
  - GET DATA – optional tag type not supported
  - PUT DATA – optional tag type not supported