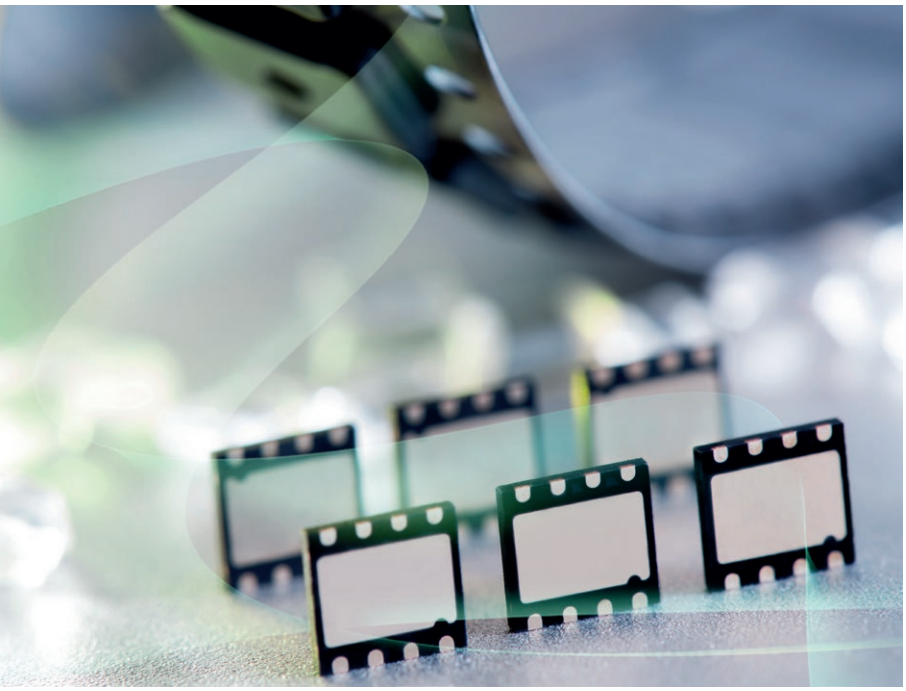
G+D Mobile Security

Technical data sheet



Sm@rtSIM® CX 97 IN-CAR SMD

The automotive grade solderable SIM for the in-car applications

Hardware Features

Operating Characteristics
- Voltage Class: A, B, C (1.8V – 5.0V ±10%)
- Temperature Range: -40 to +105°C (grade 2) (Voltage Class: A, B, C)

CPU
- 32-bit CPU core

Memory
- 1MB Flash
- 32kB RAM
- Min. 500,000 erase/write cycles per page
- Up to 16,5m erase/write cycles for one hot spot per sector (at 85°C)
- 17 years data retention

Serial I/O
- Hardware UART (conforms to ISO7816)
- optional: SPI, SWP

Cryptography
- Symmetric: DES/TDES, AES
- Asymmetric: RSA, ECC (optional)
- True RNG, CRC-16/32

Automotive grade 2
- Form factor: MFF2 (ETSI 102 671 definition)
- AEC-Q100 qualification plan
- PPAP documentation on request
- Tape and reel packing for delivery
- ICCID laser marking on single package level

Software Features

Key Features
- Release 10 LTE
- 2G / 3G / LTE
- Milenage, TUAK, CAVE COMP128-2/3/4
- DPA-/SPA-/DFA-resistant
- DES, AES, MD5, Korean Seed, SHA 1/256-Hashing ECC 521 optional: RSA 2048
- Java Card: 3.0.4
- Java API
  - UICC and USAT API (Rel6)
  - Smart de-fragmentation
  - Support of Integer
- GP 2.2.1 GP 2.2 Amd A / B / D / E
- OTA Support
  - OTA via SMS / HTTPs / BIP CAT-TP
  - Remote File Management
  - Remote Applet Management
- ISIM Rel10 / GBA
- R-UIM / CSIM
- EAP AKA / EAP SIM
- Enhanced Memory Management for 3rd party applications
- Enhanced Administrative Commands
- Intelligent Memory Management system to enhance erase/write cycles

Automotive enhancement
- GSMA eSIM Management
- JC Glonass Application
- QoS SIM Application
- M2M device detection & lock

Key Standard Compliance

ETSI
- 101 220 ETSI numbering system for telecommunication application providers
- 102 127 Transport protocor for CAT applications Stage 2
- 102 221 UICC-Terminal interface; Physical and logical characteristics
- 102 222 Administrative commands for telecommunications applications
- 102 223 Card Application Toolkit (CAT)
- 102 225 Secured packet structure for UICC based applications
- 102 226 Remote APDU structure for UICC based applications
- 102 241 UICC Application Programming Interface (API) for Java Card
- 102 268 Test specification for UICC Application Programming Interface (API) for Java Card
- 102 613 UICC - CLF Interface; Part 1: Physical and data link layer characteristics

3GPP
- 43.019 Subscriber Identity Module Application Programming Interface (SIM API) for Java Card Stage 2
- 51.011 Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
- 51.013 Test specification for Subscriber Identity Module (SIM) Application Programming Interface (API) for Java Card
- 51.014 Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
- 51.017 Subscriber Identity Module (SIM) conformance test specification
- 31.048 Security mechanisms for the (U)SIM application toolkit; Test specification
- 31.101 UICC-Terminal Interface; Physical and Logical Characteristics
- 31.102 Characteristics of the USIM Application
- 31.103 Characteristics of the IP Multimedia Services Identity Module (ISIM) application
- 31.111 USIM Application Toolkit (USAT)
- 31.115 Secured packet structure for (U)SIM Toolkit applications
- 31.116 Remote APDU Structure for (U)SIM Toolkit applications
- 31.122 USIM conformance test specification
- 31.130 (U)SIM API for Java Card
- 31.133 ISIM API for Java Card
- 31.213 Test Specification: Applicaton Programming Interface (API) for Java Card
- 31.900 SIM/USIM Internal and External Interworking Aspects
- 31.919 2G/3G Java Card API based applet internet working

3GPP2
- C.S0016-C Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards, Rev.C V2.0
- C.S0023-C Removable User Identity Module for Spread Spectrum Systems, Rev.D V1.0
- C.S0035 CDMA Card Application Toolkit (CCAT), Rev.A V1.0
- C.S0065-A cdma2000 Application on UICC for Spread Spectrum Systems, Rev.A V1.0

Sun/Oracle Specifications
- JCRE 3.0.4 Runtime Environment Specification, Java, Classic Edition Card Platform
- JCVM 3.0.4 Virtual Machine Specification, Java Card Platform, Classic Edition
- JCAPI 3.0.4 Application Programming Interface, Java Card Platform, Classic Edition

GlobalPlatform Specifications
- GlobalPlatform Card Specification, V2.2.1
- GP 2.2 AmdA Confidential Card Content Management
- GP 2.2 AmdB Remote Application Management over HTTP
- GP 2.2 AmdC Contactless Services
- GP 2.2 AmdD Secure Channel Protocol 03
- GP 2.2 AmdE Security Upgrade for Card Content Management
- GP Java Card API

GSMA
- SGP.01 Embedded SIM Remote Provisioning Architecture
- SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification
- SGP.21 RSP Architecture
- SGP.22 RSP Technical Specification

Giesecke+Devrient
Mobile Security GmbH
Prinzregentenstrasse 159
81677 Munich
Germany

P +49 89 41 19-0
mobilesecurity@gi-de.com
www.gi-de.com/mobile-security

May 2018