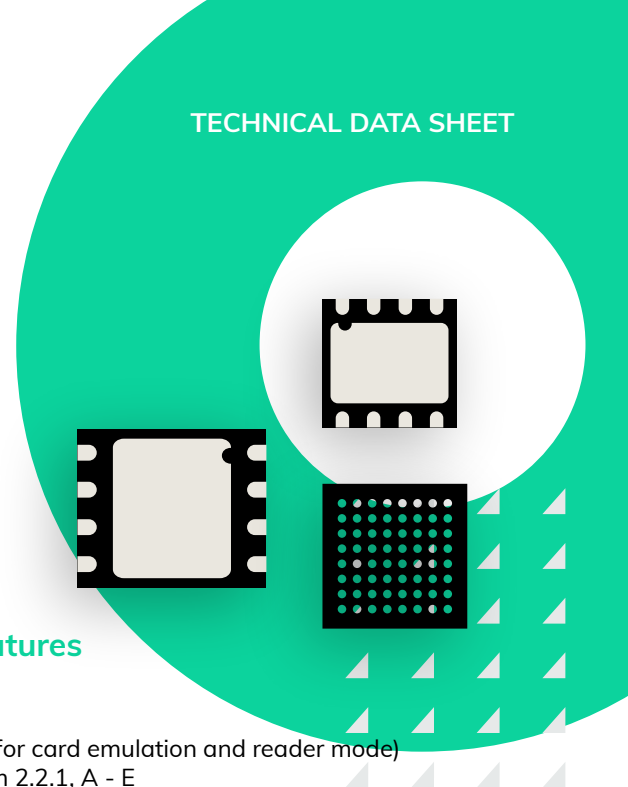


1oT eSIM

MFF2/EMBEDDED



Hardware Features

Operating Characteristics

- Voltage Class A, B & C (1.8V – 5.0V ±10%)
- Temperature Range: -30 to +85°C for MFF2

CPU

- 32-bit CPU core

Memory

- Up to 1.3 MB nonvolatile memory
- 30kB RAM
- Min. 100,000 erase / write cycles for page at room temperature
- Data retention of 10 years at room temperature
- Dynamic memory management with smart defragmentation

Serial I/O

- Hardware UART (conforms to ISO7816)
- Concurrent SWP, SPI, and GPIO interfaces

Cryptography

- Built-in hardware DES, TDES, AES, RSA
- Hardware random number generator (RNG)

Others

- 16-bit random number generator
- Parity calculator for 8/16/32 bit
- CRC-16 / 32 calculator
- 16-bit programmable interval timers
- Form factors: MFF2, DFN 8, plugable SIM

Software Features

Key Features

- NFC (support for card emulation and reader mode)
- GlobalPlatform 2.2.1, A - E
- Memory Quota
- Access Control (ARA)
- Java Card: 3.0.4
- Java API
- ETSI Contactless API extension (Rel9)
- Extensive crypto support (3DES, AES, RSA 2048, ECC 521, DSA, Korean Seed, SHA & HMAC-SHA 512 MD5, HMACMD5)
- All security-relevant methods are DPA / SPA /DFA-secured
- ANSI X9.17 software secure random number generator
- Scalable crypto API with DES encryption

NFC Applications

- Fully certified Visa, Master-Card, Amex, PBOC
- MIFARE Classic reader and card emulation, CC EAL 5+ certified MIFARE DESFire, MIFARE4Mobile
- CIPURSE, Calypso, HID
- mPOS
- GP Amd C compliant wallets

eSE Features

- OS Replication
- Key Diversification
- CLF Firmware Upload
- Smart APDU Gate

Optional eUICC Features

- GSMA eSIM Management
- UICC and USAT API (Rel8)
- SAT API (Rel5)
- Release 10 LTE
- ISIM, GBA
- EAP-SIM, EAP-AKA
- 2G, 3G, LTE, CDMA
- Milenage, TUAK, COMP128-1 / 2 / 3 / 4
- OTA Support
- OTA via SMS, HTTPs, BIP CAT-TP
- Remote File Management (RFM)
- Remote Applet Management (RAM)
- Browsers: WIB 1.3, WIB 2.0, S@T v4, S@T2007



Key Standard Compliance

ETSI

- 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
- 102 613 UICC - CLF Interface; Part 1: physical and data link layer characteristics
- 102 622 UICC - CLF Interface; Host Controller Interface (HCI)
- 102 705 UICC Application Programming Interface for Java Card for Contactless Applications

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
- 51.014 Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
- 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
- 31.130 (U)SIM API for Java Card
- 31.133 ISIM API for Java Card
- 31.919 2G/3G Java Card API based applet internet working

GSMA

- SGP.01 Embedded SIM Remote Provisioning Architecture
- SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification

3GPP2

- 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.B V2.0

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
- GP Java Card Contactless API for Card Specification V2.2.1

