Classic USIM

Product Overview

Gemalto Recommended Solution — Bearer Independent Protocol

THALES

gemalto
a Thales company

VERY IMPORTANT NOTICE TO CUSTOMER

Gemalto does not represent and/or warrant that the products conform to the state of the art in electronic security mechanisms at the time they were made. Gemalto only warrants that the products are manufactured in accordance with the specifications agreed upon with the client in a writing signed by an authorized representative of Gemalto (i.e., an employee of Gemalto that is expressly empowered to bind Gemalto). Unless a different period of warranty is expressly agreed between Gemalto and Customer, such limited warranty expires no later than one (1) year after delivery of the Products.

Customer is deemed to have provided and is responsible for all designs, plans, data (e.g., personalization data), electronic security mechanisms and architecture, and specifications with respect to Products (collectively, "Designs"). If Gemalto makes suggestions with respect to the Designs, at Customer's request or otherwise, Customer will be responsible for analyzing the same and determining whether to incorporate them into the Designs.

Customer represents and warrants that by placing an order for the products (a) it relies on its own knowledge and judgment in the selection and use of the products as well as the electronic security mechanism and/or architecture installed in the products, and (b) it has read, understood and accepted the electronic security mechanisms and/or architecture offered by the products.

GEMALTO SHALL NOT BE LIABLE IN ANY MANNER WHATSOEVER WITH RESPECT TO FAILURE OF OR ATTACK ON THE ELECTRONIC SECURITY MECHANISMS AND/OR ARCHITECTURE OF THE PRODUCTS.

PLEASE NOTE that Gemalto reserves the right to extend the card OS capabilities by including non-active additional features (information upon request). If present, these extensions may be activated by OTA at post-issuance for the benefit of the mobile network operator at its sole own request.The use of these extensions through services provided by Gemalto will be subject to a prior commercial agreement with Gemalto related to the use and activation of these extensions.

Document Reference: D1351870B

Product Reference: T1029413

February 12, 2020

THALES

gemalto
a Thales company

Classic USIM

Card Physical Characteristics

- ETSI TS 102.221 for electrical characteristics and communication protocol.
- Supports class A (5V), B (3V), and C (1.8V) mobile equipment.
- Communication protocol: T=0.
- PPS procedure (support of speed enhancement):
  - Default speed: F=512, D=32 (223200 bauds at 3.57 MHz).
  - Max. speed: F=512, D=64 (446400 bauds at 3.57 MHz).

Authentication and Cryptographic Algorithms

Algorithms	Use Cases
DES, TDES	Java Card API, OTA Encryption
Comp128 V1, V2, V3, and GSM Milenage	2G Network Authentication
Milenage	3G Network Authentication
AES (128, 192, 256 bits)	Java Card API, SMS and BIP CAT-TP OTA Encryption
SHA-1	Java Card API
CRC-32	Basic Calculation

Features and Applications

The card supports the following features and applications:

- Bearer Independent Protocol (BIP)
  - Faster and reliable data transmission via the high-speed data channel provided by the General Packet Radio Service (GPRS), and support of other bearers such as CSD and Bluetooth.
  - Optimized remote management of SIM profiles, download and management of applications, and ease access to SIM upgrade.
  - Best user experience to LinqUs Service Engine and Phonebook Backup Engine.
- LinqUs Service Engine (available upon request)
  - Access to value-added services through the SIM menu.
  - Remote management for active services.
  - Introduction of new services through interactive promotional SMS push.
- LinqUs Device Detection Engine (available upon request)
  - Automatic configuration of handset settings when user inserts the SIM to a new handset.
  - Automatic gathering of handset capabilities.
- LinqUs Phonebook Backup Engine (available upon request)
  - Synchronization of contacts with Phonebook Backup server.
  - Restoration of entire phonebook in case of loss.
  - Automatic registration and synchronization.

Compliance

- Java Card
  - Java Card™ 2.2.1 API Specification.
  - Java Card™ 2.2.1 Runtime Environment Specification.
  - Java Card™ 2.2.1 Virtual Machine Architecture Specification.
- GlobalPlatform
  - GlobalPlatform 2.1.1 (supports multiple security domains and application extraditions).
- ETSI
  - ETSI TS 101.220: ETSI numbering system for telecommunication application providers; (V6.5.0).
  - ETSI TS 102.221: Physical and Logical Characteristics; (V6.14.0).
  - ETSI TS 102.222: Administrative commands and Telecommunications applications; (V6.11.0).
  - ETSI TS 102.224: Security mechanisms for UICC based Applications - Functional requirements; (V7.1.0).
- 3GPP
  - 3GPP TS 23.040: Technical realization of the Short Message Service (SMS); (V6.5.0).
  - 3GPP TS 23.041: Technical realization of Cell Broadcast Service (CBS); (V6.2.0).
  - 3GPP TS 23.048: Security Mechanisms for the (U)SIM application toolkit; Stage 2; (V5.8.0).
  - 3GPP TS 31.101:UICC-Terminal Interface; Physical and Logical Characteristics; (V6.5.1).
  - 3GPP TS 31.102: Characteristics of the USIM Application; (V6.7.0).
  - 3GPP TS 31.111: USIM Application Toolkit (USAT); (V6.8.0).
  - 3GPP TS 31.115: Secured packet structure for USIM Toolkit applications; (V6.5.0).
  - 3GPP TS 31.116: Remote APDU Structure for USIM Toolkit applications; (V6.8.0).
  - 3GPP TS 43.019: SIM API for Java Card; Stage 2; (V5.6.0).
  - 3GPP TS 51.011: Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) Interface; (V4.15.0).
  - 3GPP TS 51.014: Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; (V4.5.0).
- BIP and CAT-TP
  - ETSI TS 102.127: Transport protocol for CAT applications; Stage 2; (V6.9.0).
  - ETSI TS 102.223: Card Application Toolkit (CAT); (V6.13.0).
  - ETSI TS 102.225: Secured packet structure for UICC based applications; (V6.8.0).
  - ETSI TS 102.226: Remote APDU structure for UICC based applications; (V6.17.0).
  - ETSI TS 102.431: Test specification for the Transport Protocol of CAT Applications (CAT_TP) validation; (V7.0.0).
- Comp128
  - 3GPP TS 43.020: Security-related network functions; (V9.1.0).
- Milenage
  - 3GPP TS 33.102: 3G Security; Security architecture; (V6.1.0).
  - 3GPP TS 35.205: 3G Security; 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; (Release 8).
  - 3GPP TS 35.206: 3G Security; 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; (Release 8).
- Comp128v4/GSM-Milenage
  - 3GPP TS 55.205: Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8; (V9.0.0).
- Aspects and Integri Tests
  - 3GPP TS 31.048: Security mechanisms for the (U)SIM application toolkit; Test specification; (V5.1.0).
  - 3GPP TS 31.122: USIM conformance test specification; (V7.1.0).
  - 3GPP TS 51.013: Test specification for Subscriber Identity Module (SIM) Application Programming Interface (API) for Java Card; (V5.4.0).
  - 3GPP TS 51.017: Subscriber Identity Module (SIM) test specification; (V4.2.0).

THALES

gemalto
a Thales company

Default Answer to Reset

Byte	Value	Description
TS	3Bh	Direct convention.
T0	9Eh	TA1 and TD1 are present, 14 historical characters
TA1	96h	Clock Rate Conversion Factor FI = 9 (Fi = 512). Baud Rate Adjustment Factor DI = 6 (Di = 32).
TD1	80h	Only TD2 is present.
TD2	1Fh	Only the global interface byte TA3 is present.
TA3	C7h	Clock stop is supported in either low or high electrical state (no preference). Voltage class A, B, and C are supported.
T1	80h	Status information format.
T2	31h	Card service data tag.
T3	E0h	SELECT full or partial AID, EF_{DIR} present.
T4	73h	Card capabilities tag.

Byte	Value	Description (Continue)
T5	FEh	All types of DF selection are supported, EF management with record ID is not supported.
T6	21h	Data coding on 2 nibbles.
T7	1Bh	4 logical channels are supported (Channels assigned by the card and interface device).
T8	66h	Pre-issuing data tag.
T9	D0h	The unique identity of this product.
T10	02h	
T11	17h	
T12	C7h	
T13	11h	
T14	00h	
TCK	C3h	Checksum byte.