Classic LTE

Product Overview

CCIOTTRISIMS (TRIO)

Gemalto Recommended Solution

- Bearer Independent Protocol
- Extensible Authentication Protocol
- IP Multimedia Services Identity Module and GBA

gemalto
security to be free

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: D1410394A

September 2, 2016

Classic LTE

Physical Characteristics

- ETSI TS 102.221 for electrical characteristics and communication protocol.
- Supports class A (5V), B (3V), and C (1.8V) supply voltages.
- Communication protocol: T=0.
- PPS procedure (support of speed enhancement):
  - Default speed: PPS 96, F=512, D=32 (223200 bauds at 3.57 MHz).
  - Max. speed: PPS 97, F=512, D=64 (446400 bauds at 3.57 MHz).

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.
- Extensible Authentication Protocol (EAP)
  - An authentication framework which supports two authentication methods:
    - Extensible Authentication Protocol for 3rd Generation Authentication and Key Agreement (EAP-AKA).
    - Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM).
- IP Multimedia Services Identity Module (ISIM)
  - Contains the parameters for identification and authentications of the user to the IP Multimedia Subsystem.
  - Provides the session keys for integrity protection.
- Poll Interval Negotiation
  - Supports Procedure of Negotiation of Poll Interval as defined in ETSI TS 102.223; (Release 12).
  - The UICC allows the terminal to propose and negotiate a proactive poll interval, in order to best match the power and usage pattern of the terminal. The UICC can accept, modify or reject the proposed poll interval.
- USAT Application Pairing
  - Restricts the use of USIM to a specific mobile equipment.
  - Supports USAT Pairing as defined in 3GPP TS 33.187; (Release 12) and 3GPP TS 31.102; (Release 12).
- USIM Supported URI
  - Supports the IMS URI field in the Call Control address field.
  - Supports the URI truncated field.
  - IMS URI address field is added in MT Call Event.
  - Supports URI format in address data field for Send Short Message, MO Short Message, Set Up Call, and Envelope SMS-PP Download.
- Geographical Location
  - Supports the proactive command **Geographical Location Request** and the envelope command **Geographical Location Reporting** to allow UICC to request and receive the current geographical location information from mobile equipment.
- OTA Advanced Polling (available upon request)
  - Polls the server through an HTTP channel for RFM and RAM updates.
  - Polling is done at every configured interval or on a specific date.
  - Polling can also be done by SMS.
- OTA Advanced Refresh (available upon request)
  - Issues a Refresh proactive command to the device upon trigger by the server after an RFM/RAM update on HTTP.
- Admin Agent (available upon request)
  - An HTTP client that is available on the card to manage all HTTP communications and HTTP security.
- DNS R12 (available upon request)
  - An application that retrieves OTA IP addresses and manages DNS requests.
- 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.

Authentication and Cryptographic Algorithms

Algorithms	Use Cases
DES, TDES	Java Card API, OTA Encryption
Comp128 V1, V2, V3	2G Network Authentication
Milenage	3G and LTE Network Authentication
TUAK	3G and LTE Network Authentication
AES (128, 192, 256 bits)	Java Card API, SMS and BIP CAT-TP OTA Encryption, HTTP (TLS) OTA Encryption
SHA-1	EAP, GBA, Java Card API, HTTP (TLS 1.0 and 1.1)
SHA-256	GBA, Java Card API, HTTP (TLS 1.2)
HMAC-SHA-1	EAP, HTTP (TLS 1.0, 1.1, and 1.2)
HMAC-SHA-256	GBA, HTTP (TLS 1.2)
HMAC-MD5	HTTP (TLS 1.0 and 1.1)
MD5	Java Card API, HTTP (TLS 1.0 and 1.1)
PRF	HTTP (TLS 1.0, 1.1, and 1.2)
CRC-32	Basic Calculation

Supported TLS Cipher Suite

Cipher Suite	Key Exchange	Confidentiality	Integrity
TLS 1.0, 1.1, and 1.2	TLS PSK	3DES EDE CBC	SHA
TLS 1.0, 1.1, and 1.2	TLS PSK	AES 128 CBC	SHA
TLS 1.0, 1.1, and 1.2	TLS PSK	Null	SHA
TLS 1.2	TLS PSK	AES 128 CBC	SHA-256
TLS 1.2	TLS PSK	Null	SHA-256

Compliance to Standards (Electrical and Functional)

- Java Card
  - Java Card™ 3.0.1 API Specification.
  - Java Card™ 3.0.1 Runtime Environment Specification.
  - Java Card™ 3.0.1 Virtual Machine Architecture Specification.
- GlobalPlatform
  - GlobalPlatform 2.2 Amendment B, V1.1 (Remote Application Management over HTTP).
  - GlobalPlatform 2.1.1 (supports multiple security domains, application extraditions, and SCP01).
- ETSI
  - ETSI TS 101.220: ETSI numbering system for telecommunication application providers; (V7.11.0).
  - ETSI TS 102.221: Physical and Logical Characteristics; (V8.2.0).
  - ETSI TS 102.222: Administrative commands and Telecommunications applications; (Release 7).
  - ETSI TS 102.223: Card Application Toolkit (CAT); (V8.2.0).
  - ETSI TS 102.224: Security mechanisms for UICC based Applications - Functional requirements; (V8.0.0).
  - ETSI TS 102.225: Secured packet structure for UICC based applications; (V9.2.0).
  - ETSI TS 102.226: Remote APDU structure for UICC based applications; (V9.6.0).
  - ETSI TS 102.310: Smart Cards; Extensible Authentication Protocol support in the UICC; (V6.2.0).

- 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; (V5.9.0).
  - 3GPP TS 31.101:UICC-Terminal Interface; Physical and Logical Characteristics; (V8.0.0).
  - 3GPP TS 31.102: Characteristics of the USIM Application; (V8.6.0).
  - 3GPP TS 31.103: Characteristics of the IP Multimedia Services Identity Module (ISIM) application; (V12.0.0).
  - 3GPP TS 31.111: USIM Application Toolkit (USAT); (V8.6.0).
  - 3GPP TS 31.115: Secured packet structure for USIM Toolkit applications; (V8.5.0).
  - 3GPP TS 31.116: Remote APDU Structure for USIM Toolkit applications; (V8.0.0).
  - 3GPP TS 31.133: IP Multimedia Services Identity Module (ISIM) Application Programming Interface (API); ISIM API for Java Card™; (V12.0.0)
  - 3GPP TS 33.203: 3G security; Access security for IP-based services; (V6.11.0).
  - 3GPP TS 33.220: Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA); (V6.13.0).
  - 3GPP TS 33.234: 3G security; Wireless Local Area Network (WLAN) interworking security; (V6.9.0).
  - 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; (V6.10.0).
  - ETSI TS 102.267: Connection Oriented Service API for the Java Card™ platform; (V7.0.0).
  - ETSI TS 102.431: Test specification for the Transport Protocol of CAT Applications (CAT_TP) validation; (V7.0.0).
- UICC/USIM APIs
  - 3GPP TS 31.130: USIM API for Java Card™; (V8.1.0).
  - 3GPP TS 31.213: Test specification for (U)SIM; API for Java Card™; (V6.1.0).
  - ETSI TS 102.240: UICC API and Loader Requirements; Service description; (V7.0.0).
  - ETSI TS 102.241: UICC API for Java Card™; (V8.0.0).
  - ETSI TS 102.268: Test specification for the UICC API for Java Card™; (V6.0.0).
- Comp128
  - 3GPP TS 43.020: Security-related network functions; (V9.1.0).
- Milenage
  - 3GPP TS 33.102: 3G Security; Security architecture; (V8.2.0).
  - 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).
- TUAK
  - 3GPP TS 35.231: Specification of the TUAK algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm specification; (V12.1.0).

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, EFDIR 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	XXh	Proprietary historical bytes—these values vary, depending on the final product and its version.
T10	XXh	
T11	XXh	
T12	XXh	
T13	XXh	
T14	XXh	
TCK	XXh	Checksum byte.