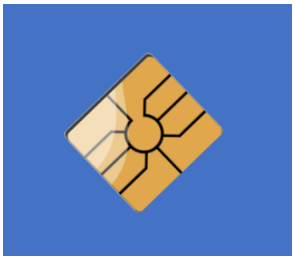
# The crypto secure memory card Operating System for contact smart card

UniQrypt



**Crypto secure memory for contact smart cards**

2 Kbits / 4 Zones

Qilium

®**UniQrypt** is a **Qilium** product offering a range of solutions based on various user memory size options shared between different user zones. It has been developed to provide a crypto secure memory for sensitive information and to ensure a durable integrity of stored data.

With inherent security features and advanced cryptography, **UniQrypt** offer 4, 8 or 16 zones. Those are individually secure thanks to different read and write protection including independent passwords of 3 bytes length. With **UniQrypt**, you can also use **Secure Session** (MAC+ENC) established with AES-128 KEY.

Most Smart card solutions provided today are based on ROM memory, at the contrary, **Qilium** works with FLASH based memory chip. The purpose is to provide product such as **UniQrypt** as long as the system integrator need it, even if it needs a platform (IC) migration.

Moreover, flexibility given by Flash memory allows **Qilium** to keep lead times and costs at their lowest level.

To summarize, ®**UniQrypt** offers the following features:

- Product sustainability
- Advanced security
- Lower cost
- Short lead time

**UniQrypt** is provided by **Qilium**, a European company with several years of solid experience developing smart card products.



Qilium Smartcard Technology

## Application sectors

- Identification
- Sensitive Data Storage
- Secure Authenticate
- Web Authentication
- Loyalty Program

## Main Characteristics

- **ISO 7816 -3**
- **T=0 communication protocol**
- Supported data rates up to **446 kpbs**
- **2048 bits** divided in **4 zones**
- Transport/Admin key
- **Change Admin Key** possibility
- **Transaction protection** system
- **Anti-tearing** system
- Ultra-Compact **Flash** Smart Card Integrated Circuit
- **10 years** data retention
- > 100.000 cycles
- 8/16 bit CPU accelerated architecture
- Up to 40 MHz internal CPU clock

## Security

- Passwords
  - Protect READ and WRITE commands
  - **Up to 8 for read and 8 for write commands** (3 bytes length)
- Keys (v2)
  - **Mutual Authentication**
  - Up to **4 AES-128 KEYS**
  - **Secure Messaging** with MAC or MAC + ENC

# Memory Structure

## UniQrypt 2Kbits / 4 zones

| ATR | |
|---|---|
| **ADMINISTRATIVE CONFIGURATION** | |
| ACCESS CONDITIONS | |
| READ PASSWORD 1 | WRITE PASSWORD 1 |
| READ PASSWORD 2 | WRITE PASSWORD 2 |
| READ PASSWORD 3 | WRITE PASSWORD 3 |
| READ PASSWORD 4 | WRITE PASSWORD 4 |
| KEY 1 | KEY 2 |
| KEY 3 | KEY 4 |
| **USER MEMORY** | |
| **Zone 0** | **64 bytes** |
| **Zone 1** | **64 bytes** |
| **Zone 2** | **64 bytes** |
| **Zone 3** | **64 bytes** |

## Other User Memory Configuration

®**UniQrypt** is operationally compatible with a series of commands already used by integrators. Based on the ISO 7816-3 standard, ®**UniQrypt** offers all above-mentioned features and is available with other configuration than 2Kb and 4 zones:

| System | User memory | Zones |
|---|---|---|
| **UniQrypt** | 1 Kbits | 4 zones |
| | 4 Kbits | 4 zones |
| | 8 Kbits | 8 zones |
| | 16 Kbits | 16 zones |
| | 32 Kbits | 16 zones |
| | 64 Kbits | 16 zones |
| | 128 Kbits | 16 zones |
| | 256 Kbits | 16 zones |

## Command set overview

| | Command | CLA* | INS |
|---|---|---|---|
| **Administrative** | System Write | $$ | B4 |
| | System Read | $$ | B6 |
| | Write Password | $$ | BA |
| | Read Password | $$ | BA |
| **Operational** | Set User zone | $$ | B4 |
| | Read User Zone | $$ | B2 |
| | Write User Zone | $$ | B0 |
| | Mutual Authenticate | 80 | 82 |
| | Verify Password | $$ | BA |

*$$ = 0 to FF

## Command description

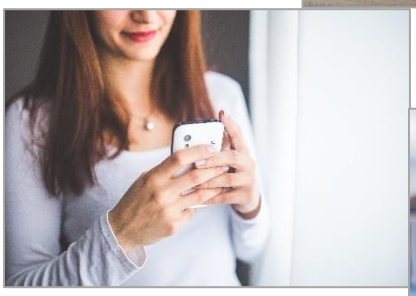
| Commands | Description |
|---|---|
| System Write* | Write Passwords, Keys and Access conditions in the system area |
| System Read* | Read System Area (cf. previous row) |
| Write Password* | Set up read/write passwords (up to 8 by type) |
| Read Password | Get read/ write passwords (up to 8 by type) |
| Set User zone | Select active Area |
| Write User Zone** | Write User Data |
| Read User Zone | Get User Data |
| Mutual Authenticate (v2) | Establish Secure Session<br>(cf. c) Secure Messaging) |
| Verify Password | Check Password Validity |

*Command allowed after PASSWORD presentation

** Command allowed after access data conditions completion

## Secure messaging (v2)

| SM Mode | CLA | Description |
|---|---|---|
| Not activated | 00 | - |
| Authentication | 04 | MAC added to data |
| Encryption and Authentication | 04 | Data Encrypted (command and response)<br>+ MAC added |



***Qilium**: the company developing and providing operating systems for smart cards*

Smart cities, e-Payment, Access Control,
Loyalty, Public Transport, Telecommunication, Internet of Things...

Today, these business areas are facing new challenges and trying to bring innovative services to market. The way banks and governments digitalize their customer's experience is a perfect example of the new services in development. This shows that innovation is leading us to a world increasingly connected where subjects such as personal data security will be of central concern.

In this context, **Qilium** has been developing for over 7 years operating systems that manage functionalities, commands and security that smart cards can offer.

In its improvement research, **Qilium** puts forward flexible and quality system allowing cards to become multi-applicative in a secure environment. In a sector where customized solutions are uncommon, **Qilium** optimizes the functionalities and safeness of its products in an improvement driven vision.

Beyond our activities of component supplier, we support our partners during the full project life cycle. Requirements analysis, specifications writing, Javacard applet development and personalization are examples of services that we offer to your card manufacturer. All this ensures optimal maintenance and allows Qilium to help its partners in reaching their objectives in terms of innovation, security and quality.

# Contact


## Qilium

2, Rue des Foudriers
B-7822 Ghislenghien
Belgium

Tel: +32 (0) 68 65 65 27
thw@qilium.com