

# MULTIQ<sup>®</sup>

ICAO - eMRTD

E-Identity | E-Passport | E-Driving Licence



## MULTIQ<sup>®</sup> ICAO is a Secure Element for Electronic Machine-Readable Travel Document



ICAO - eMRTD  
ISO/IEC 18013  
TrLDS1.7



E-Identity &  
E-Driving Licence



Secure  
Access Control



CC EAL5+ High  
Certified HW



E-Service  
Secure Access

MULTIQ is a card operating system (COS) providing a large set of configurations in contact, contactless and dual interface. Complying with **ISO/IEC 7816-3** and **ISO/IEC 14443 A/B** standards, MULTIQ allows to address multiple projects with a single solution. Offering best-in-class technology in terms of data transfer rates (up to 848 Kbps), anti-tearing and transaction protection mechanism, MULTIQ characterises QILIUM state-of-the-art Integrated Circuit (IC) technology.

Embedded into smart card and passport, MULTIQ let access to **ICAO TrLDS1.7** structure complying with **ISO/IEC 18013** standard. Its **4-stages lifecycle** confers to MULTIQ a true flexibility permitting to easily manage data structure, access conditions and keys during electric personalisation and configuration.

From *Advanced Access Control systems* verifying Biometrics (Finger prints, Iris or Face) with Match-on-Device to *Governmental e-services access with NFC-device*, MULTIQ provides an easy-to-integrate **ISO/IEC 7816-4** compliant solution. Featuring best-in-class security with secure messaging and mutual authentication, MULTIQ provides ICAO Access control and security features such as Basic Access Control (**BAC**), Supplemental Access Control (**EAC**, **PACE**) and Authentication (**PA**, **AA**).

### MAIN FEATURES

- Adaptable and flexible file structure
- File system based on ISO/IEC 7816-4
- No restriction in applications quantity
- Delete of file without memory loss
- Transport key protection
- Customizable ATR
- Anti-tearing system
- Transaction protection system
- Detection of Fraudulent chips
- Anti-collision

### SECTORS

- GOVERNMENT
  - E-Identity | E-Driving Licence
  - E-Passport
  - E-Health

### ICAO – MRTD SECURITY

- **BASIC ACCESS CONTROL**
  - Basic Access Control (BAC)
- **SUPPLEMENTAL ACCESS CONTROL**
  - Extended Access Control (EAC)\*
  - Password Authenticated Connection Establishment (PACE)\*
- **INTEGRITY - AUTHENTICITY**
  - Passive Authentication (PA)
- **ANTI-COUNTERFEITING**
  - Active Authenticate (AA)\*

\*To be integrated

All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner. The information presented in this document does not form part of any quotation or contract, is believed to be accurate and reliable and may be changed without notice. No liability will be accepted by the publisher for any consequence of its use. Publication thereof does not convey nor imply any license under patent - or other industrial or intellectual property rights.

©2018 Qilium S.A.



## SECURITY

- PIN CODE
  - at card level
  - at application Level
- KEY FILE
  - at card level
  - at application Level
- SECURE MESSAGING
  - MAC
  - MAC + ENC
- MSE (Manage security environment)

## CRYPTOGRAPHIC ALGORITHMS

- DES/3DES
- AES (up to 256-bit)\*\*
- SHA 1 & 2
- RSA (up to 4096-bit)\*\*
- ECC (up to 521-bit)\*\*

\*\* Depends on semiconductor and its cryptographic library.

## PACKAGING

- Sawn wafer
- Contact module
  - 8 pins
  - 6 pins
- Contactless module
- Prelaminates
  - PVC
  - Polycarbonate
- Inductive technology
  - Coil on Module
  - SPS

## OPTIONS

| ICAO – MRTD SECURITY                                   | BASIC | SUPPLEMENTAL |
|--|-------|--------------|
| Basic Access Control - BAC                             | X     | X            |
| Passive Authentication - PA                            | X     | X            |
| Extended Access Control - EAC                          |       | X            |
| Active Authenticate - AA                               |       | X            |
| Password Authenticated Connection Establishment - PACE |       | X            |

\*\*\* Common Criteria EAL5+ high HW

## COMMUNICATION PROTOCOLS

### Contact

- ISO/IEC 7816-3 | T=0 / T=1
- High speed data transfer up to 215 Kbits/s

### Contactless

- ISO/IEC 14443 | A/B
- High speed data transfer up to 848 Kbits/s

### Dual interface

- ISO/IEC 7816-3 | T=0 / T=1
- ISO/IEC 14443 | A / B

## CONFIGURATIONS

- MULTIQUIS ISO/IEC 7816-4
- ICAO / MRTD ICAO DOC 9303
- NFC NDEF
- SECURE NDEF