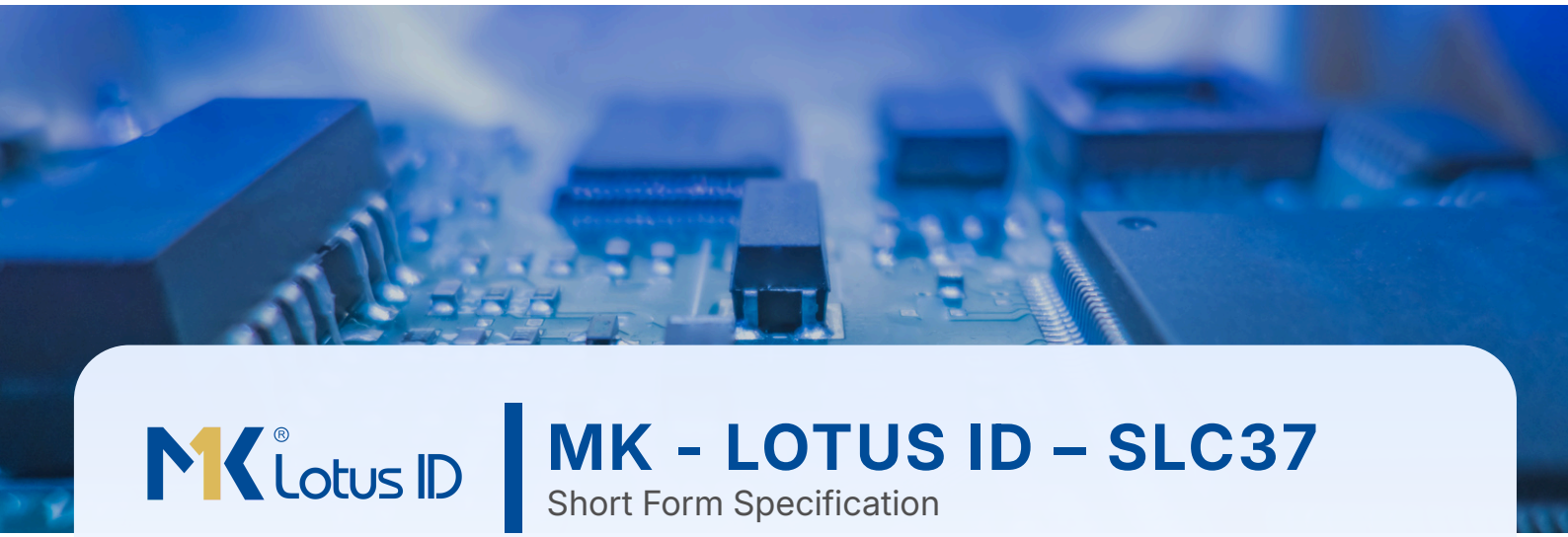
MK® Americas
Smart Digital Security



MK - LOTUS ID – SLC37

Short Form Specification

1. PRODUCT OVERVIEW

MK Lotus is a secure dual-interface ID system-on-chip solution based on a certified JC platform. It is designed for government ID documents and targets high flexibility for card manufacturers, personalization bureaus, and issuing agencies. The product builds on global standards extending memory capacity, configurability, and application flexibility

2. PLATFORM AND STANDARDS

- JC 3.0.5 Classic Edition operating system
- GlobalPlatform® 2.3.1
  - Secure Channel Protocols: SCP02 and SCP03
  - Multiple security domains
  - Delegate management
  - Physical delete with garbage collection

3. PLATFORM AND STANDARDS

- Infineon SLC37PDA secure microcontroller
- 32-bit Security Controller
- 40nm flash technology
- Up to 130 KB user non-volatile memory (NVM)
- Best-in-class RF performance
- Dual-interface support
  (COM & soldering - contact and contactless)

4. INTERFACES AND PROTOCOLS

- ISO/IEC 7816 T=0 and T=1 contact protocol
- ISO/IEC 14443 Type A contactless interface

5. CRYPTOGRAPHIC CAPABILITIES

- **Cryptographic coprocessors**
  - RSA and ECC acceleration
- **Advanced Encryption Standard (AES)**
- **Triple Data Encryption Standard (3DES)**
- **Signature algorithms**
  - DES MAC
  - AES MAC
  - RSA (SHA1, -2)
  - ECC (GF_p, GF_2m)
- **Key agreement**
  - DH, ECDH
- **Random Number Algorithms**
  - PSEUDO_RANDOM, SECURE_RANDOM
  - AIS31 DRNG (pseudo random)
  - NIST SP 800-90A DRNG compliance (pseudo
  - random)
  - ANSI X9.31 DRNG (pseudo random)
- **Message Digest & Initialized Message Digest Algorithms**
  - SHA-1,
  - SHA-224/256/384/512
- **Key Sizes**
  - DES: 64/128/192 bits
  - AES: 128/192/256 bits
  - RSA: 1024 – 4096 bits (transient up to 2048-bit)
  - ECC: up to 521-bit for GF(p)
- **Key Types (includes all JC3.0.x transient keys)**
  - DES, AES: PERSISTENT, TRANSIENT
  - RSA: PUBLIC, PRIVATE,

https://mkamericas.com | Khang@mkamericas.com

6. GOVERNMENT ID AND APPLICATION SUPPORT

The platform supports preloaded ID applets and allows post-manufacturing configuration prior to card issuance.

Supported or targeted ID applications include:

- **ePassport, eID, eResidence Permit**
  - ICAO DOC 9303
  - AA
  - EAC
  - Native Acceleration BAC, PACE
- **eDrivers License**
  - ISO/IEC 18013
  - AA
  - EAC
  - Native Acceleration BAP, PACE
- **Match on Card**
  - NIST / MINEX certified
- **eSign**
- **FIDO**
- **Combinations of above**
- **Customized applications based on JC and GP framework**

7. PERSONALIZATION AND ISSUANCE

- Applet load/delete features for flexible stock management
- Global Platform standard personalization
- RF tuning capability to adapt to different card bodies, modules, and antenna designs
- Personalization packages:
  - Issuer
  - Preconfigured
  - MK Smart

8. DELIVERY FORMS

- **Sawn wafers**
- **Dual-interface micromodules**
  - gold and silver variants
  - Coil on module
  - Soldering
- **Inlay**
  - Sheet format 3*8 (ID1)
  - Sheet format 2-up (ID3)
- **Card (ID1)**
  - White card
  - Pre-printed
  - Pre-printed & Personalized
- **Datapage (ID3)**
  - White
  - Pre-printed
  - Pre-printed & Personalized

9. DEVELOPMENT AND ECOSYSTEM SUPPORT

- Sample scripts and personalization support
- Engineering assistance for development, validation, production and issuance

10. CERTIFICATION

- **OS & Applets**
  - PP0055 - CC EAL4+ (BAC)
  - PP0056v2 - CC EAL5+ (EAC)
  - PP0068v2 - CC EAL5+ (PACE)
- **Development & Manufacturing:**
  - GP (FIME)
  - ICAO (ICube)
  - CC MINSSR
  - Intergraph
  - ISO 27001
  - ISO 9001

MK Americas
Smart Digital Security

Headquarters:
2445 NE Division Street.
Suite 200
Bend. OR.97701

https://mkamericas.com
khang@americas.com
+84-24-90 344 5945