

CLXSU512KJ3/DIJ

Dual Interface Java Card

CREDENTIALS™ from CardLogix securely enables an enterprise to authenticate employees, control access, and integrate multiple functions on a single card. The CREDENTIALS family of cards is a mission critical component for the infrastructure you need to keep your system available and secure. Build confidence in your chain of trust with proven Java card technology and CardLogix.

CREDENTIALS is designed for the next generation in Identity Badges with multiple-use applications. These cards function as contactless tokens as well as secure network sign-on passes with full authentication. Other built in functions can be combined with healthcare, transportation, e-commerce, and stored value systems applications.

CREDENTIALS-J cards lower the total cost of ownership by adhering to many industry standards and by utilizing the market strength of the Java Card API. This allows use of existing 3rd party applets that can decrease your time to market.

CardLogix smart cards can grow with your system, evolving through post issuance of on-card applications. The CREDENTIALS-J card is based on mature Java Card™ and Global Platform architectures and is readily deployable into existing or new PKI environments.

CardLogix CREDENTIALS cards give you the greatest degree of design flexibility. The CLXSU512KJ3/DIJ card is a blank canvas which lets you create the system that is right for you. Built-in functionality includes issuer configurable advanced PIN/Password security logic, AES, DES, TDEA, and RSA Public Key Encryption, SHA-1 and SHA-256 bi-directional authentication, and an advanced file management system.

CREDENTIALS-J cards comply with all major open standards such as ISO 7816-1-5, 8, 9, 15, ISO 14443B, Java Card 2.2.1, Global Platform 2.1.1, PCSC, Microsoft CAPI, and PKCS 11.

The CPU is both hardened for security and performance enhanced. The CLXSU512KJ3/DIJ card features a 72k Byte user memory (EEPROM), a high speed encryption co-processor, a hardware random number generator, and 256 bytes of RAM for fast key management.

Durability is built in with patented flexible bump bonding technology. The cards feature a robust, long-life, printable body that can be customized with a variety of physical security mechanisms. Applet development is supported by the latest open source tools and libraries.

With CREDENTIALS™ You Can:

- Build National IDs
- Reduce costs and complexity
- Provide a single federated source for all credentials
- Dynamically add applications as needed

Supported algorithms:

- AES-128
- MD5
- DES
- TDEA
- RSA-1024
- RSA-2048
- SHA-1
- SHA-256

Certifications & Accreditations:

- EAL 5+
- FIPS 140-2 Level 2 (overall)
 - Roles, Services, and Authentication: Level 3
 - Physical Security: Level 4
 - EMI/EMC: Level 3
 - Design Assurance: Level 3

Other Features:

- RSA Signature Algorithm for certificate signing
- Each file can be read and/or write protected
- Triple layer programmable password security
- On-Card key generation
- The card management key is only accessible through the contact interface.
- ATR configuration and T=0, serial interface in accordance with ISO 7816 and ISO 14443B
- Optional high speed communications “PTS” negotiated mode up to 115k baud
- Operating voltage range: 3V to 5V
- Ultra low power CMOS (100 µA standby, 10 mA active)
- Data retention > 10 years
- Endurance: Minimum of 5x10⁵ write/erase cycles
- Electro-static discharge protection > 4,000V

CardLogix

16 Hughes, Suite 100 • Irvine, California 92618 • PH: (949) 380-1312 • FAX: (949) 380-1428

Feature	Subfeature	
JC API	Supported Cryptographic Functions	
javacard.security. KeyBuilder	JC 2.2.1 LENGTH_DES LENGTH_DES3_2KEY LENGTH_DES3_3KEY LENGTH_RSA_2048 LENGTH_RSA_1024 LENGTH_RSA_768 LENGTH_RSA_512 TYPE_AES	LENGTH_AES_128 TYPE_DES TYPE_AES_TRANSIENT_RESET TYPE_DES_TRANSIENT_DESELECT TYPE_DES_TRANSIENT_RESET TYPE_RSA_CRT_PRIVATE TYPE_RSA_PRIVATE TYPE_AES_TRANSIENT_DESELECT TYPE_RSA_PUBLIC
	The key builder package supports the generation of DES, Triple DES and AES keys of 128 bits, as well as RSA 512, 768, 1024 and 2048.	
java.security. KeyPair	ALG_RSA	ALG_RSA_CRT
	Standard and CRT key pairs from 512-2048-bits in increments of 32-bits may be generated.	
java.security. MessageDigest	ALG_SHA ALG_MD5	
javacard.security. RandomData	ALG_PSEUDO_RANDOM	ALG_SECURE_RANDOM
javacard.security. Signature	ALG_AES_MAC_128_NOPAD ALG_DES_MAC8_ISO9797_M1 ALG_DES_MAC8_ISO9797_M2 ALG_DES_MAC8_NOPAD ALG_RSA_SHA_ISO9796	ALG_RSA_SHA_PKCS1 ALG_SHA_256 MODE_SIGN MODE_VERIFY
javacardx.crypto. Cipher	ALG_AES_MAC_128_NOPAD ALG_AES_BLOCK_128_CBC_NOPAD ALG_AES_BLOCK_128_ECB_NOPAD ALG_DES_CBC_ISO9797_M1 ALG_DES_CBC_ISO9797_M2 ALG_DES_CBC_NOPAD ALG_DES_ECB_ISO9797_M1	ALG_DES_ECB_ISO9797_M2 ALG_DES_ECB_NOPAD ALG_RSA_NOPAD ALG_RSA_PKCS1 MODE_DECRYPT MODE_ENCRYPT

On-Card Security Features

Bus & Current scrambling
 Internal guards against side channel analysis (SPA, DPA, SEMA, and DEMA)
 Velocity checking
 Documentation control, restricted access to data, thru NDAs, wafer/die monitoring
 Dummy computations
 Error counter authentication
 Hardware MMU, acts as firewall
 Memory encryption
 No regular layout structures
 No test mode for the I/O port. Test circuitry physically removed at die scribe
 Randomized instructions, wait states, and encryption algorithms - randomizes power consumption
 Self-timed memories (not related to input clock)
 Transport code / Unique chip IDs
 Use of lower physical layers for EEPROM
 Voltage / Frequency control (glitch protection)

CardLogix

16 Hughes, Suite 100 • Irvine, California 92618 • PH: (949) 380-1312 • FAX: (949) 380-1428

©2007 CardLogix Corporation®. All information is preliminary and CardLogix retains the right to change and/or withdraw any portion without notice. This document and its contents are covered under U.S. copyright and register laws. All rights reserved.

7400021F