Credentsys™

Dual Interface Smart Card Family Selection Guide

CardLogix

CREDENTSYS™ CARD FAMILY

Credentsys™ is a secure smart card family that is designed for national ID systems, passports, and multi-use enterprise security environments. The family is certified to FIPS 140-2 and 201-1/SP800-73-1 specifications.

CardLogix Credentsys smart cards achieve high security assurance by resisting identity fraud and tampering, using rapid electronic authentication.

Credentsys cards offer a combination of high performance and cost-effectiveness by running on advanced 32-bit RISC processor cores with DES & PKI Crypto acceleration. Two different configurations are available, supporting Java™ and MULTOS™ applets. All cards include contactless communication protocol ISO 14443 Type A or B.

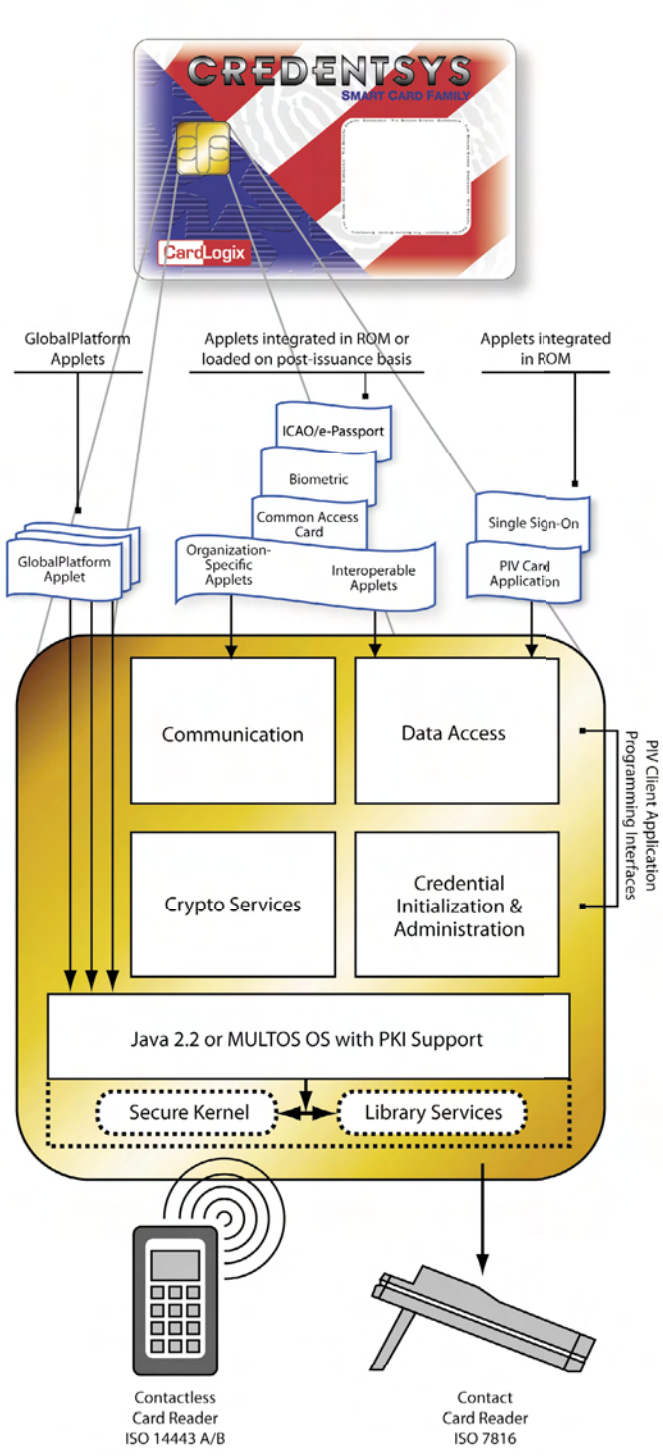
Credentsys cards offer a high level of built-in security with abnormal condition detection sensors to uncover changes in voltage, light, temperature, frequency, and other forms of tampering, such as glitch generation.

All cryptographic key objects, PIN objects and other sensitive data are always stored in non-volatile memory in an encrypted format. Integrity checks are performed on all critical system and data components prior to each access in order to detect tampering, allowing the Credentsys secure kernel to take defensive action. The memory protection unit is used for secure isolation of applications and OS code. All supported chips have received Common Criteria EAL 5+ certification.

The Credentsys card's crypto library utilizes hardware crypto accelerators for 3DES, RSA, and DSA operations. The chips and OS's are designed to withstand differential timing (DTA) and power (DPA) attacks and are fully compliant with FIPS 140-2 level 3 requirements. On-card RSA asymmetric key pair generation is supported up to 2048 key lengths.

The Credentsys card family also supports full implementation of a logical credential data model that includes, but is not limited to, PIV II, Card Holder Unique ID, and PIV Authentication data as well as biometric, facial, and fingerprint data. The optional extension to the PIV data model includes dedicated key pairs with a certificate for digital signatures and key management, plus a special authentication key for additional physical access applications. All standard PIV key reference values are supported in the PIV II interface.

Credentsys cards are ideal for U.S. government Personal Identity Verification (PIV II) projects as mandated by the HSPD-12 Directive.



Features:

- Operating ranges from 2.7 V to 5.5 V
- Power-saving Wait and Very-Low-Power Stop modes
- Power-up detection
- Full GlobalPlatform support

Memory:

- 72k - 128k bytes of user EEPROM

FIPS 140-2 Level 2 and 201-1 SP800-73-1 Certified:

- Full support for high-level PIV client APIs and low level interface commands at card edge
- Built-in PIV II Card Application with CHUID data object; post-issuance applications can be loaded as required
- Authentication of an individual is performed via PIN or by utilizing Biometric methods

Security:

- Dedicated hardware for protection against SPA/DPA/DEMA/SEMA attacks
- Velocity checking
- Advanced protection against physical attacks
- Environmental protection systems
- Voltage monitor
- Frequency monitor
- Temperature monitor
- Light protection
- Secure memory management/access protection (Supervisor Mode)

Application Resources (Depending on Device):

- Persistent Memory (EEPROM): 62 kB - 128 kB
- Transient Memory (RAM): 2 kB - 8 kB
- Transaction Buffer: 512 bytes
- APDU Buffer Size: 261 bytes

Communication Protocols:

Contact Mode:

- ISO 7816 T=1, baud rates from 9600 to 650k

Contactless Mode:

- Contactless Interface Controller (CIC) with full support for ISO/IEC 14443 Type A & B protocols
- Supply voltage clamp and regulation
- Reader-to-Card:
  - ISO/IEC Type A: 100% ASK modulation and modified Miller bit coding
  - ISO/EIC Type B: 10% ASK modulation and NRZ Bit coding
- Card-to-Reader:
  - ISO/IEC Type A: Generation of 847.5 kHz subcarrier with OOK modulation and Manchester bit coding
  - ISO/IEC Type B: Modulation of incoming RF carrier by resistive load switching / generation of 847.5 kHz subcarrier with BPSK modulation / NRZ data encoding
- Baud Rates: Up to 424 kbps
- RF Frame: Up to 256 Bytes

On-Card Registry:

- Number of applets limited only by available persistent memory
- Fast search times for any entry selection

Data Objects Supported:

- X.509 certificate / card validation key
- CHUID
- Cardholder biometrics

CREDENTSYS PRODUCT SELECTOR

CardLogix Part Number	O.S. Type	Product Functionality/ Applications	Supported Algorithms	Communication Protocols	User Memory	Standard Applets
CLXSU512KJ3/ DIJ	Java Java Card Platform, Version 2.2.1 Global Platform 2.1.1	National ID Programs Healthcare Informatics Driver Licenses Voter Registration Enterprise IDs	AES-128 MD5 DES TDEA RSA-1024 RSA -2048 SHA-1 SHA-256	T=0, T=1 ISO 14443 Type B	72k Bytes	PIV II – Provides enablement of the card edge abstractions as defined in the FIPS 201 SP800-73 documentation for complete government interoperability. -or- SafeSIGN - Provides digital signatures and PC domain login. For Win XP and Vista. The applet supports PKCS#11: Cryptographic Token Interface Standard and includes a Cryptographic Service Provider (CSP). -or- ICAO
CLXSU001MJ4/ DIJ (Coming Soon)	Java Java Card Platform, Version 2.2.1 Global Platform 2.1.1	National ID Programs Healthcare Informatics Driver Licenses Voter Registration Enterprise IDs	AES-128, 192, 256 MD5 DES TDEA RSA-1024 RSA -2048 SHA-1 SHA-256 ECC-163, 233, 283	T=0, T=1 ISO 14443 Type B	144k Bytes	PIV II – Provides enablement of the card edge abstractions as defined in the FIPS 201 SP800-73 documentation for complete government interoperability. -or- SafeSIGN - Provides digital signatures and PC domain login. For Win XP and Vista. The applet supports PKCS#11: Cryptographic Token Interface Standard and includes a Cryptographic Service Provider (CSP). -or- ICAO
CLXSU512KC6/ DIM	MULTOS	National ID Programs Healthcare Informatics Driver Licenses Voter Registration Enterprise IDs	DES TDEA RSA -1024 RSA-2048 SHA-1	T=0, T=1 ISO 14443 Type A & B	72k Bytes	PIV II – Provides enablement of the card edge abstractions as defined in the FIPS 201 SP 800-73 documentation for complete government interoperability. -or- ICAO

Middleware Support

- All Standardized PIV II Middleware that meets SP800-73-1 requirements
- ImageWare Systems Card Management System (CMS)
- Intercede CMS
- RSA PIV II Middleware and CMSs
- SafeSIGN Middleware Cryptographic Service Provider (CSP)
- SafeSIGN Token Manager
- Worldwide Trust CMS

Additional Card Options *

- Lithographic Card Printing
- Guilloche and Rosettes
- Microprinting
- Laser Engraving
- Magnetic Stripes (HiCo, LoCo, and colored)
- Card Punching
- Optically Variable Devices (OVDs)
- Holograms and Holomags
- Barcode Printing
- Serialization and Variable Image Printing
- Tamper-Evident Signature Panels
- Tamper-Evident Packaging
- Ultraviolet Inks
- Hidden Images (Card Validator™ graphics)
- Color Shifting Inks
- Colored Interlayers

Encoding Options

CardLogix can program your card orders, including Mag-Stripe encoding and software loading. Other options include fulfillment (e.g. affixing cards to special carriers such as promotional collateral). You can also order cards serialized and inserted into envelopes that can be stamped and mailed. Card lots can also be individually sleeved or shrink-wrapped for non-secure delivery.

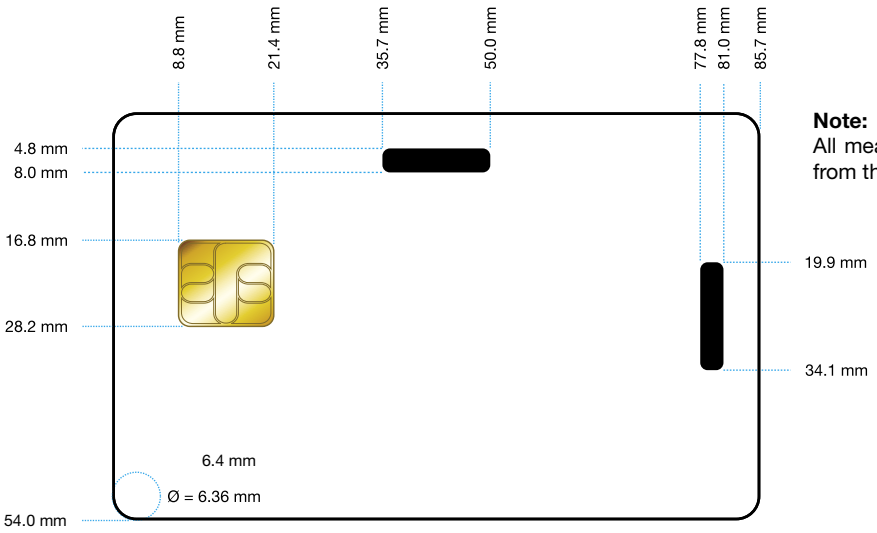
Magnetic Stripe: Can be encoded to various industry specifications. Our Magnetic Stripe cards can be encoded to the specifications set by leading manufacturers of automated banking equipment for tracks 1, 2, and 3.

Applet & Data Loading: CardLogix can load both Java and MULTOS applets and all standard types of data, such as identification records, health histories, etc.

Certificate Key Loading: For security applications, CardLogix can load the card with digital certificates, transport and encrypted keys.

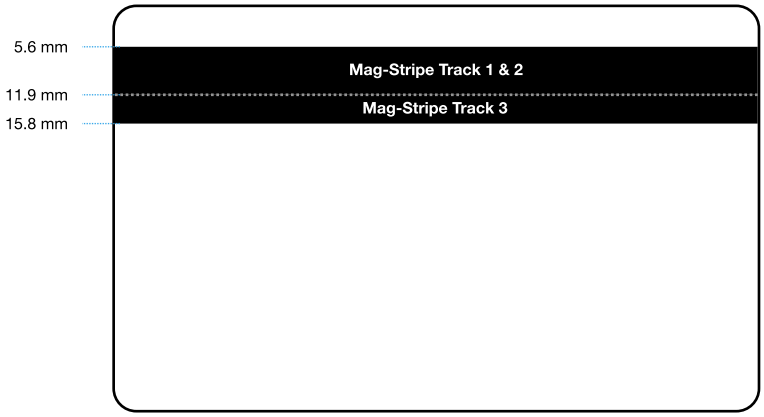
*Please see CardLogix Graphics & Security Printing Guide for further details.

Dimensions for Smart Card Options

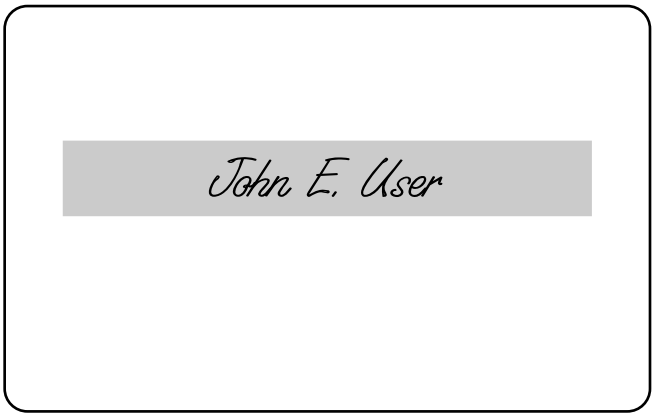


Note:
All measurements are made from the top left corner.

Please note that the module placement on CardLogix's dual interface cards is atypical of usual module placement, but still abides by ISO standards.

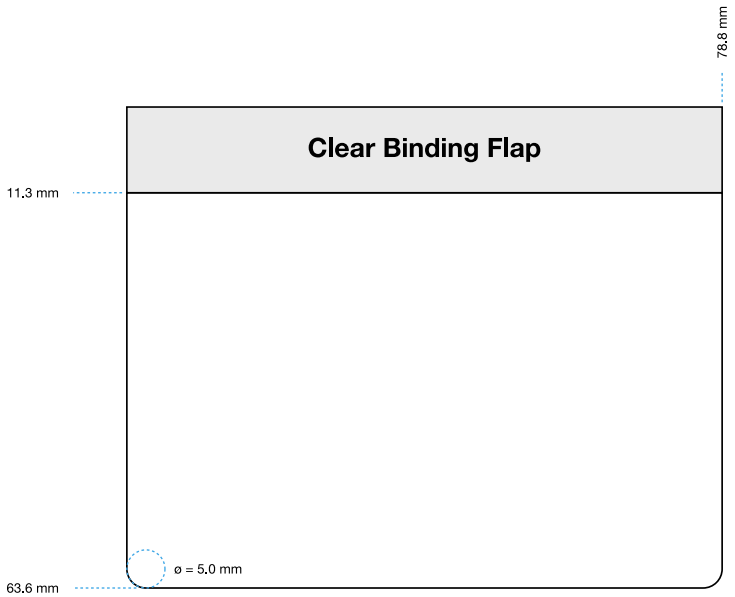


Magnetic stripe cards are available in track 1, 2, and 3 configurations in either high-coercivity or low-coercivity. Colored and holographic stripes are available as options.



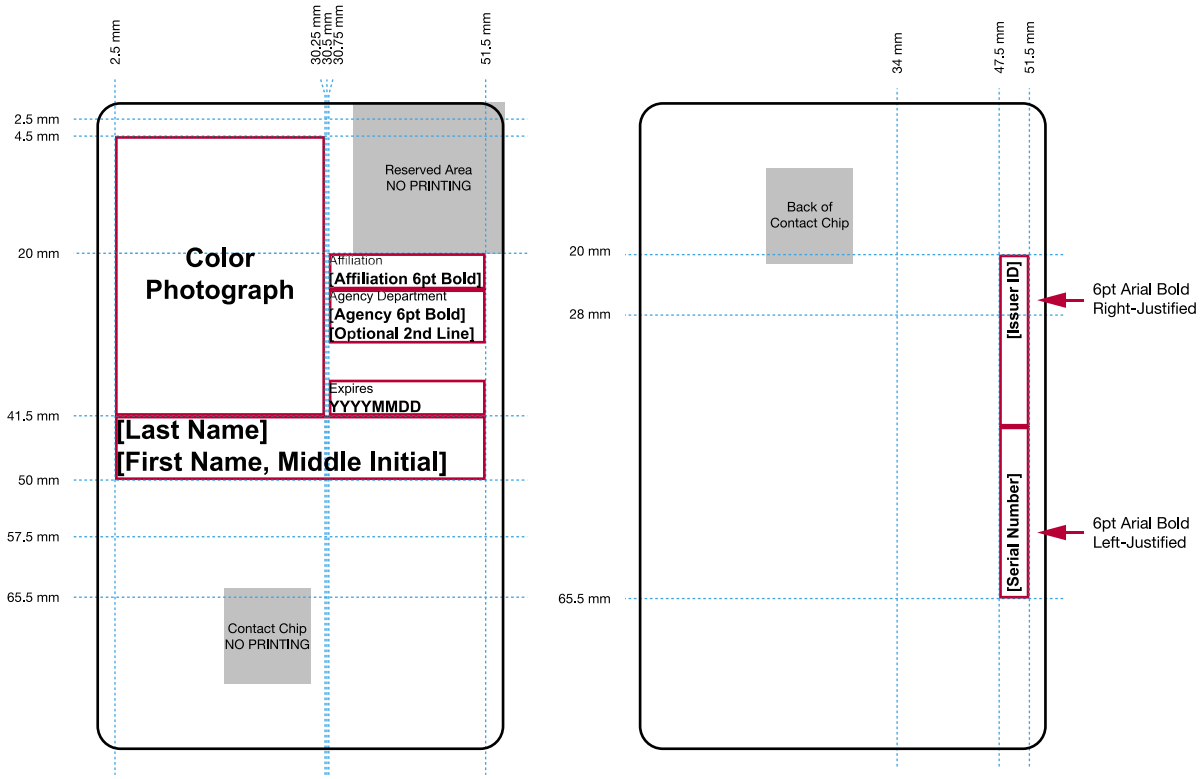
Signature panels can be placed on any area of the card, provided that it does not overlap any other card option element such as a badge punch-out or mag-stripe. Optional tamper-evident and custom signature panels are also available.

Standard ePassport Card Insert Dimensions



Please note that the ePassport Card Insert diagram is shown at 70% scale.

Standard PIV Card Topology



Only PIV data required by the National Institute of Standards and Technology is displayed. Additional optional data can be included as well. Please call CardLogix for further details.

Quality

CardLogix Corporation is absolutely committed to providing defect-free products and services to our customers in partnership with equally committed suppliers and authorized dealers.

- California C Corporation
- CA Resale# SREAA 97-124323
- D&B# 867418899
- SIC Codes# 3577, 3089, 5162
- UNSPCSC Code# 32101617
- Harmonized Code# 8542.10.0000
- NAICS Codes# 334119, 326199, 334418, 334519, 42261, 51421
- CAGE Code# 1KV39
- Congressional District# 47

16 Hughes, Suite 100 · Irvine, CA 92618 · United States
Phone +1 949 380-1312 · Fax +1 949 380-1428 · www.cardlogix.com · sales@cardlogix.com