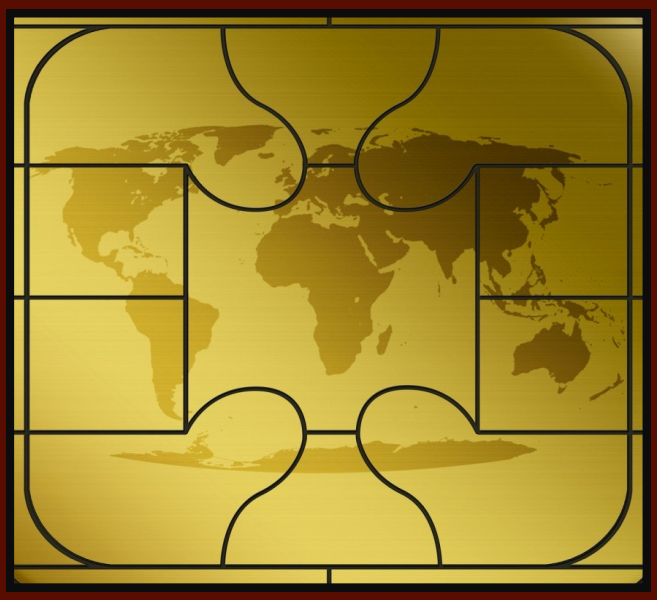
SecureXperts Crypto Micro-SD



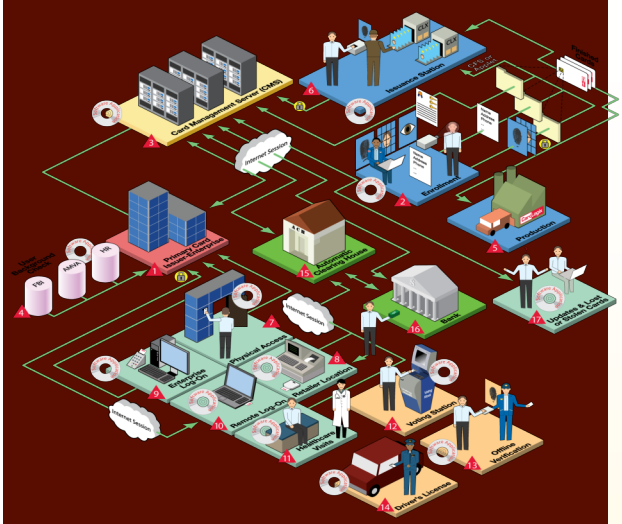
Cryptographically Secure Embedded Devices/Solutions

NASA Space Life Sciences Center

505 Odyssey Way, Kennedy Space Center, FL 32953

Telephone (877) 230-7011

"When Security is not an Option"



ABOUT SECUREXPERTS

SecureXperts is a consulting firm with over 14 years' experience providing mission centric services and solutions to government, enterprise commercial and public/private organizations, we have earned the trust and confidence as a partner excelling in meeting customer requirements and demands effectively and proficiently.

Product/Solution Features:

High Performance

Onboard processor for cryptographic applications

High Assurance

Protection for sensitive data stored on the chip

High Scalability

Designed for integration with single sign on (SSO) applications and interoperability with disparate systems.

Technology at work for you

CONNECTING YOUR BUSINESS TO THE TECHNOLOGY RESOURCES YOU NEED.

The SecureXperts Micro SD solution is an encryption unit known as a "secure element", or cryptographic security module (CSM) that exceeds the necessary requirements for NIST and DoD derived credential enabled mobile devices. The secure element is FIPS 140 Level 3 compliant chip and provides high assurance key management and encryption capabilities. Using this solution, only approved software is able to execute on the SD micro unit, which validates the integrity of the software upon each power up. The secure element can support up to 512 keys and 32 certificates, well above the amount required for the PKI Federal Bridge and the DoD PKI. The supported libraries a full NSA Suite B, including AES and Elliptic Curve Cipher Suites

SecureXperts develops and provides embedded technology services that works with NIST approved cryptographic micro-SD cards are FIPS 140-Level 3 validated and provide Level of Assurance LOA-4 credentials (network authentication/digital signing/digital encryption) to physical security manufacturers and systems developers requiring compliance and certification/validation within high assurance environments.

For the purposes of derived credential implementation, hardware based cryptographic micro-SD is most well suited because it can generate federally and commercially trusted public/private key pairs on the cryptographic module externally, instead of using the device hardware. This separates the security functions of the devices from the processing (cryptographic co-processor), making the system easier to design, test, and evaluate at the board, component, and chip layer.

Smart phones, tablets, laptops computers, and other specialized devices (access control card readers, intrusion detection devices, explosives/chemical sensors, video surveillance cameras) can use a this cryptographic Micro-SD card for law enforcement, national defense, and high-assurance critical key (CKIP) infrastructure protection systems, and Industrial Control Systems (ICS) applications, making them extremely robust and resilient to attack.

A cryptographic micro-SD card acts in a similar manner to the smart chip on a smart card. The processors on a cryptographic micro-SD card allow for the generation of a public/private key pair with a restriction on the exportation of the private key. The private key can be PIN protected in the same way that the smart card user PIN protects its private key. Since the CAC is too large to be plugged into a mobile device, a FIPS 140 approved cryptographic micro-SD card is an extremely viable option to implement secure derived credentials on mobile devices. As derived credentials become more defined and more widely implemented by NIST and DoD, commercial companies will continue to develop more specialized and more customized NIST approved cryptographic micro-SD cards and mobile devices.

Technology Infrastructures Supported:

- Mobile devices, workstations, servers, switch, firewalls
- Federally Trusted Certificate Authorities
- Embedded Crypto API for video Management Systems
- Secure HSM Interface for physical devices
- Certificate Validation/Enrollment across federated systems
- Enterprise Interconnectivity with disparate physical security systems
- Hashing and cyclical redundancy checks of digitally stored video

Standards :

Federal Guidelines

(FIPS 140-2 Level 3) and Federal ICAM guidelines

Modules Supported

SDIO Physical Layer Standard (mini/micro) version 2.0

Emerging Standards

NIST Supply Chain Management, Digital Media Source and Authentication

Application	**Device Interface**	
Middleware	**PKCS#11**	**SecureXperts API**

Encryption Grades

Government (Non-Exportable) (2048bit)	**Commercial U.S. (2048 bit)**
	Exportable (1024 bit)

Mobile Device Security Hardware Generated Derived Credentials

The public/private keys are generated on a hardware cryptographic module that is FIPS 140 validated Level 3. By generating the keys on a removable (micro -SD) hardware token for the mobile device, the derived credential provides a Level of Assurance LOA-4. The private key on the hardware token is protected by a 6 digit PIN. The hardware token would provide a means to protect the derived credential after a certain number of consecutive failed authentication attempts.

A hardware cryptographic module provides multiple advantages over the software cryptographic module. Hardware tokens are intrinsically more secure than a software credential. One major advantage of the hardware generated credential is that the private key is generated on the hardware module itself. Therefore, only the person in possession of the cryptographic token and with knowledge of the PIN are able to use the private key for any PKI function. Since the private key never leaves the hardware token, all cryptographic operations using the private key are performed on the token and not in software. In essence, a removable hardware cryptographic token would provide the same security features as a smart card just sized to integrate into a mobile device.

PKI smart card embedded into Mini-Micro SD- Can be integrated into trusted platforms for Government, Commercial, Public Safety, Industrial, Healthcare, Medical, Defense, and other applications requiring trusted computing platforms.

Benefits- Provides the highest certified and trust security levels available in trusted markets today using hardware based digital certificate Public Key Infrastructure (PKI)

Technical Specifications:

- ARM based smart chip encoding supporting encryption of voice, video, and data
- RSA 1024/2048 Bit AES Algorithms (Exportable)
- ECC 4096 Bit ECC-NSA Sweet B (Non-Exportable)

U.S. Department of
Homeland Security
Federal Protective Service

"Industry's best practice to bind people and devices to trusted logical information technology and trusted network infrastructure"

SecureXperts Crypto Micro-SD

SECUREXPERTS

INFORMATION SECURITY CONSULTING

505 Odyssey Way
Kennedy Space Center, FL 32953

Toll Free: 877-230-7911
Fax: 800-786-1752
Www.securexperts.com