HID Combo card with Cosmo v7 chip

Combo Cards Overview

HID delivers ready to use smart cards that combine in a single card the capabilities required to deliver secure physical and logical access control. For most customers, the Crescendo line of cards are the most appropriate solution since they provide out-of-the-box compatibility with a large number of applications and existing systems and are available as off-the-shelf products through the global network of HID partners.

However, there are occasions where specific mandates makes the use of a specific contact chip a requirement, and for those cases HID is able to custom manufacture *combo* cards that combine in a single card different technologies used for physical access and a particular contact chip.

The combo cards with Oberthur Cosmo v7 chip provides customers with a contact chip that has been certified to FIPS 140-2 Level 3 with the certificate number 2437 of the NIST Cryptographic Module Validation Program.

Key Benefits

- Single card for physical and logical access
- Available with combinations of HID Prox, iCLASS, Mifare or DESFire physical access technologies
- Compatible with HID ActivID Credential Management System
- Compatible with HID ActivClient middleware for CryptoAPI and PKCS#11 compatibility

Features

HID Como cards combine the capabilities of the HID card body that includes technologies with physical access with the specific features of the chip that is embedded in the card body. In the case of the combo card with Oberthur Cosmo v7 there are specific capabilities of that chip that are available in the finished card.

ID One Cosmo Features

- Contact Interface IS0 7816 T=0/T=1
- GlobalPlatform version 2.1.1
- JavaCard version 2.2.2
- Extended Length APDU
- RSA key up to 2048bits
- Elliptic curves DSA key up to 521 bits
- EC Diffie-Hellman
- DES/3DES
- AES 128/192/256 bits

- Hash SHA up to 512bits
- Cryptography compliant with NSA suite B recommendation

Security Certification

The validated module under certificate #2437 is a single chip embodiment validated to FIPS 140-2 Overall Security Level 3. It is the combination of the HID Global ActivID Applet Suite v2.6.2B (denoted ActivID Applet Suite below) running on the Oberthur ID-One Cosmo v7-n (denoted platform below). The platform has been previously validated with certificate #1236.

The platform provides an operational environment for the ActivID Applet Suite: all cryptographic algorithm implementations and associated self-tests, random number and key generation, card lifecycle management, and key storage and protection are provided by platform. The code for this functionality is contained in the platform ROM, unchanged from Cert. #1236. However, the factory configuration of the module constrains the module to the set of services provided by the platform's Card Manager (implementing a standard set of Global Platform services) and the ActivID Applet Suite.

Cryptographic Functionality

The module uses the FIPS Approved and Non-FIPS Approved but allowed cryptographic functions listed next.

Algorithm	Description	Certificate
RNG	[FIPS 186-2] Random Number Generator.	#480
Triple-DES	[SP 800-67] Triple Data Encryption Algorithm. The module supports the 2-Key and 3-Key options CBC and ECB modes. (Note: The module does not use 2-Key Triple-DES to encrypt or to wrap keys.)	#698
Triple-DES MAC	[FIPS113] Triple-DES Message Authentication Code. Vendor affirmed, based on Cert. #698	#698
RSA	[PKCS#1] RSA key generation and signature generation. The module supports 2048-bit RSA keys. All uses of RSA signature generation require hash off-card.	#403

Table 1. FIPS Approved Cryptographic Functions

Algorithm	Description
NDRNG	Hardware RNG used to seed the Approved RNG.
RSA key Decapsulation	The module supports RSA key decapsulation using 2048-bit keys; key establishment method provides 112 bits of encryption strength.
Symmetric Key Unwrap	Symmetric key unwrap allowed by IG D2 and SP 800-38F for key transport; key establishment method provides 112 bits encryption strength.

Table 2. FIPS Allowed Cryptographic Functions

Part Numbers

HID Combo cards are available in quantities of more of 1000 cards per order. For smaller quantities, consider the use of standard Crescendo cards that are available off-the-shelf through HID distributors. The part numbers that correspond to the combo card with Cosmo v7 chip are listed below.

SKU	Description
4002-B03A	Combo iCLASS 32K with Oberthur Cosmo v7
4003-B03A	Combo MIFARE Classic 4K with Oberthur Cosmo v7
4006-B03A	Combo MIFARE DESFire EV1 8K with Oberthur Cosmo v7
400A-B03A	Combo iCLASS 32K and HID Prox with Oberthur Cosmo v7
400C-B03A	Combo MIFARE Classic 4K and HID Prox with Oberthur Cosmo v7
400G-B03A	Combo MIFARE DESFire EV1 8K and HID Prox with Oberthur Cosmo v7