d'Cryptor™ ZE

Cryptographic Module

Security Policy

Hardware Versions

Model ZE-N2 : 3.0
Model ZE-N4 : 3.0

Firmware Versions

Kernel : 3.0
LFM : 1.0
AFM : 1.0

Document Number : DC/ZE-0003/FIPS
Document Version : 1.4
17 February 2006

Configuration Control

Document details

File Name:	ZE Security Policy.doc
Document Title:	*d'Cryptor* ZE Cryptographic Module – Security Policy
Document Number:	DC/ZE-0003/FIPS
Document Revision No.:	1.4
Author:	Quek Gim Chye
Approved By:	Antony Ng
Number of pages:	23
Revision Date:	17 February 2006
Remarks	Final version

Revision History

Revision	Date	Author	Comments on Revision
1.0	19 Aug 2005	QGC	Inserted certificate numbers for Approved algorithms Corrected a typo in Chapter 6.
1.1	12 Sep 2005	QGC	Revised after reviewer's comments
1.2	2 Feb 2006	QGC	Updated after reviewer's comments (amended Tables 5, 7 and 8)
1.3	15 Feb 2006	QGC	Updated Table 6
1.4	17 Feb 2006	QGC	Updated Figure 1 and the words above it

Contents

1 Scope

This document contains the specifications for the non-proprietary security policy for the *d'Cryptor*™ ZE cryptographic module. This information is required in order to satisfy in part the requirements for the validation of the *d'Cryptor* ZE at level 3 of the FIPS 140-2 standard.

This document applies to d'Cryptor ZE hardware version 3.0 and firmware versions 3.0 (Kernel), 1.0 (library firmware) and 1.0 (application firmware).

2 Introduction

The *d'Cryptor* ZE cryptographic module ("ZE") is a multi-chip embedded hardware security module designed for high security assurance applications. It accepts the field loading of up to two external firmware modules and executes loaded modules in succession after it has completed its bootstrap and other system initialization processes.

Like its predecessor the *d'Cryptor* QE, the ZE is central to the second generation *d'Cryptor* line of products where it serves as a secure cryptographic coprocessor, providing a secure operational environment and high-performance cryptographic support. The ZE supports a multitude of interfaces, including several UARTs, synchronous serial port, infrared port, smart card interface, numerous GPIOs as well as an audible buzzer driver.

The terms "ZE", "*d'Cryptor* ZE" and "the module" shall be used synonymously throughout this document.

3 Security Level

The *d'Cryptor* ZE meets the overall requirements applicable to Level 3 security of FIPS 140-2. Table 1 below shows the individual security level requirement achieved by the module:

Table 1. Security Levels

Security Requirement Area	Level Achieved
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N.A.
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N.A.

4 The *d'Cryptor* ZE

The *d'Cryptor* ZE is made up of the following four components:

- Base hardware (Hardware Version 3.0, Models ZE-N2 and ZE-N4)
- *d'Cryptor* ZE Cryptographic Kernel (Kernel version 3.0)
- Library Firmware Module, LFM (**FIPS-LFM** version 1.0)
- Application Firmware Module, AFM (**FIPS-AFM** version 1.0)

The principal hardware components of the ZE are an ARM-based processor, 80KB static RAM, NVRAM and a flash memory. It operates at a clock speed of 96 MHz.

Two hardware configurations for the ZE are available:

- Model ZE-N4, Part # DC-ZEN4-30 v3.0 : 4 MB Flash
- Model ZE-N2, Part # DC-ZEN2-30 v3.0 : 2 MB Flash

The Kernel contains the base software of the ZE, and performs the entire boot-up and initialization processes in the ZE before handing control over to the Library Firmware Module ("LFM"). Upon exit from the LFM, control is passed to the Application Firmware Module ("AFM") and thereafter to the Kernel upon exit from the AFM.

The ZE also provides a variety of cryptographic services through an internal library and an application programmer's interface (API) that resides within the Kernel. These services are made available to the LFM, and can be made available to the AFM if necessary.

The ZE, as prepared for this validation, comes with a pre-installed LFM (**FIPS-LFM v1.0**) and an AFM (**FIPS-AFM v1.0**) that provides access to all the services that are available from the internal library of the ZE. The ZE allows these modules to be replaced in the field (i.e. outside the factory). An authenticated operator who is authorized to load firmware modules will be able to load a custom-built LFM and AFM into the ZE as long as the modules to be loaded had been cryptographically signed with the correct RSA private signing key. However, the ZE would then need to be re-validated.

4.1 Cryptographic Module Diagram

Figure 1 shows a plan view of the *d'Cryptor* ZE and its cryptographic boundary. Both are indicated by the contiguous dotted red line.

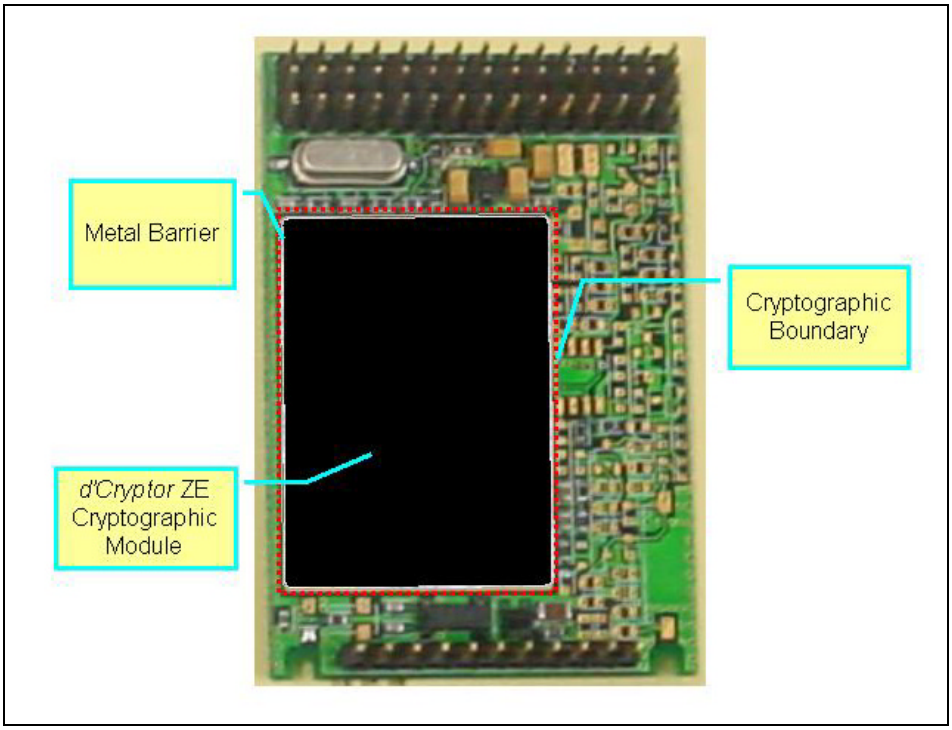

Figure 1. Plan view of *d'Cryptor* ZE (dotted red line)

4.2 ZE Interfaces

The ZE, as presented for this validation effort, uses only the UART3 port for all the communications with the outside world that it performs via service calls. The rest of the interfaces are not used in any way by the ZE, but are intended to be used by future applications that may be loaded into the module. The UART3 interface is also called the *diagnostic port*, as it outputs diagnostic status messages and accepts control commands for activation of services.

The FIPS interfaces of the ZE is made up of all the physical traces leaving the cryptographic boundary. These physical traces on the ZE PCB are presented as 77 physical access points in the form of a 45-pin main connector and a 11-pin alternate connector located on the topmost side of the ZE at opposite sides of the cryptographic boundary as well as 26 other access points on the PCB baseboard (see Figure 1). Table 2 shows the standard logical interfaces (as mandated in FIPS 140-2) and their mappings to the actual physical access points on the ZE. Pins on the main connector are numbered from 1 to 45, while pins on the alternate connector are labelled by alphabets from 'A' to 'L' (Note that 'I' is omitted). Signals that goes to the other access points are indicated with a "–". Note that of the 45 pins on the main connector, 5 pins are unused and not applicable for this validation.

Table 2. Mapping of Logical Interfaces to Physical Ports

Logical Interface	Physical Port Mapped
Data Input Interface	UART1 (44), UART2 (14), UART3 (A) All GPIOs (2, 3, 11, 14, 15, 18 to 29, 31, 32, 34 to 43, J, K, L) IRDA (E), SSP (–), Smart Card (8, 9)
Data Output Interface	UART1 (45), UART2 (11), UART3 (B) All GPIOs (2, 3, 11, 14, 15, 18 to 29, 31, 32, 34 to 43, J, K, L, –) IRDA (D), SSP (F, H), Smart Card (5, 6, 8, 12)
Control Input Interface	UART3 (A) CLK_CFG (–), EXT_CLK (G), CLK_TST (–) ST32KIN (–), STPLLIN (–), ST32KOUT (–), STPLLOUT (–) RTC_X1 (–), RTC_X2 (–)
Status Output Interface	UART3 (B) Buzzer (17)
Power Interface	Power supply (10, 13) Battery supply (16) Grounds (16, C)

4.3 Approved Algorithms

The ZE employs seven Approved algorithms, as shown in Table 3.

Table 3. List of Approved Algorithms

Security Function	Certificate Number	Remarks
TDEA	371	2-key and 3-key
AES	298	128, 192 and 256 bit keys
SHA-1	372	
HMAC-SHA-1	108	HMAC with SHA-1
RSA ANSI X9.31-1998 [ANSI X9.31]	90	1024, 1536, 2048 bits
ANSI X9.31 DRNG	125	Using AES with 128 bit key
DES	328	For use with legacy systems only. Transitional phase only. Valid until May 19, 2007.

4.4 Overview of Security Features

The ZE exists in one of two states, operating or non-operating, based on presence of the main power supply. In non-operating mode, the processor is not powered. All cryptographically sensitive parameters (keys) are stored in encrypted form in Flash memory. Encryption is done with AES-CBC and using a *Key Encryption Key* (KEK). The KEK is in turn stored in the NVRAM. The NVRAM is backed up via a backup supply that originates in a battery. The source of the backup supply is external to the ZE and would be configuration specific.

After power up and completion of self-tests, the KEK is extracted from the NVRAM and used to decrypt and validate all encrypted keys in the Flash memory. The decrypted and validated keys are then stored in the on-chip SRAM for quick access by applications. When the module is powered off, the contents of the SRAM are lost. All operational cryptographic keys remain safely encrypted in the Flash memory.

The ZE ensures that only *trusted* external firmware modules can be loaded by requiring all loadable modules to be digitally signed using a ANSI X9.31 digital signature scheme. Upon each power-up, the ZE verifies the digital signature(s) of all installed firmware modules and executes them in succession only upon successful verification.

The factory Certificate Authority generates the private and public key pairs that are used to sign and verify the external firmware modules. The public key certificates are loaded into the ZE as part of the final stage in manufacturing whereas the private keys are maintained outside the ZE and held securely by the assigned individuals (entities) who are responsible for generating and signing the external firmware modules.

The ZE provides a host of cryptographic support through an internal library and an API. All keys and cryptographic processing are isolated within this internal library and the d'Crypt Secure Micro O/S running in the ZE ensures that this region is accessible by the LFM/AFM only through the API and never directly.

The services from the ZE's internal library are always available to the LFM, but not always available to the AFM. The Kernel controls, through the LFM, the list of services that can be called by the AFM. This allows separate entities to develop codes for the LFM and for the AFM. The LFM developer may choose to expose all the internal library services to the AFM, or expose only some or even none of the services to the AFM, together with other APIs that are coded within the LFM itself. Usually, the LFM would be used for implementing software drivers for accessing ZE interfaces, and other intermediate library APIs that are needed by an end application in the AFM.

For physical security, the ZE implements a hard, opaque epoxy potting to protect the hardware and software components as well as CSPs and other cryptographic keys.

5 Approved Mode of Operation

When shipped from the factory, the ZE always operates in a FIPS 140-2 Approved mode of operation. This is indicated by the message "`Operating mode = FIPS`" that is displayed via the diagnostic port after powering up (Figure 2):

```
...
Operating mode = FIPS
...
[ZE launches the library firmware automatically if present]
```

Figure 2. Indication of the Approved Mode of Operation

If the ZE contains a library firmware or application firmware that is not FIPS validated, the ZE loses its FIPS validation and displaying the following:

```
...
Operating mode = Non-FIPS
...
[ZE launches the library firmware automatically if present]
```

Figure 3. Indication of a Non-FIPS Validated Module

6 Roles, Identities and Authentication

The ZE provides identity-based authentication to ensure that only authenticated individuals are allowed to operate the ZE and access its cryptographic services. It does not support concurrent operators or any maintenance role.

6.1 Identities

The ZE supports the following seven distinct identities:

- The **Crypto-Officer** represents the entity who is responsible for managing the security configuration of the module. This entity always assumes the **crypto-officer** role.
- The user identities **User1 to User6** represent the entities who will assume the **user** role in order to operate the module in its normal mode of operation.

6.2 Roles

The ZE provides two distinct roles – a **crypto-officer** role (CO) and a **user** role.

- The **crypto-officer** corresponds to the *Crypto Officer* role as defined in FIPS 140-2. This is a special role that typically has overall authority over the ZE. This authority is manifested in the permissions accorded to this role that grants it the right to *modify* all keys and *write* all non-system keys in the key-bank when the ZE is *first* booted up after delivery from the factory.[1] The **crypto-officer** role is assumed when performing key management-related functions such as changing keys and their attributes. The **crypto-officer** does not operate the ZE during operational modes.
- The **user** role corresponds to the User role as defined in FIPS 140-2 and represents that of a operator of the ZE in its normal mode of operation. In particular, a user role should not be permitted to carry out critical key management services.

6.3 Transition of Roles

The ZE always boots up in a "Unauthenticated role" state. In this state, no security relevant services can be performed. However, non-security relevant services are available for execution.

The ZE remains in this state until one of three things happen:

- The **Crypto-Officer** logs in successfully via the ZE's authentication services. The ZE then transits to the **crypto-officer** role and can now perform services that are available to the **crypto-officer**.
- The **User** logs in successfully via the ZE's authentication services. The ZE then transits to the user role and can now perform services that are available to that user role.
- The ZE powers down or goes to sleep (via the **Module Shutdown** service).

6.4 Authentication

An operator authenticates to the ZE by proving knowledge of the appropriate authentication key through a challenge-response protocol that employs the AES algorithm. A login request to the ZE specifies the ID of the role to be assumed after login. From the ID, the ZE uses the respective key (see Table 4) in the challenge-response protocol to ensure that the operator requesting for login possesses that key.

[1] Note that the **crypto-officer** can relinquish this right (if the operational security policy calls for it) by changing the permissions of non-system keys to deny itself this right.

Table 4. Authentication Matrix

Identity	Role to assume after login	ID	Key used for Authentication	
Crypto-Officer	**crypto-officer**	**CO**	Crypto-Officer Authentication Key	COAK
User1	**user**	**U1**	User 1 Authentication Key	U1AK
User2	**user**	**U2**	User 2 Authentication Key	U2AK
User3	**user**	**U3**	User 3 Authentication Key	U3AK
User4	**user**	**U4**	User 4 Authentication Key	U4AK
User5	**user**	**U5**	User 5 Authentication Key	U5AK
User6	**user**	**U6**	User 6 Authentication Key	U6AK

6.4.1 Strength of Authentication

The strength of the authentication mechanism depends on both the lengths of the challenge (128-bit) and the authentication key (256-bit). It can be shown that the probability that a random attempt at authentication will succeed is of the order of 2^{-128}. This is significantly smaller than the "one in 1,000,000" requirement in FIPS 140-2.

Empirical tests have demonstrated that at most 18,000 authentication attempts can be performed within a one minute period. It follows that the probability that at least one of multiple attempts over a one-minute period will succeed is very much smaller than "one in 100,000"[2].

There is no feedback of any authentication data to the operator during an authentication session.

6.5 Protection of Authentication Data

The data (CSPs) that are used in authentication are the components of the challenge-response protocol, namely a random challenge, the computed response and the authentication key. These are all maintained in the ZE's internal SRAM. In addition, a permanent copy of all authentication keys are stored encrypted in the ZE's FLASH. Both SRAM and FLASH are protected by the hard opaque epoxy that covers the entire surface of the ZE, thus offering the requisite protection of the authentication data.

In addition, all the authentication keys are endowed with special key permissions (via the *key-mask*) that allow these keys to be *read* and *modified* only by the **crypto-officer** role. All other user roles have no means of access to these keys. In this way, the ZE achieves protection against unauthorized disclosure or modification of the authentication keys. Furthermore, because none of the roles have *write* permission, it is not possible for any role (including the **crypto-officer** role) to modify the permissions to make the keys visible or accessible to any other roles.

[2] This probability is "1 – Prob(all 18000 attempts fail) = 1 – Prob(an attempt fail)^{18000} = 1 – (1 – 2^{-128})^{18000} ≈ 1 – (1 – 18000.2^{-128}) < 6×10^{-35}, which is clearly smaller than 10^{6}.

6.6 Initialization of Authentication Data

During the final stage of manufacturing in the factory, a set of default values of the Crypto-Officer Authentication Key and six User Authentication Keys are installed into the ZE. The values of these keys are given to customers to allow them to perform authentication to these roles for the first time. The customer is expected to change the values of these keys by logging into the **crypto-officer** role before module deployment. See Section 13.3.

7 Services

7.1 Operator Services

There are five categories of services provided by the ZE:

- Key Management Services
- Crypto Services
- Operator Management Services
- System Management Services
- Utilities Services

These services are available as internal APIs[3] that can be called from the Kernel. For the current ZE undergoing validation and loaded with **FIPS-LFM v1.0** and **FIPS-AFM v1.0**, these services are initiated via the diagnostic port via a series of menus. After the ZE has successfully powered up, the LIB menu is displayed via the diagnostic port (see Figure 4).

```
[LFM] : (K)ey.. (C)rypt.. (O)perator.. (S)ystem.. (U)tilities..
```

Figure 4. The LIB Menu

Sending the characters "**k**", "**c**", "**o**", "**s**" and "**u**" into the diagnostic port causes the ZE to display respective sub-menus for "Key Management Services", "Cryptographic Services", "Operator Management Services", "System Management Services" and "Utilities Services".

The relationship between roles and services and the types of access services have to CSPs/SPs ("keys") is summarized in Table 5. The access types are explained as follows:

- **A** *("access")* – The key can only be referenced for use with its associated service via its key index. The key-material and key-argument remain opaque to service.
- **R** *("read")* – The key-material and key-argument of the key can be read out by the service.
- **W** *("write")* – The service can write a new key to the key-bank and modify any key-component of an existing key.
- **M** *("modify")* – The service can only modify the key-material and key-argument of an existing key and cannot change any of the other key-attributes.

[3] With the sole exception of **Module Zeroize-all** and **External Firmware Erase** which are available only from the Main menu. For more information, refer to DC/ZE-0004/FIPS, "*d'Cryptor ZE Cryptographic Module – Module Specifications*".

Table 5. Roles vs. Services and Access Types to CSPs/SPs

Service	Description	UR	CO	U1 - U6	CSP/SP	Access Type[1]
Key Management Services						
Key-Type	Returns key-type	×	✓	✓	key-specific	A
Key-Mask	Returns key-mask	×	✓	✓	key-specific	A
Key-Size	Returns size of key-material	×	✓	✓	key-specific	A
Key-Link	Returns key-link	×	✓	✓	key-specific	A
Key-Perm	Returns key-perm (permanence) of key	×	✓	✓	key-specific	A
Key-Type Mnem	Returns key-type in the form of 4-char mnemonic	×	✓	✓	key-specific	A
Key-Bank Size	Returns the number of keys that can be stored in the key-bank	✓	✓	✓	–	–
Key Read	Reads a key from the key-bank	×	✓	✓	key-specific	R
Key Modify	Updates the key-material for a key	×	✓	✓	key-specific	M
Key Write	Writes a key into the key-bank	×	✓	✓	key-specific	W
Key Delete	Deletes a key from the key-bank	×	✓	✓	key-specific	W
Module Zeroize	Zeroizes all keys in the key-bank	✓	✓	✓	**ALL**	W
Module Zeroize-all	Zeroizes all keys in the key-bank and all default keys in the ZE	✓	×	×	**ALL+**	W
Cryptographic Services						
Symmetric Key Generate	Generates random symmetric key	×	✓	✓	DRNG key DRNG Seed	A
RSA Key Pair Generate	Generates random RSA key-pair	×	✓	✓	DRNG key DRNG Seed	A
DES Context Init	Initializes DES context in preparation for a DES operation	×	✓	✓	key-specific	A
DES Context Execute	Performs DES encryption/decryption using a DES context	×	✓	✓	key-specific	A
DES Context Quit	Frees a DES context	×	✓	✓	key-specific	A
DES Execute	Performs DES encryption/decryption in ECB/CBC/CFB/OFB modes	×	✓	✓	key-specific	A
TDEA Context Init	Initializes TDEA context in preparation for a TDEA operation	×	✓	✓	key-specific	A
TDEA Context Execute	Performs TDEA encryption/decryption using a TDEA context	×	✓	✓	key-specific	A
TDEA Context Quit	Frees a TDEA context	×	✓	✓	key-specific	A
TDEA Execute	Performs TDEA encryption/decryption in ECB/CBC/CFB/OFB modes	×	✓	✓	key-specific	A
AES Context Init	Initializes AES context in preparation for a AES operation	×	✓	✓	key-specific	A
AES Context Execute	Performs AES encryption/decryption using a AES context	×	✓	✓	key-specific	A
AES Context Quit	Frees a AES context	×	✓	✓	key-specific	A
AES Execute	Performs AES encryption/decryption in ECB/CBC/CFB/OFB modes	×	✓	✓	key-specific	A
RSA Context Init	Initializes RSA context in preparation for an RSA operation	×	✓	✓	key-specific	A
RSA Context Execute	Performs RSA sign/verify using ANSI X9.31 mechanisms and an RSA context	×	✓	✓	key-specific	A
RSA Context Quit	Frees an RSA context.	×	✓	✓	key-specific	A
RSA Execute	Performs RSA sign/verify using ANSI	×	✓	✓	key-specific	A

Service	Description	UR	CO	U1 - U6	CSP/SP	Access Type[1]
	X9.31 mechanisms					
SHA-1 Context Init	Initializes SHA-1 context in preparation for a SHA-1 operation	×	✓	✓	–	–
SHA-1 Context Execute	Performs SHA-1 computation	×	✓	✓	–	–
SHA-1 Context Quit	Frees a SHA-1 context and computes the final hash	×	✓	✓	–	–
SHA-1 Execute	Computes SHA-1 hash	×	✓	✓		
HMAC Context Init	Initializes HMAC context in preparation for a HMAC operation	×	✓	✓	key-specific	A
HMAC Context Execute	Performs HMAC computation	×	✓	✓	key-specific	A
HMAC Context Quit	Frees a HMAC context	×	✓	✓	key-specific	A
HMAC Execute	Computes HMAC SHA-1 hash and computes the final hash	×	✓	✓	key-specific	A
Random Number Generate	Generates pseudo-random bytes using the ANSI X9.31 RNG	×	✓	✓	key-specific	A
Operator Management Services						
Role Login	Request for authentication to a role (request for challenge)	✓	✓	✓	–	–
Role Verify	Verifies authentication data (verifies the response)	×	✓	✓	COAK, U1AK to U6AK	A
Role Logout	Logs out from current role	–	✓	✓	–	–
Current Role	Returns the current role of the ZE	✓	✓	✓	–	–
System Management Services						
Library Firmware Load	Loads external library firmware	×	✓	✓	–	A
Library Firmware Install	Installs library firmware into FLASH	×	✓	✓	–	A
Application Firmware Load	Loads external application firmware	×	✓	✓	–	A
Application Firmware Install	Installs application program into FLASH	×	✓	✓	–	A
Application Firmware Loaded	Checks whether the application firmware has been loaded	✓	✓	✓	–	–
External Firmware Erase	Erases both the library firmware and application firmware	✓	✓	✓	–	–
Module Shutdown	Shuts down the ZE (into standby mode)	✓	✓	✓	–	–
Module Reboot	Reboots the ZE (soft reboot)	✓	✓	✓	–	–
Utilities Services						
Flash Memory Write	Writes data to the Flash File System	✓	✓	✓	–	–
Flash Memory Erase	Erases data from the Flash File System	✓	✓	✓	–	–
Flash Memory Size	Returns size of the Flash File System	✓	✓	✓	–	–
Factory ID	Returns the factory ID of the ZE	✓	✓	✓	–	–
Serial Number	Returns the serial number of the ZE	✓	✓	✓	–	–
Firmware Version	Returns the firmware version of the ZE	✓	✓	✓	–	–
Hardware Version	Returns the hardware version of the ZE	✓	✓	✓	–	–

Notes: "✓" is "allowable" "**x**" is "unallowable" "–" is "not applicable"
"**ALL**" is "all keys in the key-bank"

"**ALL+**" is "all keys in the key-bank and all default system keys in the System Firmware"

"UR" means "Unauthenticated Role"

7.2 Mandatory Services

This section explains how the services mandated by the FIPS 140-2 requirements are implemented by the ZE.

7.2.1 Show Status

The current status of the ZE can be observed via the diagnostic port and can be displayed on a PC's terminal console using any serial communication program.

7.2.2 Perform Self-Tests

The power-up self-tests can be initiated by one of the following two methods:

- Power cycle the ZE;
- Perform the service **Module Reboot**.

The results of the self-tests are sent out via the diagnostic port as they are being executed.

7.2.3 Perform Approved Security Function

The ZE employs seven Approved security functions as listed in Table 3. These services are activated via the Cryptographic sub-menu under the LIB menu (see Figure 4).

8 Access Control Policy

8.1 Role

As described in Sections 6.1 and 6.2, the ZE supports seven identities and two roles. The **Crypto-Officer** identity always assumes the **crypto-officer** role after login, and each of the six **User** identities assumes the **user** role after login. Authentication of the identity of an operator and the authorization of the operator to assume its assigned role is thus automatically achieved.

There are no provisions for an authenticated operator to change roles or to assume a set of roles other than his assigned role as specified by the operator ID.

8.2 Access to Services

Access to a cryptographic service in the ZE is controlled by the type of access a role has to the keys that are used by that service. The availability of services to the roles in the ZE has been covered in Section 7.

8.3 List of CSP and SPs

The CSPs and SPs that are relevant for the current validation of the ZE, together with the modes of access available to roles, are listed in Table 6. These are the 13 cryptographic system keys that are always present in a ZE, the KEK as well as other operational user keys that are loaded into the ZE for the purpose of this validation.

Table 6. Modes of Access to CSPs/SPs

CSP/SP	Type	Modes of Access	
		CO	U1 to U6
COAK	Symmetric key (CSP) Used internally by the ZE to authenticate the **Crypto-Officer**	**A***	–
U1AK	Symmetric key (CSP) Used internally by the ZE to authenticate **User1**	–	**A***
U2AK	Symmetric key (CSP) Used internally by the ZE to authenticate **User2**	–	**A***
U3AK	Symmetric key (CSP) Used internally by the ZE to authenticate **User3**	–	**A***
U4AK	Symmetric key (CSP) Used internally by the ZE to authenticate **User4**	–	**A***
U5AK	Symmetric key (CSP) Used internally by the ZE to authenticate **User5**	–	**A***
U6AK	Symmetric key (CSP) Used internally by the ZE to authenticate **User6**	–	**A***
ALVK	Public key (SP) Used internally by the ZE to verify the integrity of an application firmware that is loaded into the ZE.	–	**A**
LLVK	Public key (SP) Used internally by the ZE to verify the integrity of a library firmware that is loaded into the ZE.	–	**A**
Sys DRNG Key	Symmetric key (CSP) Used internally by the ZE for RNG initialization	–	–
Sys DRNG Seed	Secret seed (CSP) Used internally by the ZE for RNG initialization	–	–
DRNG Key	Symmetric key (CSP) Used by the DRNG to generate random numbers	**A**	**A**
DRNG Seed	Secret seed (CSP). Used by the DRNG to generate random numbers	**A**	**A**
Key-Encryption Key	256-bit Symmetric key (CSP) Used internally by the Kernel to encrypt the key-bank	–	–
DES key	Symmetric key (CSP) Used by the DES services in FIPS-LFM/FIPS-AFM	**RMW**	**A**

TDEA-192 key	Symmetric key (CSP) Used by the TDEA services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
TDEA-128 key	Symmetric key (CSP) Used by the TDEA services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
AES-128 key	Symmetric key (CSP) Used by the AES services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
AES-192 key	Symmetric key (CSP) Used by the AES services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
AES-256 key	Symmetric key (CSP) Used by the AES services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
RSA-1024 key pair	Asymmetric key (CSP/SP) Used by the RSA sign/verify services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
RSA-1536 key pair	Asymmetric key (CSP/SP) Used by the RSA sign/verify services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
RSA-2048 key pair	Asymmetric key (CSP/SP) Used by the RSA sign/verify services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
HMAC-80 key	Symmetric key (CSP) Used by the HMAC services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
HMAC-96 key	Symmetric key (CSP) Used by the HMAC services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
HMAC-112 key	Symmetric key (CSP) Used by the HMAC services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
HMAC-128 key	Symmetric key (CSP) Used by the HMAC services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
HMAC-144 key	Symmetric key (CSP) Used by the HMAC services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
HMAC-160 key	Symmetric key (CSP) Used by the HMAC services in FIPS-LFM/FIPS-AFM	**RMW**	**A**
DRNG key	Symmetric key (CSP) Used by the DRNG service in FIPS-LFM/FIPS-AFM	**RMW**	**A**
DRNG seed	Symmetric key (CSP) Used by the DRNG service in FIPS-LFM/FIPS-AFM	**RMW**	**A**

Explanatory Notes on Modes of Access:

A, **R**, **M**, **W** → As used for Table 5.
A* → Internal access for authentication purposes only
– → No permissions

9 Self-Tests

The ZE performs a series of self-tests during power-up and on-demand to ensure that all the cryptographic operations it provides are functioning properly. Two types of self-tests are implemented: power-up self-tests, which are performed when the ZE is powered up, and conditional self-tests, which are performed whenever a security function is invoked.

If any of the self-tests (other than the Memory Test and the Firmware Load Test) fails, the ZE immediately enters a *Critical Error state* and repeatedly zeroizes all keys in the key-bank, thus leaving the ZE in a zeroized and unusable state and requiring a return of the module to the factory for recovery.

9.1 Power-Up Self-Tests

The power-up self-tests consists of the following tests, shown in Table 7:

Table 7. Power-Up Self-Tests

Self-Test	Description
Memory Test	Read/write tests on selected regions of the FLASH and SRAM
Cryptographic Algorithm Tests	Known-answer test for all cryptographic algorithms implemented in ZE: ▪ Encryption and Decryption : DES (ECB, CBC, CFB64, OFB64) : TDEA (ECB, CBC, CFB64, OFB64) : AES (ECB, CBC, CFB128, OFB128) ▪ Sign/Verify : RSA (ANSI X9.31-1998) ▪ Message digest : SHA-1 ▪ Keyed-message digest : HMAC-SHA-1 ▪ Random number generator : DRNG
Firmware Integrity Test	Kernel : 16-bit Error Detection Code (EDC) Library firmware : 2048-bit digital signature (ANSI X9.31-1998) Application firmware : 2048-bit digital signature (ANSI X9.31-1998)
Critical Function Test	Key Validity Test : 16-bit CRC for each key in the key-bank DRNG Test : Test functionality of the DRNG to ensure it is generating random numbers according to specifications

9.2 Conditional Tests

The conditional tests consists of the tests shown in Table 8:

Table 8. Conditional Tests

Conditional Test	Description
Pair-wise Consistency Test	Performed each time a RSA key pair is generated using the **RSA Key Pair Generate** service.
Firmware Load Test	Performed each time an external firmware library or application is loaded by computing a digital signature based on the ANSI X9.31-1998 standard
Continuous RNG Test	Performed each time the DRNG is called to generate random numbers
Building DES key schedule	Performed each time a DES service is called, to verify that the DES key has odd parity and is not a weak key
Building TDEA key schedule	Performed each time a TDEA service is called, to verify that the associated DES keys have odd parity and are not weak keys

10 Zeroization of CSPs/Cryptographic Keys

The module provides software means to zeroize all CSPs and other cryptographic keys in the key-bank. This is achieved by calling the services **Module Zeroize** or **Module Zeroize-all**. The latter service, in addition to zeroizing the key-bank, also erases all default key values in the Kernel.

11 Physical Security Policy

11.1 Physical Embodiment

The ZE is a multi-chip embedded cryptographic module.

11.2 Physical Security Mechanisms

The ZE uses standard production-quality components that meet typical commercial-grade specifications. Both sides of the PCB are completely covered with a hard opaque tamper-evident epoxy that meets the hardness required of level 3 of FIPS 140-2. The epoxy is also removal-resistant.

11.3 Physical Security Checks

The following physical check on the ZE should be carried out periodically to ensure that physical security is maintained:

- Inspect both exposed surfaces of the module (that is, the epoxy surface) for any signs of physical tamper. Such signs might include deep scratches or any irregularity (discontinuity of smoothness) on the surface of the epoxy.

It should be noted that the interval between inspections would depend on the application that the ZE is used for, as well as the security threat that the ZE is exposed to under its operational environment. It is recommended that the epoxy surface examination be carried out at least once every 6 months.

12 Mitigation of Other Attacks Policy

The ZE is not designed to mitigate any specific attacks.

13 Secure Operation of ZE

13.1 Factory Defaults

A *d'Cryptor* ZE is delivered from the factory in an Approved mode of operation, pre-installed with firmware modules **FIPS-LFM v1.0** and **FIPS-AFM v1.0**, and initialised with a set of 13 default (transport) cryptographic system keys and 20 user cryptographic keys.

13.2 Operating the ZE

The ZE operates in an Approved mode of operation when it is shipped from the factory. This can be determined by powering up the ZE and observing that the printable output displayed via the diagnostic port appears as in Figure 2.

To operate the ZE using the pre-installed firmware modules, an operator has to access the ZE's diagnostic port and enter the corresponding keyboard characters to activate services available through the various menus. Before activating any cryptographic service, the operator would have to authenticate into an authorized role by logging on as either the **Crypto-Officer** identity or one of the six **UserK** identities.

If an un-validated library firmware or application firmware is loaded into the ZE (thus replacing **FIPS-LFM** and/or **FIPS-AFM**), the ZE loses its FIPS 140-2 level 3 validation. For the ZE to continue operating in an Approved mode after loading a new library firmware or application firmware, the new library/application firmware needs to be validated to FIPS 140-2 Level 3.

13.3 Security Rules

13.3.1 Operational Security Policy

- A proper operational security policy should be in place that requires the COAK to be kept under lock and key, and known only to the **Crypto-Officer**.
- Before a ZE is deployed for operational use, the designated security officer should replace all the system keys (with the exception of the LLVK and the ALVK, which is assigned non-modifiable and non-writeable attributes) to ensure that the module does not get deployed with default transport keys. Note that system keys can be replaced by the **Key Modify** service using a customized LFM or AFM that invokes the service in a manner consistent with the requirements of FIPS 140-2 level 3.
- The validated module does not allow entry or output of CSPs. However, potential LFM/AFM developers should ensure that all CSPs should be entered or output either in encrypted form or using the split knowledge method.

13.3.2 Authentication Security Rules

The roles are each accorded *priorities* in the following manner:

- The **crypto-officer** role has a higher priority than the **user** role.

Authorized logins are subjected to the following rules:

- Logging in with a higher-priority role automatically logs out any lower-priority role.
- A lower-priority role cannot log in while a higher-priority role is logged in.
- Logging in with an authorized role automatically logs out the present role if the impending role is the same as the present role.
- It is not possible for the **Crypto-Officer** to assume any of the **user** roles.
- It is not possible for a **User** to assume the **crypto-officer** role.

14 Applicable Documents

FIPS Documents:

Name of Document		Date
FIPS 140-2	Security Requirements for Cryptographic Modules (With Change Notices 1, 2, 3, 4)	May 25, 2001
DTR for FIPS 140-2	Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*	March 24, 2004 (Draft)
ANSI X9.31 - 1998	American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*	September 9, 1998

Internal Documents:

Reference Number	Name of Document	Date
DC/ZE-0004/FIPS	*d'Cryptor* ZE Cryptographic Module – Module Specifications	18 Aug 2005
DC/ZE-0005/FIPS	*d'Cryptor* ZE Cryptographic Module – Cryptographic Key Management	18 Aug 2005
DC/ZE-0008/FIPS	*d'Cryptor* ZE Cryptographic Module – Software Developer Manual	2 Aug 2005

Other Documents:

Reference Number	Name of Document	Date
–	–	–

15 Glossary

15.1 Acronyms

AFM	Application Firmware Module
ANSI	American National Standard Institute
ALSK	Application load signing key
ALVK	Application load verification key
COAK	Crypto-Officer Authentication Key
CSP	Critical security parameter(s)
DRNG	Deterministic Random Number Generator
DTR	Derived Test Requirements
FIPS	Federal Information Processing Standards
GPIO	General-Purpose Input/Output
KEK	Key-Encryption Key
LFM	Library Firmware Module
LLSK	Library load signing key
LLVK	Library load verification key
SP	Security Parameter(s)
UART	Universal Asynchronous Receiver/Transmitter
UxAK	User x Authentication Key (where "x" is "1" to "6")

15.2 Definitions

key or *full key*	A 6-entry tuple consisting of a *key-type*, a *key-mask*, a *key-size*, a *key-link*, a *key-argument* and *key-material* of the given key size
key-argument	A general-purpose argument that forms one of the key contents associated with a key.
key-attribute	A key-component of a key that describes a particular characteristic of the key. There are altogether 5 attributes assigned to a key, namely, *key-type*, *key-mask*, *key-size*, *key-link* and *key-perm*.
key-bank	A region of the ZE's memory that is used to store keys.
key-index	A non-negative integer that identifies a key in the key-bank
key-link	An attribute of a key that is only valid for RSA public/private keys and for DRNG/SEED keys, since in the ZE, there are the only keys that appear as key-pairs. The key-link of the public (respectively private) key provides the key-index of the corresponding private (respectively public) key of the key-pair. The key-link of the SEED points to the DRNG key which in turn has a zero link.
key-mask	A user-defined quantity that is associated with a key and is used to identify the role or group of roles that are allowed to access this key; sometimes referred to as *key permission mask*.
key-material	Refers to all the bits of a cryptographic key, and is used synonymously with the usual meaning of a cryptography key used in conjunction with a cryptographic algorithm
key pair	A pair of keys that are related cryptographically. Two types of key pairs are used in the ZE: RSA key pair and DRNG/SEED key pair. A RSA key pair comprises a public key and a private key. A DRNG/SEED key pair comprises an AES key, and a seed for seeding the DRNG.
key-perm	An attribute of a key that indicates the permanence of the key. A key can be a *temporary key* (available only as long as the module is powered, and be lost upon reboot), or a permanent key (stored permanently in the key-bank).
key-size	The number of bits in the key-material of a key
key-type	Indicates the cryptographic algorithm associated with a key
mode of operation	The mode in which the ZE is operating. This is either *FIPS mode* (which is the *Approved mode of operation*) or *non-FIPS mode* (any mode which is not an *Approved mode of operation*).
security parameter	Security-related information (e.g. public cryptographic keys) whose modification can compromise the security of a cryptographic module. Note the distinction between *SP* and *CSP*. The *disclosure* of a SP does not affect the security of the module.
system keys	A set of 13 cryptographic keys that are installed by default in the ZE. These keys occupy key-indices 0 to 12.
trusted application	An application firmware module that has been FIPS 140-2 validated.
trusted library	A library firmware module that has been FIPS 140-2 validated.