Software House
iSTAR eX Controller

(Hardware Version: STAREX004W-64
Firmware Version: 4.1.1.12045)

FIPS 140-2
Non-Proprietary Security Policy

Level 2 Validation

Document Version 0.7

Prepared for:

Software House
70 Westview Street
Lexington, MA 02421
Phone: (781) 466-6660
Fax: (781)466-9550
http://www.swhouse.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2006-11-24	Cas Stulberger	Initial draft.
0.2	2007-03-12	Cas Stulberger	Updated Security Policy to address lab questions.
0.3	2007-03-26	Darryl H. Johnson	Updated Security Policy to address lab questions.
0.4	2007-09-04	Darryl H. Johnson	Updated to address CMVP comments.
0.5	2007-10-30	Darryl H. Johnson	Updated to address CMVP comments regarding roles and services.
0.6	2007-12-14	Darryl H. Johnson	Updated to address CMVP comments regarding the definition of roles, inclusion of clusters, and use of RSA.
0.7	2008-01-04	Darryl H. Johnson	Updated to address CMVP comments regarding the power-up integrity test.

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the iSTAR eX Controller from Software House. This Security Policy describes how the iSTAR eX Controller meets the security requirements of FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS 140-2 details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/cryptval/.

The iSTAR eX Controller is referred to in this document as the iSTAR eX, the Master Controller, Cluster member, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 Cryptographic Module Security Policy. More information is available on the module from the following sources:

- The Software House website (http://www.swhouse.com) contains information on the full line of products from Software House.
- The CMVP website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Software House. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Software House and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Software House.

2 iSTAR eX Controller

2.1 Overview

The iSTAR eX Controller is a hardware module developed by Software House. The iSTAR eX Controller is a door controller which is connected to at least one card reader and a door. After a card is swiped through a connected card reader, the information contained on the card about the person to whom the card is assigned is transmitted to the iSTAR eX. The iSTAR eX then consults its database and determines whether to allow access to the person by opening the door. The iSTAR eX will then send a message to open the door if access is allowed. If access is not allowed, then the door will not open and the user is denied entry.

2.1.1 Module Components

The iSTAR eX Controller is composed of the following hardware components (pictured below in Figure 1):

- iSTAR eX General Control Module (GCM) board
- Power Management Board (PMB)
- LCD Display
- 12V DC Power Supply
- Battery

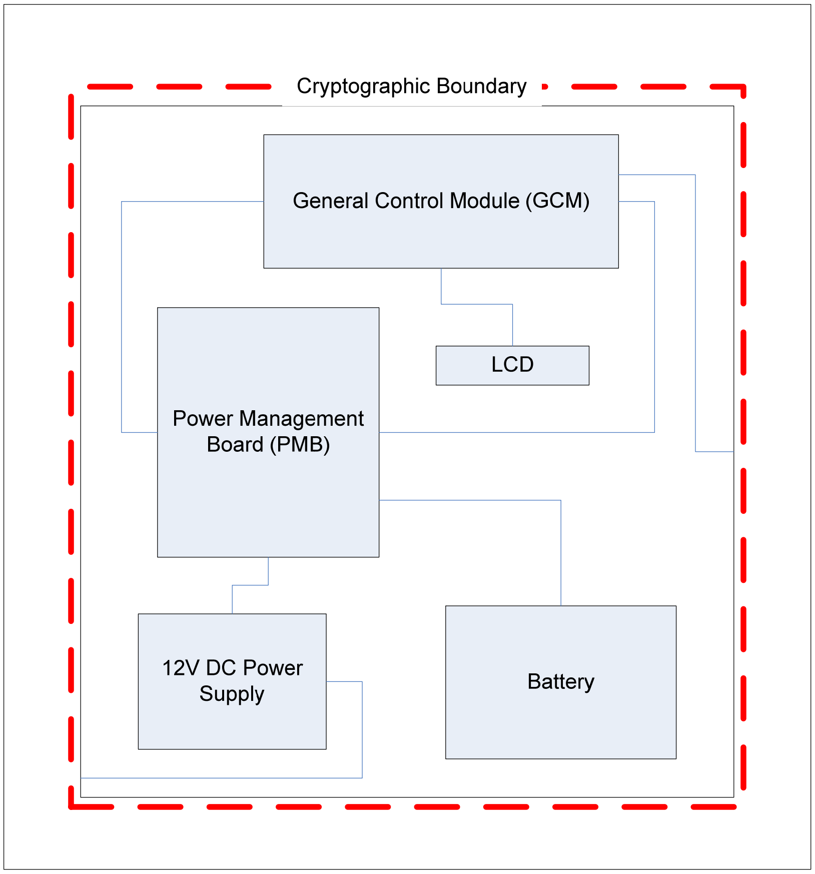


Figure 1 – iSTAR eX Controller Logical Diagram

There is one processor located inside the iSTAR eX and it is located on the GCM board. The PMB contains a microcontroller which is responsible for managing power distribution within the iSTAR eX and controlling power to all peripheral modules and card readers.

The GCM board contains a 400 MHz PXA255 Microprocessor, a member of the Intel XScale family of ARM processors that runs Microsoft Windows CE 5.0. The GCM board controls the input and output to and from the card readers connected to the GCM board and the PMB board.

The PMB board contains an Atmel ATMEGA32 Microcontroller, which communicates with the GCM via the Serial Peripheral Interface (SPI) bus. The PMB microcontroller manages the power system and backup facility of the iSTAR eX. The PMB microcontroller charges the battery, detects power loss, restores main power, and manages switching between main and battery power, as well as supplying power to the GCM board.

The LCD Display is an internal display that is used during setup and configuration of the iSTAR eX to monitor the status of the device and the self tests. The 12V DC Power Supply is connected to the PMB and supplies the power to the iSTAR eX. The battery is a 17.2 Ah lead acid battery. If the voltage drops below 12 volts, battery power will be supplied to all iSTAR eX circuit boards, peripherals, and readers, which enables the system to be fully functional under battery power. The battery will keep a typical system operational for a minimum of 4 hours. The battery will be fully recharged in 24 hours or less.

2.1.2 Deployment

The iSTAR eX Controller provides for secure communications in a network environment for enterprise-wide access control. Multiple iSTAR eX appliances can be networked into user-defined, logical groups called clusters. Clusters contain up to 16 iSTAR eX controllers. A host can be connected to several clusters (see Figure 2). Each cluster has one controller that serves as the master; other controllers in the cluster are cluster members. The master controller handles the communication of all event and cardholder data between the cluster and a C●CURE 800/8000 host. The cluster members communicate through the master to the other controllers in the cluster to link events and share cardholder status and location to mitigate the occurrence of such activities as “tailgating” (following another cardholder into a secured area without presenting a separate badge) and “passback” (passing back a card to another person to use) in the area secured by this cluster of controllers.

NOTE: FIPS mode is set at the cluster level; thus, every controller in the cluster will reflect the same FIPS status. For this validation, however, it is critical to note that a cluster can consist of a single controller. Thus, any discussion in this document referencing “clusters” (except where multi-controller configurations are expressly stated) refers to a single-controller cluster, which represents the module.

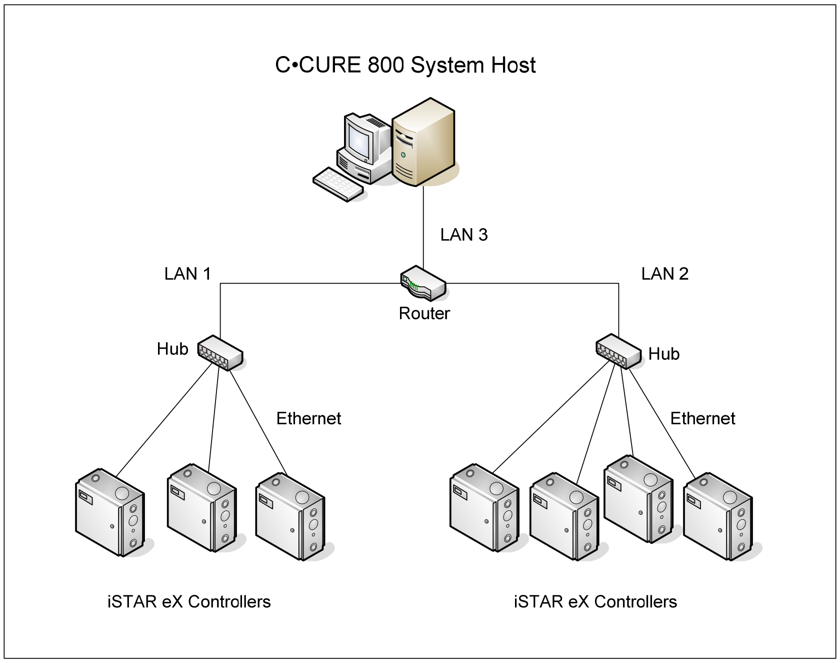


Figure 2 – Network Topology

The following table details the security level achieved by the iSTAR eX Controller in each of the eleven sections of FIPS 140-2.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

To ensure continuous connectivity, an iSTAR eX cluster can be configured with multiple communication paths to the C●CURE 800/8000. These paths can be set up using either a single master controller or two alternative master controllers. The single master configuration employs one cluster member as the master controller, providing a "primary" and "secondary" connection to the network. The alternate master configuration employs two cluster members to act as "primary" and "secondary" master controllers, with each having a single connection to the network. Figure 3 shows primary and secondary communication lines using a single master (left) and alternate master (right).

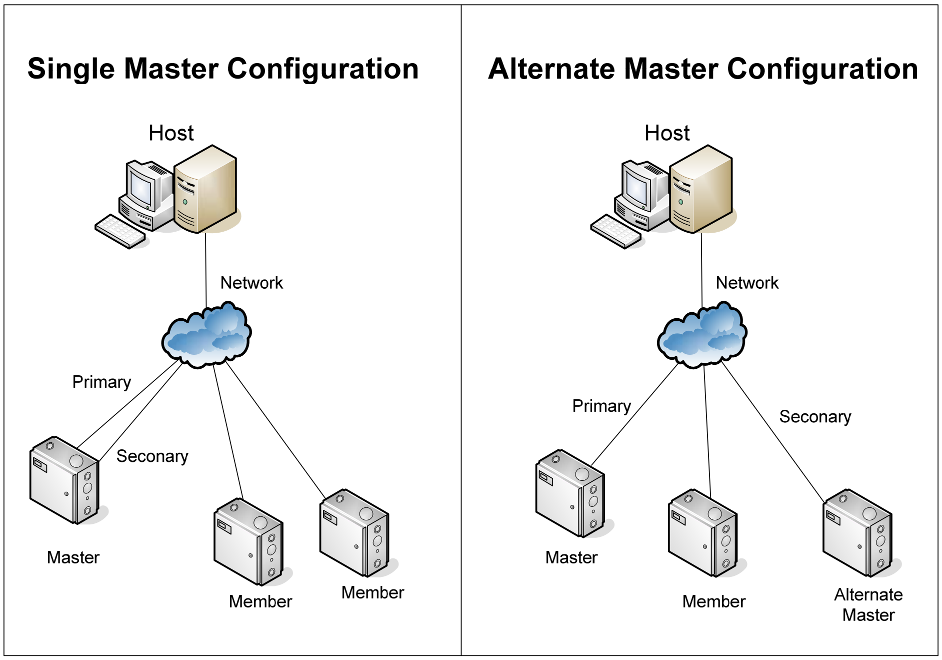


Figure 3 – Single and Alternate Master Configurations

Figure 4 below consists of two diagrams illustrating how communications occur (1) between a cluster member and the C●CURE 800/8000 Host Server and (2) between two cluster members. The diagram on the left of the figure shows how cluster member A communicates with the host via the master. The diagram on the right of the figure shows how cluster member A communicates with cluster member B via the master. The numbered arrows in the diagrams illustrate the order and direction of the communications path between the various network nodes.

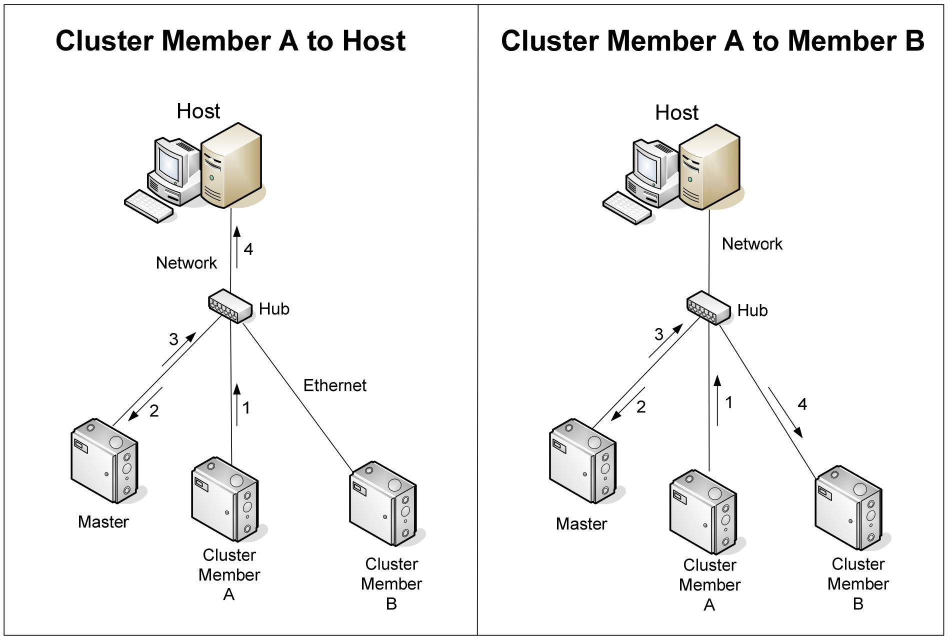


Figure 4 – Cluster Member Communication Paths

2.2 Module Interfaces

The iSTAR eX Controller is a multi-chip standalone module that meets overall level 2 FIPS 140-2 requirements. The cryptographic boundary of the iSTAR eX Controller is defined by the module's steel case enclosure.

Each iSTAR eX Controller has the following interfaces:

- Power plug/adapter
- RS-485 port
- 2 RJ-45 Ethernet ports
- 4 Direct Wiegand Reader ports
- Reader Bus

The power plug/adapter provides power to the iSTAR eX. The RS-485 port is used to communicate with card readers. The Ethernet ports are used for establishing Transport Layer Security (TLS) communications with other iSTAR eXs and the C●CURE 800/8000 host server. The four Direct Wiegand Reader ports and the Reader bus are used for connecting card readers to the iSTAR eX. Figure 5 below shows pictures of some of the types of card readers that can be connected to the iSTAR eX.

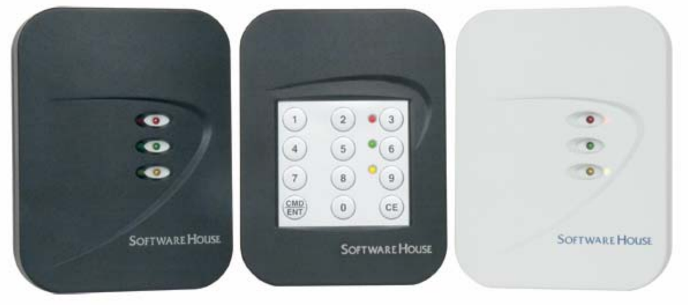


Figure 5 – Multi Technology Card Readers

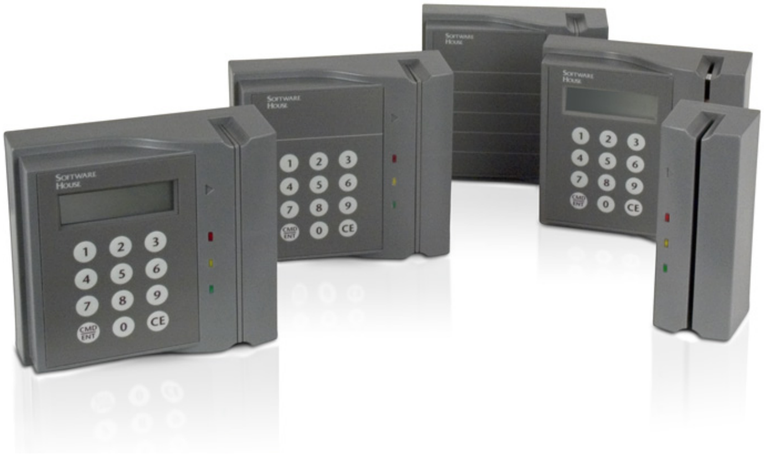


Figure 6 – RM Readers

Figure 7 – Wiegand Readers

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	iSTAR eX Controller Port/Interface
Data Input	RS-485 port, 2 Ethernet ports, 4 Direct Wiegand Reader ports, Reader Bus
Data Output	RS-485 port, 2 Ethernet ports, 4 Open Collectors
Control Input	2 Ethernet ports
Status Output	2 Ethernet ports
Power	Power plug/adapter

2.3 Roles and Services

The module supports role-based authentication. There are three roles in the module that operators may assume: a Crypto Officer role, a User role, and a Cluster Member role. These roles are described in the paragraphs that follow.

The module can only be accessed through well-defined commands and interfaces. All operators accessing these commands are assuming their roles and are authorized.

2.3.1 Crypto Officer Role

The Crypto Officer role is responsible for the initialization and management of the cryptographic functions provided by the module. This role is generally assumed by module's management applications (acting on behalf of a human operator): the iSTAR Configuration Utility (ICU) and the C•CURE 800/8000 host server. The ICU provides iSTAR eX configuration, diagnostic, and troubleshooting options. The ICU is used to designate the master controller, define master IP addresses, and define the IP address of the host server. Other configuration information is defined and downloaded from the C●CURE 800/8000 host server. To ensure correct configuration, the information that is entered in the ICU must match the information that is entered in the C●CURE 800/8000 Administration Application.

The module receives configuration information via the control input interface, and any status resulting from the input is communicated via the module's status output interface. Information-passing via these interfaces occurs via secured TLS sessions. The module uses RSA for the verification of host server. The Crypto Officer is authenticated by providing a digital certificate containing it RSA public key to the module during the TLS handshake.

Descriptions of the services available to the Crypto Officer role are provided in the table below.

Table 3 – Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Configure the module	Configure the module using the required IP address and connection data.	IP data via management application	None	None
Configure the module for FIPS-approved mode of operation	Configure the module for FIPS-approved mode of operation.	FIPS selection from the configuration screen	None	None
Create database of access card rights	Create database of access card rights	User names and applicable authorization data	None	None
Reboot the module	Command the module to reboot and restart.	Reboot command	Module reboots (and, if configured for FIPS mode, initiates power up self-tests)	None
Generate new RSA key pairs and certificate	Generate new RSA key pairs and certificate.	Message from the C●CURE 800/8000 Server to generate new RSA key pair	New RSA key pair and certificate generated	RSA key – Read / Write PRNG seed – Read
Establish a secure TLS session	Establish a secure TLS session with a C●CURE 800/8000 Server.	Digital certificate	Secure connection established	AES key – Read RSA key – Read PRNG seed – Read
Encrypt data for transmission.	Encrypt data for transmission.	Plaintext data to be transmitted	Encrypted data	AES key – Read RSA key – Read PRNG seed – Read
Decrypt received data.	Decrypt received data.	Ciphertext data received	Decrypted data	AES key – Read RSA key – Read
Terminate a secure TLS session	Terminate a secure TLS session.	None	Secure connection terminated	None
Show status	Display module status information.	Selection of the appropriate menu item on the C●CURE 800/8000 Server	Status window is displayed on the C●CURE 800/8000 Server.	None
Perform self-tests	Initiate and run all power-up self-tests.	Reboot command	Module reboots and initiates power up self-tests	AES key – Write PRNG seed – Read

2.3.2 User Role

The User role performs general security services and has access to the module's general security functionality. The User is a human with an access control card. The User initiates the access request process by sliding the card through a card reader that is hard-wired to the module. The sliding of the card sends a request to the controller, which contains the access control database created by the Crypto Officer via the host server and uploaded into the module.

The module receives access request data from the User via the data input interface, and any data to be sent back is communicated via the module's data output interface.

The User role is implicitly assumed by swiping the access card through the attached card reader. Descriptions of these services available to the User role are provided in the table below.

Table 4 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Initiates access request process	Request access to controlled area.	Access rights information (via card swipe on card reader)	Opened door for approved access request	None
Receive access request response	Receive a response to the access request	Access request	Access approval or denial	None

2.3.3 Cluster Member Role

The Cluster Member role is another user-type role that is assumed by a networked controller in a single- or multi-controller environment. In the multi-controller environment, the module is designated as the master controller; as such, all other controllers in its cluster can communicate with it, but can only communicate with each other by first relay the information through the module (refer to Figure 4 above). The Cluster Member role is responsible for establishing the TLS session with the module and for the encryption and transmission of access control data to the module.

The module receives access event data and access requests from the Cluster Member role via the data input interface, and any data to be sent back is communicated via the module's data output interface. The module uses RSA for the verification of Cluster Member credentials and the exchange of encryption keys. The Cluster Member is authenticated by providing a digital certificate containing its RSA public key to the module during the TLS handshake.

Descriptions of the services available to the Cluster Member role are provided in the table below.

Table 5 – Mapping of Cluster Member Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Initiate a secure TLS session	Initiate a secure TLS session with a module.	Digital certificate	Secure connection established	AES key – Read RSA keys – Read
Encrypt data for transmission.	Encrypt data for transmission.	Plaintext data to be transmitted	Encrypted data	AES key – Read
Determine access rights	Check access card rights database	Access rights information	Access approval or denial	None
Decrypt received data.	Decrypt received data.	Ciphertext data received	Decrypted data	AES key – Read
Terminate a secure TLS session	Terminate a secure TLS session.	None	Secure connection terminated	None

2.3.4 Non-FIPS Services

When the iSTAR eX is running in FIPS mode, it goes Dark (i.e., it functions as a black box) and inhibits the following services:

- ICU broadcast messages
- ICU configuration
- Simple Network Management Protocol
- NanView - a Software House development tool
- iSTAR web page

When the iSTAR eX is running in non-FIPS mode, these services are normally allowed. However, they must be disabled when running in FIPS mode. The disabling of these services is discussed in Section 3 of this document.

2.4 Physical Security

The iSTAR eX Controller is a multi-chip standalone cryptographic module. The GCM, PMB, LCD, power supply, and battery of the iSTAR eX Controller are entirely contained within a steel case enclosure. When punch-outs are removed to make necessary power and network connections, the gaps in those punch-out holes must be properly secured to resist probing. When properly installed, and after all open punch-out holes are properly secured, the module's enclosure is resistant to probing and is opaque within the visible spectrum.

The iSTAR eX Controller has a door on the front which contains a lock. The door is protected with tamper-evident seals in order to reveal tampering with the door. The iSTAR eX Controller has punch-out holes for Ethernet and power cables. Unused punch-out holes are covered with tamper-evident seals to prevent tampering. See Secure Operation in Section 3 below for instructions on how to affix the tamper-evident seals.

2.5 Operational Environment

The module does not provide a modifiable general-purpose operating system to the user. The module does not offer any method for an operator to load new software on the module. The operating system is stored on the module's flash and executes the code on the processor chip.

2.6 Cryptographic Key Management

The module employs a system-wide Key Management mode that the host and all iSTAR eX controllers in the same cluster must use. In FIPS mode of operation, the use of specific key management modes is required; custom certificates must be either generated by the controller (**Custom Controller Management** mode) or the host (**Custom Host Management** mode).

2.6.1 Approved Algorithms

The iSTAR eX implements the following FIPS-approved algorithms:

- Advanced Encryption Standard (AES) CBC[1] mode 256-bit – FIPS 197 (certificate #433)
- Deterministic Random Number Generator (RNG) – Appendix A.2.4 of ANSI X9.31 (certificate #283)
- SHA-1 – FIPS 180-2 (certificate #575)
- RSA[2] 1024-bit key used for signature generation/verification (certificate #219)

2.6.2 Non-Approved Algorithms

The iSTAR eX implements the following non-FIPS-approved algorithms:

- RSA 1024-bit key (key wrapping methodology provides 80 bits of encryption strength)
- Pseudo-Random Number Generator (PRNG) – hardware implementation

[1] CBC – Cipher Block Chaining

[2] RSA – Rivest Shamir and Adleman

The module supports the following critical security parameters:

Table 6 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Session Key	256-bit AES symmetric key	Generated internally	Never output	Stored in RAM for duration of the session	Deleted after session is over	Encrypting data transferred during TLS with the server
C●CURE 800/8000 RSA public key	1024-bit RSA public key	Input during TLS negotiations	Never output	Stored in volatile memory	Deleted after session is over	Used along with certificate to authenticate the C●CURE 800/8000 host server.
iSTAR eX RSA public key	1024-bit RSA public key	a) Generated internally (when in **Custom Controller Key Management** mode) b) Generated by the C●CURE 800/8000 host server and downloaded to module (when in **Custom Host Key Management** mode)	Transmitted during TLS session negotiation; sent to C●CURE 800/8000 for signature.	Stored in non-volatile memory	When a new RSA key pair is generated.	Used along with certificate to authenticate the iSTAR eX.

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
iSTAR eX RSA private key	1024-bit RSA private key	a) Generated internally (when in **Custom Controller Key Management** mode) b) Generated by the C●CURE 800/8000 host server and downloaded to the module (when in **Custom Host Key Management** mode)	Never output	Stored in non-volatile memory	When a new RSA key pair is generated.	Encrypting AES symmetric key.
PRNG seed	160 bits of seed value	Internally generated by the non-FIPS approved RNG	Never output	Stored in Flash memory	Upon restart of the iSTAR eX	Generating pseudo random numbers for generation of RSA and AES keys

2.6.2.1 Key Generation

The AES Symmetric Key is used to encrypt communications from the module to the C●CURE 800/8000 host server (and a master controller when the module is used in a multi-controller cluster environment). This key is generated during the TLS session as allowed per FIPS 140-2 Implementation Guidance 7.1 (updated June 26, 2007).

2.6.2.2 Key Input and Output

The RSA public/private key pair used for the TLS sessions is generated internally, and the RSA private key is never output from the module.

2.6.2.3 Key Storage and Zeroization

AES Symmetric keys and PRNG seeds are stored in volatile memory in plaintext and zeroized after use or on reboot.

The RSA public/private key pair generated by the module is also stored in the Flash memory in plaintext. The RSA public/private key pair can be zeroized by creating a new key pair.

2.7 Self-Tests

The iSTAR eX Controller performs the following self-tests at power-up:

- Firmware integrity test
- Cryptographic algorithm tests
    - Known Answer Tests (KATs)
        - AES KAT
        - SHA-1 KAT
        - RSA KAT
        - ANSI X9.31 Appendix A.2.4 PRNG KAT

The iSTAR eX Controller performs the following conditional self-tests:

- Continuous RNG test for FIPS-Approved PRNG
- Continuous RNG test for non-FIPS-approved hardware PRNG
- Pairwise consistency test for RSA

If one of the KATs or the firmware integrity test fails, then the iSTAR eX will not boot into FIPS mode. The iSTAR eX will try again to boot into FIPS mode. If the device cannot boot into FIPS mode, the problem may need to be diagnosed by the Crypto Officer.

If one of the conditional self tests fails, TLS communications will not occur. If the continuous RNG test fails, the RNG will generate another number until it does not equal the previous number.

2.8 Design Assurance

Software House's source code, user manuals, and procedures are all maintained in Rational ClearCase. The version of Software House's code and documents are labeled in ClearCase to uniquely identify the code associated with that version. The user manuals are tailored for each specific customer and are updated with each version of the iSTAR eX.

Additionally, Microsoft Visual SourceSafe (VSS) version 6.0 is used to provide configuration management for the iSTAR eX Controller's FIPS documentation. This software provides access control, versioning, and logging.

The modules are distributed in cartons sealed by Software House. The iSTAR eX GCM, PMB, and power supply each have their own unique serial number printed on them. These are then scanned and assigned to the iSTAR eX assembly serial number, which is printed on a label on the outside of the box. Software House ships the modules using recognized package delivery companies. The Crypto Officer receives the module from Software House via this secure delivery mechanism.

Upon receipt of the module, the end-user must examine the package for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging.

Since the modules do not enforce an access control mechanism before the module is initialized, the end-user must maintain control of the module at all times until the iSTAR eX Controller has been installed and sealed with tamper-evident stickers.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 level 2 requirements for this validation.

3 Secure Operation

The iSTAR eX Controller meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Installation

It is the responsibility of the end-user to ensure that the module is properly mounted, and that the power and Ethernet cables are properly connected. The iSTAR eX hardware does not include mounting hardware for an installation. Mounting hardware depends upon the site and must be approved by a structural engineer or other certified professional. All installation activities not performed directly by the end-user (including the removal of punch-out holes from the module and the securing of punch-out openings after connections are made) must be performed by a certified professional under the end-user's direct supervision.

3.2 Initial Setup

When the iSTAR eX is running in FIPS mode, it goes Dark (i.e., it functions as a black box) and inhibits the following services:

- ICU broadcast messages
- ICU configuration
- Simple Network Management Protocol
- NanView - a Software House development tool
- iSTAR web page

When iSTAR eX is running in non-FIPS mode, these services are normally allowed. If the iSTAR eX is instructed to change from non-FIPS mode to FIPS mode, a new set of public/private keys is downloaded to the controller (Custom Host Key Management mode) or generated by the controller (Custom Controller Key Management mode) before the change occurs.

For maximum protection, these services must be dynamically inhibited to prevent the private key from being accessed. The host sends a "Go Dark" message to instruct the iSTAR eX to prepare for the public/private key download or generation.

A controller running in FIPS mode can be set to run in non-FIPS mode through one of three ways:

- Reset the controller with clear-memory switch set. After reboot, this controller can be treated as a new controller.
- On the cluster configuration screen, turn off FIPS mode. This will cause all the on-line iSTAR eX controllers within the cluster to reboot. After reboot, they will run in non-FIPS mode.
- (In multi-controller cluster environments) Remove the controller from the FIPS cluster. The controller will then operate in non-FIPS mode.

When entering FIPS mode, the driver notifies the iSTAR eX to "Go Dark" and to prepare to accept the private key or certificate file download.

Changing from non-FIPS mode to FIPS mode or from FIPS mode to non-FIPS mode will cause all of the connected iSTAR eX controllers to reboot. Upon successful reboot, the changes will take effect.

Upon booting into FIPS mode, the system will check for custom certificates. If the system does not detect a custom certificate, the system displays an error message. The cluster configuration screen stays open after selecting the <OK> button and displays the error message.

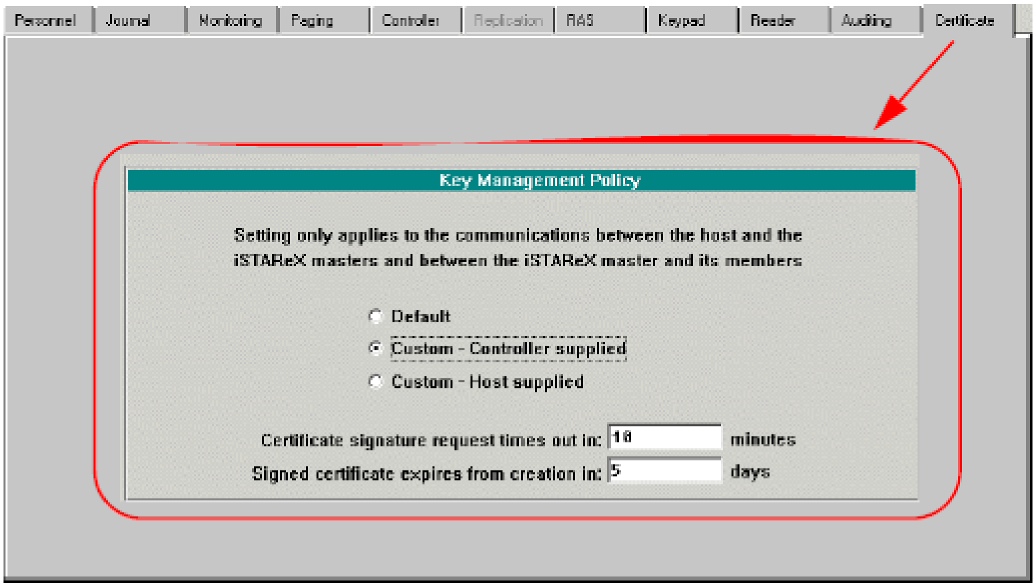
3.2.1 Putting the iSTAR eX in FIPS 140-2 Mode of Operation

FIPS mode can only be activated if the C●CURE system is set to use custom certificates to enforce maximum security.

1. Turn on FIPS mode via the Cluster Configuration screen by selecting **FIPS**, then selecting **OK**.
2. All the on-line iSTAR eX controllers in the cluster will reboot and reconnect back to the host.

3.2.2 Setting up a Custom Certificate for FIPS Mode

In FIPS mode of operation, the use of specific key management modes is required; custom certificates must be either generated by the controller (**Custom Controller Management** mode) or the C●CURE host (**Custom Host Management** mode). See Figure 8 below.



Key Management Policy

Setting only applies to the communications between the host and the iSTAReX masters and between the iSTAReX master and its members

○ Default
● Custom - Controller supplied
○ Custom - Host supplied

Certificate signature request times out in: 10 minutes
Signed certificate expires from creation in: 5 days

Figure 8 – Key Management Policy Screen

2.2.3.1 Setting up a Custom Controller Certificate

To set up a custom controller certificate:

1. Generate CA and host certificate at the module.
2. On the "System Variable => Key Management Policy" screen of the Admin program, select the **Custom Controller Certificates** option.
3. The system will automatically copy and download the new custom certificates to the host.
4. Send the signing request to a designated monitoring station.
5. All communicating iSTAR eX controllers will reboot and come back using the new certificates.
6. For each cluster, change its encryption mode to FIPS.
7. The system automatically tells the controllers to run in FIPS mode.
8. Stunnel service running on the C●CURE host restarts.
9. All communicating controllers reboot and come back in FIPS mode

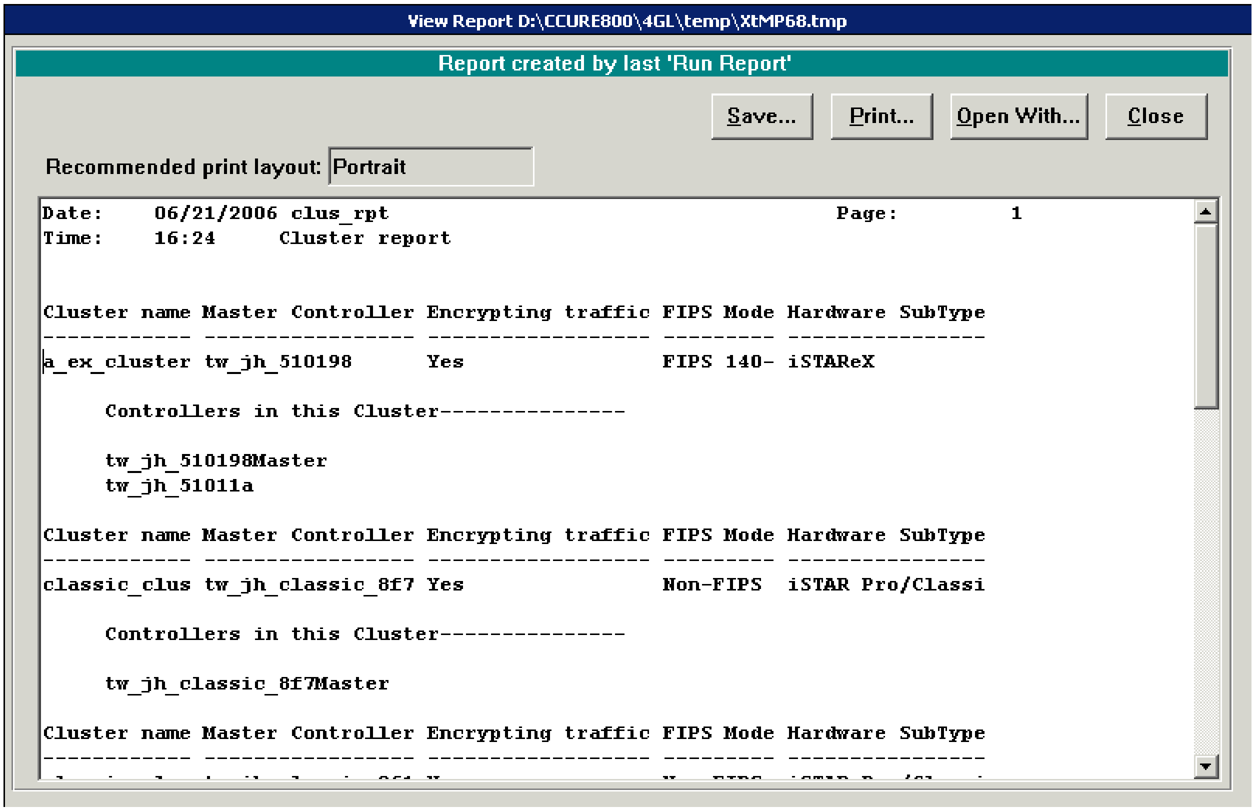
2.2.3.2 Setting up a Custom Host Certificate

To set up a custom controller certificate:

1. Generate CA, host, and controller certificate.
2. On the "System Variable => Key Management Policy" screen of the Admin program, select the **Custom Host Certificates** option.
3. The system will automatically copy and download the new custom certificates to the host and to the controllers.
4. All communicating iSTAR eX controllers will reboot and come back using the new certificates.
5. For each cluster, change its encryption mode to FIPS.
6. The system automatically tells the controllers to run in FIPS mode.
7. Stunnel service running on the C●CURE host restarts.
8. All communicating controllers reboot and come back in FIPS mode

3.2.3 Verifying FIPS Mode of Operation

To see if you are operating in FIPS mode, go to Report => Hardware => iSTAR Cluster in the C●CURE 800/8000 host server, and it will generate a report for you. There is a column in the generated report which will indicate in what mode the cluster is running. It will either say "*non-FIPS*" or "*FIPS 140-*" (see in Figure 9 below).


View Report D:\CCURE800\4GL\temp\XtMP68.tmp
Report created by last 'Run Report'
Save...
Print...
Open With...
Close

Recommended print layout: Portrait

```
Date:    06/21/2006 clus_rpt                                      Page:        1
Time:    16:24      Cluster report


Cluster name Master Controller Encrypting traffic FIPS Mode Hardware SubType
------------ ----------------- ------------------ --------- ----------------
a_ex_cluster tw_jh_510198      Yes                FIPS 140- iSTAReX

     Controllers in this Cluster---------------

     tw_jh_510198Master
     tw_jh_51011a

Cluster name Master Controller Encrypting traffic FIPS Mode Hardware SubType
------------ ----------------- ------------------ --------- ----------------
classic_clus tw_jh_classic_8f7 Yes                Non-FIPS  iSTAR Pro/Classi

     Controllers in this Cluster---------------

     tw_jh_classic_8f7Master

Cluster name Master Controller Encrypting traffic FIPS Mode Hardware SubType
------------ ----------------- ------------------ --------- ----------------
```

Figure 9 – FIPS Mode Report

3.3 Crypto Officer Guidance

The Crypto Officer is the person responsible for setting up, configuring, and administrating the iSTAR eX.

3.3.1 Initialization

The Crypto Officer must ensure that the module is properly mounted, and that the power and Ethernet cables are properly connected. All installation activities not performed by the Crypto Officer (including the removal of punch-out holes from the module and the securing of punch-out openings after connections are made) must be performed by a certified professional under the direct supervision of the Crypto Officer.

Before the iSTAR eX is installed the following must be performed:

- Check equipment (hardware, software, power supply, and wiring). Verify that the contents of the shipped boxes match the packing lists. Contact Software House if any items are missing or damaged.
- Check power, wiring, equipment clearances and code compliance at the site.
- Ensure proper tools for mounting and wiring the iSTAR eX are available.

The iSTAR eX hardware does not include mounting hardware for installation. Mounting hardware depends upon the site and must be approved by a Structural Engineer or other certified professional. Software House recommends anchoring systems to a structure capable of sustaining a 75 lb. (34.1 kg) load. The iSTAR eX will need to be mounted and the power and Ethernet connected before the tamper evidence labels can be applied.

The tamper-evident labels are applied across all unused punch-out holes and across the door on the front of the iSTAR eX. The following steps detail application of the labels for the iSTAR eX.

1. Ensure the system is unplugged.
2. Clean the areas to which the tamper-evident labels will be applied to remove any grease, dirt, etc. Rubbing alcohol can be used for this purpose.
3. Apply a tamper-evident label across any unused punch out holes on the sides, top, and bottom of the iSTAR eX. Make sure that about half the label is not on the punch out hole so that the label must be removed in order to punch out the hole from the casing.
4. Apply a tamper-evident label perpendicular to the seam between the door and the rest of the enclosure along the top, bottom, and side of the case.
5. Log the serial numbers of the applied labels.
6. Allow a minimum of 24 hours for the labels to cure.

The Crypto Officer must periodically check the module for evidence of tampering (including unusual dents, scrapes, or damage to tamper-evident labels) and verify the tamper-evident labels still have the proper serial numbers. Additionally, the Crypto Officer should monitor logs and alerts for the module for strange activity. If indications of suspicious activity are found, the Crypto Officer should immediately take the module offline and investigate.

3.3.2 Management

Management of the iSTAR eX is handled through the C●CURE 800/8000 host server and the ICU. The ICU is a diagnostic tool for setting parameters on the iSTAR eX - IP address, host IP address, etc. - and it can download new firmware to the iSTAR eX. The ICU, however, is disabled in the FIPS mode of operation, so all management while in the FIPS mode of operation occurs through the C●CURE 800/8000. The C●CURE 800/8000 is the access control system. This is where you have a database of the personnel, doors, iSTAR eXs, panels, etc. The C●CURE 800/8000 is used to set-up the rules governing access & actions. Those rules are then downloaded as a database file to the iSTAR eX so it can make its own decisions.

3.3.3 Zeroization

The AES symmetric key is a temporary key and is automatically zeroized after the TLS session is terminated. The iSTAR eX's public/private RSA key pair is deleted and overwritten when a new RSA key pair is generated.

3.4 User Guidance

The User is a human with an access control card requesting access to a controller-secured area. The User accesses the module’s cryptographic functionalities. Although the User does not have any ability to modify the configuration of the module, they should check that the host application is enabled and providing cryptographic protection.

4 Acronyms

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GCM	General Controller Module
ICU	iSTAR Configuration Utility
IP	Internet Protocol
KAT	Known Answer Test
LCD	Liquid Crystal Display
NIST	National Institute of Standards and Technology
PCMCIA	Personal Computer Memory Card International Association
PC	Personal Computer
PMB	Power Management Board
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SPI	Serial Peripheral Interface
TLS	Transport Layer Security
VSS	Visual SourceSafe