Key Token
Security Policy

Document Version 1.15

Sun Microsystems, Inc.

July 29, 2008

Contents

Figures

Tables

1 Module Overview

The Sun Microsystems Key Token is a multi-chip standalone cryptographic module encased in a hard opaque commercial grade plastic case (Hardware Part Number 314478004 Version G, Firmware Version 1.20). The Key Token is part of the larger Sun Microsystems' Encrypted Data-At-Rest Solution (EDRS). The primary purpose for this device is to provide secure data storage and key transport between the two other EDRS components. The additional two components that the EDRS includes are the Key Management Station (KMS) and the Encrypting Tape Drive (ETD). For more information on these components please contact Sun Microsystems. The Key Token provides status via its Ethernet interface on the rear of the module, and also via its eight LEDs on the front of the module. The cryptographic boundary of the Key Token is the hard, opaque plastic case which encompasses all Token hardware and firmware. The figure below illustrates the cryptographic boundary as defined:

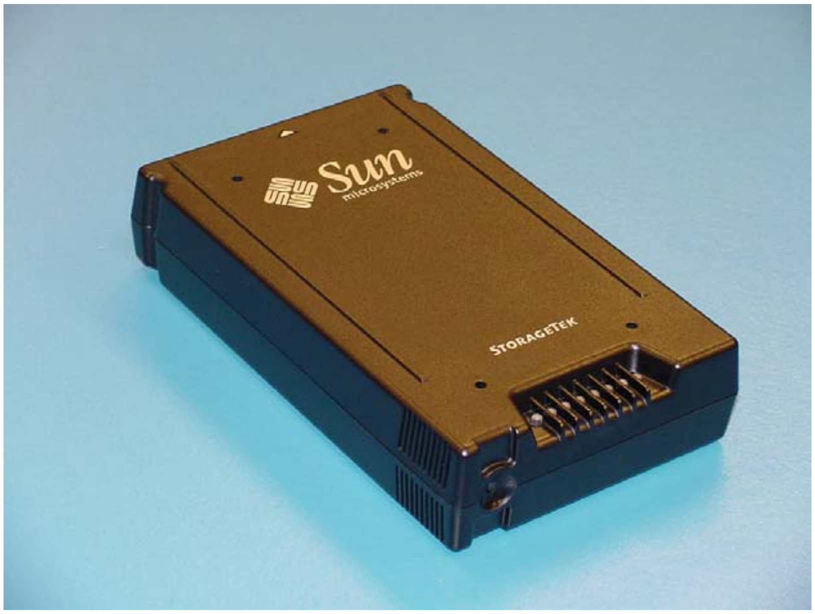

Figure 1 -- Image of the Key Token

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 1 -- Module Security Level Specification

Security Requirements Section	**Level**
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

3 Modes of Operation

3.1 Approved mode of operation

The validated Key Token cryptographic module always operates in FIPS-mode and does not have to be configured into the approved mode. It supports FIPS Approved algorithms as follows:

- AES ECB in CCM mode with 256-bit keys (Certificate #636), which provides for the following operations:
    - Encryption

3.2 Non-FIPS Mode of Operation

The Key Token does not support a non-FIPS mode of operation.

3.3 Module States

The Key Token has two main key establishment states.

Enabling Key Token

The first state is to establish Device Keys which are used to then protect Media Keys in transport from the Key Token to the Drives. When the Key Token is in this state it is referred to as an Enabling Key Token and will indicate status of this state via both the LEDs and event logs.

Operational Key Token

The second state is used to securely establish Media Keys to the Key Token. When the Key Token is in this state it is referred to as an Operational Key Token and will indicate status of this state via both the LEDs and event logs.

4 Ports and Interfaces

The Key Token cryptographic module provides the following physical ports and logical interfaces:

Table 2 -- Physical Ports and Logical Interfaces

Physical Port	Qty	Logical interface definition	Technical Specification
Ethernet	1	Data Input, Data Output, Status Output, Control Input	This is the Key Token's communications interface to both the KMS and the ETD's. Its primary use is for management of the ETD's.
Reset Button	1	Control Input	The Reset Button can be used by any operator to (1) erase all CSPs stored in the Key Token, (2) return the Key Token to its factory default state, and (3) transmit a reset message to a set of ETD's.
LEDs	8	Status Output	These interfaces provide status output to any operator of the Key Token.
Power	1	Power Input	12V DC ±10%, 1.5A

Figure 2 and Figure 3 show the front and rear views of the Key Token, respectively. All physical ports of the Key Token are visible in these two Figures.

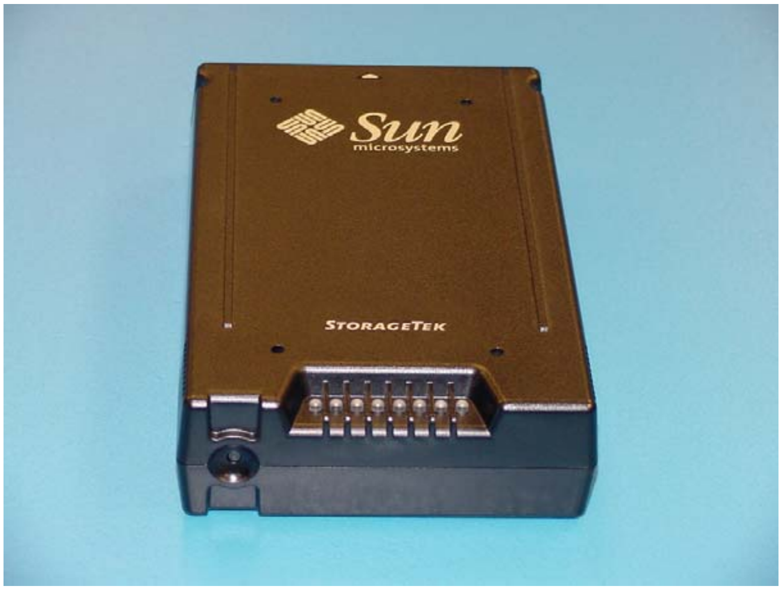

Figure 2 -- Front View of the Key Token. Recessed Reset Button shown on the left, 8-element LED Array centered

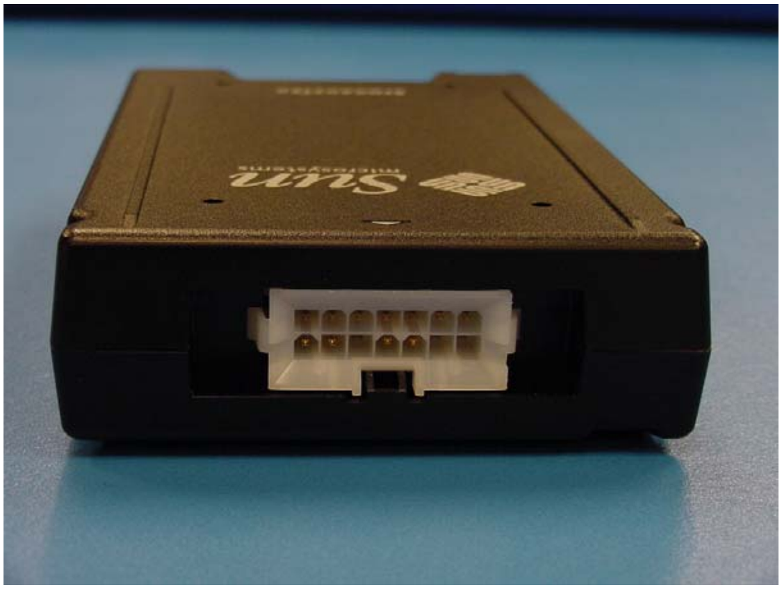

Figure 3 -- Rear View of the Key Token, 14-pin Connector. Pin allocation: 9 Ethernet port pins, 2 pins for DC PWR/GRD, 3 pins removed.

5 Identification and Authentication Policy

5.1 Assumption of roles

The Key Token cryptographic module, part of the EDRS, supports two distinct approved operator roles, a User and a Cryptographic Officer. The module is a FIPS 140-2 Level 1 module and hence does not support authentication of the Cryptographic Officer or User. Role selection is based on the TCP port specified during communication.

6 Access Control Policy

6.1 Roles and Services

The following three tables provide a summary of the services accessible to the Cryptographic Officer, the User, and the No Role, respectively.

Table 3 -- Description of Module Services accessible to the Cryptographic Officer

Service Name	**Service Description**
Report IP Settings	Reports Key Token IP settings and identification data.
Receive Permanent IP Settings	Changes the Key Token's power up IP settings.
Receive Temporary IP Settings	Changes the Key Token's IP current settings. Temporary settings are discarded when the Key Token power-cycles.
Create Enabling Key Token (EKT)	Initializes the Key Token as an EKT. The EKT stores data intended for delivery to a set of ETD's.
Create Operational Key Token (OKT)	Initializes the Key Token as an OKT. The OKT stores media key packages intended for delivery to a set of ETD's.
Clear EKT	Erases all device key packages stored in the EKT.
Clear OKT	Erases all media key packages stored in the OKT.
Reset Token	Forces the Key Token to reboot.
Show Status	Provides Key Token information that includes the Key Token type (EKT, OKT, or neither), MAC address, version information, and event log records. An event log record is created when either: 1. The Key Token detects an internal error or an error related to incorrect/illegal input from an operator. 2. The Key Token has delivered a key package to an ETD 3. An ETD informs the OKT that the ETD is missing a MEKey needed to read a tape The Key Token reset button has been pressed.
Delete Event Log Records	Removes a set of stored event log records from the Key Token.
Get Diagnostic Information	Acquires a firmware execution trace from the Key Token.
Echo	Used to verify that TCP/IP communication connection has not been dropped.

Table 4 -- Description of Module Services accessible to the User

Service Name	**Service Description**
OKT Key Output	Output an encrypted media key package from the OKT.
OKT Receive Key Missing Error	Receive a packet containing the KeyID of a MEKey needed by the User.
EKT Key Output	Output a device key package from the EKT.
EKT Device Key Package Deletion	The ETD specific device key package will be deleted from the EKT after the ETD acknowledges device key package delivery.

Table 5 -- Description of Module Services accessible without the assumption of an authorized role (No Role)

Service Name	**Service Description**
Zeroize EKT using Reset Button	Erases all CSPs stored in the EKT. Returns the Key Token to a factory default condition.
Clear EKT using Reset Button	Erases all device key packages from the EKT. A reset message will be sent to the set of ETD's known to the EKT.
Zeroize OKT using Reset Button	Erases all CSPs stored in the OKT. Returns the Key Token to a factory default condition.
Clear OKT using Reset Button	Erases the media key package from an OKT. A reset message will be sent to the set of ETD's known to the OKT.
Show Status using LEDs	Status is provided by LEDs which are at the boundary and can be viewed by any operator who can visualize the Key Token.
Self-Test	Power cycle the module in order to initiate FIPS Power up Self-tests.

6.2 Definition of Critical Security Parameters (CSPs) and System Keys

The only CSP contained within the Key Token is the OCKey. Please see the Table 6 below for a description.

Table 6 -- CSP Descriptions

Communication Key (OCKey)	Communication Keys are 256-bit AES keys used to encrypt communications between an OKT and an ETD. The OCKey is one of the three device keys stored in an EKT as part of an ETD-specific encrypted device key package.

From a FIPS 140-2 perspective the Key Token contains only one CSP, which is the OCKey. The OCKey is used to protect communications with an Encrypting Tape Drive (ETD). However, the Key Token is also used to passively store and distribute system keys, which are used by the other two modules in the EDRS system. System keys are encrypted by the Key Management Station

(KMS) and are then stored in the Key Token for manual transport to an Encrypting Tape Drive. These keys are protected by other mechanisms within the KMS and ETD, but not the Key Token. The Key Token never handles these keys other than to allow input and output of them. System keys are not considered CSPs in relationship to the Key Token; the Security Policy is including a description of these keys for completeness only.

The module contains two different types of System Keys, Device Keys which protect keys during storage and support encrypted key entry and output to and from the ETD, and Media Keys which are used to encrypt the user data written to magnetic tape, by the ETD. The following table contains a list of all supported System Keys contained within the module:

Table 7 -- System Key Descriptions[1]

Key	Description/Usage
Media Key (MEKey)	Media Keys are 256-bit AES CCM keys generated outside the ETD by KMS. An ETD uses a Media Key (MEkey) to encrypt and decrypt the customer bulk data it processes. MEKeys are stored in encrypted form in the OKT.
Device Split Key (DSKey):	Device Split Keys are 256-bit AES keys used as the first level of protection for Media Key values. The DSKey value is exclusive-ORed with the MEKey value by the KMS when media keys are sent out by the KMS. The DSKey is also used by the KMS to encrypt the packet of Device keys for any Device Key transfer other than for initialization or a transfer following a reset. DSKey is one of the three device keys stored in an EKT as part of an ETD specific encrypted device key package.
Wrap Key (WKey)	Wrap Keys are 256-bit AES-keys used to build the Media Key package sent to the Key Token. The Media Key package for any one ETD consists of a set of paired values for each Media Key to be sent to the ETD. The pair of values for each key is the Key ID and combination of DSKey XORed with the MEKey. The objective of this process is to add an additional layer of encryption security to the Media Key. WKey is one of the three device keys stored in an EKT as part of an ETD specific encrypted device key package.

6.3 Definition of CSPs Modes of Access

Table 9 defines the relationship between access to the OCKey, System Keys, and the different module services. For each module service, entries under the four key column headings may have one of several values:

Delete: The key is zeroized in flash memory.

Input: The key is input into the module.

Output: The key is output from the module.

Decrypt: Indicates the key is the key being used to decrypt incoming data.

[1] System Keys are not considered CSPs in relation to the Key Token module. These keys are protected in other mechanisms present in the Key Management Station and Encrypting Tape Drive.

Encrypt: Indicates the Key is the key being used to encrypt outgoing data.

Table 8 -- CSP and System Key Access Rights

Crypto-graphic Officer	**User**	**No Role**	**Service Name**	**OCKey**	**System Keys (Non-CSPs)**		
					MEKey	**DSKey**	**WKey**
X			Receive Permanent IP Settings				
X			Receive Temporary IP Settings				
X			Create Enabling Key Token (EKT)			Input	Input
X			Create Operational Key Token (OKT)	Input	Input		
X			Clear EKT	Delete		Delete	Delete
X			Clear OKT	Delete	Delete		
X			Reset Token				
X			Show Status				
X			Delete Event Log Records				
X			Get Diagnostic Information				
X			Echo				
X			Report IP Settings				
	X		EKT Device Key Package Deletion			Delete	Delete
	X		EKT Key Output			Output	Output
	X		OKT Key Output		Output		
	X		OKT Receive Key Missing Error				
		X	Show Status using LEDs				
		X	Self-Test				

Cryptographic Officer	User	No Role	Service Name	OCKey	System Keys (Non-CSPs)		
					MEKey	DSKey	WKey
		X	Zeroize EKT using Reset Button			Delete	Delete
		X	Clear EKT using Reset Button			Delete	Delete
		X	Zeroize OKT using Reset Button	Delete	Delete		
		X	Clear OKT using Reset Button	Delete	Delete		

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Key Token does not contain a modifiable operational environment.

8 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module provides two distinct authenticated operator roles the Cryptographic Officer role and the User role.
2. The cryptographic module performs the following power up self-tests:
    - Cryptographic Algorithm Tests: AES-256 CCM Known Answer Test
    - Firmware Integrity Test (32-bit CRC)
    - Critical Functions Tests: Key Package Integrity Test (32-bit CRC)
3. An Operator is able to command the module to perform the power up self-test by initiating a power cycle of the module.
4. The cryptographic module inhibits data output during self-tests, during the zeroization process, and while the module is in a error state.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module supports up to two concurrent Cryptographic Officers, and supports up to four concurrent Users.
7. The module does not support updates to its firmware.

9 Cryptographic Officer Guidance

An operator should first check LED status indicators on the Key Token to determine which key establishment state it is currently in (EKT, OKT). Please see Appendix A of the *Sun Crypto Key Management Station Configuration and Startup Guide*.,

9.1 Zeroization Procedure for OKT (Using KMS GUI Interface)

1. Insert the Key Token into the Sun Token Drive Bay connected to a KMS.
2. Push and hold the reset button after power up has finished.
3. As the Cryptographic Officer utilizes the Create Enabling Key Token service and selects all currently created drives, up to 13. If less then 13 drives have been created then simply reissue the command 8 times with one drive selected, and the “local token” check box unchecked.

9.2 Zeroization Procedure for EKT

1. Push and hold the reset button during power up.
2. Zeroization Procedure for EKT

9.3 Key Token Usage

The Key Token shall not be network attached, such that simultaneous communication with both the KMS and any ETD are allowed. In other words, Cryptographic Officers and Users should not be allowed to concurrently access the Key Token.

10 Physical Security Policy

10.1 Physical Security Mechanisms

The Key Token multi-chip standalone cryptographic module is contained within a production grade hard opaque removable enclosure.

11 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2.

12 References

[1] T 10000 A Encryption Product Architecture Specification, Document No: E001, Version 3.0, Date:11/11/05

[2] Titanium A Encryption Product Contract, Document No: E002, Version 2.0, Date:10/05/05

[3] NIST Special Publication 800-38C, *Recommendation for Block Modes of Operation: The CCM Mode for Authentication and Confidentiality*. U.S. DoC/NIST, May 2004. Available at http://csrc.nist.gov/publications/nistpubs/index.html

[4] Sun Microsystems T10000 Encrypting Tape Drive Concept of Operations Document

[5] Sun Microsystems, Crypto Key Management Station: Configuration and Startup Guide, Part Number: 96261, Revision B

13 Definitions and Acronyms

AES	Advanced Encryption Algorithm
CCM	Counter with CBC-MAC
CSP	Critical Security Parameter
DSKey	Device Split Key
EDC	Error-Detection Code
EKT	Enabling Key Token
ETD	Encrypting Tape Drive
GUI	General User Interface
KMS	Key Management Station
MEKey	Media Key
OCKey	Operational Communication Key
OKT	Operational Key Token
WKey	Wrap Key