Thales e-Security keyAuthority®

FIPS 140-2 Level 3 Security Policy

- Firmware version: 3.0.3
- Hardware Version: 1.0

Thales e-Security, Inc.
2200 North Commerce Pkwy, Suite 200
Weston, FL 33326, USA
http://iss.thalesgroup.com

Document Revision 002

1. Introduction

This document provides the Security Policy for the keyAuthority product, conforming to the FIPS 140-2 Security Requirements [1]. This security policy describes how the appliance meets the security requirements of FIPS 140-2 and how to run the module in an approved mode of operation. This document was prepared as part of the Level 3 FIPS 140-2 validation of Thales e-Security keyAuthority®.

Further information on keyAuthority is available from the Thales web site: http://iss.thalesgroup.com.

2. Overview

keyAuthority is a standards-based, FIPS-validated key management appliance that enables organizations to confidently manage encryption for multiple types of encrypting endpoints. The appliance enables the management of client encryption keys throughout their lifecycle to meet security policy and regulatory compliance requirements. A vendor-neutral approach ensures broad support for encryption devices, including native compatibility for IBM tape and disk products through Tivoli® Key Lifecycle Manager (TKLM) integration. Fabric-based encryption management is provided through support for the Brocade Encryption Switch.

The keyAuthority appliance offers the following advantages:

- Provides an open (encryption vendor neutral), enterprise-class, key lifecycle management module.
- Manages key lifecycle policy comprehensively by following industry standards.
- Enables secure controls over key material when shared with business partner encryption products to achieve unrivaled security, operational efficiency, and ease –of-use.
- Delivers automated synchronization for continuous high availability to support seamless disaster recovery.

1.1 Major Functions

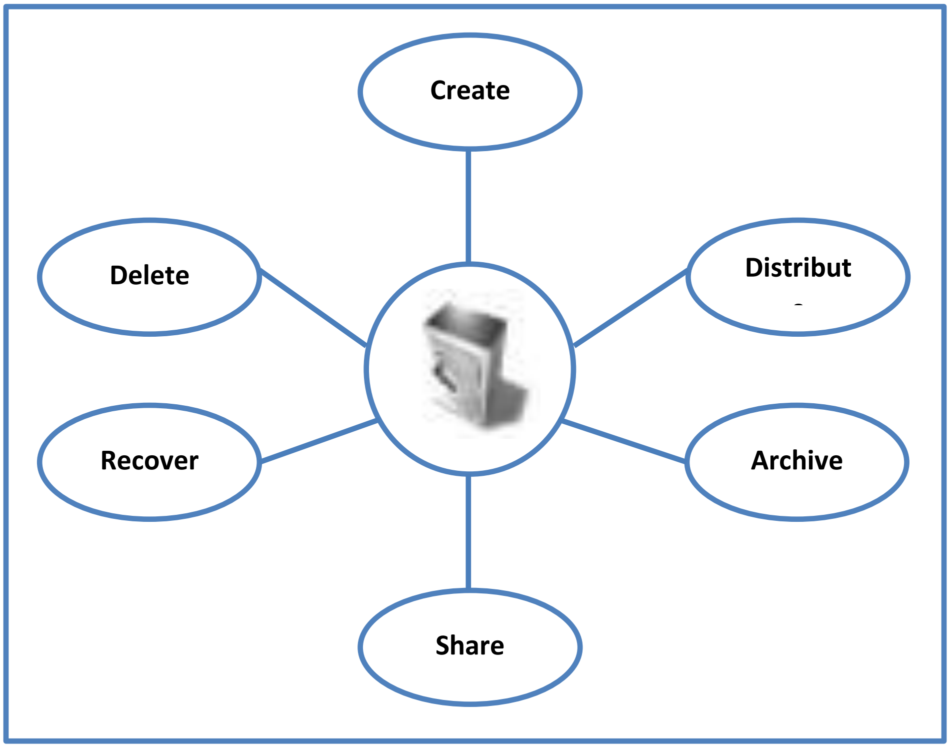

Figure 1- Major Functions

The keyAuthority module performs the following functions, as illustrated in the figure above:

- Create – keyAuthority creates random keys to ensure data privacy. All random keys are generated by FIPS approved RNGs implemented by the module.
- Distribute – Secure transport and automated key distribution for multi-site access to keys, as well as secure replication channels in support of device redundancy.
- Archive – Meets compliance requirements for secure long-term archiving.
- Share – Secure and simple sharing of encrypted data with business partners.
- Recover – Recovery of encrypted data and keys at any site. To assure highest security, keys are not accessed until actually needed.
- Delete – Enforcement of data destruction across multiple sites to meet compliance requirements.

1.2 Encryption Key Management

The inefficiencies and complexities of safely managing enterprise encryption keys is too great if depending upon unreliable manual operations. The opportunity for user error is too high of a security risk in critical situations such as disaster recovery. Thales e-Security keyAuthority automates all of the essential key lifecycle controls to greatly reduce the risks of data loss and provide long-term access to keys.

When using Thales e-Security keyAuthority, security managers automate key lifecycle policy and create trust relationships to share keys with devices, groups, and users. Group relationships automatically ensure that keys are available when they are needed and only by authenticated encryption devices. Primarily focused on Data-at-rest applications, the solution with partner devices supports data stored on tape or disk media to meet long-term data retention policies. The appliance provides a comprehensive set of tools that enable a global company to automate key recovery across multiple sites.

The keyAuthority module delivers secure, automated, and open centralized key management for third-party encryption devices as part of a solution ecosystem, as demonstrated in the figure below:

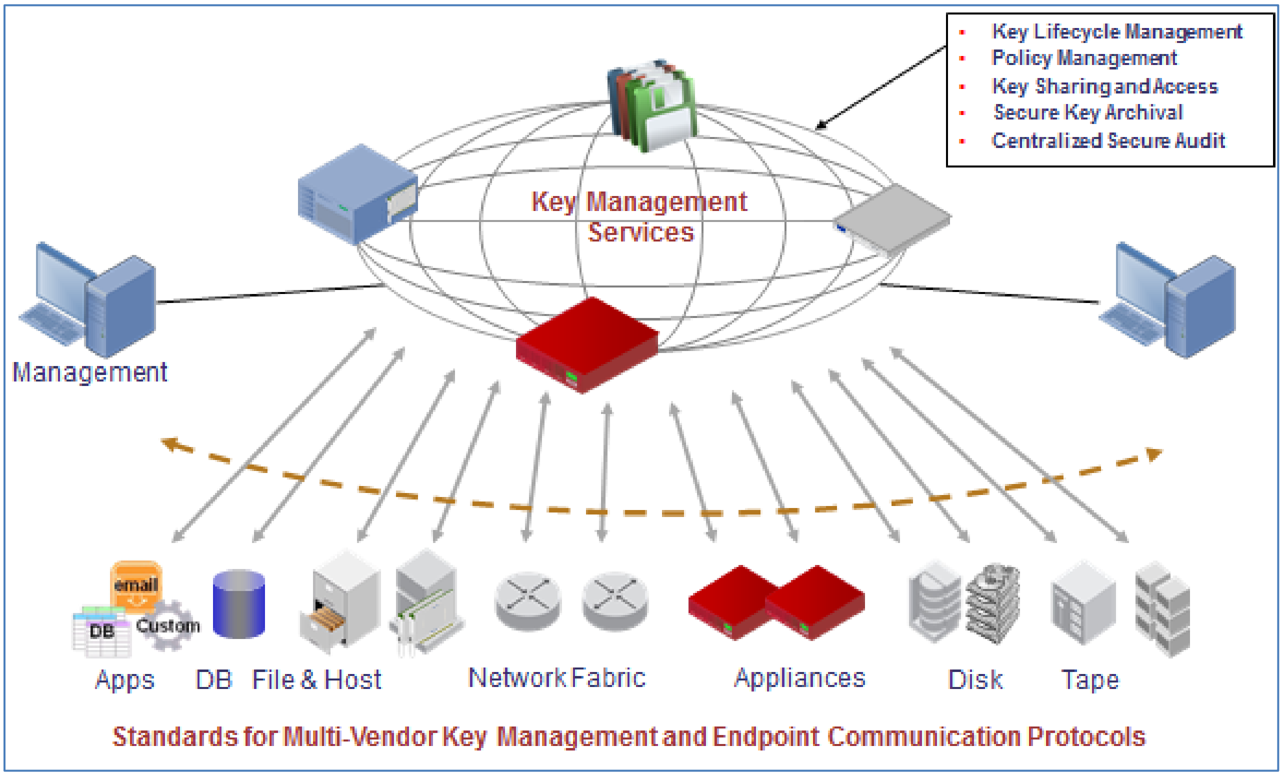

Figure 2 - Centralized Key Management

3. Physical Ports and Interfaces

The keyAuthority module has a number of physical ports and logical interfaces. The physical ports provided by keyAuthority are described in the following table:

Table 1 - Physical Ports and Status Indicators

Port	Description
MGMT Port	Connects to a private management network for providing remote and local secure management capabilities.
MGMT Port LEDs	ACT LED indicates network link status. LNK LED indicates network activity.
PORT 1	Connects to the network and provides services to network attached clients.
PORT 1 LEDs	ACT LED indicates network link status. LNK LED indicates network activity.
PORT 2	Currently unused and reserved for future use.
PORT 2 LEDs	Currently unused and reserved for future use.
CONSOLE Port	Connects to a local terminal for initialization of the module and limited local management capabilities.
Smart card Interface	ISO card compliant smart card reader for local authentication and key management.
Smart card LED	Indicates smart card insertion status.
LCD Front Panel Display	Provides device status information.
Front Panel Controls	Currently unused and reserved for future use.
Top Power Interface	PCI Compact Power Adapter for supporting power supply redundancy and high availability.
Top Power Interface LED	Power LED indicates status of removable power supply.
Lower Power Interface	PCI Compact Power Adapter for supporting power supply redundancy and high availability.
Lower Power Interface LED	Power LED indicates status of removable power supply.

The physical ports are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output as described in the following table:

Table 2 - Physical Port to Logical Port Mapping

Logical Interface	Physical Interface Mapping
Data Input Interface	MGMT Port PORT 1 Smart card Interface
Data Output Interface	MGMT Port PORT 1 Smart card Interface
Control Input Interface	MGMT Port CONSOLE Port
Status Output Interface	MGMT Port MGMT Port LEDs PORT 1 PORT 1 LEDs CONSOLE Port Smart card LED LCD Front Panel Display Top Power Interface LED Bottom Power interface LED
Power Interface	Top PCI Compact Power Connector Bottom PCI Compact Power Connector Internal Rechargeable batteries

4. Identification and Authentication Policy

The keyAuthority module supports identity-based authentication for all roles. The two FIPS roles associated with the keyAuthority module are:

- Crypto Officer – responsible for all management activities associated with the module.
- User – This role is assumed by client applications requiring key management services.

The module supports eight unique roles, which are mapped into the two FIPS roles above as follows:

Table 3 - keyAuthority Roles Mapping to FIPS Roles

Role	FIPS Mapping	Authentication Data
Administrator	Crypto Officer	The operator is granted access to keyAuthority console or GUI after providing proper user ID and corresponding password.
Security Officer	Crypto Officer	The operator is granted access to keyAuthority console or GUI after providing proper user ID and corresponding password.
Group Manager	Crypto Officer	The operator is granted access to keyAuthority GUI after providing proper user ID and corresponding password.
Auditor	Crypto Officer	The operator is granted access to keyAuthority GUI after providing proper user ID and corresponding password.
Recovery Officer	Crypto Officer	The operator is granted access to keyAuthority console or GUI after providing proper user ID and corresponding password.
P 1619 User	User	The operator is given access after the module verifies a signature supplied in the TLS connection set-up messages
TKLM User	User	The operator is given access after the module verifies a signature supplied in the TKLM connection set-up messages
Replication User	User	The operator is given access after the module verifies a signature supplied in the TLS connection set-up messages

The keyAuthority module supports concurrent operators. The keyAuthority module is delivered with only one default Administrator role and one default Security Officer role. But once additional operators are enrolled as different roles, the module does not allow the deletion of roles beyond the minimum required, which includes one Security Officer, one Administrator, three Recovery Officer and one Auditor role. The module can have only one Replicating partner so only one Replication user role. Additionally, the maximum number of concurrent TKLM and P1619.3 users/clients are restricted by the specification of the respective licenses installed on the module.

The separation between concurrent operators is achieved through the following:

- Serial processing of the requests that are routed through the main daemons.
- Strict role separation between operators; combining roles is prohibited.
- The login session state belonging to each operator is maintained separately.

When an operator successfully logs into the module, the authorized role is allowed. The operator is not permitted to alter their role while logged into the module.

4.1 Crypto Officer Role

The keyAuthority module can be managed by the Crypto Officer using any of the following methods:

- Console via the direct attached Console Serial Port
- Remote console via a SSHv2 secure connection to the MGMT Port
- Graphical User Interface (GUI) using HTTPS (via TLS) secure connection to the MGMT Port

All Crypto Officers authorized to access the module are required to enter a username and password. Optionally, a two factor authentication mechanism can be enabled which requires the user to also present a smart card which contains a pre-placed RSA key pair protected by a PIN. Operator use one or both of these mechanisms to authenticate to the system in order to perform authorized tasks.

When using two-factor authentication, the keyAuthority module supplies a new, random nonce value to the smart card for signature to prove ownership of the private key associated with the operator in question.

The system enforces the following password security policy for all Crypto Officers:

- Passwords must be at least 8 characters long and at most 32 characters long.
- Passwords must be a mix of at least two out of three of:
    - Letters
    - Numbers
    - Special Characters

4.2 User Role

The module can be accessed by the User using the following methods:

- Replication Client – Authenticates using a signed X.509 RSA 2048-bit Certificate over TLS protocol. The user certificate is issued by the keyAuthority CA.
- P1619.3 Client – Authenticates using a signed X.509 RSA 2048-bit Certificate over TLS protocol. The user certificate is issued by either the keyAuthority CA or an external trusted CA.
- TKLM Client – Authenticates using a signed X.509 RSA 2048-bit Certificate over TKLM protocol. The user certificate is issued by an external trusted CA.

4.3 Unauthenticated Operator

An unauthenticated operator is one who accesses the module without providing authentication credentials. The unauthenticated operator only has access to the following services:

- Power-cycle the module to cause reboot. This also causes the module to run its power-up self-tests again.
- Observe the power supply and network ports statuses by viewing the respective LEDs.
- Observe the module status from the LCD on the front panel of the module.

Table 4 - Unauthenticated Operator Services

Module State	Indication
Power off	LCD off
Power-up self-tests running	LCD on but not ready

Module State	Indication
Error	LCD indicates error
Operational	LCD reads "ready"

4.4 Authentication

The types and strengths of authentication for each Role identified for the keyAuthority module are given in the tables below.

Table 5 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity Based	Username and Password
Crypto Officer	Identity Based, two-factor	Username, Password, and RSA Key Pair (smart card)
User	Identify Based	Signed X.509 Digital Certificate

Table 6 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	Given the case where a user chooses to meet the minimum password policy requirements, the number of password permutations with eight characters selected from a possible of 52 alpha characters (upper and lower), 10 digits and 10 special characters giving 72 possibilities is 72^8 = (72*72*72*72*72*72*72*72) = 722,204,136,308,736 total permutations. The module actually places additional restrictions on these passwords, requiring at least one character from two of the three categories of letters, digits, and special characters. So, the actual number of possible passwords is even less than this. Therefore the probability of guessing a password is significantly less than one in 1,000,000. Multiple attempts to use this authentication mechanism will be gated by the method of authentication chosen. When authenticating over SSH or HTTPS, the authentication mechanism will lock the account after three failed tries. Therefore, an attacker will only be able to choose 3/722,204,136,308,736 passwords before the account would become locked out. See the section following this table for details on User Account Lockout. When authenticating over the serial console, the system imposes a minimum of a 1 second delay for each login attempt. After four unsuccessful login attempts, the serial console disconnects. Therefore, an attacker could at most try one password per second. Assuming that on average half of the passwords would have to be tried (e.g. 361,102,068,154,368), then the attacker would require an average of over 11,442,869 years to guess the authentication of a specific Crypto Officer.

Authentication Mechanism	Strength of Mechanism
	There is no feedback of authentication data to the Crypto Officer that might serve to weaken the authentication mechanism.
Username, Password, and RSA Key Pair	The module allows Crypto-Officers to log in with a combination of username-password and a RSA key pair authentication (available with the use of a smart card). The strength of this mechanism relies upon the strength of the Username and Password mechanism (shown in the row above) combined with the strength of a 2048 bit RSA Private Key (as illustrated in the row below). Because both mechanisms far exceed the FIPS requirements, we can conclude that the combination of Username, Password and RSA Private Key exceed the FIPS requirement. There is no feedback of authentication data to the Crypto Officer that might serve to weaken the authentication mechanism.
Signed X.509 Digital Certificate	The strength depends upon the size of the private key space. The keyAuthority module relies upon RSA 2048-bit signature verification of the User role certificates. This provides an encryption strength of 112 bits, so the probability of a random success will be 1 in 2^112, which is significantly less than one in 1,000,000. Multiple attempts to use the authentication mechanism during a one-minute period do not constitute a threat for secure operation of the keyAuthority module. This is because each attempt requires the module to check the signature on the certificate that is to be loaded. Therefore the total number of attempts that can be made in a one-minute period will be limited by the keyAuthority signature verification and response operation, which takes on average approximately 30 seconds, so two such attempts can be possible in one-minute. The majority of this time is accounted for by the communications overheads since the signature checking operation within the module is relatively fast. Given the very large size (2048 bits) of the private key space used by the FIPS Approved signature algorithm (RSA) utilized by the keyAuthority module, it follows that the probability that an intruder will be able to guess the private key, and thereby gain authentication, by making multiple attempts, the probability of success will be 1 in (2^112)/2, which is significantly less than one in 100,000. There is no feedback of authentication data to the User that might serve to weaken the authentication mechanism.

4.4.1 User Account Lockout

For login attempts from a remote location, the Crypto Officer authentication mechanism is designed with an account-locking feature where three consecutive login failures for a given user ID will lockout access to that operator. The account can only be unlocked by an Administrator.

> *NOTE: The locking feature does not apply to Administrator privileged login failures through the console in order to prevent permanent lockout of the module. However, the requirement is met because of the 1-second delay implemented at the console login. Read below for details.*

When keyAuthority locks an administrator account, the administrator must login via the serial console and change their own password, or another administrator must reset their password. When keyAuthority locks a security officer account, the officer must login via the serial console and change their password.

On the serial console, for all operators including the Administrator role, the system imposes a minimum of a 1-second delay for each login attempt. After four unsuccessful login attempts, the serial console disconnects. Assume a worst-case scenario that an attacker attempts to guess password on the serial console. Further, assume that the attacker is able to reconnect immediately to the console after a serial port disconnect. Such an attacker would be able to guess passwords at a rate of one guess per second.

On average, a well-chosen 8-character password would require an attacker to try half of the possible password permutations (361,102,068,154,368 password attempts). At a rate of one guess per second, an attacker would require an average of over 11,442,869 years (361,102,068,154,368 / (60 * 60 * 24 * 365.2425)).

5. Secure Operation Rules

5.1 Setup and Initialization

The Crypto-Officer is expected to follow the vendor guidelines to setup and install the module after it is received from the vendor. These setup procedures briefly include the following:

1. Unpacking and mounting the appliance in a rack, if required.
2. Use default Security Officer and default Administrator role credentials to login to the module.
3. Configuring network settings on the physical ports.
4. Generating System Keys and Root CA.
5. Add and modify users, as required.

5.2 FIPS-Approved Mode

The module is meant to always operate in a FIPS-Approved mode and does not support a non-FIPS mode. No operator-initiated configurations are required to enable the FIPS-mode on the module. After completing the setup procedures, the module is ready for use in FIPS-Approved mode and stays in this mode forever.

6. Access Control Policy

6.1 Services

6.1.1 Crypto Officer Services

The sections below enumerate the authorized services available for each Crypto Officer role within the keyAuthority module. All services require authentication to the module. For services marked with a '*' character, the service requires a multi-user quorum authentication. Quorum authentication requirements are provided in the Description column.

For further details of each operation, refer to the keyAuthority Users Guide [4].

6.1.1.1 Administrator

Table 7- Services Authorized for the Administrator

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Access Module	Crypto Officer authentication to the module	Passwords (R) 2-Factor Authentication Public Key (R)
GUI Open Connection	Create a browser connection	TLS Key Pair (R) TLS Certificate (R) TLS Session Keys (W)
SSH Open Connection	Create a secure shell connection	SSH Key Pair (R) SSH Session Keys (W)
Create User	Sets unique username and password	Passwords (W)
Delete User	Delete specific user account Only access to certain users is permitted	Passwords (W)
Modify User	Modify specific user account information Only access to certain users is permitted	None
View Users	Retrieve and display list of users	None
Change User Password	Change own password	Passwords (W)
Reset User Password*	Reset password for a specific user *Quorum of one Administrator and one Security Officer required	Passwords (W)
Set Network Settings	Display/edit module's port configuration	None
Set Date & Time Settings	Display/edit module's date and time	None
View Event Log	Review event log entries	None
Export Event Log	Export event logs for Thales support	None
Restore System Data*	Restore encrypted database from remote file system *Quorum of one Administrator and one Security Officer required	KEK (R) KMAC (R)
Upgrade Firmware	Update module firmware	Software Update Key (R/W) TKLM Root CA Certificate (W)
Prepare Smart Card	Initialize a smart card for use in the system	None

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Reset Config*	Restores module to factory state *Quorum of one Administrator and one Security Officer required	All persistent CSPs in the module with the exception of the Software Update Key and License Validation Key. (Z)

6.1.1.2 Security Officer

Table 8 - Services Authorized for the Security Officer

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Access Module	Crypto Officer authentication to the module	Passwords (R) 2-Factor Authentication Public Key (R)
GUI Open Connection	Create a browser connection	TLS Key Pair (R) TLS Certificate (R) TLS Session Keys (W)
SSH Open Connection	Create a secure shell connection	SSH Key Pair (R) SSH Session Keys (W)
Modify User	Modify specific user account information Only access to certain users is permitted	None
View Users	Retrieve and display list of users	None
Change User Password	Change own password	Passwords (W)
Reset User Password*	Reset password for a specific user *Quorum of one Administrator and one Security Officer required	Passwords (W)
Generate CSR for TLS Public Key	Generate certificate signing request for TLS Public Key	TLS Key Pair (R)
Install TLS Certificate signed by a third-party CA	Import certificate signed by external CA	TLS Public Key Certificate (Z/W)
Create/Edit Domain	Create/Edit Logical Domain	None
Delete Empty Domain	Delete Logical Domain	None
View Domain	View Logical Domain	None
Create Group	Create a group	GEK (W) GMAC (W)
Delete Group	Delete a group	GEK (Z) GMAC (Z)
Edit Group	Modify group attributes	None
View Group	View group attributes	None
Create, Edit, Delete Data Policy	Create, modify or delete a specific data policy Limited to module and domain levels	None
View Data Policy	Review a specific data policy Limited to module and domain levels	None
View Audit Log	Review audit log entries	None
Generate System Key	Creates top level system key	KEK (W) KMAC (W)

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Destroy System Key	Destroy system keys	KEK (Z) KMAC (Z)
Generate System Key Shares	Create all the system key shares	KEK (R) KMAC (R) System Key Shares (W)
Erase System Key Shares	Destroys all System Key Shares	System Key Shares (Z)
Commit Recovered System Key*	Commit reconstituted KEK and KMAC *A quorum of Recovery Officer "Import System Key Share" operations must have occurred prior to this operation.	KEK (W) KMAC (W)
Abort System Key Recovery	Abort a System Key recovery operation	System Key Shares (Z)
Backup System Data	Backup encrypted database to remote file system	KEK (R) KMAC (R) All other persistent keys and CSPs (R) in encrypted form
Restore System Data*	Restore encrypted database from remote file system *Quorum of one Administrator and one Security Officer required	KEK (R) KMAC (R) All other persistent keys and CSPs (W) in encrypted form
Reset Config*	Restores module to factory state *Quorum of one Administrator and one Security Officer required	All persistent CSPs in the module with the exception of the Software Update Key (Z)

6.1.1.3 Group Manager

Table 9- Services Authorized for the Group Manager

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Access Module	Crypto Officer authentication to the module	Passwords (R) 2-Factor Authentication Public Key (R)
GUI Open Connection	Create a browser connection	TLS Key Pair (R) TLS Certificate (R) TLS Session Keys (W)
SSH Open Connection	Create a secure shell connection NOTE: Functionality limited to only viewing the system summary	SSH Key Pair (R) SSH Session Keys (W)
View Users	View own user information	None
Change User Password	Change own password	Passwords (W)
Sign P1619.3 CSR	Process P1619.3 Client CSR and generate Certificate Limited to clients in own group	Local CA Key Pair (R) P1619.3 Client Public Certificates (W)
View P1619.3 Client Certificates	View P1619.3 client certificates Can view certificates in all groups.	P1619.3 Client Public Certificates (R)

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Revoke P1619.3 Client Certificate	Revoke P1619.3 client certificate Limited to clients in own group	P1619.3 Client Public Certificates (Z)
Export P1619.3 Client Certificate	Export P1619.3 Client Certificate and keyAuthority Root CA Certificate Limited to clients in own group	P1619.3 Client Public Certificates (R) Root CA Certificate (R)
View Group	View group attributes Limited to our own group	None
Create Trust	Establish cross-group trust	None
Delete Trust	Remove cross-group trust	None
Edit Trust	Modify cross-group trust attribute	None
View Trust	View trust attributes	None
Modify Client Data*	Modify client data attributes * Requires a quorum of two Group Managers	None
View Client Data	View client data attributes	None
Client Data Import	Import encrypted client data	KEK (R) KMAC (R) GEK (R) GMAC (R)
Client Data Export	Export encrypted client data	KEK (R) KMAC (R) GEK (R) GMAC (R)
TKLM Import	Import TKLM client data from external TKLM server	None
TKLM Export	Export TKLM client data to external TKLM server	None
Create, Edit, Delete Data Policy	Create, modify or delete a specific data policy Limited to policies within our own group	None
View Data Policy	Review a specific data policy Limited to our own group	None
View Event Log	Review event log entries Limited to our own group	None
View Audit Log	Review audit log entries Limited to our own group	None

6.1.1.4 Auditor

Table 10- Services Authorized for the Auditor

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Access Module	Crypto Officer authentication to the module	Passwords (R) 2-Factor Authentication Public Key (R)
GUI Open Connection	Create a browser connection	TLS Key Pair (R) TLS Certificate (R) TLS Session Keys (W)

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
View Users	View own user information	None
Change User Password	Change own password	Passwords (W)
View Event Log	Review event log entries	None
View Audit Log	Review audit log entries	None
Export Audit Log	Export audit logs	None

6.1.1.5 Recovery Officer

Table 11 - Services Authorized for the Recovery Officer

Service	Cryptographic Keys and CSP Access (R/W/Z)	Cryptographic Keys and CSP Access (R/W/Z)
Access Module	Crypto Officer authentication to the module	Passwords (R) 2-Factor Authentication Public Key (R)
GUI Open Connection	Create a browser connection	TLS Key Pair (R) TLS Certificate (R) TLS Session Keys (W)
SSH Open Connection	Create a secure shell connection	SSH Key Pair (R) SSH Session Keys (W)
View Users	View own user information	None
Change User Password	Change own password	Passwords (W)
Export System Key Share	Export a specific System Key Share	System Key Share (R)
Import System Key Share	Import a System Key Share	System Key Share (W)

6.1.2 User Services

The sections below enumerate the authorized services available for each User role within the keyAuthority module. All services require authentication to the module.

For further details of each operation, refer to the keyAuthority Users Guide [4]

6.1.2.1 P1619.3 Users

Table 12 - Services Authorized for P1619.3 Users

Service	Cryptographic Keys and CSP Access (R/W/Z)	Cryptographic Keys and CSP Access (R/W/Z)
P1619.3 Open Connection	Create secure P1619.3 connection	TLS Key Pair (R) TLS Certificate (R) TLS Session Key (W)
P1619.3 Put data	Receive P1619.3 data	TLS Session Key (R)
P1619.3 Get Data	Send P1619.3 data	TLS Session Key (R)

6.1.2.2 TKLM Users

Table 13 - Services Authorized for TKLM Users

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
TKLM Open Connection	Create secure TKLM connection	TKLM Root CA Certificate (R)
TKLM Put data	Receive TKLM data	None.

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
TKLM Get Data	Send TKLM data	None.

6.1.2.3 Replication Users

Table 14 - Services Authorized for Replication Users

Service	Description	Cryptographic Keys and CSP Access (R/W/Z)
Replication Open Connection	Create secure Replication connection	Replication Key (R) Replication Certificate (R) Replication Session Key (W)
Replication Put Client Information	Receive Replication data	Replication Session Key (R) KEK (R) KMAC (R) GEK (W) GMAC (W)
Replication Get Client Information	Send Replication data	Replication Session Key (R) KEK (R) KMAC (R) GEK (R) GMAC (R)

7. Diagnostics

A variety of diagnostics are available to maintain secure operation. These diagnostics include cryptographic mechanisms, critical functions and module status monitoring. Log files are maintained in the keyAuthority module and can be viewed, exported, or printed.

If the keyAuthority module is faulty, as indicated by the failure of a self-test diagnostic, it will render itself inoperable until the fault is rectified.

7.1 Power-Up Tests

Upon power-up, the module performs Known Answer Tests (KATs) on all FIPS-Approved cryptographic algorithms used by the module. In addition, the integrity of all firmware is checked. Upon completion of the Power-Up Tests, the keyAuthority module writes a message to the event log and the LCD Display reads "Ready". If any Power-Up Test fails, the module enters the error state, outputs the error message on LCD screen and logs the error in Event Log and Audit Log and halts the entire module operation.

The Power-Up Tests can be executed on demand by cycling the module's power.

The following table enumerates the module Power-Up Tests.

Table 15 - Power-Up Tests

Test	Description
Firmware Integrity Test	Validates the firmware image integrity.
keyAuthority Random Bit Generator Library	Performs the following KAT Tests: • SHA KATs • DRBG KATs
OpenSSL KAT Tests	Performs the following KAT Tests: • AES KATs • HMAC KATs • RSA KATs • SHA KATs
IBM JCE Self-Tests (if TKLM is Licensed) (Val #1081)	Performs the following KAT Tests: • AES KATs • SHA KATs • HMAC KATs • RSA KATs • RNG KATs

7.2 Conditional Tests

The keyAuthority module performs multiple conditional tests during the operational states of the device.

The outputs of the hardware random number generator, the SHA-256 Hash DRBG, and the IBM JCE RNG are checked whenever random data is requested from these RNGs by the module. Subsequent random numbers are compared against the last generated value to verify that these values are not the same.

All RSA key pairs generated by the module are validated using an RSA Pair-Wise Consistency Test (PWCT) which validates that information encrypted by one key can be decrypted by the matching key to ensure that the public and private keys are indeed asymmetric.

In the case of a firmware upgrade, the new firmware images are digitally signed by a Thales controlled CA using RSA 2048 which will allow the module to verify the image, thus preventing unauthorized firmware upgrades.

The following table enumerates the conditional tests:

Table 16 - Conditional Tests

Function Checked	Description
Hardware RNG	CRNG
SP 800-90 SHA-256 Hash DRBG	CRNG
FIPS 186-2 RNG	CRNG
OpenSSL RSA Key Pair Generation	PWCT
IBM JCE RSA Key Pair Generation	PWCT
Firmware Upgrade Authentication	Firmware Validation Test

8. Security-Relevant Information

8.1 Cryptographic Algorithms

The module utilizes the following FIPS-Approved algorithms.

Table 17 - FIPS Approved Algorithms

Library	Algorithm	FIPS Certificate Number
keyAuthority Random Bit Generator Library	DRBG	128
	SHA	1573
OpenSSL	RSA	898
	AES	1795
	SHA	1577
	HMAC	1059
IBMJCE	RNG	463
	RSA	387
	AES	805
	SHA	803
	HMAC	445

The module also makes use of the following Non-Approved but Allowed key establishment methods while in the FIPS-Approved mode:

1) RSA Key Transport
   Used as part of TLS key exchange. Provides 112 bits of security strength.
2) Diffie-Hellman Key Agreement
   Used as part of SSH and TLS key exchanges. Provides between 80 and 256 bits of security strength.

8.2 Cryptographic Keys and CSPs

The cryptographic keys and CSPs stored in the keyAuthority module are listed in the table below.

Table 18 - Keys and CSPs

Keys/CSPs	Description	Key/CSP Type and Size	Generated or Established	Stored	Zeroized
Software Update Key	The public key used to validate the signature on new software and firmware.	RSA 2048	Generated externally and loaded at manufacturing time.	Non-volatile memory – hard disk.	Not required to be zeroized

Keys/CSPs	Description	Key/CSP Type and Size	Generated or Established	Stored	Zeroized
Key Encrypting Key (KEK)	Encrypts all non-volatile Keys and CSPs stored on the module.	AES-256	If not present at startup, it is generated using the module's FIPS approved DRBG. Alternatively this key can be loaded from a quorum of System Key Shares stored on smart cards.	Plaintext in Battery Backed RAM; HMAC'ed in EEPROM using KMAC	On tamper detect or upon user's command.
Key Message Authentication Code (KMAC)	Authenticates all non-volatile Keys and CSPs stored on the module.	HMAC-SHA-512	If not present at startup, it is generated using the module's FIPS approved DRBG. Alternatively this key can be loaded from a quorum of System Key Shares stored on smart cards.	Plaintext in Battery Backed RAM.	On tamper detect or upon user's command.
System Key Share	Secure portion of the KEK and KMAC after splitting using Shamir secret sharing algorithm.	N/A	Generated by the Security Officer using the 'Generate Share'.	Non-volatile memory – hard disk (encrypted).	Effectively zeroized on tamper due to erasure of KEK/KMAC.
Group Encrypting Keys (GEK)	Encrypts group-specific Keys stored on the module.	AES-256	Generated using the module's FIPS approved DRBG.	Non-volatile memory – hard disk (encrypted).	Effectively zeroized on tamper due to erasure of KEK/KMAC.
Group Message Authentication Code Keys (GMAC)	Authenticates group-specific keys stored on the module.	HMAC-SHA-512	Generated using the module's FIPS approved DRBG.	Non-volatile memory – hard disk (encrypted).	Effectively zeroized on tamper due to erasure of KEK/KMAC.
TLS Key Pair	Used by HTTPD and P1619.3 services for secure communications	RSA 2048	Generated using module's approved RSA Key Generation mechanism. Generation initiated by Security Officer during initial system configuration.	RSA Keys stored in non-volatile memory (encrypted).	Key destroyed on "reset config" operation. Key overwritten when Security Officer re-executes initial system configuration.

Keys/CSPs	Description	Key/CSP Type and Size	Generated or Established	Stored	Zeroized
P1619.3 Public Key Certificate	Used by P1619.3 service for secure communications	RSA 2048	Established upon TLS Key Pair generation. Generation initiated by Security Officer during initial system configuration.	P1619.3 Public Key Certificate stored in non-volatile memory.	Certificate destroyed on "reset config" operation. Certificate overwritten when Security Officer re-executes initial system configuration.
TLS Public Key Certificate	Used by HTTPD service for secure communications	RSA 2048	First established upon TLS Key Pair generation. Overwritten upon new certificate import signed by external CA.	TLS Public Key Certificate stored in non-volatile memory.	Certificate destroyed on "reset config" operation. Certificate overwritten during import process initiated by the Security Officer. Certificate overwritten when Security Officer re-executes initial system configuration.
Replication Key Pair	Used by replication service for a TLS connection to the replicating partner	RSA 2048	Generated using module's approved RSA Key Generation mechanism. Generation initiated by Security Officer during initial system configuration.	RSA Keys stored in non-volatile memory (encrypted).	Key destroyed on "reset config" operation. Key overwritten when Security Officer re-executes initial system configuration.
Replication Public Key Certificate	Used by replication service for initiating and maintaining a secure TLS connection to the Replicating keyAuthority	RSA 2048	Established upon Replication Key Pair generation. Generation initiated by Security Officer during initial system configuration.	Replication Public Key Certificate stored in non-volatile memory.	Certificate destroyed on "reset config" operation. Certificate overwritten when Security Officer re-executes initial system configuration.

Keys/CSPs	Description	Key/CSP Type and Size	Generated or Established	Stored	Zeroized
TLS Diffie-Hellman public and private values	A Diffie-Hellman key pair to provide session authentication for every TLS connection established by the HTTPD and P1619.3 and Replication services.	DH (80 to 256 bits of security strength)	Generated internally using the FIPS-approved DRBG	Temporal keys, stored in volatile RAM	Keys are destroyed upon session teardown.
TLS Pre-Master Secret	When RSA key transfer is used as part of TLS session establishment, this pre-master secret is used to derive the session encryption key and session authentication key for each TLS session (HTTPD, P1619.3, or Replication)	Secret (48 bytes)	Sent by the TLS client encrypted with the module's public key	Temporal keys, stored in volatile RAM	Keys are destroyed upon session teardown.
TLS Session Key	A unique session key for each TLS session (HTTPD and P1619.3 and Replication services) for providing session encryption	AES-256	Entered encrypted with the module's public key sent by the TLS client if using RSA key exchange. If using Diffie-Hellman exchange, this is derived from the shared secret.	AES keys are temporal and stored in volatile memory.	Keys are destroyed upon session teardown.
TLS Integrity key	A unique integrity key for each TLS session (HTTPD and P1619.3 and Replication services) for providing session authentication	HMAC-SHA-512	Entered encrypted with the module's public key sent by the TLS client if using RSA key exchange. If using Diffie-Hellman exchange, this is derived from the pre-master secret.	Temporal key, stored in volatile RAM.	Keys are destroyed upon session teardown.
P1619.3 Client Public Key Certificates	A list of P1619.3 Client Certificates issued by keyAuthority module.	RSA 2048	Client CSRs imported into the module and root CA-signed client certificates are generated by the module.	Non-volatile memory – hard disk (encrypted).	Certificates are destroyed upon certificate revocation. Certificate destroyed on "reset config" operation.
SSH Key Pair	Used by SSH service for secure communications	RSA 2048	Generated using module's approved RSA Key Generation mechanism. Generation initiated by Security Officer during initial system configuration.	RSA Keys stored in non-volatile memory (encrypted).	Key destroyed on "reset config" operation. Key overwritten when Security Officer re-executes initial system configuration.

Keys/CSPs	Description	Key/CSP Type and Size	Generated or Established	Stored	Zeroized
SSH Diffie-Hellman public and private values	Diffie-Hellman key pair used by the module during the SSH session establishment	DH (80 to 256 bits of security strength)	Generated internally using the FIPS-approved DRBG	Temporal keys, stored in volatile RAM	Keys are destroyed upon session teardown.
SSH Session Key	Used by SSH service for providing session encryption	AES-256	Derived from the Diffie-Hellman shared secret.	AES keys are temporal and stored in volatile memory.	Keys are destroyed upon session teardown.
SSH Integrity key	Used by SSH service for providing session authentication	HMAC-SHA-512	Derived from the Diffie-Hellman shared secret.	Temporal key, stored in volatile RAM.	Keys are destroyed upon session teardown.
Replication Session Key	Used by replication service for TLS session encryption	AES-256	Generated using FIPS approved DRBG. Generation initiated during session key negotiation phase.	AES keys are temporal and stored in volatile memory.	Keys are destroyed upon session teardown.
Replication Session Integrity Key	Used by replication service for TLS session integrity	HMAC-SHA-512	Generated using FIPS approved DRBG. Generation initiated during session key negotiation phase.	Session keys are temporal and stored in volatile memory.	Keys are destroyed upon session teardown.
TKLM Root CA Certificate	The public key CA certificate used to validate TKLM clients.	RSA 2048	Generated externally and loaded at manufacturing time.	Non-volatile memory – hard disk.	When the key is deleted or replaced by a subsequently issued key.
2-factor Authentication Public Key	Additional authentication method for user access to module.	RSA 2048	Generated externally on a smart card, and loaded when Security Officer assigns operator to a smart card.	Non-volatile memory – hard disk (plaintext).	N/A
Operator Passwords	Authentication	N/A	Generated using the module's approved DRBG, or set by a unique user.	Non-volatile memory – hard disk (HMAC-SHA-512 of the password)	Erased upon deletion of user account.
Local or Root CA Key Pair	Root trust authority for keyAuthority management.	RSA 2048	Generated using module's approved RSA Key Generation mechanism. Generation initiated by Security Officer during initial system configuration.	RSA Keys stored in non-volatile memory (encrypted).	Keys zerioized during re-generation process initiated by the Security Officer. Keys destroyed on "reset config" operation.

Keys/CSPs	Description	Key/CSP Type and Size	Generated or Established	Stored	Zeroized
DRBG Entropy Input String	Initial entropy provided to the DRBG during module instantiation	Hash_DRBG, SHA-256, 4096 bytes	Generated via internal hardware RNG.	Not stored persistently.	Zeroized when a subsequent seed key is generated.
DRBG internal state	Hash DRBG V and C values belonging to its internal state	440 bits each	V is initially the seed and is updated during each call to the DRBG per the SP800-90 standard. C is always derived using V.	Not stored persistently.	Zeroized upon next update.

8.2.1 Key Storage & Destruction

The system keys (KEK and KMAC) are stored in clear text in secured NVRAM and are not accessible to anyone without tampering the unit, which will cause the hardware to overwrite the key with zeros.

The GEK and GMAC are stored in the database encrypted with the KEK and MAC'ed with the KMAC. The GEK and GMAC keys are used to protect P1619.3 client data.

All other sensitive keys enumerated in Table 18 as being encrypted, are protected using the system key (KEK and KMAC).

8.2.2 Manual Key Destruction

A security officer can manually clear (overwrite with zeros) the system key (KEK & KMAC) by issuing the "Destroy Keys" command from the Web UI or console. If this is followed by a "Reset Config", then the module is returned to factory default conditions and all persistently stored secret and private cryptographic keys and CSPs of the module also get zeroized. The "Reset Config" operation requires a quorum operation between an Administrator and Security Officer.

All other keys in the module are stored in encrypted form and are thus are not required to be zeroized.

8.2.3 Random Number Generation

The primary Random Number Generator consists of a hardware random number source providing entropy and seed data to a FIPS Special Publication 800-90[3] approved SHA-256 Hash DRBG. This DRBG is utilized for the generation of all private and secret keys of the keyAuthority, with the exception of the operations in the TKLM server. The TKLM server utilizes a FIPS 186-2 Appendix 3.1[2] Approved pseudo random number generator for the generation of all private and secret keys.

8.2.4 Algorithm Usage

The keyAuthority module utilizes the following algorithms:

- SHA-256 Hash DRBG
- AES-256 for data encryption and privacy
- RSA-2048 for signature generation, signature verification, and key agreement
- SHA-1, SHA-256, and SHA-512 hashing algorithms
- SHA-512 HMAC for authentication

9. Physical Security Policy

The keyAuthority module is a multi-chip standalone cryptographic module designed to meet FIPS 140-2, level 3 for physical security. The module consists of production grade components with standard passivation techniques applied.

The keyAuthority module is protected by a strong, metal, production-grade enclosure that is opaque within the visible spectrum and utilizes tamper evident labels and tamper response mechanisms. Attempts to access the module without removing the cover will cause visible physical damage to the module and/or tamper evident labels.

The module's ventilation holes in the housing are protected from undetected probing using internal baffles.

The module has a removable top cover which is protected by tamper-evident labels and tamper response circuitry, which zeroizes all plaintext keys and CSPs on a tamper-event. Access to the internal components of the module necessitate that the cover be removed.

The module's cryptographic boundary (FIPS 140-2[1], section 2.1) is the physical extent of its external casing but excludes the field replaceable dual redundant power supplies and the quad-redundant field replaceable fans.

9.1 Inspection/Testing of Physical Security Mechanisms

The following guidelines should be considered when producing a Security Policy for the environment for which the module is deployed.

The keyAuthority enclosure should be periodically checked by the Crypto Officer for evidence of tampering, in particular, damage to the two tamper-evident labels and any physical damage to the enclosure material. In addition, front panel LCD display and the audit logs should be checked for activation of the tamper response mechanism.

The frequency of a physical inspection depends upon the information being protected and the environment in which the unit is located. At a minimum, it would be expected that a physical inspection would be made by the Crypto Officer at least monthly and audit logs daily.

The tamper evident labels are applied at the Thales facility, are serialized, and are not available for order or replacement from Thales. The labels are designed and intended to say in place and intact for the entire life of the module.

Two tamper evident labels are required to be visible, undamaged and containing a clear continuous color hologram for each module to be operated in a FIPS approved mode of operation. They are applied by Thales in the positions illustrated in Figure below. One tamper seal is placed on the left side of the keyAuthority module and the other tamper seal is placed on the right side of the module.

Figure 3: Thales keyAuthority Module

Figure 4 - Tamper Evident Labels On Chassis (outlined in yellow for emphasis)

Each tamper seal sits over a screw on the lid and extends over the lid seam to the module chassis, as illustrated in Figure below. The only way to remove the cover is to break or damage the tamper seals.

Figure 5 – Tamper Evident Label Close-Up (outlined in yellow for emphasis)

The tamper label has an embedded holographic pattern which is visible while viewing the label from various viewing angles. The holographic pattern consists of the phrase, "VOID IF REMOVED, SECURED" repeated throughout the entire label, on alternating lines, with the text inverted on subsequent lines. The figure below illustrates the holographic word pattern.

Figure 6 - Tamper Evident Label Close-Up Showing Holographic Pattern

10. Mitigation of Other Attacks Policy

The keyAuthority currently does not claim to mitigate any other attacks.

11. Acronyms and Abbreviations

The table below contains a reference of acronyms and abbreviations used throughout this document.

Table 19 - Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
CLI	Command Line Interface
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
CSEC	Communications Security Establishment
CSR	Certificate Signing Request
CSP	Critical Security Parameter
DES	Data Encryption Standard
EMI/EMC	Electromagnetic interference/electromagnetic compatibility
FIPS	Federal Information Processing Standard
FW	Firmware
GEK	Group Encryption Key
GMAC	Group Message Authentication Key
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hyper-Text Transfer Protocol, Secured
KAT	Known Answer Test
KEK	Key Encryption Key
KMAC	Key Message Authentication Code
LAN	Local Area Network
LCD	Liquid Crystal Display
LUN	Logical Unit Number
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
PCI	Peripheral Component Interconnect
PKCS	Public Key Cryptography Standards
PWCT	Pair-Wise Consistency Test
RNG	Random Number Generator
RSA	RSA is an algorithm for public-key encryption
SAN	Storage Area Network
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
SSH	Secure Shell
SW	Software
TKLM	Tivoli Key Lifecycle Manager, an IBM-Proprietary protocol.
UI	User Interface

12. References

The list below contains the external references required by the document.

1) FIPS 140-2 Security Requirements for Cryptographic Modules, Federal Information Processing Standards Publication, 25th May 2001. Including Change Notices 2, 3, & 4: 12/03/2002. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.
2) FIPS 186-2 Digital Signature Standard, Federal Information Processing Standards Publication, 27th January 2000. Including Change Notice 1: 5th October 2001.
3) FIPS Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.
4) Thales e-Security keyAuthority® User Guide, Version 3.0.0, 05 December 2011.

13. Document History

The table below contains version and date information for the revisions of this document.

Table 20 - Document Revision History

Revision	Date	Description
001	Jan 10, 2012	Initial submission.
002	June 15, 2012	Addressed comments from NIST.